AEC

ASSOCIATION FOR ELECTRONICS AND COMPUTERS Ltd.

LLOYD'S REGISTER QUALITY ASSURANCE · ISO9001

IRONWARE

Security Suite

7

IronWare® Security Suite – Client 7. 2

Příručka uživatele

Technická podpora: +420 (0)5 4123 5468
Váš lokální kontakt: support@aec.cz
srpen 2000

Obsah

• Základní charakteristika

IronWare® Security Suite je softwarový systém poskytující dokonalou ochranu dat před zneužitím, a to pomocí šifrování na stanicích a serverech, které mohou být propojeny v síti LAN i WAN.

Jedná se o univerzální a modulární ochranný software, založený na mezinárodních standardech pro komunikaci a bezpečnost.

Jeho jádrem a hlavní součástí je **PKI** (Public Key Infrastructure), které odpovídá mezinárodním standardům a je navíc rozšířeno o další možnosti a funkce, užitečné a nezbytné při tvorbě aplikací v oblasti IT Security. Proto byl pro AEC PKI zvolen komerční název **Complex-PKI** (C-PKI). Pomocí C-PKI je možno postavit jakoukoliv bezpečnou aplikaci pro e-commerce, e-payment, secure web a mnohé další.

- obsahuje bezpečnostní aplikace s centralizovanou správou založenou na technologii klient/server.
- disponuje víceuživatelským chráněným přístupem, centralizovanou správou šifrovacích klíčů a sadou nástrojů pro šifrování dat. Dále jsou k dispozici doplňkové nástroje, jako například bezpečný skartovač dat IronWare® Shredder.
- je využitelný třetími stranami jako vývojové prostředí pro programování vlastních aplikací založených na propracované bezpečnosti šifrování pomocí IronWare®.
- šifrovat lze data uložená v souborech na pevných i výměnných médiích, elektronickou poštu, přenos souborů apod.

Minimální konfigurace

IronWare® Security Suite – Client vyžaduje ke své činnosti minimálně tuto hardwarovou konfiguraci:

16 MB RAM pro instalaci do Windows 95
32 MB RAM pro instalaci do Windows NT
15 MB diskového prostoru
procesor Pentium a vyšší.

• Quick Start

Prvním krokem je instalace aplikace na váš počítač. Vložte instalační CD do mechaniky. Automaticky se spustí program, ve kterém si můžete vybrat software, který chcete nainstalovat na váš počítač. Pokud máte vypnuto automatické spouštění programů po vložení CD, potom musíte tento program spustit sami, například z nabídky *Start/Spustit...*. Program se jmenuje **Start.exe** a nachází se v kořenovém adresáři CD disku.

Instalace IW Security Suite - Server

V případě, že budete provozovat IW Security Suite v konfiguraci klient/server, je třeba nejprve nainstalovat IW Management Server. Program IW Management Server se musí nainstalovat na počítač, který bude sloužit jako server. Nemusí se nezbytně shodovat s centrálním firemním souborovým serverem. Je možno jej nainstalovat na operační systémy Windows 95/98, NT Workstation i NT Server. Samotný průběh instalace je řízen standardním instalačním průvodcem. Po spuštění instalace a nastavení cesty pro instalační adresář proběhne kopírování souborů a po jeho ukončení budete vyzváni k zadání jména a hesla administrátora, a tří privilegovaných uživatelů. To jsou uživatelé, kteří mají právo (za předem definovaných bezpečnostních podmínek) zobrazit heslo kteréhokoliv z uživatelů. Zavedení privilegovaných uživatelů je v instalaci volitelné.

Důležitou informací, kterou si musíte pro instalaci klientů pamatovat, je IP adresa IW Management Serveru a Security ID, které jednoznačně server identifikuje a je generováno při instalaci. Při instalaci klientské části je třeba zadat IP adresu serveru a Security ID je uživateli zobrazeno pro přesnou identifikaci serveru, ke kterému se klient bude připojovat. První přihlášení klientské části k serveru probíhá k účtu administrátora, který je připraven při instalaci serveru. Administrátor po nainstalování prvního klienta může připravit stovky a tisíce předdefinovaných účtů uživatelů a při instalaci dalších klientských částí se již uživatelé k serveru přihlašují pomocí svých, administrátorem předdefinovaných, účtů. Po přihlášení si uživatelé změní přístupová hesla a přizpůsobí si, v rámci svých možností, účet pro svoje použití.

Instalace IW Security Suite - Client

Samotný průběh instalace je řízen standardním instalačním průvodcem. Ten zkontroluje přítomnost potřebných komponent pro práci s daty na vašem počítači, a pokud zjistí, že některá z nich chybí, pak se postará o její instalaci. Během instalace je nezbytné postupně zadat jméno uživatele, firmu, cílovou složku (cílová složka je přednastavena, ale je

možné ji změnit) a typ instalace. Začátečníkům je doporučena plná instalace.

Je nutné určit, zda program bude pracovat s lokální databází klíčů a uživatelů (volba *Tento počítač bude připojen k IronWare® Management Serveru, C-PKI databáze bude nainstalovaná lokálně*), nebo bude počítač připojen do sítě, databáze klíčů bude uložena na síťovém IW Management Serveru (volba *Tento počítač bude připojen k IronWare® Management Server a bude používat centrální databázi uživatelů a klíčů*). Dále je nezbytné se rozhodnout, kterou metodu šifrování budete používat. K dispozici je on-line (volba IW FileProtect), nebo off-line (volba IW FolderProtect).
Následně pak proběhne kopírování souborů a po jeho dokončení se spustí průvodce, který se liší podle druhu používání PKI. Jestliže se budete připojovat na PKI lokálně, pak budete vyzváni k zadání jména a hesla administrátora, a tří privilegovaných uživatelů. To jsou uživatelé, kteří mají právo (za předem definovaných bezpečnostních podmínek) zobrazit heslo kteréhokoliv z uživatelů.

Pokud se rozhodnete pro instalaci s centrální databází, je nutno zadat IP adresu nebo jméno počítače, na kterém je spuštěn IW Management Server. Údaje o administrátorovi a privilegovaných uživatelích se v tomto případě nezadávají, protože jsou již zadané v centrální databázi.

Posledním krokem je generování klíčů, které systém potřebuje pro svou interní potřebu. Instalační průvodce pak oznámí úspěšné ukončení instalace a po restartu Windows je IronWare® Security Suite Client připraven k použití.

Vytvoření šifrovacích klíčů

První věcí, kterou je třeba po nainstalování systému IronWare® Security Suite a prvním restartu provést, je vytvořit alespoň jeden tajný šifrovací klíč pro šifrování souborů a jeden pár asymetrických šifrovacích klíčů na šifrování elektronické pošty. Připojte se do IronWare® jako administrátor a spusťte *KeyManager* z nabídky *Start/Programy/ IronWare® Security Suite*.

Osobní tajný klíč vytvoříte v nabídce *Klíče/Nový uživatelský klíč/Tajný*. Zadáte jméno klíče, zvolíte typ šifrovacího algoritmu a stupeň utajení. Po nasbírání náhodných čísel se klíč vytvoří. Pak vytvořte soukromý klíč. Lze to provést volbou *Klíče/Nový uživatelský klíč/Soukromý* v nabídce. Kromě jména a typ šifrovacího algoritmu je nutné zadat i tzv. účel klíče, tedy k čemu má klíč sloužit (jen šifrování, jen podepisování…). K tomuto klíči je třeba vytvořit i certifikát. S takto vytvořeným klíčem můžete dešifrovat přišlou elektronickou poštu a elektronicky podepisovat odesílanou elektronickou poštu. Uživatel, kterému je pošta určena, však musí k dešifrování pošty mít soukromý klíč, k němuž byl vytvořen certifikát použitý pro zašifrování

(certifikát obsahuje mimo jiné veřejnou část klíče), kterým byl dopis zašifrován. Proto, pokud chcete někomu posílat šifrované zprávy, musíte si nějakým způsobem opatřit nějaký z adresátových certifikátů. Stejně tak pokud někdo má posílat zašifrované e-maily vám, je nutné mu doručit certifikát vytvořený „jako protikus" k některému z vašich soukromých klíčů. Nejjednodušším způsobem je poslat mu (případně si nechat poslat) zprávu, která bude elektronicky podepsaná vaším (jeho) klíčem (certifikát je součástí podepsané zprávy). Tento certifikát pak bude automaticky importován do adresátova (vašeho) PKI. Při tomto způsobu je však nutno (zvláště v případě *self signed* certifikátů) zaručit, že se nejedná o podvrh.

Vytvoření nového uživatele

Nové uživatelské účty je možné vytvořit v IW *KeyManageru* v nabídce *Uživatelé/Nový uživatel*. Vyplníte přihlašovací jméno, skutečné jméno, případně skupinu (je vhodné takto vytvářet hierarchickou strukturu uživatelů). Dále pak stupeň důvěrnosti dat ke kterým bude mít nový uživatel přístup a jeho heslo. Máte–li k dispozici některý z podporovaných typů čteček čipových karet nebo otisků prstů, můžete zapsat heslo na čipovou kartu a uživatel se pak může hlásit do systému touto kartou, anebo uložit otisky prstů tohoto uživatele do databáze (pak se bude moci identifikovat přiložením prstu na čtečku). Máte možnost též přidělit uživateli obyčejná, administrátorská či auditorská práva a umožnit mu automatické přihlášení do systému Windows po přihlášení do IronWare® (tzv. single sign-on). Administrátor sám však může vytvářet jen uživatele či administrátory, zatímco auditory smí vytvářet pouze auditor. Z tohoto důvodu se při instalaci vytváří auditorský účet Auditor s prázdným heslem, který ihned po instalaci přebírá některý z definovaných auditorů a heslo mu změní.

Každý uživatel, který vlastní osobní tajný klíč, může šifrovat své soubory. Je k dispozici on-line šifrování dat *IW FileProtect*, off-line šifrování složek *IW FolderProtect,* a nebo *IW JustProtect,* který provede šifrování souborů na požádání. V případě prvních dvou způsobů je nutné vybranou složku nejprve vybrat k šifrování. Provádí se to výběrem (přidělením) klíče v záložce *IW FileProtect* nebo *IW FolderProtect* podle toho, jakou metodu šifrování jste instalovali, v nabídce *Vlastnosti* každé složky.

Kromě toho umožňuje IW Security Suite i šifrování bez klíčů, konkrétně heslem do samorozbalovacího .EXE souboru. V nabídce vyvolané pravým tlačítkem myši na jméně souboru či složky zvolte přímo *Zašifrovat*. Zatrhněte volbu Do souboru *EXE…,* zadejte název cílového souboru a heslo.

Šifrování dat posílaných po síti

Kliknutím na *IronWare® FTP Client* ve složce *IronWare Security Suite* v nabídce programů spustíte FTP Client, aplikaci umožňující posílání dat pomocí protokolu FTP, která kromě standardních služeb umožňuje navíc

šifrování souborů, vytvoření autentizovaného a šifrovaného tunelu mezi programy FTP Client a IW FTP Server a navázání SSH spojení s SSH Serverem.

Nastavení

Různá nastavení můžete po instalaci měnit v IW ConfigManageru, který lze spustit z položky *IronWare® Security Suite* v nabídce *Start/Programy*.

Odinstalace

V položce *IronWare® Security Suite* naleznete i nabídku *Odinstalace IronWare® Security Suite - Client.* Potřebujete – li IW Security Suite odinstalovat či přeinstalovat, mějte na paměti, že se v případě vlastní databáze uživatelů a klíčů ztrácejí všechny vytvořené klíče a uživatelské účty! Proto je nutné odšifrovat všechna zašifrovaná data na disku a sdělit rozhodnutí všem komunikačním partnerům. V případě serverové instalace se všechny vaše účty, klíče a certifikáty zachovávají v centrálním PKI a je jedno kdy a kde a kdy nainstalujete klientskou část znovu. Vše bude k dispozici po prvním přihlášení.

IronWare® Security Suite se skládá z následujících částí:

IronWare® Security Suite C-PKI

IW GINA
Umožňuje autorizovaný přístup do systému C-PKI na serverové nebo klientské části. Současně umožňuje automatické přihlášení uživatele do systému a použití hardwarových přihlašovacích předmětů pro autorizovaný přístup uživatelů k datům.

IW ScreenWall
Po použití „horké“ klávesy (hot-key), po nečinosti počítače stanovenou dobu či po vytažení přihlašovacího předmětu ze čtečky se počítač zablokuje a zobrazí na obrazovku šetřič, který může být odstraněn pouze použitím přihlašovacího předmětu či zadáním platného hesla aktuálně přihlášeného uživatele.

IW ConfigManager
Umožňuje globální nastavení modulů celého systému IronWare®, včetně typu hardwarových přihlašovacích předmětů a dalších vlastností.

IW KeyManager
Umožňuje správu uživatelských účtů a klíčů, a to jak na ochranu dat na discích, tak i pro posílání zpráv po Internetu. Je centrálně řízený na základě Server/Klient technologie. Generuje šifrovací klíče, vydává žádosti o certifikáty, importuje klíče a certifikáty a je ve spojení s Certifikační autoritou.

IW AuditLog
Slouží pro kontrolu systému. Podle nastavení v ConfigManageru zaznamenává akce, ke kterým v systému dochází, aby byla možná pozdější kontrola těchto akcí.

IW Management Server

Slouží k centralizované správě šifrovacích klíčů a uživatelských účtů celého systému Ć-PKI IronWare®. Je určen především pro velké a střední společnosti a státní instituce.

IW Certificate Server

Ve spojení s vypracovanou Certifikační politikou vytváří Certifikační autoritu (CA). Ta slouží pro vydávání, odvolávání, pozastavování a evidenci důvěryhodných certifikátů veřejných klíčů. Je nezbytná pro bezpečnou komunikaci, elektronický obchod a výměnu informací.

IW LDAP Server

Slouží pro přístup k certifikátům vydaným certifikačním serverem (certifikační autoritou) pomocí standardu LDAP. Nedílnou součástí IW LDAP Serveru je i replikační plánovač, který ve stanovených intervalech aktualizuje LDAP databázi certifikátů. IW LDAP Server uchovává záznamy o uživatelích a jejich certifikátech.

IW LDAP Search Client

Umožňuje uživatelům snadný přístup k certifikátům, které vydala certifikační autorita a následně vystavil LDAP server. Dovoluje vyhledávání certifikátů podle různých kritérií.

IW Tray

Je modul, který se spouští při startu Windows a minimalizuje se do pravé části úlohového panelu. Umožňuje komplexní spouštění modulů systému IronWare®. Podporuje operace se schránkou Windows a aktuálním oknem pomocí modulu IW MailProtect.

IronWare® Security Suite - Protection

IW FileProtect

On-line šifrování souborů na pevných discích, síti a na výměnných médiích. Využívá skupinových nebo osobních tajných klíčů pro šifrování souborů. Dovoluje šifrování výměnných médií (FD, JAZZ, Bernoulli…). Dovoluje také šifrování souborů nebo pevných disků v síti. Umožňuje promyšlený výběr šifrovaných souborů, složek nebo oddílů (obtékání).

IW FolderProtect

Off-line šifrování dat při odhlášení ze systému nebo odšifrování při přihlášení do systému. Soubory ve vybraných složkách jsou zašifrovány/odšifrovány na vyžádání nebo při odhlášení/přihlášení do systému. Pro šifrování souborů využívá osobních nebo skupinových tajných klíčů.

IW JustProtect

Provádí šifrování na požadavek aktuálně přihlášeného uživatele s využitím jeho tajných klíčů. Klíče používané JustProtectem jsou kompatibilní s klíči FolderProtectu. Je zde možné více způsoby vybírat soubory nebo složky pro šifrování. Umožňuje zašifrovat soubor(y) či složky do .EXE souboru, který je zašifrován na základě hesla, jež je pak nutné zadat pro jeho odšifrování. K odšifrování přitom nevyžaduje žádný speciální software.

IW Shredder

Je to aplikace nezávislá na PKI, dokonale odstraní data, cookies, tmp, swp, vyčistí volný prostor na pevných i výměnných médiích atd. Mezi funkce IW Shredderu patří „panické“ skartování (tj. skartování důležitých dokumentů na příkaz horké klávesy), skartování na vyžádání předdefinovaných souborů nebo složek a on-line skartování všech souborů, které jsou mazány.

IronWare® Security Suite - Communication

IW MailProtect

Zašifrovává/odšifrovává e-maily jako plug-in v MS e-mail systému. Zašifrovává/odšifrovává vybrané soubory nebo schránku Windows. Šifruje, podepisuje, komprimuje, zaručuje kontrolu integrity dat. Je S/MIME kompatibilní. Je využito soukromých klíčů ze Session Manageru a certifikátů z PKI. Soubory mohou být bezpečně zasílány prostřednictvím modemu, GSM… Je kompatibilní s podobnými produkty jiných výrobců.

IW FTP Client

Umožňuje bezpečně komunikovat s FTP servery pomocí Bezpečného tunelu, autentizace mezi serverem, klienty a konzolou podle X.509 v.3. Zašifrovává/odšifrovává soubory on-line, během propojení mezi serverem a klientem. Využívá soukromých klíčů ze Session Manageru a certifikátů z PKI. Integrita paketů nebo souborů je zajištěna.

IW FTP Server

Umožňuje komunikaci pomocí bezpečného tunelu, autentizaci mezi serverem, klienty a konzolou podle X.509 v.3. Zašifrování/odšifrování souborů on-line, během propojení mezi serverem a klientem. Je využito soukromých klíčů a certifikátů z PKI. Integrita paketů nebo souborů je zajištěna.

• Dodávané typy instalací

Všechny typy instalace (kromě samostatné instalace IW Shredder a IW JustProtect) obsahují základní moduly z C-PKI, kterými jsou IW GINA, IW ScreenWall, IW ConfigManager, IW KeyManager.

IW Security Suite – Client

Obsahuje volitelné moduly z IW Security Suite Protection, kterými jsou IW FileProtect, IW FolderProtect, IW JustProtect a IW Shredder. Kromě toho i IW Security Suite Communication, konkrétně IW MailProtect, IW FTP Client.

IW Security Suite – Management Server

Je tvořen IW Management Serverem z C-PKI.

IW Security Suite – FTP Server

Obsahuje IW FTP Server z IW Security Suite Communication.

IW Security Suite – Certificate Server

Tvoří samostatný IW Certificate Server z C-PKI.

IW Shredder

Samostatná aplikace IW Shredder pracuje zcela nezávisle, bez nutnosti připojení k C-PKI.

IW LDAP Server

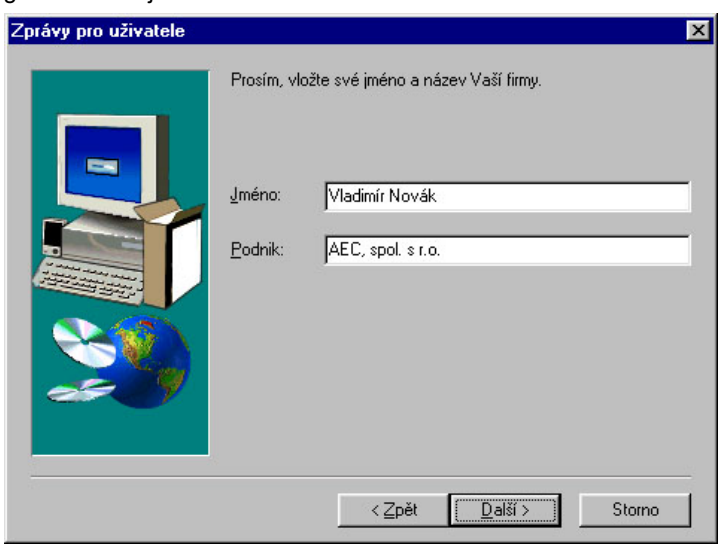
Instaluje se společně s IW Certificate Serverem a slouží pro přístup k certifikátům vydaným certifikačním serverem (Certifikační Autoritou) pomocí standardu LDAP. Nedílnou součástí IW LDAP Serveru je i replikační plánovač, který ve stanovených intervalech aktualizuje LDAP databázi certifikátů.

IW JustProtect

Samostatná aplikace IW JustProtect pracuje zcela nezávisle, bez nutnosti připojení k C-PKI, ale umožňuje pouze šifrování do EXE souborů.

Instalace IronWare® Security Suite - Client

Instalace i odinstalace probíhá formou standardního instalačního průvodce. Je vhodné před instalací zavřít všechny aplikace, neboť po jejím dokončení je vyžadován restart systému. Instaluje se spuštěním programu ***Setup.exe*** umístěného v instalačním adresáři systému IronWare®. Instalaci můžete kdykoliv ukončit kliknutím na tlačítko *„Storno“* umístěné vpravo dole ve všech oknech průvodce. Jsou tu i dvě další tlačítka a to tlačítko *„<- Zpět“* a tlačítko *„Další ->“*. Pomocí těchto tlačítek se můžete pohybovat po jednotlivých stránkách průvodce. Celá instalační procedura se skládá z několika fází, které jsou ovlivněny druhem instalace. Nejprve instalátor znázorní průběh přípravy k instalaci. Poté se spustí vlastní instalační proces, který v prvních krocích zjistí zda je nainstalovaný Internet Explorer verze 4.01 nebo vyšší. Tento program je nutný pro zabezpečení správné funkce některých modulů systému IW Security Suite. Jestliže program nemáte nainstalovaný, tak vás na tuto skutečnost upozorní a nabídne vám ukončení instalace a pokračování později, až budete mít IE 4.01 nainstalovaný nebo pokračování dále v instalaci. Dále pak upozorní na zákonnou ochranu produktu a vyžádá si souhlas s licenčními podmínkami. Bez něho není možné v instalaci pokračovat. Následuje zadání jména uživatele a názvu společnosti. Standardní údaje jsou zobrazeny podle údajů zadávaných při instalaci Windows, ale můžete je změnit dle svých iniciálů. Příklad dialogového okna je zobrazen níže.



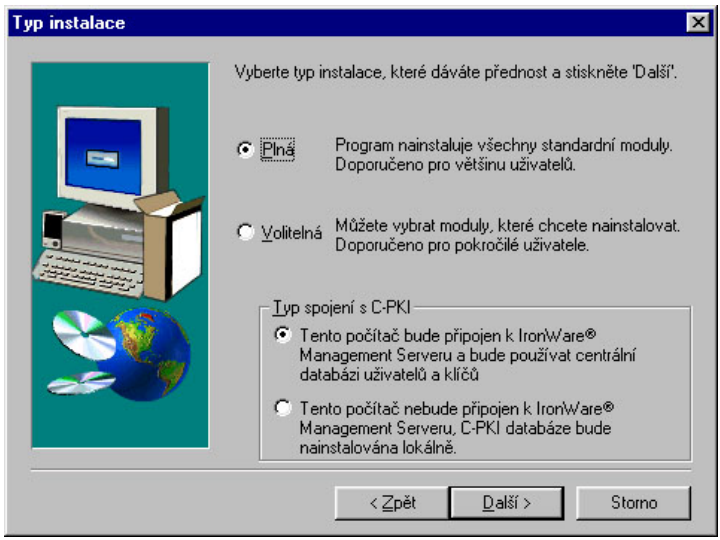
Obr.1. Instalace – informace o uživateli

Obr. 2. Instalace – automaticky nadefinovaná cesta pro instalaci

Obr. 3. Instalace - manuální vyhledání adresáře pro instalaci

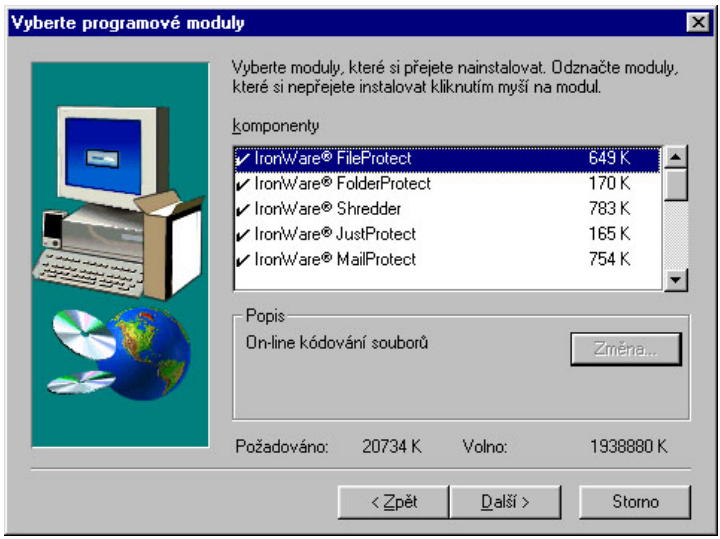
Poté je uživatel dotázán na cílový adresář. Program nabídne implicitní cestu, kam se má IW Security Suite nainstalovat. V případě, že vám přednastavená cesta z nějakého důvodu nevyhovuje, je možné zadat jinou pomocí volby *Procházet*.

V dalším okně se zadává typ instalace. Uživatel může vybrat instalaci plnou nebo volitelnou a nezávisle na tom zvolit lokální PKI či připojení k nějakému IW Management Serveru. Volba *Plná* slouží pro méně zkušené uživatele a nainstaluje všechny součásti produktu IronWare®.



Obr. 4. Instalace - Volba typu instalace a spojení s C-PKI

V případě volby instalace *Volitelná* je uživateli ponechána možnost výběru, které části IW Security Suite se budou instalovat (ve stejném okně současně zobrazuje potřebné a volné místo na disku).



Obr. 5. Instalace - Volba typu instalace

Po zadání typu instalace je zobrazeno varování, že po dokončení instalace budete potřebovat spuštěný IronWare® Management Server a jestli si přejete pokračovat v instalaci nebo ne.

Dalším krokem instalace je zadání jestli chcete používat IronWare® FolderProtect (Off – line šifrování adresářů) nebo IronWare® FileProtect (On – line šifrování souborů). Oba dva druhy šifrování nemohou být nainstalovány současně, proto musíte zvolit jeden z nich. Implicitně je zvolena volba IronWare® FolderProtect (Off – line šifrování adresářů).

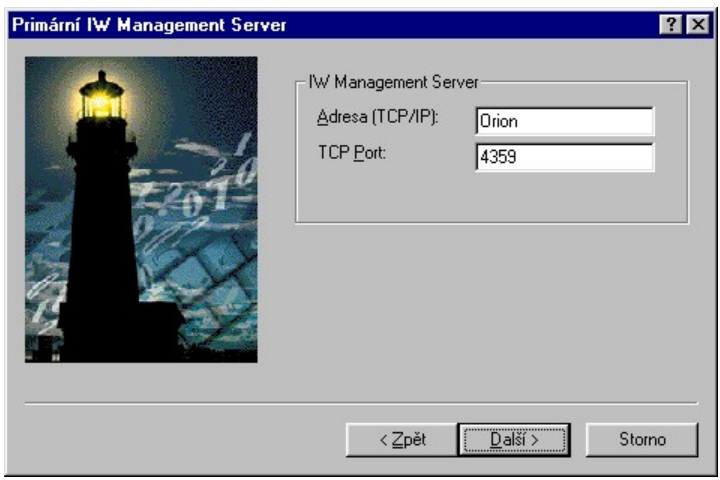
Obr. 6. Instalace - Volba metody šifrování při instalaci

Následně jste požádáni o zadání programové složky. Jde o položku, která se má vytvořit v nabídce *„Start“*. Pod touto položkou budou uloženy odkazy na všechny instalované programy IronWare® Security Suite a můžete je odtud pohodlně spouštět. Implicitně je vložena položka *„IronWare Security Suite“* v nabídce *„Start\Programy“.*

V dalším okně jsou konečné informace o instalaci ještě než se začne produkt instalovat na pevný disk. Jsou zde zobrazeny informace o uživateli, informace o instalaci a vybrané programové moduly. Zkontrolujte, prosím, tyto informace a případně se můžete pomocí tlačítka *„Zpět“* vrátit a opravit volbu dle vašich představ. Samotné kopírování souborů se začne kliknutím na tlačítko *„Další“*. Po dobu kopírování souborů zobrazuje instalátor na indikátoru stav zkopírovaných souborů.

Po dokončení kopírování se spustí instalační průvodce IronWare® Security Suite, ve kterém bude možné provést nastavení důležitých částí IronWare® Security Suite. Pro centrální databázi se musí nastavit k jakému se budete připojovat IW Management Serveru a nebo pro lokální databázi musíte zadat administrátora a další nastavení nutné pro připojení do systému.

Pro nastavení používání centrální databáze uživatelů a klíčů je zapotřebí, aby v tuto dobu byl spuštěn na nějakém počítači IronWare® Management Server. Okno které se vám zobrazí je použito pro zadání adresy IW Management Serveru. Do tohoto pole můžete vložit IP adresu počítače nebo přímo jméno počítače v síti, např. „Orion“ apod. Do dalšího editačního pole je pak třeba vložit TCP Port, což je připojovací port a je implicitně nastaven na hodnotu 4359.

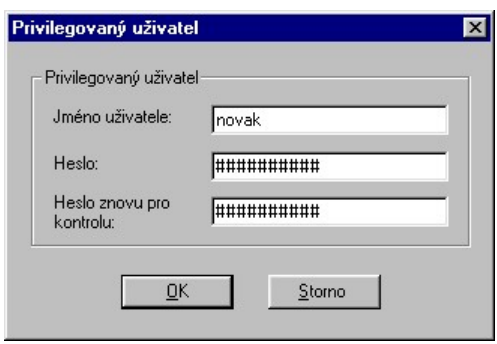


Obr. 7. Instalace - Nastavení připojení k IW Management Serveru

Po vložení žádaných hodnot si průvodce nastavením systému IronWare® zjistí přítomnost IW Management Serveru a v případě, že jej nenalezne, zobrazí zprávu o tom, že se nelze připojit k IW Management Serveru a je vám nabídnuto znovu okno pro zadání správných hodnot. Jestliže jsou vložené hodnoty správné a na nějakém počítači je spuštěn IW Management Server, pak si průvodce z tohoto serveru zjistí SecurityID a vy jste požádáni o jeho kontrolu. Toto SecurityID si můžete ověřit se SecurityID uvedeném v dialogovém okně *„O Programu …“* v IW Management Serveru. Pokud jste SecurityID ověřili a je správné, pak je konfigurace připojení k centrální databázi ukončena,a jste vyzváni k restartování počítače. Uzavřete, prosím, všechny programy a stiskněte tlačítko *„Restartovat počítač“*. Tímto je instalace IronWare® Security Suite hotova.

Jestliže budete používat lokální databázi uživatelů a klíčů, musíte zadat, zda chcete používat systém obnovy hesel a uživatelské jméno a heslo administrátora. Nejdříve jste dotázáni, zda používat systém obnovy hesel. K tomu je třeba zadat tři privilegované uživatele, kteří mohou později např. při ztrátě hesla, heslo obnovit resp. zjistit.

Obr. 8. Instalace - Nastavení systému obnovy hesel a tří privilegovaných uživatelů

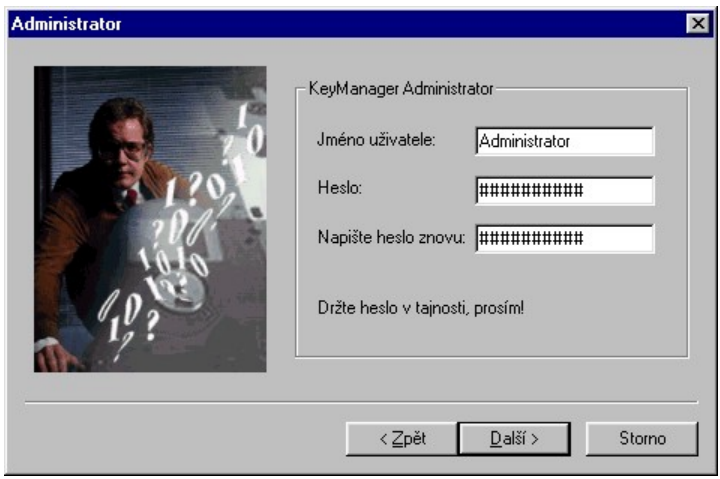


Obr. 9. Instalace - Vytvoření privilegovaného uživatele

Privilegovaného uživatele vytvoříte tak, že kliknete na tlačítko *„Změnit“* u každého privilegovaného uživatele. V tomto okně jsou tři pole pro zadání privilegovaného uživatele. Tlačítko *„Změnit“* vyvolá dialogové okno, ve kterém se zadává jméno privilegovaného uživatele a heslo. Třetí editační

pole slouží pro zopakování zadávaného hesla. Privilegovaného uživatele pak uložíte nebo změníte kliknutím na tlačítko *„OK“*.

Po zadání všech privilegovaných uživatelů, jestliže chcete používat systém obnovy hesel se musí zadat jméno a heslo administrátora. Pod tímto jménem se vytvoří v databázi uživatelů a klíčů na lokální PKI účet s právy administrátora a heslem pro přístup k tomuto účtu. Heslo držte v tajnosti, protože pod tímto heslem budete mít přístup k celé databázi uživatelů a hesel. Další nové administrátory pak můžete vytvořit v programu IW KeyManager ze systému IronWare® Security Suite volbou nabídky *„Start/IronWare Security Suite/IronWare® KeyManager“* nebo volbou nabídky IW KeyManager programu IW Tray z panelu úloh Windows.



Obr. 10. Instalace - Vytvoření administrátorského účtu v lokální databázi

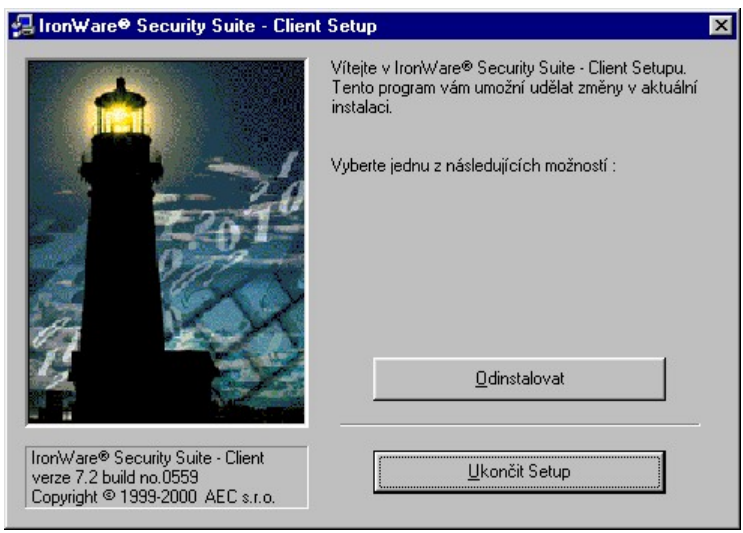
Po kliknutí na tlačítko *„Další ->“* začne generování náhodného klíče pro vámi právě vytvořený administrátorský účet. Náhodný klíč se generuje pomocí pohybu myši po okně a nebo stiskem náhodných kláves na vaší klávesnici.

Obr. 11. Instalace - Generování náhodného klíče

Po vygenerování náhodného klíče administrátora se ukončí instalační průvodce a zobrazí se okno pro restart počítače. Uzavřete, prosím, všechny programy a stiskněte tlačítko *„Restartovat počítač“*. Po restartu je instalace IronWare® Security Suite hotova.

• Odinstalace Client

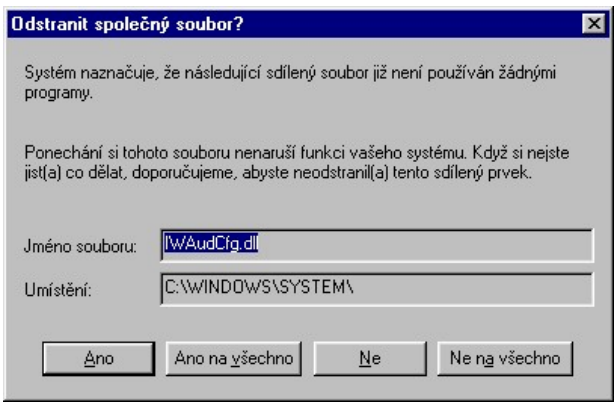
Odinstalovat IronWare® Security Suite můžete dvěma způsoby. První způsob je kliknout na položku *„Odinstalace IronWare® Security Suite - Client“* v nabídce *„Start\Programy/IronWare Security Suite“*. Druhou možností je spustit *„Ovládací panely/Přidat nebo ubrat programy“*. Klikněte na položku *„IronWare® Security Suite – Client“* a pak klikněte na tlačítko *„Přidat či odebrat“*.



Obr. 12. Odinstalace - Odinstalační okno IronWare® Security Suite

Spustí se část instalačního průvodce zajišťující odinstalaci. Jestliže máte spuštěný nějaký program ze systému IronWare® Security Suite, který má být odstraněn při této instalaci, odinstalační průvodce zahlásí chybu a je třeba nejprve program ukončit a pak odinstalovat znovu. V případě, že máte zašifrovaná nějaká data a chcete odinstalovat systém, pak vás odinstalační průvodce také upozorní, a pomůže vám tyto data dešifrovat. Pokud máte opravdu nějaká data zašifrovaná a chcete opravdu systém IronWare® Security Suite ze systému odstranit, je třeba vzít na vědomí, že již nebude možné tyto data znovu šifrovat, a že budou uloženy nezašifrovaná a budou vystavena možnému nebezpečí. Jestliže je vše v pořádku, instalační

průvodce si vyžádá potvrzení pro provedení odinstalace a spustí odstraňování souborů. Některé z nich jsou označeny jako sdílené i pro jiné aplikace, a z tohoto důvodu je u nich pak vyžádáno potvrzení pro jejich odstranění.



Obr. 13. Odinstalace - Dotaz na odstranění sdíleného souboru

Jestliže vyberete *„Ano“*, pak odstraníte sdílený soubor. Jestliže zvolíte *„Ano na všechno“*, odinstalátor se zeptá, jestli chcete odebrat všechny sdílené soubory ze systému. Volba *„Ne“* ponechá sdílený soubor v systému. Jestliže zvolíte volbu *„Ne na všechno“,* ze systému se neodstraní žádný sdílený soubor. Smazání sdíleného souboru může, ale nemusí mít vliv na některé jiné aplikace.

Po odstranění všech souborů klikněte na tlačítko *„OK“* a budete vyzváni k restartu počítače. Poté je odinstalace hotová a IronWare® Security Suite je odstraněn ze systému.

Obr. 14. Odinstalace - Požadavek na restart počítače

IronWare® Complex-PKI

IronWare® Security Suite je založen na **PKI (Public Key Infrastructure)** spolu s povinnými moduly jako je správa uživatelských účtů, tajných uživatelských klíčů pro symetrické šifry, skupinových tajných klíčů pro skupiny uživatelů, zabezpečení přístupu do počítače a mnoho dalších (dále jen PKI), což z tohoto programového balíku činí silný nástroj pro vývoj bezpečnostních aplikací s centralizovanou správou založenou na technologii klient/server. Protože PKI (jak je definováno v mezinárodních standardech), je pouze jednou ze součástí celého programového balíku, nazývá se tento produkt Complex-PKI, zkráceně C-PKI.

• Registrační klíče

C-PKI je systém, který může být spuštěn v demonstračním režimu, a to pouze na omezené časové období od instalace, takzvaná Trial verze. Importem souboru, který je registračním klíčem, se systém stává trvale funkční bez časového omezení. Klíči jsou omezeny i volitelné moduly. V okně *„O Programu …“* se zobrazuje jméno a název společnosti uživatele, počet licencí a doba platnosti. Pro ostrou verzi klíče je v informačním okně vyznačeno, že platnost klíče není časově omezena a jsou zde vyjmenovány registrované moduly.

• IW GINA a přihlašování uživatele do systému

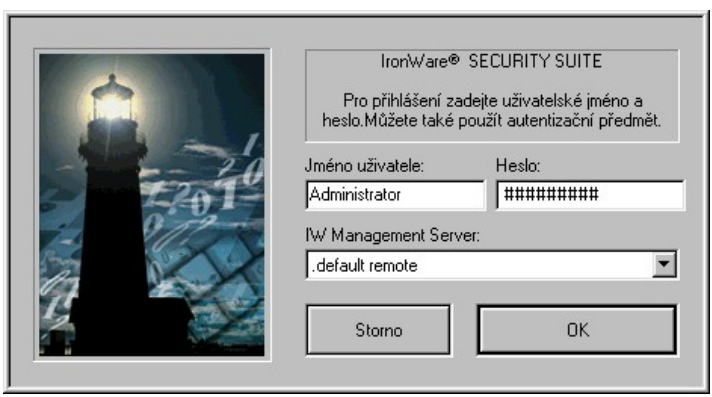
• GINA pro Windows 95, 98

Jedná se o přihlašovací proces, který zajistí zjištění identity uživatele a načtení sady jeho šifrovacích klíčů a osobních údajů.

Přihlásí uživatele do systému PKI jeho jménem a heslem, které uživatel zadá ručně, z čipové karty či jiného hardwarového autentizačního předmětu. Povolí také přihlášení anonymního uživatele stisknutím tlačítka *„Storno“* v přihlašovacím okně. Anonymní uživatel nemá k dispozici žádné klíče ani certifikáty a jeho účet je podobný anonymnímu uživateli ve Windows. Uživatel je (v případě použití centrální databáze PKI) implicitně přihlašován k IW Management Serveru. Pokud není přístupná síť a uživatel požaduje připojení k IW Management Serveru, systém zobrazí chybové hlášení. V tomto případě je nezbytné provést přihlášení k lokálnímu PKI.

Umožňuje automatické přihlášení uživatele do systému Windows současně s přihlášením k PKI. Tato funkce se nazývá *single sign-on*.

Všechny změny v lokálním PKI budou zrušeny při prvním přihlášení k centrálnímu IW Management Serveru, protože v této chvíli je lokální PKI aktualizováno centrální kopií.



Obr. 15. IW GINA - Přihlášení uživatele jménem a heslem

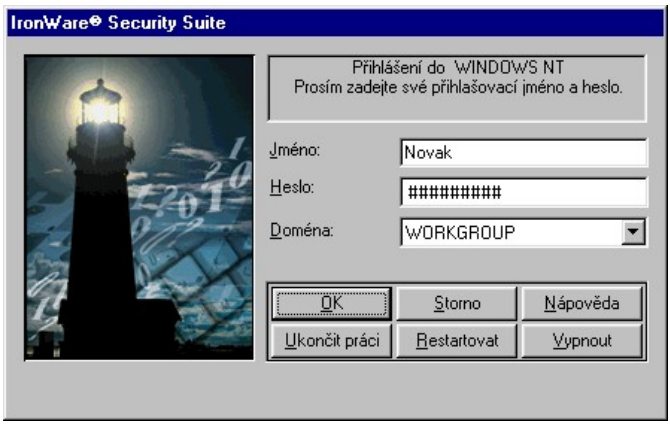
- **GINA pro Windows NT**

Jedná se o přihlašovací proces, který má kromě přihlášení uživatele a načtení jeho sady klíčů řadu dalších funkcí, např. *Zamknout stanici* (zablokování počítače při krátkodobém odchodu obsluhy) aj. IW GINA ve Windows NT se liší od GINY ve Windows 98 a 95 také bezpečným spořičem obrazovky IW ScreenWall, který zabezpečuje zamknutí stanice na požádání nebo po nastavené době nečinnosti. Základní rysy má společné s GINOU pro Windows 95 a 98. Umožňuje podobně jako GINA pro Win95, 98 *single sign-on* přihlášení a použití *autentizačních předmětů*.

- **Hlavní znaky**

Přihlásí uživatele do systému IronWare® Security Suite (PKI) jeho jménem a heslem, které uživatel zadá ručně nebo z čipové karty. Je možné též provést přihlášení anonymního uživatele zadáním uživatelského jména *Anonymous* či *Guest* v přihlašovacím okně.

Obr. 16. IW GINA - Přihlášení uživatele do IronWare® Security Suite



Obr. 17. IW GINA - Přihlášení do Windows NT

Přihlásí uživatele do systému Windows NT jménem a heslem, které uživatel přímo zadá do přihlašovacího okna, a nebo použije data z nastavení tohoto uživatele (single sign-on). Pokud si uživatel přeje (a má to povoleno), jméno a heslo do Windows NT se uloží pro příští použití.

Obr. 18. IW GINA - Uzamčení stanice ve Windows NT

Pro úspěšné přihlašování je nutné mít správně nakonfigurovanou podporu ODBC. Pokud nainstalujete software s novou verzí této podpory, nemusí být možné se přihlásit do systému jako autorizovaný uživatel. V tomto případě se přihlaste pod anonymním účtem "guest" a po

restartu počítače nutném pro konfiguraci ODBC by další přihlášení mělo proběhnout bez potíží.

- **Autentizační předměty**

Uživatel se může systému PKI identifikovat zapsáním svého jména a zadáním hesla v přihlašovacím okně z klávesnice. V některých případech si však uživatelé přejí řešení zahrnující pro autentizaci i jiné možnosti, jako jsou hardwarové autentizační prostředky, či biometrické snímače.

IronWare® Security Suite v současné době podporuje dva druhy přímo ovládaných čipových karet, všechny systémy připojené přes PC/SC rozhraní a snímač otisků prstů. Tyto autentizační předměty je možno mezi sebou vzájemně výhodně kombinovat. Speciální kombinace jsou pro klienty připravovány na přání a po dohodě s klientem. Standardní instalace dovoluje kombinovat libovolná hardwarová zařízení a zadávání údajů z klávesnice.

Čtečky čipových karet umožňují například použití čipových karet, v jejichž paměti je uloženo uživatelské jméno a heslo, které je chráněno proti neautorizovanému čtení a přepsání. Karta může být použita pro jednoduchou autentizaci uživatele pouhým vsunutím do čtečky. Systém detekuje vsunutí karty a přečte z ní potřebné údaje. Tento systém může být na přání uživatele rozšířen o požadavek zadání PIN, jako je tomu například u bankovních kreditních karet.

Zadání PIN může být nahrazeno sejmutím otisků prstu přihlašovaného. Tak dojde ke zkombinování čipové karty pro autentizaci uživatele a potvrzení jeho identifikace pomocí otisku jeho prstu. Takto je velmi efektivně zabráněno možnosti zneužití odcizené čipové karty.

Snímač otisků prstů je další hardwarové zařízení, které může být použito k autentizaci uživatele. Při vytváření či modifikaci účtu uživatele mohou být nasnímány otisky tří prstů a tyto pak budou sloužit pro jeho identifikaci. Při přihlašování uživatel do GINY napíše svoje jméno a přitiskne jeden z nasnímaných prstů ke snímači. V případě souhlasu jména a otisku bude uživatel autentizován a přihlášen. Vzhledem k tomu, že výrobce tohoto zařízení neposkytuje ovladače pro operační systém Windows NT, není tato funkce ve Windows NT implementována.

Návod k instalaci jednotlivých hardwarových prostředků je dodáván společně s těmito prostředky. Všeobecně se však dá říci, že detekce hardwarových prostředků systémem IronWare® Security Suite probíhá po nainstalování driverů k těmto prostředkům (dodávaných jejich výrobci) automaticky.

• IW ScreenWall

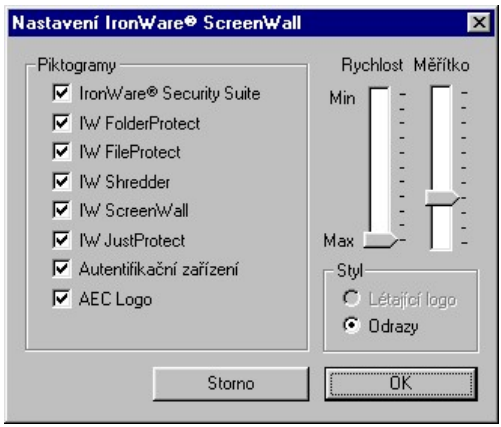
Uživatel může při krátkodobém opuštění pracoviště zablokovat počítač pomocí horké klávesy, vytažením čipové karty ze čtečky, nebo je možné toto zablokování spustit po nastavené době nečinnosti uživatele. Po aktivaci ScreenWallu se na obrazovce objeví šetřič obrazovky a systém se zablokuje. Odblokovat se může pouze vložením přihlašovacího předmětu zpět do čtečky nebo zadáním hesla aktuálně přihlášeného uživatele z klávesnice či pomocí snímače otisků prstů.

Zda bude IW ScreenWall používán, lze nastavit včetně doby nečinnosti, po které bude spuštěn, ve *Vlastnostech obrazovky* ve Windows. Zde se jako spořič obrazovky zvolí IW ScreenWall a nastaví se doba, za kterou se v případě nečinnosti uživatele aktivuje. Volbou tlačítka „*Nastavení*“ lze změnit vizuální nastavení IW ScreenWallu.

Obr. 19. Nastavení IW ScreenWallu jako spořič obrazovky

V záložce *Obecné* v IW ConfigManageru lze nastavit, zda se bude IW ScreenWall aktivovat při vytažení čipové karty ze čtečky, aktivační klávesa pro spouštění IW ScreenWallu a vizuální nastavení.

Obr. 20. IW ConfigManager - záložka Obecné – nastavení IW ScreenWallu

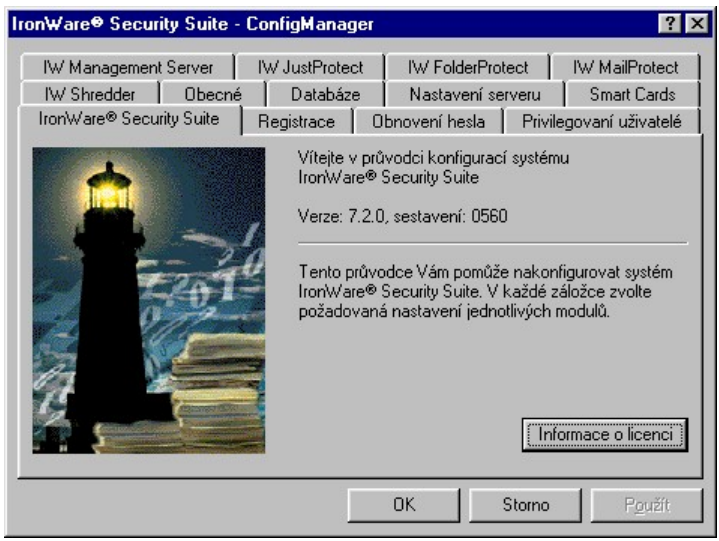


Obr. 21. IW ConfigManager – záložka Obecné – vizuální nastavení IW ScreenWall

V tomto okně můžete zvolit, které piktogramy chcete, aby se zobrazovaly v IW ScreenWallu. Dále se zde nastavuje rychlost jejich pohybu a jejich velikost. Vámi zvolené nastavení se uloží kliknutím na tlačítko *„OK“* a zruší kliknutím na tlačítko *„Storno“*.

• IW ConfigManager

Pro globální nastavování parametrů a vlastností systému IronWare® Security Suite je určena aplikace IW ConfigManager Prostřednictvím záložek umožňuje konfiguraci a správu všech nainstalovaných součástí produktu. IW ConfigManager je možno kdykoliv ukončit bez uložení provedených změn stiskem tlačítka „*Storno*“. Po provedení jakékoliv změny v konfiguraci se aktivuje tlačítko „*Použít*“, které umožňuje průběžné ukládání nastavení, aniž by se IW ConfigManager ukončil. Stiskem tlačítka „*OK*“ se uloží změny a ukončí program. Výše zmíněná tlačítka jsou umístěna v levé dolní části programu.

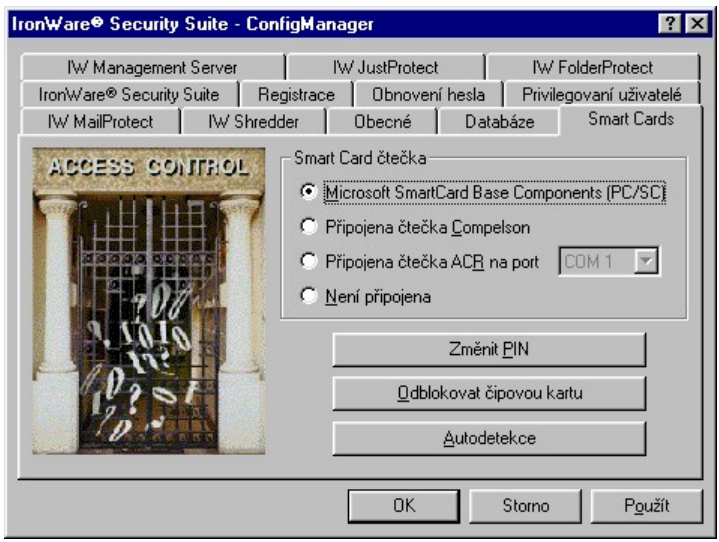


Obr. 22. IW ConfigManager - záložka IronWare® Security Suite

Po spuštění IW Config Manageru se objeví záložka IronWare® Security Suite. Je tu uvedena verze instalovaného produktu a číslo sestavení. Po stisku tlačítka *„Informace o licenci“* budou zobrazeny informace o názvu a verzi produktu, vlastníku a čísle licence.

- **Záložka Smart Cards**

Tato záložka umožňuje nastavení čipových karet, připojených k počítači. Nastavuje připojení a typ čtecího zařízení autentizačních předmětů. Záložka *Smart Cards* umožňuje přímo nastavit hodnoty, nebo pokud si nejste jisti, můžete kliknout na tlačítko *„Autodetekce“* a systém se pokusí zjistit připojenou čtečku čipových karet. Lze zde také změnit PIN na čipové kartě a odblokovat čipovou kartu s PIN.



Obr. 23. IW ConfigManager - záložka Smart Cards

Pokud máte problém s připojením čtecího zařízení, zkontrolujte nastavení sériových portů vašeho počítače v nabídce *„Start/Nastavení/Ovládací panely“*.

- **Záložka Obecné**

Záložka *Obecné* umožňuje nastavit nastavení pro modul IW ScreenWall a modul IW GINA.

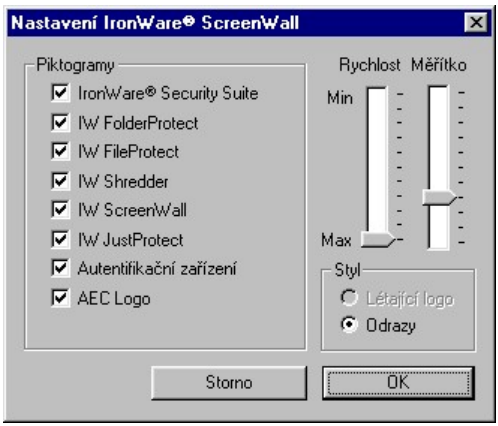
Obr. 24. IW ConfigManager - záložka Obecné

Do okna *"ScreenWall horká klávesa"* je po stisknutí vámi vybrané kombinace kláves automaticky zapsána klávesová zkratka pro spuštění zablokování systému v podobě spořiče obrazovky.

Zaškrtnutím volby *„Vždy používat ScreenWall s čipovými kartami"* je možné aktivovat spouštění IW ScreenWall při vyjmutí autentizačního předmětu ze čtecího zařízení a deaktivovat při vložení autentizačního předmětu do čtecího zařízení.

Tlačítko „*ScreenWall vizuální nastavení …"* nastavuje rychlost pohybu objektů po obrazovce, velikost objektů a jaké objekty se mají zobrazovat, je-li aktivní ScreenWall.

Tlačítko *„Nastavit IW Ginu jako prvotní přihlášení do Windows"* slouží pro nastavení, aby se IW Gina spouštěla jako první přihlašovací modul. Je to z toho důvodu, že by v případě nějakého jiného nainstalovaného programu, který by se nastavil jako primární, nefungovala plná bezpečnost systému a nefungovala by „single sign-on" funkce. Pokud tedy budete instalovat nějaký program, který se zaregistruje jako primární přihlašovací systém a nebo provedete nějaké změny v nastavení sítě na vašem počítači, pak klikněte na toto tlačítko.



Obr. 25. IW ConfigManager - Vizuální nastavení IronWare® ScreenWall

- **Záložka Obnovení hesla**

Obr. 26. IW ConfigManager - záložka Obnovení hesla

Pokud jste při instalaci IronWare® Security Suite či IW Management Serveru povolili funkci obnovování hesel, objeví se v IW ConfigManageru

pro všechny uživatele záložka *Obnovení hesla*. Po vyplnění hesel libovolných dvou privilegovaných uživatelů je možné obnovit heslo libovolného jednoho zvoleného uživatele. Pro obnovení hesla každého dalšího uživatele je nutno opětovně zadat hesla dvou privilegovaných uživatelů.

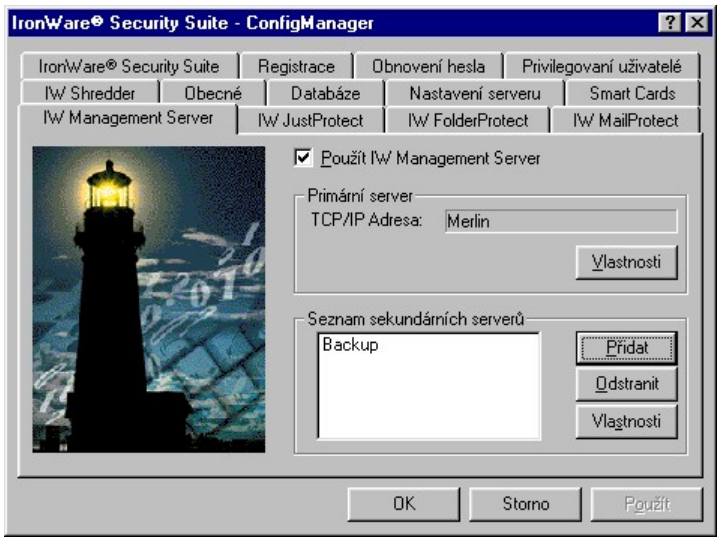
- **Záložka Privilegovaní uživatelé**

Obr. 27. IW ConfigManager - záložka Privilegovaní uživatelé

Je–li při instalaci IronWare® Security Suite či IW Management Serveru povoleno obnovování hesel, může si kterýkoliv z privilegovaných uživatelů v průběhu života systému měnit svoje heslo. Jelikož privilegovaní uživatelé nejsou v systému zavedeni do struktury uživatelských účtů, provádí změnu svého hesla přes tuto záložku, která je přístupná jen administrátorům.

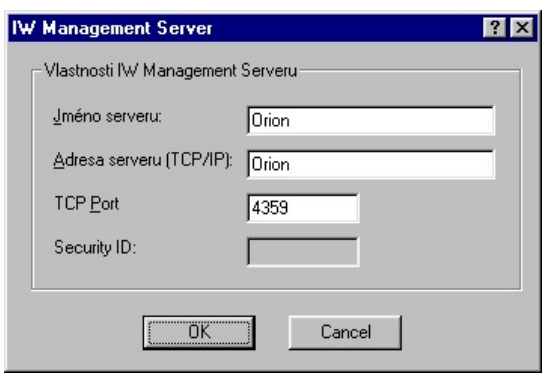
Tato záložka dále umožňuje v případě nutnosti změnit jméno a heslo třetího privilegovaného uživatele (na principu sdíleného tajemství). Je k tomu ovšem nutná přítomnost libovolných dvou ze tří privilegovaných uživatelů, kteří musejí zadat svá hesla.

- **Záložka IW Management Server**



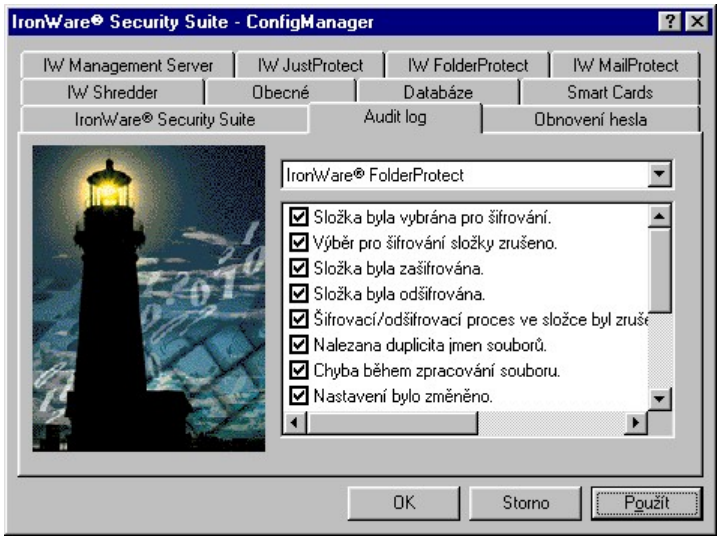
Obr. 28. IW ConfigManager - záložka IW Management Server

Zde je možné nastavit, zda má systém IronWare® Security Suite používat IW Management Server a případně měnit jeho adresu. V části *Primární server* lze určit, který server bude sloužit jako primární, v *Seznamu sekundárních serverů* je možné přidání, odebrání a nastavení vlastností případných dalších IW Management Serverů, ke kterým bude možné se připojit.



Obr. 29. IW ConfigManager - přidání dalšího Management Serveru

- **Záložka Audit Log**



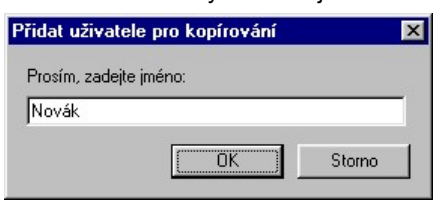
Obr. 30. IW ConfigManager - záložka Audit Log

Záložku Audit Log mají přístupnou pouze auditoři, kteří zde provádějí nastavení událostí, které se v systému IronWare® Security Suite mají zaznamenávat. Pomocí seznamu v horní části okna si volí modul, u něhož mají zájem změnit nastavení a poté zaškrtnou události, které se mají zaznamenávat.

- **Záložka Databáze**

Obr. 31. IW ConfigManager - záložka Databáze

Zde je možné stanovit, které části databáze se mají kopírovat na lokální stanici ze zvoleného IW Management Serveru. Implicitně je nastaveno, že se má vždy zkopírovat účet aktuálně přihlášeného uživatele, lze však kopírovat i více účtů uživatelů podle seznamu, bez ohledu na to, kdo je přihlášen, nebo celou databázi. Do lokální databáze se budou kopírovat pouze zde zvolené záznamy a žádné jiné.

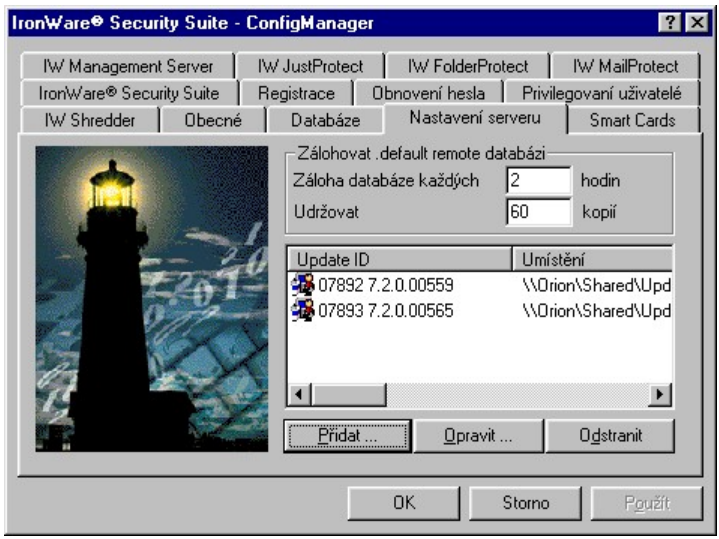


Obr. 32. IW ConfigManager - zadání uživatele pro pravidelné kopírování databáze

Další nastavení této záložky je četnost zálohování celé databáze (pro případ poškození) a volba automatického kopírování certifikátů. Pokud je nastaveno kopírování celé databáze, je nutné nastavit také periodu tohoto mirroru. Perioda se nastavuje v rozmezí od 0 do 99, přičemž 0 znamená, že se vždy bude na lokální počítač kopírovat celá databáze při loginu, a každá jiná hodnota určuje po kolika dnech se bude databáze kopírovat celá. Je – li

zapnuto automatické kopírování certifikátů, dochází při každém přihlášení ke kopírování všech certifikátů obsažených v databázi bez ohledu na nastavení mirroru celé databáze.

- **Záložka Nastavení serveru**



Obr. 33. IW ConfigManager - záložka Nastavení serveru

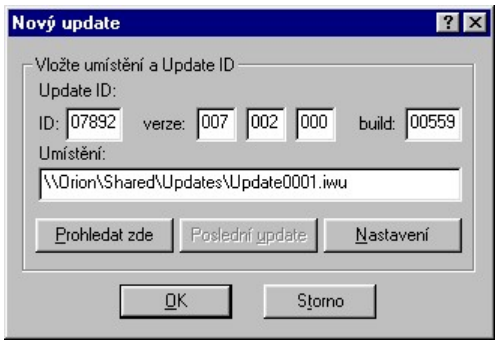
Tato záložka slouží k nastavení automatického zálohování PKI databáze.

Je možné zde nastavit jak často (po kolika hodinách) se má automatická záloha vytvářet a kolik kopií se má uchovávat.

Implicitní nastavení automatického zálohování databáze je, že se zálohuje jednou za 24 hodin a uchovává se 14 záloh. Název souboru má formát PKI_RRRR_MMDD_hhmm.DAT, kde R je rok, M měsíc, D den, h hodina a m minuta. Čas nejbližší zálohy se zobrazuje v *About* dialogu v IW Management Serveru. Zálohy se provádějí na počítač s nainstalovým IW Management Serverem. Když počet záloh překročí uživatelem nastavený počet, je nejstarší záloha automaticky odstraněna z počítače.

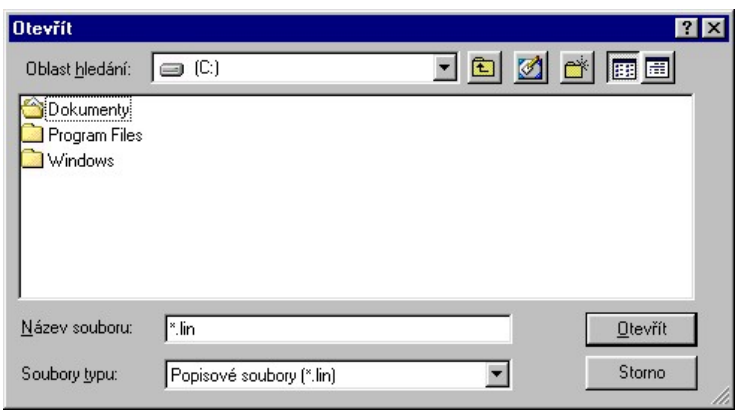
Záložka též slouží k editaci updatů systému IronWare® Security Suite. Administrátor si může přidat do databáze updatů odkaz na nejnovější update a pak si jej „stáhne“ z přednastaveného serveru nebo lokální adresy. Update se pak nainstaluje automaticky sám při dalším přihlášení do systému.

Přidání nebo oprava se provádí v okně, které se objeví po kliknutí na tlačítko „Přidat …“ nebo „Opravit …“. Odkaz na update lze i odstranit a to kliknutím na tlačítko „Odstranit“.



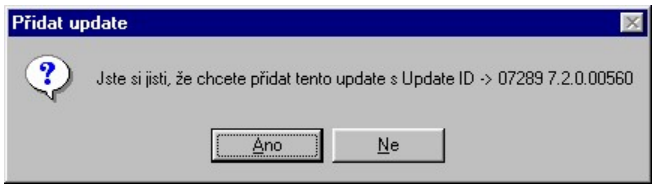
Obr. 34. IW ConfigManager - přidání nového update nebo oprava update

Toto dialogové okno přidá nový odkaz na update do databáze Umožňuje také opravení existujících odkazů na updaty. Do editačních polí *„Update ID“* se zadává identifikační číslo updatu, číslo verze a číslo sestavení. Do editačního pole *„Umístění“* se musí vložit adresa, kde je update umístěn. Tato adresa může být jakákoliv UNC, URL adresa nebo adresa síťového počítače v síti LAN, jak ukazuje obrázek. Pokud zvolíme tlačítko *„Prohledat zde“*, zobrazí se vám okno, ve kterém lze najít a otevřít soubor s extenzí *„*.lin“*, který popisuje samotný update soubor. V tomto popisném souboru je uvedena lokace updatu, identifikační číslo, číslo verze i číslo sestavení.



Obr. 35. IW Config Manager - vyhledání a otevření popisujícího souboru

Po otevření souboru se zjistí informace o updatu a vyplní se příslušná editační pole. Jednotlivé části můžete editovat a kliknutím na tlačítko *„OK“* update přidat do databáze. Před přidáním updatu do databáze budete požádání o potvrzení operace.



Obr. 36. IW Config Manager - potvrzení přidání updatu do databáze

Jestliže zvolíte *„Ano“*, update se přidá do databáze updatů.

Update lze přidat ještě jedním způsobem, a to kliknutím na tlačítko *„Poslední update“*. Z vámi nastavené adresy je zjištěn automaticky nejnovější update, který se zobrazí v příslušných editačních polích a je možno jej přidat do databáze updatů. Adresa, odkud se bude zjišťovat nejnovější update se nastavuje v okně, které se zobrazí po kliknutí na tlačítko *„Nastavení“*.

• Konfigurace IW Security Suite Protection

V následující části je uveden pouze stručný popis konfigurace IW Security Suite Protection. Podrobný popis je uveden níže.

• Záložka IW FileProtect

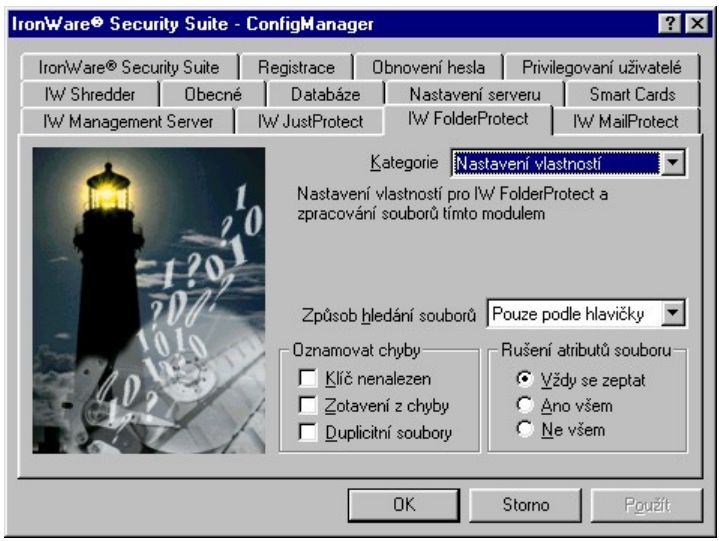
Tato záložka obsahuje pouze jednu funkci, kterou je vypnutí šifrovacího ovladače a je k dispozici pouze tehdy, je-li IW FileProtect instalován a je-li přihlášen některý z administrátorů. Po zaškrtnutí a potvrzení volby *Vypnout šifrovací ovladač* nebudou soubory na vašem disku odšifrovány (zašifrovány). Tato volba slouží především na vytváření archivů v šifrované podobě, tzn. je-li tato volba zapnuta a je-li provedena archivace dat na záložní medium (CD, ZIP, JAZZ...), zůstanou data na tomto médiu šifrovaná i po kopírování.

Obr. 37. IW ConfigManager - záložka IW FileProtect

V případě použití lokální PKI databáze jsou takto uložená data na médiu čitelná pouze tehdy, nedojde-li k přeinstalování systému IronWare® nebo pokud se šifrovací klíč, kterým jsou data na archivu šifrována uloží k pozdějšímu použití.

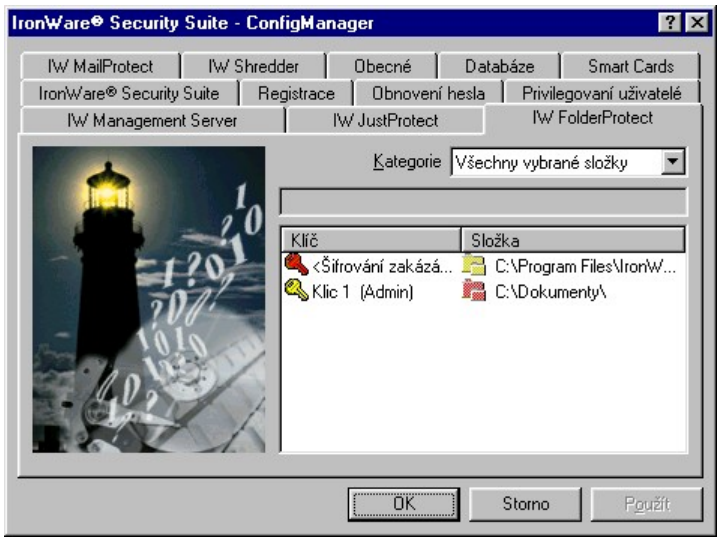
- **Záložka IW FolderProtect**

Zde je možné provádět nastavení vlastností IW FolderProtectu, zobrazit přehled všech složek, které jsou určeny k šifrování tímto modulem a také spravovat databázi složek určených k šifrování. Správa databáze je však umožněna pouze uživatelům, kteří mají administrátorská práva.

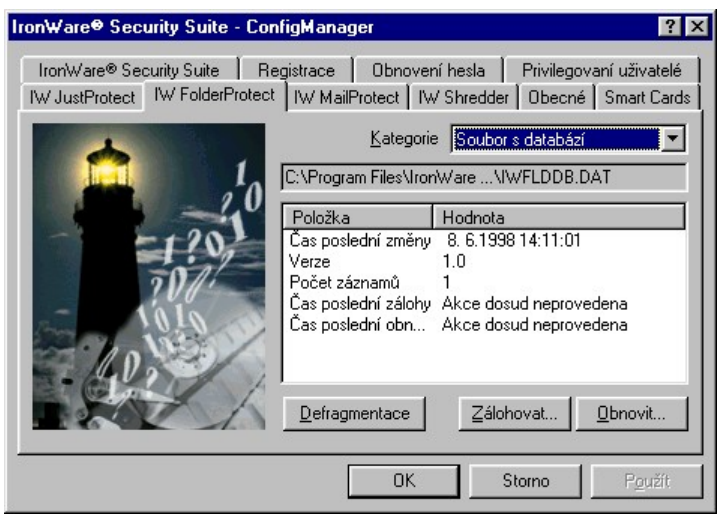


Obr. 38. IW ConfigManager - záložka IW FolderProtect –Nastavení vlastností

Dále lze nastavit, jakým způsobem bude modul IW FolderProtect zjišťovat, zda jsou soubory ve složce vybrané ke zpracování zašifrovány nebo odšifrovány (volba *Způsob hledání souborů*). Lze určit, zda mají být uživateli zobrazována varování a chyby, k nimž může během šifrovacího procesu dojít (volby *Klíč nenalezen*, *Zotavení z chyby* a *Duplicitní souboty*). Nastavuje se zde také způsob reakce modulu IW FolderProtect na situaci, kdy v průběhu šifrování narazí na soubor, který má nastaveny atributy jen pro čtení, skrytý či systémový.



Obr. 39. IW ConfigManager - záložka IW FolderProtect – Všechny vybrané složky



Obr. 40. IW ConfigManager - záložka IW FolderProtect – Soubor s databází

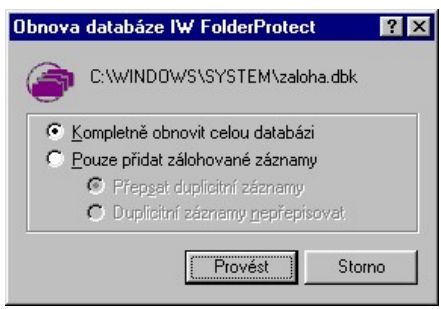
Pro správu databáze slouží tlačítka *Defragmentace*, *Zálohovat* a *Obnovit* ve spodní části záložky.

Volba *Defragmentace* odstraní z databáze prázdná místa.

Tlačítko *Zálohovat* umožňuje zálohování databáze.

Obr. 41. Dotaz na název a umístění vytvářeného souboru se zálohou

K obnově dat v databázi slouží tlačítko *Obnovit*.



Obr. 42. Volba způsobu obnovy databáze

Podrobnější popis péče o databázi je v kapitole IW FolderProtect - Off-line šifrování.

- **Záložka IW JustProtect**

Obr. 43. IW ConfigManager - záložka IW JustProtect

V této záložce je možné nastavit, jakým způsobem bude JustProtect zjišťovat, zda jsou soubory ve složce vybrané ke zpracování zašifrovány, nebo odšifrovány (volba *způsob hledání souborů*). Lze určit, zda mají být uživateli zobrazována varování a chyby, k nimž může během šifrovacího procesu dojít (volby *Klíč nenalezen, Zotavení z chyby* a *Duplicitní soubory*). Nastavuje se zde také způsob reakce modulu JustProtect na situaci, kdy v průběhu šifrování narazí na soubor, který má nastaveny atributy jen pro čtení, skrytý, či systémový.

- **Záložka IW Shredder**

Obr. 44. IW ConfigManager - záložka IW Shredder

Tato záložka je k dispozici, pouze je-li IW Shredder instalován. Nastavení IW Shredderu spočívá ve zvolení tzv. přepisovacího vzoru, což je sekvence znaků, kterou bude prováděno přepisování. Tato sekvence je buď tvořena znakem 00 a znakem FF, které se při každém dalším přepisu vymění (jeden přepis je proveden znakem 00 a druhý pak znakem FF), náhodnou (generovanou) sekvencí znaků, nebo speciálními náhodnými znaky pro úplné vymazání skartovaných dat na fyzické úrovni. V této záložce je také možnost zadat počet přepisování mazaných souborů, a to v rozsahu 1 až 26. Maximální bezpečnost poskytuje 26 přepisů, avšak úměrně počtu přepisů se také prodlužuje doba přepisování.

Velmi užitečnou pomůckou při mazání souborů a složek je možnost volby potvrzení prováděné akce. Před každým smazáním souboru nebo složky si modul IW Shredder vyžádá potvrzení této akce. Potvrzení může být vyžadováno na smazání souboru, smazání složky, smazání souboru s nastaveným atributem jen pro čtení a smazání skrytého či systémového souboru.

- **Konfigurace IW Security Suite Communication**

- **Záložka IW MailProtect**

Obr. 45. IW ConfigManager - záložka IW MailProtect

Je – li nainstalován IronWare® MailProtect, je v IW ConfigManageru také tato záložka. Slouží pro nastavení klíče, který bude použit pro podepisování zpráv, šifrovacího algoritmu, jímž se budou zprávy šifrovat, i hashovací funkce. Je zde také možné nastavit, do kterých složek budou ukládány šifrované zprávy, i některé další vlastnosti IW MailProtectu.

Volba ***Preferovaný klíč*** slouží pro výběr osobního soukromého klíče, který bude jako výchozí používán pro podpis zpráv nebo souborů.

Volba ***Zašifrování zprávy*** určuje, kterým šifrovacím algoritmem budou zprávy či soubory zašifrovány. Pro výběr jsou k dispozici tyto algoritmy: **RC2-40**, **RC2-128**, **DES**, **3DES**, **CAST** a **BLOWFISH**.

Volba ***Digitální podpis*** určuje, pomocí které hashovací funkce se bude provádět podpis zpráv nebo souborů. K dispozici jsou nabídnuty funkce **SHA** a **MD5**.

Volbou ***Kopírovat zprávy do adresáře „Bezpečné zprávy“*** lze nastavit, zda se budou zašifrované přijaté zprávy ukládat do složky *Bezpečné zprávy*.

Volba ***Uložit po přečtení zprávu odšifrovanou*** určuje, zda se budou přijaté zašifrované zprávy ukládat odšifrované nebo zašifrované.

Volbou ***Uložit S/MIME přílohu na disk*** lze nastavit, zda se budou přijaté zprávy kódované v S/MIME formátu ukládat jako **p7m** soubory do zvolené složky. Implicitně je nastavena složka *Download* v instalačním adresáři, tedy např. *C:\Program Files\IronWare Security Suite\Download*.

Volba ***Konvertovat text/soubory do S/MIME formátu*** určuje, že se budou všechny šifrované či podepsané zprávy ukládat ve formátu S/MIME – jako *smime.p7m* příloha.

Volbou ***Vždy se ptát při ukládání*** lze nastavit, zda se systém bude ptát na umístění a jméno pro uložení S/MIME přílohy. Pokud není tato volba zapnutá, S/MIME příloha se uloží v aktuální složce.

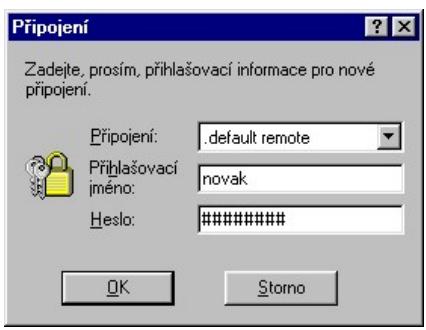
Volbou ***Clear sign zapnut*** lze nastavit používání odděleného podpisu. Zpráva podepsaná clear sign je čitelná a podpis je připojen až na konci zprávy.

• IW KeyManager

IW KeyManager je aplikace, pomocí které uživatel, auditor nebo administrátor systému provádí práci s PKI. Jedná se o komplexní aplikaci zajišťující širokou škálu služeb, např. přidávání a rušení uživatelů, přidávání, změny a rušení šifrovacích klíčů, práci s certifikáty atd. Aplikace pracuje s lokálním PKI i s centrálním (vzdáleným) PKI podle přihlášení uživatele.

• Spuštění modulu

Po spuštění modulu se provede připojení k předdefinovanému lokálnímu nebo vzdálenému PKI. V přihlašovacím okně je možné ve volbě *Změnit PKI server* zvolit přihlašovací PKI (lokální nebo některý síťový server). Toto okno se objeví v případě, že si uživatel přeje připojit se k jinému PKI, než ke kterému je momentálně připojen, a nebo pokud je do systému IronWare® přihlášen jako anonymní uživatel (účty *Guest* a *Anonymous*). Dostupné přihlašovací servery může nastavit kterýkoliv z administrátorů v modulu IW ConfigManager v záložce IW Management Server.



Obr. 46. IW KeyManager - přihlášení uživatele do PKI

V případě, že se jedná o lokální instalaci systému IronWare® , je jedinou možností přihlášení k lokálnímu PKI.

Při spouštění probíhá automatická kontrola databáze, zda neobsahuje poškozená data. Průběh připojování a načítání dat z databáze je indikován v informačním okně. V případě, že IW KeyManager nalezne v databázi poškozený záznam, podá o tom hlášení a příslušný záznam pak označí červeným vykřičníkem.

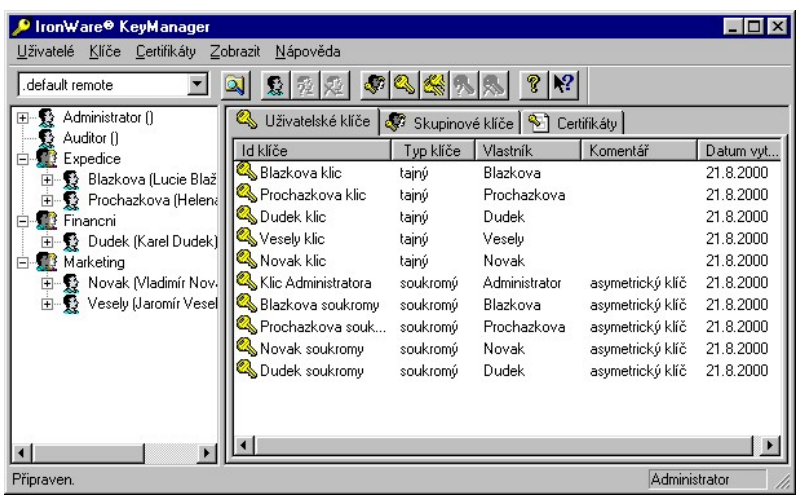
V případě poškozeného záznamu existuje několik možností řešení této situace. V případě, že poškozený záznam a jeho klíče nebyly použity je většinou možné jej vymazat, ovšem v případě, kdy je poškozena hlavička záznamu se může stát, že záznam není možné odstranit. Pokud záznam nelze použít, nebo jsou poškozeným klíčem zašifrována nějaká data, je nejvhodnější obnovit poškozená data ze zálohy.

Dále je pro přihlášení do IW KeyManageru možné použít přihlašovací jméno a heslo uživatele, který může být odlišný od uživatele přihlášeného do systému IronWare® pomocí IW GINA. Tato vlastnost umožňuje administrátorům přihlášení do modulu IW KeyManager bez toho, aniž by museli restartovat stanici. Při spuštění IW KeyManageru je vždy implicitně přihlášen ten uživatel a k takovému PKI, jako byl přihlášen v IW GINA při startu systému.

Po úspěšném přihlášení je možné kdykoliv změnit PKI, ke kterému je uživatel přihlášen pomocí menu volby *Uživatelé/Změnit PKI Server* nebo pomocí rozbalovacího seznamu umístěného na začátku nástrojové lišty.

• Organizace modulu

Po úspěšném přihlášení je program spuštěn. Zobrazí se hlavní okno modulu, které je zachyceno na následujícím obrázku.



Obr. 47. IW KeyManager - hlavní okno

- **Menu a nástrojová lišta**

IW KeyManager je možné ovládat z menu a nástrojové lišty, kde jsou soustředěny základní funkce pro práci se seznamem uživatelů, klíčů a certifikátů. Nástrojová lišta je pomůcka pro rychlé vyvolání nejběžněji používaných funkcí.

Obr. 48. IW KeyManager – nástrojová lišta

Obr. 49. IW KeyManager – výběr PKI databáze

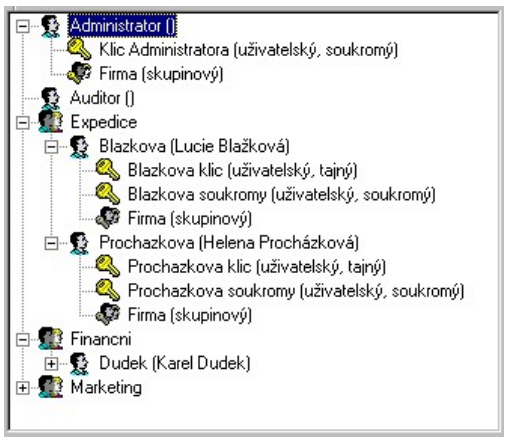
Menu	Podmenu		Popis
Uživa-telé	Přidat		Založí nový uživatelský účet.
	Odstranit		Smaže účet vybraného uživatele. Uživatel pro smazání musí být vybrán v seznamu uživatelů.
	Vlastnosti		Umožní změny v nastavení vybraného uživatelského účtu. Účet musí být vybrán v seznamu uživatelů.
	Změnit PKI server		Umožní přihlášení k jinému PKI. Uzavře komunikaci k právě otevřenému serveru a nechá vás přihlásit k jinému.
	Změnit PIN čipové karty		Pokud jsou používány čipové karty, změní PIN na kartě aktuálně přihlášeného uživatele.
	Znovu načíst		Provede znovunačtení seznamu uživatelů, klíčů a certifikátů. Znovunačtení se provede z aktuálně otevřeného PKI.
	Konec		Ukončí práci s programem KeyManager
Klíče	Nový skupinový klíč		Vytvoří nový skupinový tajný klíč pro skupinu uživatelů. Funkce je vázána na seznam sdílených klíčů.

	Nový uživatelský klíč		**Secret:** Vytvoří nový tajný symetrický šifrovací klíč. Funkce je vázána na seznam osobních tajných klíčů
	Nový uživatelský klíč		**Private:** Vytvoří nový soukromý asymetrický šifrovací klíč. Funkce je vázána na seznam soukromých klíčů
	Pře-generovat		Přegeneruje vybraný klíč. Tuto volbu je vhodné spouštět například po odebrání uživatele ze skupiny, která sdílela klíč. Použitím této funkce se zvýší bezpečnost systému. Data přegenerování klíčů jsou pak vidět ve vlastnostech klíče.
	Generovat certifikát		Dovolí vygenerovat certifikát z vybraného soukromého klíče.
	Smazat		Smaže vybraný klíč. Pokud není žádný klíč vybrán, je tato položka vypnutá.
	Odebrat klíč uživateli		Vztahuje se ke skupinovému tajnému klíči. Jeho sdílení lze odebrat ve vztahu ke konkrétnímu uživateli. Po použití této funkce je dobré provést přegenerování skupinového tajného klíče.
	Export klíče		Provede export klíče pro konkrétního uživatele. Tato funkce je používána například pro předávání dat po odchodu pracovníka a v podobných případech. Export klíče může provádět pouze majitel klíče.
	Import klíče		Provede import exportovaného klíče. Tyto funkci aplikuje nový majitel klíče.
	Vlastnosti		Nastavení vlastností klíče. Zde je k dispozici popis klíče, jeho typ, zvolený algoritmus (u symetrických klíčů), historie klíče atd. Informace se vztahují k aktuálně zvolenému klíči.
Certifi-káty	Import		Importuje certifikát ze souboru.
	Export		Exportuje certifikát do souboru

	Odstranit		Zruší certifikát ze seznamu certifikátů. Akce se vztahuje k aktuálně vybranému certifikátu.
	Generovat revokační žádost		Vytvoří žádost o zrušení platnosti vybraného certifikátu. Tato žádost je pak dopravena Certifikační Autoritě.
	Import seznamu revokací		Provede import revokačního listu.
	Vlastnosti		Zobrazí vlastnosti certifikátu.
Zobra-zit	Panel nástrojů		Zapne/vypne zobrazování nástrojové lišty.
	Stavový řádek		Zapne/vypne zobrazování stavového řádku v dolní části hlavního okna. Tento řádek obsahuje aktuální stav subsystému, krátkou nápovědu k aktuálně prováděné akci a aktuálně přihlášeného uživatele.
	Rozvinout skupiny		Rozbalí strom všech uživatelů
	Sbalit vše		Zobrazí pouze seznam skupin uživatelů
	Všichni uživatelé		Zobrazí všechny uživatele bez ohledu na vlastnictví vybraného klíče.
	Pouze vlastník klíče		Zobrazí pouze uživatele, kteří jsou vlastníky vybraného klíče.
Nápově-da	O aplikaci		Zde naleznete informace o aktuální verzi modulu. Je zde také možné zobrazit informace o vlastníku licence.
			Při kliknutí na tuto ikonu dostane kurzor speciální podobu otazníku. Kontextovou nápovědu pak získáme tak, že na příslušné místo klikneme tímto otazníkem.

- **Seznam uživatelů a příslušných klíčů**

Seznam uživatelských účtů a k nim příslušejících klíčů je základním nástrojem pro zavedení bezpečnostního systému IronWare®. Je prezentován pomocí stromové struktury v levém okně KeyManageru. V první úrovni tohoto stromu jsou zobrazeny skupiny uživatelů a někteří uživatelé (jejich přihlašovací a plná jména). Ve druhé úrovni jsou zobrazovány v případě uživatelů nepatřících do žádné skupiny klíče a v případě skupin uživatelé, ve třetí úrovni pak klíče. Z pohledu uživatele je v první úrovni vždy jméno a ve druhé klíče, neboť uživatel vidí pouze sám sebe.



Obr. 50. IW KeyManager - Struktura uživatelských účtů a jim příslušejících klíčů.

V systému jsou rozlišováni uživatelé tří základních typů:

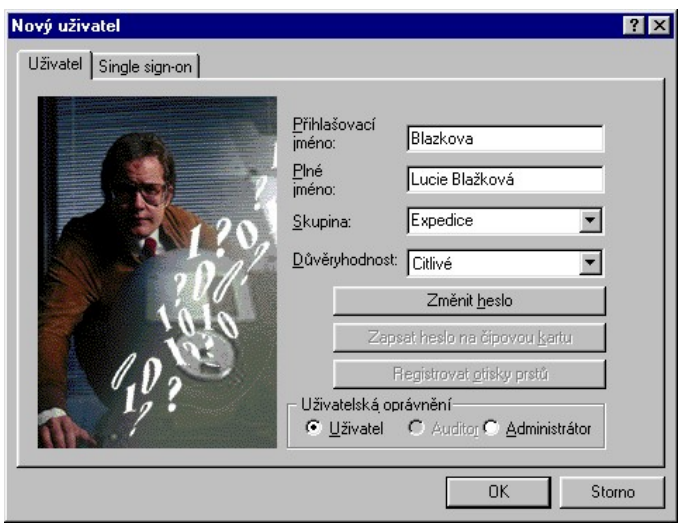
Administrátor smí přidávat a rušit uživatelské účty běžných uživatelů a administrátorů, nemůže však přidávat či rušit účty auditorů. Při vytváření účtu přiřazuje uživateli přihlašovací jméno, typ uživatele (uživatel, administrátor), úroveň důvěrnosti (u administrátora je automaticky top secret) a zařazení do určité skupiny. Při vytváření účtu může administrátor případně přednastavit uživateli heslo. Administrátor generuje a spravuje skupinové tajné klíče. Smí mazat všechny jím vytvořené klíče (osobní tajné, soukromé i skupinové tajné), ale nemůže mazat soukromé klíče vytvořené jinými uživateli, ani osobní tajné klíče uživatelů. Může však mazat či přegenerovávat všechny skupinové klíče, které vlastní (jím vytvořené). Pokud nezná heslo, nemůže měnit uživatelem provedené nastavení single

sign-on (může jen povolit či zakázat jeho použití). V kooperaci s privilegovanými uživateli může spravovat systém obnovy hesel. Smí importovat certifikáty Certifikační autority. Smí přidělit složku k šifrování skupinovým klíčem, nebo vyloučit ze šifrování.

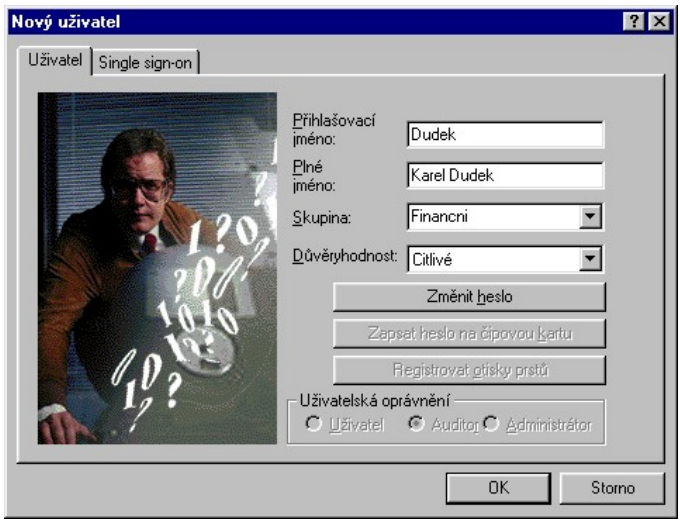
Uživatel má právo měnit si své přístupové heslo, generovat, mazat i přegenerovat osobní tajné šifrovací klíče, generovat a mazat své soukromé klíče a certifikáty, zapisovat si svá přihlašovací data do čipové karty či vkládat otisky prstů, které pak mohou sloužit místo přihlašovacího hesla. Smí importovat certifikáty, kromě certifikátů Certifikační autority. Uživatel si může dle svého přání nastavit systém jednotného přihlašování. Může v tomto systému libovolně měnit přihlašovací jméno a heslo do Windows i doménu, do níž se hlásí. Může šifrovat složky svými tajnými osobními klíči.

Auditor má veškerá práva běžného uživatele - navíc má zpřístupněny všechny operace s Audit logem (včetně jeho mazání). Na rozdíl od uživatelů má také právo vytvářet další účty uživatelů – auditorů a vidí celou strukturu uživatelských účtů a klíčů.

- **Přidání uživatele**



Obr. 51. IW KeyManager – přidání nového uživatele administrátorem



Obr. 52. IW KeyManager – přidání nového auditora jiným auditorem

Kterýkoliv z administrátorů má právo zakládat účty nových běžných uživatelů a administrátorů. Kterýkoliv auditor má právo zakládat účty nových auditorů. To lze provést pomocí kontextového menu nad databází uživatelů, z hlavního menu nebo z nástrojové lišty.

Položky v okně mají následující význam:

Přihlašovací jméno přihlašovací jméno. Pomocí tohoto jména se bude uživatel autentizovat systému. V přihlašovacím jménu se nerozlišují malá a velká písmena. Přihlašovací jméno musí být v systému jedinečné (nelze založit dva uživatelské účty se stejným přihlašovacím jménem).

V tomto poli lze používat jen číslice a znaky abecedy a není povoleno vytvářet uživatelské účty se jménem **Guest** a **Anonymous**.

Plné jméno plné jméno uživatele slouží v systému IronWare® pro přesnější identifikaci uživatele (například pro oslovování), ale nemusí být uvedeno.

Skupina určuje skupinu uživatelů, do níž bude uživatel začleněn ve struktuře uživatelů a klíčů, odkud je vidět, že uživatel je zaměstnancem např. mzdového oddělení.

Důvěryhodnost určuje úroveň důvěrnosti informací, jež by mohl daný uživatel používat a mít ve svých složkách či poště.

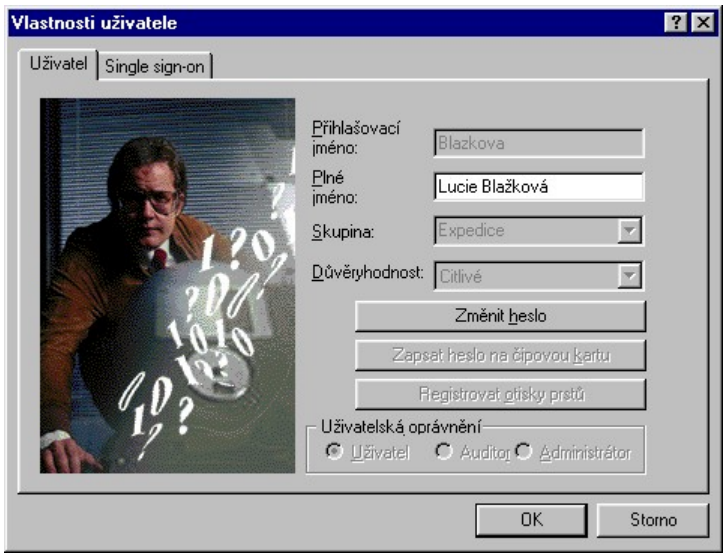
Změnit heslo nastavení přihlašovacího hesla. Zde může administrátor nastavit prvotní přihlašovací heslo. Uživatelé sami pak mají možnost si heslo kdykoliv samostatně změnit. Po stisknutí tlačítka je nutné zadat a potvrdit nové přihlašovací heslo uživatele, v případě následné změny je nutné nejprve zadat platné heslo. Pro hesla platí standardní pravidla pro zadávání hesel. IW KeyManager kontroluje, zda je heslo dostatečně bezpečné. V opačném případě je administrátor (resp. uživatel) při změně svého hesla varován:

Obr. 53. IW KeyManager - varování před použitím slabého hesla

Zapsat heslo na čipovou kartu zapíše přihlašovací jméno a heslo na čipovou kartu. Tímto způsobem je možné připravit uživatelům i tyto prostředky pro přihlášení. Tato funkce je dostupná pouze je-li v IW ConfigManageru aktivováno používání čipových karet.

Registrovat otisky prstů zaregistruje do záznamu uživatele tři otisky prstů, které je možné využít místo přihlašovacího hesla. Tato položka je při vytváření nového uživatelského účtu neaktivní. Aktivuje se pouze v případě zobrazení vlastností uživatele své osoby.

Pokud si uživatel přeje používat pro přihlašování otisky prstů, musí nejdříve vložit své otisky do databáze. To může provést pomocí tlačítka *"Registrovat otisky prstů"* v záložce *Uživatelé* ve *Vlastnostech*. Toto tlačítko je aktivní pouze pokud je připojen snímač otisků prstů a jen při zobrazování vlastností účtu uživatele aktuálně přihlášeného do IW KeyManageru.



Obr. 54. IW KeyManager - záložka *Uživatel* v okně *Vlastnosti uživatele*

Po stisku tlačítka *„Registrovat otisky prstů“* se objeví dialog umožňující vkládání či modifikaci záznamů otisků prstů.

Do databáze je možné vložit otisky tří prstů. Chcete – li vložit nový záznam, stiskněte tlačítko *„Registrovat“*, chcete – li modifikovat existující záznam, je nutné původní nejdříve odstranit pomocí tlačítka *„Odstranit“* a teprve poté přistoupit ke vkládání záznamu.

Stisknutí tlačítka *„Registrovat“* vyvolá dialog, kde je možné zvolit, otisk kterého prstu má být zaznamenán. Uživatel může zvolit kterýkoli prst levé i pravé ruky. Po provedení volby, může uživatel přistoupit k vlastní registraci otisků. Zvolený prst je nutné čtyřikrát přiložit na snímač otisků a poté ještě jednou pro potvrzení. V průběhu registrace otisku zobrazuje první řádek instrukce usnadňující registraci a druhý řádek informuje o stavu. Pokud je registrace korektně dokončena, aktivuje se tlačítko „*Ukončit“*. Tímto způsobem je možné vytvořit či modifikovat postupně všechny tři záznamy.

Uživatelská oprávnění klasifikují uživatele podle jejich základních práv v bezpečnostním systému. Vysvětlení práv jednotlivých uživatelů naleznete na začátku této kapitoly.

Další důležitou vlastností v nastavení uživatelů je používání systému jednotného přihlašování. Naleznete je v záložce *Single sign-on* uživatele při vytváření nového uživatele nebo opravě informací o již existujícím uživateli.

Obr. 55. IW KeyManager – nastavení single sign-on

Systém single sign-on slouží k jednotnému přihlašování uživatelů do systému. Pokud je aktivován, jsou správně nastaveny jeho atributy a uživatel se správně přihlásí do PKI, pak je automaticky přihlášen i k ostatním (sekundárním) systémům a službám (například do domény Windows NT nebo k Novell NetWare či UNIX serveru). Atributy single sign-on jsou:

Přihlašovací jméno přihlašovací jméno do sekundárního systému

Heslo přihlašovací heslo do sekundárního systému

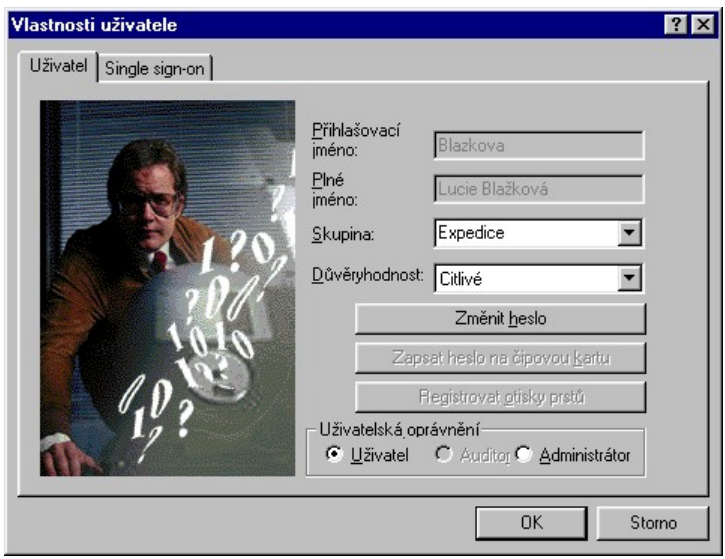
Heslo znovu potvrzení hesla, aby se zabránilo zbytečným překlepům a problémům z toho plynoucím

Doména doména, do které bude uživatel automaticky přihlašován

Povolit přihlašování single sign on zapne/vypne službu single sign-on pro aktuálně prohlíženého uživatele.

- **Editace uživatele**

Volba editace již existujícího uživatelského účtu umožňuje administrátorům a auditorům všechny akce jako přidání uživatele mimo změny přihlašovacího a plného jména. Změna hesla a nastavení single sign-on je sice umožněna, ale ke změně hesla je vyžadováno aktuální heslo. Systém jednotného přihlašování může administrátor u cizího uživatelského účtu pouze povolit či zakázat (vyjma vážných případů, kdy obnoví ve spolupráci s privilegovanými uživateli heslo náležející k danému účtu). Uživateli pak nabízí možnost úpravy vlastního plného jména, které slouží pro jeho snadnější identifikaci, a změny nastavení single sign-on.



Obr. 56. IW KeyManager - záložka Uživatel - přenastavení vlastností uživatele

Obr. 57. IW KeyManager - záložka Single sign-on - přenastavení vlastností uživatele, kdy uživatel má použití systému jednotného přihlašování povoleno a nastaveno, z pohledu administrátora.

- **Smazání uživatele**

Smazání běžného uživatele či administrátora může provést kterýkoli administrátor v systému, smazání auditora libovolný jiný auditor. Smazání označeného uživatele je možné provést z hlavního či kontextového menu, z panelu nástrojů nebo pomocí klávesy <*Delete*>.

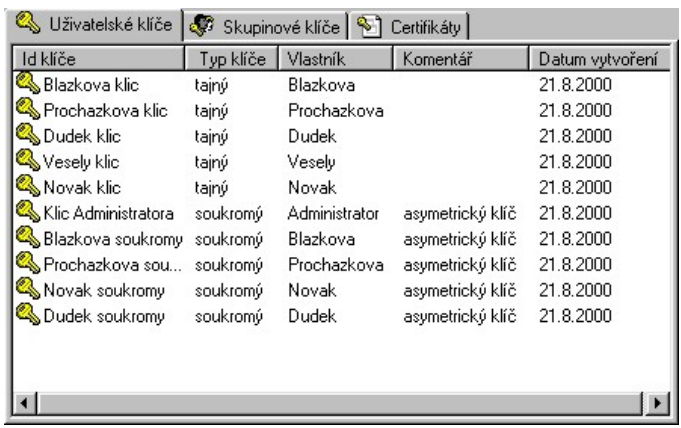
Se smazáním uživatele jsou ze systému odstraněny také šifrovací klíče tohoto uživatele.

- **Seznam klíčů a certifikátů**

V pravé části hlavního okna IW KeyManageru se nachází seznam všech osobních tajných a soukromých klíčů, skupinových tajných klíčů a certifikátů ve třech záložkách.

- **Záložka Uživatelské klíče**

V první záložce je seznam osobních tajných a soukromých šifrovacích klíčů. Chcete – li zjistit vlastníka klíče, stačí klíč označit, a v levé části okna se u vlastníka označeného klíče objeví červená tečka.



Id klíče	Typ klíče	Vlastník	Komentář	Datum vytvoření
Blazkova klic	tajný	Blazkova		21.8.2000
Prochazkova klic	tajný	Prochazkova		21.8.2000
Dudek klic	tajný	Dudek		21.8.2000
Vesely klic	tajný	Vesely		21.8.2000
Novak klic	tajný	Novak		21.8.2000
Klic Administratora	soukromý	Administrator	asymetrický klíč	21.8.2000
Blazkova soukromy	soukromý	Blazkova	asymetrický klíč	21.8.2000
Prochazkova sou...	soukromý	Prochazkova	asymetrický klíč	21.8.2000
Novak soukromy	soukromý	Novak	asymetrický klíč	21.8.2000
Dudek soukromy	soukromý	Dudek	asymetrický klíč	21.8.2000

Obr. 58. IW KeyManager s aktivní záložkou užívatelských tajných a soukromých klíčů

Zde jsou klíče dvojího typu:

A) **Uživatelské tajné klíče** – symetrické klíče určené pro osobní šifrování souborů pro vybraného uživatele

B) **Uživatelské soukromé klíče** – asymetrické klíče určené pro bezpečnou komunikaci tohoto uživatele s okolním světem (např. pro šifrování elektronické pošty)

S klíči obou typů lze provádět základní operace, jako je jejich vygenerování (založení), přegenerování (vytvoření nového klíče místo starého, přičemž starý klíč je uložen do historie, nikoliv smazán), editace, smazání a export do souboru. Tyto akce jsou dostupné pouze pro vlastníka

klíčů – tj. pouze pokud aktuálně přihlášený uživatel je totožný s majitelem klíče.

Operace pro jednotlivé typy klíčů:

Osobní tajné klíče

a) Vygenerování (založení) klíče

Vygenerování klíče lze provést v hlavním menu volbou *Klíče/Nový uživatelský klíč/Tajný* nebo v kontextovém menu volbou *Nový tajný klíč uživatele*, nebo pomocí tlačítka v nástrojové liště.

Obr. 59. IW KeyManager - zadávání dat pro generování nového klíče

V okně je nutné zadat následující data:

Název klíče Jedinečný název klíče. Tento název se nesmí u jednoho uživatelského účtu vícekrát opakovat, avšak v systému může existovat několik klíčů s totožným názvem, ale u různých vlastníků.

Komentář Komentář. Zde je vhodné zaznamenat určení klíče.

Vlastník klíče Toto pole zobrazuje vlastníka klíče, tj. aktuálně přihlášeného uživatele, který klíč vytváří (vytvořil).

Typ klíče Zde je možné zvolit šifrovací algoritmus, který bude použit při šifrování tímto klíčem. K dispozici jsou algoritmy: RC2-40, DES, IDEA, Triple DES, Triple DES3, BlowFish a CAST128.

Úroveň důvěryhodnosti Zde je možné nastavit úroveň utajení dat, k jejichž šifrování je tento klíč určen. Výběr utajení je omezen nastavením uživatele, tedy například uživatel, který má nastavenu úroveň *Vyhrazen*, nemůže mít klíč se stupněm utajení T*ajné* nebo *Přísně tajné*.

Po vyplnění těchto dat a stisknutí tlačítka *„Další“* je uživatel požádán o nasbírání náhodných dat pro generování nového klíče, v případě, že je to třeba.

Obr. 60. IW KeyManager - výběr způsobu sbírání dat pro generování

V tomto okně jsou uživateli nabídnuty tři způsoby tvoření klíče:

- *Generovat náhodný klíč* – generování klíče na základě sběru náhodných dat. Pro toto generování je nutné nasbírat dostatečné množství náhodných čísel. Neděste se však v případě, že při generování více klíčů proběhne sběr náhodných čísel pouze jednou. To je v pořádku, neboť systém sbírá náhodná čísla

pouze před prvním generováním po spuštění KeyManageru. V systému PKI je tento problém řešen pomocí snímání kliknutí myši nebo psaní na klávesnici.

- *Generovat ze zadané fráze* – místo sbíraní náhodných čísel vepíše uživatel do příslušného řádku libovolnou větu delší než 10 znaků. Při tomto způsobu je nutné pro generování každého klíče vepsat libovolnou sekvenci znaků. Povoleny jsou všechny znaky včetně semigrafických.
- *Vložit hodnotu klíče přímo* – uživatel vkládá do řádky přímo hodnotu klíče v hexadecimálním tvaru.

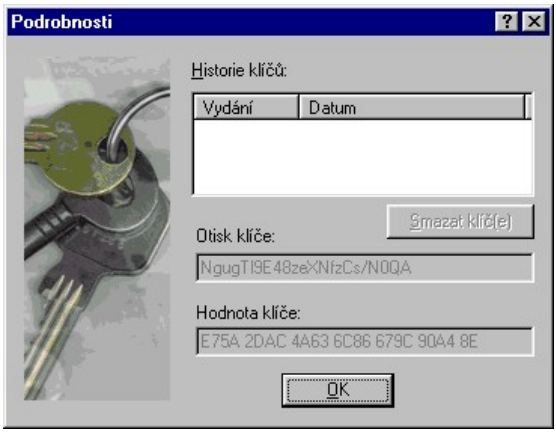
b) Vlastnosti klíče

Obr. 61. IW KeyManager - zobrazení informací o cizím klíči

Obr. 62. IW KeyManager - zobrazení informací o vlastním klíči

Zde je možné zobrazit informace o aktuálně vybraném klíči. Jediné, co však lze dodatečně změnit, je komentář k určení klíče. Tento komentář, jak je vidět na obrázcích, může změnit pouze majitel daného klíče. Nikdo jiný to udělat nemůže, a to ani v případě, že má práva administrátora. Po kliknutí na tlačítko *„Rozšířené“* se zobrazí okno s hashem klíče a v případě klíče vlastního také hodnotu tohoto klíče. Navíc je zde položka *Historie klíče* obsahující data přegenerování klíčů a položka *Datum* obsahující datum posledního přegenerování klíče.

Obr. 63. IW KeyManager - zobrazení rozšířených informací o cizím klíči



Obr. 64. IW KeyManager - zobrazení rozšířených informací o vlastním klíči

c) Smazání klíče

Klíče smí mazat pouze jejich vlastníci (administrátoři či auditoři pouze v případě rušení celého uživatelského účtu), a to pomocí volby *Smazat klíč* z hlavního nebo kontextového menu, pomocí klávesy <Delete>, či pomocí ikony z panelu nástrojů.

d) Regenerování klíče

Klíče je možné přegenerovat – tj. postupně přejít na nový klíč. Jelikož data mohou být šifrována původním klíčem, jsou uchovávány i staré verze klíče. Systém si tímto způsobem pamatuje všechny přegenerované klíče a ty jsou identifikovány datem svého generování. Osobní tajné klíče mohou být přegenerovány jen jejich vlastníkem, který musí být do systému přihlášen jako aktuální uživatel.

Soukromé klíče

a) Vygenerování (založení) klíče

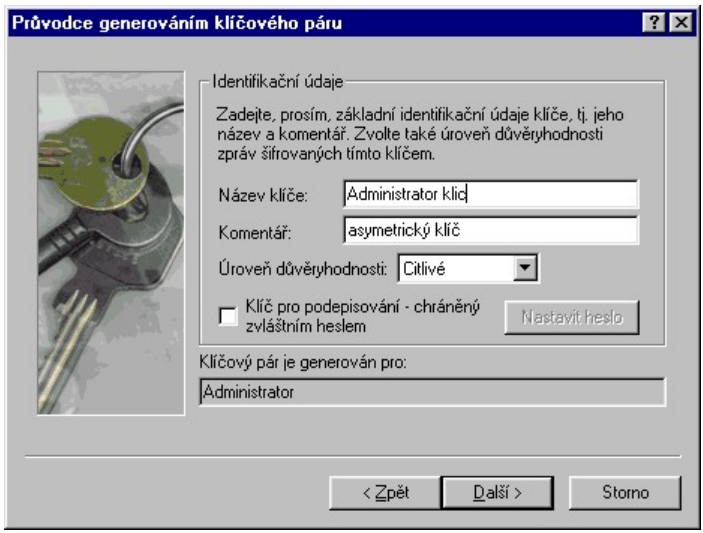
Vygenerování klíče lze vyvolat hlavniho menu volbou *Klíče/Nový uživatelský klíč/Soukromý*, z kontextového menu příkazem *Nový soukromý klíč* nebo tlačítkem na nástrojové liště. Poté se spustí průvodce generováním šifrovacího klíče.

Obr. 65. IW KeyManager - úvodní okno pro generování asymetrického soukromého klíče

Po úvodní obrazovce zobrazující vlastníka klíče je zobrazeno okno pro zadání vstupních údajů o klíči, kde je nutné zadat následující údaje:

Název klíče Jedinečný název klíče. Tento název se nesmí u jednoho uživatelského účtu vícekrát opakovat, avšak v systému může existovat několik klíčů s totožným názvem, ale různým vlastníkem.

Komentář Komentář k použití klíče. Standardně je dosazen text *asymetrický klíč*.



Obr. 66. IW KeyManager - zadání základních dat pro generování soukromého (asymetrického) klíče

Úroveň důvěryhodnosti Označuje, pro jakou úroveň citlivosti dat je klíč určen. Podobně jako u osobních tajných klíčů je stupeň utajení limitován nastavením uživatele.

Klíč pro podepisování - chráněný zvláštním heslem po zatržení zaškrtávacího boxu se aktivuje tlačítko *„Nastavit heslo“*, které uživateli nabídne dialog pro zadání hesla. Takto vytvořený soukromý klíč je možné použít pouze pro podepisování, nikoliv pro šifrování.

V následujícím kroku nabízí průvodce volbu následujících údajů:

Algoritmus Umožňuje volbu šifrovacího algoritmu a hashovací funkce. Je možné zvolit algoritmy RSA, DSA nebo ELLIPTIC a hashovací funkce SHA nebo MD5. Za primární je považováno nastavení šifrovacího algoritmu. Hashovací funkce zde nastavená slouží pouze pro výrobu certifikátu, kde je součástí jeho podpisu.

Délka klíče Délka klíče. Toto pole je plněno automaticky podle úrovně klíče (následující položka), ale je možné délku klíče zadat i ručně.

Účel použití

Určuje, k čemu bude klíč sloužit. Zda bude sloužit pouze pro šifrování pošty nebo také k podepisování. ***Podepisování žádostí o certifikát*** - klíč s tímto účelem je určen pro podepisování certifikačních žádostí daného uživatele. Jestliže je takový klíč certifikován certifikační autoritou, pak uživateli stačí jen poslat podepsanou žádost o certifikát jakéhokoliv jiného klíče na stejnou certifikační autoritu a obdrží zpět certifikát. Výsledek je stejný, jako by se byl identifikovat v certifikační autoritě osobně. Taková služba slouží k šetření administrativních nároků při generování a certifikování více klíčů. Uživatel musel vážit cestu na certifikační (či registrační) autoritu jen jednou.

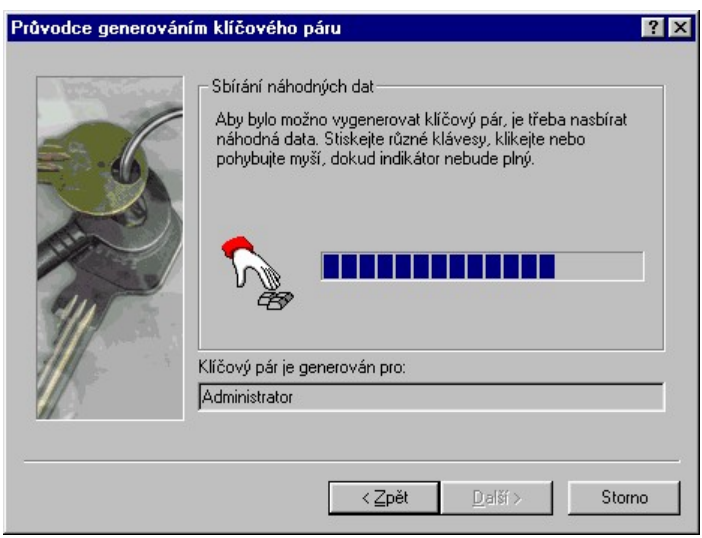
Vytváření digitálního podpisu - klíč tohoto určení slouží pouze pro podepisování dat a může být uložen pod zvláštním heslem (na přání uživatele), které nepodléhá systému obnovení hesel. Uživatel takového klíče si může být jist, že klíč nebude a nemůže být zneužit.

Šifrování dat – klíč tohoto určení slouží pouze pro šifrování dat, souborů a elektronické pošty. Určení klíčů může být kombinováno. Nejobvyklejší kombinace je jeden klíč s určením všech tří vlastností, jeden klíč pouze pro šifrování a jeden klíč pouze pro podepisování, chráněný zvláštním uživatelským heslem.

Nastavení šifrovacího algoritmu DSA (Digital Signature Algorithm) neumožňuje v poli *Účel použití* označit položku Šifrování dat, neboť slouží pouze pro podpis. Dále při volbě tohoto šifrovacího algoritmu a hashovací funkce MD5 dochází k nekompatibilitě s normou pro certifikáty. Program sice umožňuje tuto kombinaci nastavit, ale aby nekompatibilitě zabránil, takovéto nastavení ignoruje a k algoritmu DSA dosadí vždy hashovací funkci SHA.

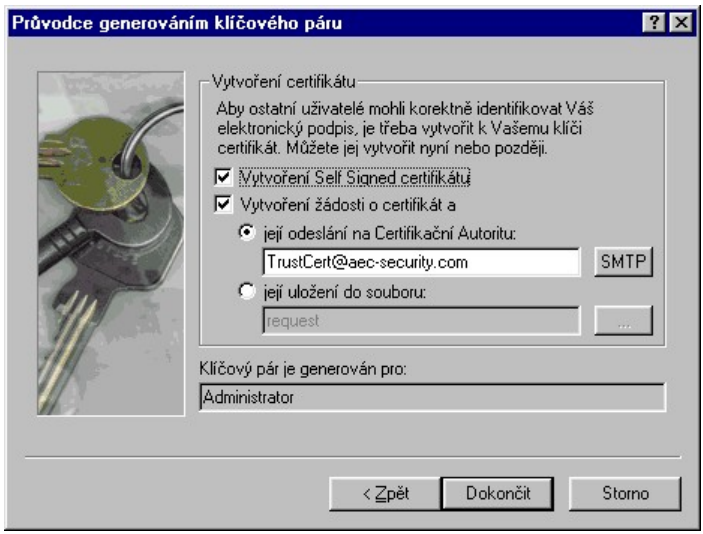
Obr. 67. IW KeyManager - zadání šifrovacího algoritmu, hashovací funkce, délky a účelu klíče pro klíč chráněný heslem

V dalším kroku průvodce nasbírá náhodná čísla pro generování klíče snímáním pohybu a klikání myši nebo psaní na klávesnici.



Obr. 68. IW KeyManager - sběr náhodných čísel při generování klíče

Dále průvodce připraví žádost o certifikát pro Certifikační autoritu nebo vytvoří tzv. Self Signed certifikát bez účasti Certifikační autority.



Obr. 69. IW KeyManager - možnosti pro vytvoření certifikátu

Možnosti podpisu certifikátu jsou následující:

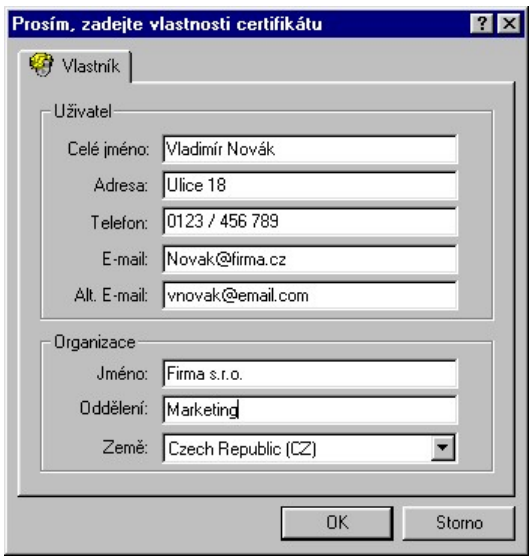
a) **Vytvoření Self Signed certifikátu** – klíč je podepsán sám sebou. Tato metoda je jediná možná v případě, že není k dispozici žádná Certifikační autorita, avšak certifikát nemá vysokou důvěryhodnost.

b) **Vytvoření žádosti o certifikát a její odeslání na Certifikační Autoritu** – zašle e-mailem žádost o certifikát k podpisu Certifikační autoritě společnosti AEC TrustCert. Tato implicitní volba může být pro uživatele na přání změněna.

c) **Vytvoření žádosti o certifikát a její uložení do souboru** – uloží žádost o certifikát do souboru. Tento soubor je následně možné nechat podepsat (ověřit) Certifikační autoritou, tj. dopravit jej Certifikační autoritě například pomocí webu, osobně na disketě, poslat e-mailem apod.

Při zasílání klíčů a certifikátů je rozdíl mezi notací MS Exchange (MS Mail), kde se zadává jen uživatelské jméno a automaticky se doplní adresa serveru, na kterém tento uživatel pracuje, a notací Internet Mail, kde je třeba zadat celou e-mailovou adresu včetně adresy poštovního serveru.

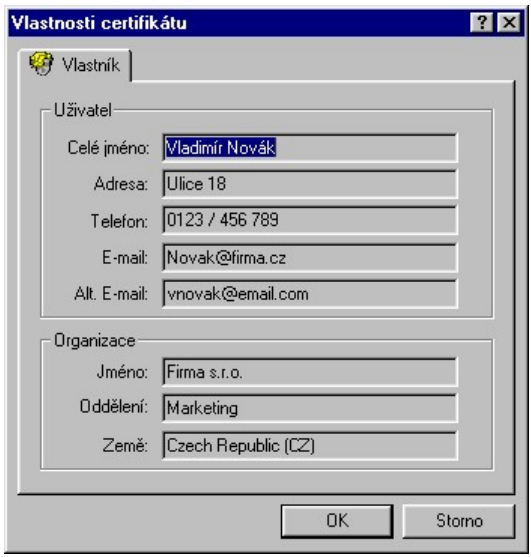
Aby bylo možné certifikát ověřit Certifikační autoritou, musí žádost o certifikát (a tedy i certifikát) obsahovat informace o jeho vlastníkovi, jak ukazuje následující obrázek. Na rozdíl od předchozích verzí IronWare® může být nyní certifikát spojen s více než jednou adresou. Při generování certifikátu je možné zadat dvě elektronické adresy a další dvě mohou být přidány kdykoliv později.



Obr. 70. IW KeyManager - vkládání údajů pro certifikát

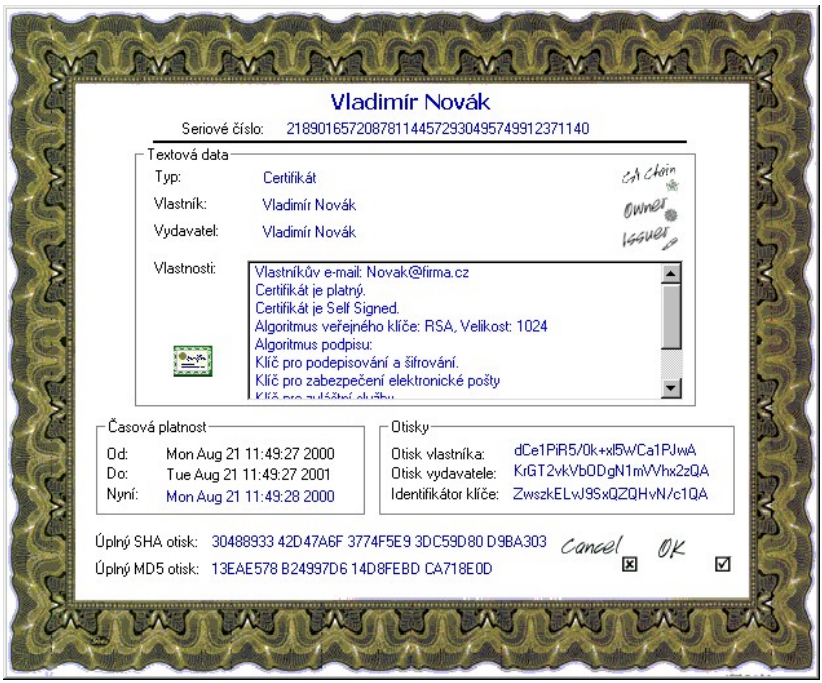
b) Vlastnosti klíče

Vlastník klíče nebo administrátor či auditor může pomocí hlavního nebo kontextového menu zobrazit informace o klíči. Informace o libovolném certifikátu může zobrazit kdokoliv.



Obr. 71. IW KeyManager - vlastnosti certifikátu - záložka Vlastník

Obr. 72. IW KeyManager - vlastnosti certifikátu - záložka Vydavatel



Obr. 73. IW KeyManager - vlastnosti certifikátu

c) Smazání klíče

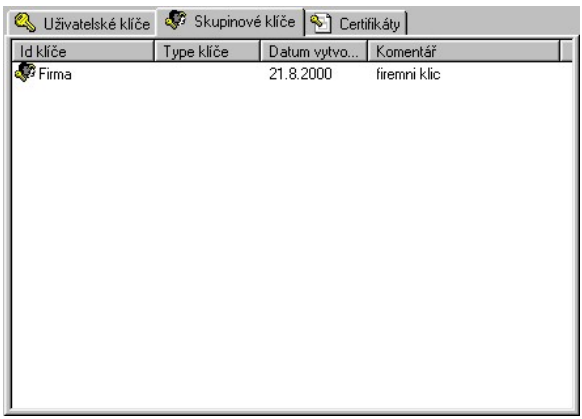
Klíč může smazat pouze jeho vlastník (administrátor a auditor pouze pokud ruší celý uživatelský účet), a to pomocí volby *Smazat klíč* v hlavním či kontextovém menu, pomocí klávesy <*Delete*>, nebo ikony z panelu nástrojů. Pokud byly ke klíči vytvořeny nějaké certifikáty, budou smazány zároveň s klíčem.

d) Vytvoření certifikátu ke klíči

Certifikát je možné buď vytvořit při generování klíče, nebo je možné jej vygenerovat později. Případně je možné existující certifikát smazat a vygenerovat nový, nebo mít u klíče certifikátů více. Nejprve je nutné označit klíč, k němuž bude certifikát generován. Pak v menu *Klíče* zvolit položku *Generovat certifikát*, která vyvolá stejné okno jako při generování certifikátu současně s klíčem.

- **Záložka Klíče skupiny**

Princip vytváření, udržování i mazání skupinových tajných klíčů je totožný s principy uvedenými pro tajné symetrické klíče. Na rozdíl od osobních tajných a soukromých klíčů může skupinové tajné klíče vytvářet a udržovat pouze některý z administrátorů. Přiřazovat skupinové tajné klíče uživatelům může pouze administrátor, který klíč vygeneroval. Samotné přidělení klíče se provádí pomocí technologie drag-and-drop – tj. uchopíme vytvořený skupinový tajný klíč v pravé části okna a ukážeme jím na uživatele, kteří jej mají sdílet. Je–li uživatel vlastníkem označeného klíče, objeví se u jeho jména červená tečka. Přegenerovat skupinový klíč smí kterýkoliv administrátor, který klíč vlastní (vytvořil jej).



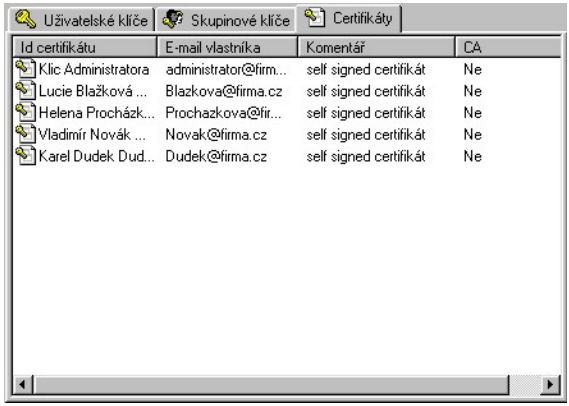
Obr. 74. IW Key Manager - záložka Skupinové klíče

Klíč je možné uživateli odejmout pomocí volby *Odebrat klíč uživateli* z kontextového nebo hlavního menu.

Po odejmutí klíče některému z uživatelů se doporučuje tento klíč přegenerovat.

- **Záložka Certifikáty**

Tato záložka nabízí uživatelům přehledný seznam všech certifikátů existujících v databázi.



Obr. 75. IW KeyManager – záložka Certifikáty

Vytváření certifikátů se provádí na záložce *Uživatelské klíče* vždy k příslušnému klíči. Certifikát může být vygenerován současně s klíčem, ale může být také vygenerován později. Vytváření certifikátů se podrobně zmiňuje v kapitole **Založení soukromého klíče** v části o **Žádosti o certifikát**.

Tato záložka umožňuje pouze správu již vytvořených certifikátů. Pokud si administrátor či auditor přejí zjistit klíč, ke kterému určitý certifikát patří, stačí označit certifikát a u ikony klíče se objeví červená tečka.

Pokud si uživatel přeje, aby v certifikátu bylo uvedeno více jeho e-mailových adres, stačí aby si pomocí kontextového menu nebo menu *Certifikáty* zobrazil *Vlastnosti*. Na záložce *E-mail* lze přidat či odebrat dvě adresy. Další dvě adresy, které se zadávají při generování certifikátu nelze nijak modifikovat.

Certifikáty je možné do PKI také importovat podobně jako klíče. Oproti klíčům ale certifikát náleží i po importu původnímu majiteli a nikoliv uživateli, který jej importoval. Certifikáty certifikační autority smí importovat pouze administrátor. Uživatel může importovat tzv. sebou podepsané certifikáty a certifikáty ověřené (podepsané) certifikační autoritou. Pro import takového certifikátu je ale nutné, aby v PKI byl nejdříve certifikát certifikační autority, podle něhož by bylo možné podpis u importovaného certifikátu ověřit. Pokud v PKI certifikát příslušné certifikační autority není, nebude uživateli import podepsaného certifikátu povolen. Nejdříve musí požádat administrátora, aby naimportoval certifikát příslušné certifikační autority.

Certifikáty je možné také odstraňovat. Odstranění certifikátu je možné provést po označení příslušného certifikátu klávesou *<Delete>*, z kontextového menu nebo z menu *Certifikáty*. Certifikáty certifikační autority smí mazat pouze aministrátoři.

Certifikáty a klíče je možné také exportovat do souborů a importovat z jiných PKI. Export se provádí z menu *Certifikáty* volbou *Export certifikátu* a probíhá podle standardu PKCS#12.

Ke každému certifikátu může být také vytvořena žádost o odvolání certifikátu. To je možné provést z menu *Certifikáty volbou Generovat revokační žádost* nebo z kontextového menu.

K operacím s certifikáty patří také import revokačního listu, což je seznam odvolaných certifikátů. Import je umožněn přes menu *Certifikáty* volbou *Import seznamu revokací*.

- **Stavový řádek**

Stavový řádek zobrazuje přihlašovací jméno aktuálně přihlášeného uživatele IW KeyManageru, který nemusí být shodný s uživatelem aktuálně přihlášeným do systému IW Security Suite, a stav modulu IW KeyManageru.

Obr. 76. IW KeyManager - stavový řádek

• Operace prováděné uživatelem a potřebné priority

V této kapitole je seznam operací IW KeyManageru s uvedením potřebných oprávnění uživatele k provádění těchto funkcí.

Změna hesla privilegovaného uživatele, změna seznamu privilegovaných uživatelů

Operaci může spustit jen administrátor v součinnosti alespoň se dvěma privilegovanými uživateli. Zobrazí se dialog s poli pro zadání starého hesla, dvakrát nového hesla privilegovaného uživatele (pro kontrolu správnosti zadání) a komentáře. Pole pro zadání komentáře bude vyplněno dosavadním komentářem. Pokud uživatel zadá špatné staré heslo (tj. jeho hash se nebude shodovat s hashem hesla jednoho z privilegovaných uživatelů) nebo se nebudou nová hesla shodovat, vypíše se chyba. Po ověření hesel se změny zapíší do příslušné tabulky. Tato operace je dostupná z hlavního menu.

Změna PKI serveru

Tuto akci může spustit kterýkoli uživatel. Po zvolení má uživatel možnost zadat jiný server, jehož PKI chce spravovat nebo lokální PKI. Objeví se dialog se seznamem, ve kterém bude výchozí server a všechny známé (sekundární) servery. Dále uživatel zadá jméno a heslo pro připojení k tomuto serveru. Pokud se přihlásí některý z administrátorů, v případě úspěšného připojení serveru se načtou všechny účty uživatelů, všechny klíče a certifikáty. Běžnému uživateli se zobrazí pouze jeho účet, klíče které vlastní a všechny certifikáty. V případě neúspěchu se zobrazí chybové hlášení. Tato operace je dostupná z hlavního menu.

Přidání uživatele

Volbu smí provést administrátor a auditor. Zobrazí se dialog pro přidání uživatele, který v případě auditora umožňuje vytvoření pouze dalšího auditora. Administrátorovi nabízí možnost vytvoření běžného uživatele či dalšího administrátora. Po zadání všech údajů a stisknutí tlačítka *„OK“* se vygeneruje sada implicitních klíčů systému pro uživatele. Pole pro zadání jména a hesla jsou filtrována tak, aby povolila uživateli zadat jen povolené znaky (ASCII 32-126). Tato akce je dostupná z hlavního menu nebo kontextového menu, které se objeví po kliknutí pravým tlačítkem myši na seznam uživatelů, nebo pomocí ikony  z panelu nástrojů.

Zrušení uživatele včetně jeho klíčů

Pokud se jedná o účet administrátora nebo uživatele, smí akci provést pouze administrátor. V případě účtu auditora jen auditor. Systém si vyžádá potvrzení akce a poté je záznam o uživateli a všechny jeho klíče vymazány

z databáze. Po úspěšném zrušení uživatele a jeho klíčů je uživatel zrušen také ze seznamu uživatelů.

Tato akce je dostupná buď z hlavního menu, nebo kontextového menu, které se objeví po kliknutí pravým tlačítkem na seznamu uživatelů, či pomocí ikony  z panelu nástrojů.

Změna hesla uživatele

Volbu je dovoleno aplikovat pouze na své vlastní heslo, s tímto omezením je přístupná každému uživateli. Akce je dostupná volbou *Vlastnosti uživatele* z hlavního menu, nebo přes kontextové menu, které se objeví po kliknutí pravého tlačítka myši v seznamu uživatelů.

Změna vlastností uživatele

Tato akce je dostupná administrátorovi, auditorovi či majiteli účtu. Po jejím vyvolání se zobrazí dialog stejný jako pro přidání uživatele. Pole pro zadání jména uživatele je však nepřístupné a nemůže být změněno. Po stisknutí tlačítka „*OK*" není přidán uživatel, ale pouze jsou modifikovány údaje v jeho záznamu v databázi. Tato akce je dostupná buďto pomocí hlavního menu nebo z kontextového menu, které se objeví po kliknutí pravým tlačítkem myši na seznamu uživatelů.

Zrušení tajného klíče

Akci smí provést pouze vlastník příslušného klíče. Po jejím zvolení a potvrzení se zruší tajný symetrický klíč, který je v seznamu klíčů označen. Spolu s klíčem se zruší i jeho historie. Poté je klíč vymazán také ze seznamu klíčů. Tato akce je dostupná buď pomocí hlavního menu nebo z kontextového menu.

Vygenerování nového tajného symetrického klíče

Volba je povolena každému uživateli, může ale vytvářet jen vlastní klíče, nikoli klíče jinému uživateli. Vygeneruje se nový symetrický klíč. Jako vlastník bude označen uživatel, který bude aktuálně přihlášen. Poté se přidá klíč do databáze a obnoví se všechny související seznamy klíčů a uživatelů. Tato akce je dostupná buďto pomocí hlavního menu nebo z kontextového menu.

Přegenerování tajného symetrického klíče

Tuto akci je povoleno aplikovat každému uživateli, ale pouze na vlastní klíče. Vygeneruje se nový klíč. Pole pro zadání jména klíče bude předem vyplněno jménem klíče (toho, který bude označen v seznamu klíčů) a bude nedostupné, tzn. jméno klíče a vlastníka se vezme ze starého klíče. Po vygenerování klíče bude starý klíč zařazen do historie a na jeho místo bude

vložen klíč nový. Akce je dostupná buď pomocí hlavního menu nebo z kontextového menu.

Vygenerování skupinového tajného klíče

Volba je dostupná pouze administrátorovi. Vygeneruje se nový klíč. Jako vlastník bude označen administrátor, který jej vygeneroval. Poté se klíč přidá do databáze a obnoví se všechny seznamy klíčů a uživatelů. Tato akce je dostupná buď pomocí hlavního menu nebo z kontextového menu.

Přegenerování skupinového tajného klíče

Akce je dostupná pouze administrátorovi, který klíč vlastní (vytvořil jej). Vytvoří se nový klíč. Pole pro zadání jména klíče je předem vyplněno jménem klíče označeného v seznamu klíčů, a toto pole je pro editaci nedostupné. Načtou se všechny klíče z tabulky sdílených klíčů s tímto jménem. Tyto klíče budou vloženy do historie a místo nich bude vložen nový klíč, jména vlastníků zůstanou zachována. Tato akce je dostupná buď pomocí hlavního menu nebo z kontextového menu.

Zrušení skupinového tajného klíče

Tato akce je dostupná pouze administrátorovi, který příslušný skupinový tajný klíč vlastní (vytvořil jej). Zruší se vybraný skupinový tajný klíč včetně historie. Poté je klíč vymazán ze všech seznamů klíčů a uživatelů. Tato akce je dostupná buď pomocí hlavního menu nebo z kontextového menu.

Přidání skupinového tajného klíče novému uživateli

Volbu může provést pouze administrátor, který vytvořil příslušný skupinový tajný klíč, pomocí funkce drag-and-drop. Přidržením tlačítka myši na vybraném skupinovém klíči a jeho přetažením na zvoleného uživatele dojde k jeho přidání.

Odebrat skupinový tajný klíč uživateli

Akce je dostupná pouze administrátorovi, který vytvořil příslušný skupinový tajný klíč. Kliknutím na zvolený skupinový klíč pravým tlačítkem myši či z hlavního menu se vyvolá položka *Odebrat klíč uživateli*. Po stisknutí tlačítka *„OK“* se vymaže záznam klíče ze záznamu uživatele.

Importovat certifikát CA

Tuto akci smí vyvolat pouze administrátor. Objeví se dialogové okno pro výběr jména souboru, ze kterého chce certifikát importovat. Tato akce je dostupná z hlavního menu nebo kontextového menu v záložce Certifikáty.

Importovat certifikát

Tato akce je dostupná každému uživateli. Objeví se dialogové okno, ve kterém uživatel vybere soubor, ze kterého chce certifikát importovat. Tato akce je dostupná z hlavního menu nebo kontextového menu v záložce Certifikáty.

Vygenerovat veřejný klíč a žádost o certifikát

Akce je dostupná všem uživatelům. Po zvolení této akce je uživatel vyzván k zadání názvu klíče, typu klíče a algoritmu, který bude používán k zašifrování a k odšifrováni. Při generování je nutné psát na klávesnici nebo klikat či pohybovat myší k vytvoření dostatečného počtu náhodných sekvencí. Po vygenerování klíče může uživatel zvolit, zda chce certifikát podepsat sám (málo důvěryhodné), exportovat do souboru či poslat Certifikační autoritě k podepsání. Je nutné vyplnit formulář žádosti o certifikát, který obsahuje osobní údaje uživatele a případně údaje firmy, kde je zaměstnán. Tato akce je dostupná buď z hlavního menu nebo z kontextového menu.

Přegenerování soukromého asymetrického klíče

Tuto akci je povoleno aplikovat každému uživateli, avšak pouze na vlastní klíče. Vygeneruje se nový klíč. Pole pro zadání jména klíče bude předem vyplněno jménem klíče (označeného v seznamu klíčů) a bude nedostupné, tj. jméno klíče a vlastníka se vezme ze starého klíče. Po vygenerování klíče bude starý klíč zařazen do historie a na jeho místo bude vložen klíč nový. Akce je dostupná buď pomocí hlavního menu nebo z kontextového menu.

Při zasílání klíčů a certifikátů je rozdíl mezi notací MS Exchange (MS Mail), kde se zadává jen uživatelské jméno a automaticky se doplní adresa serveru, na kterém tento uživatel pracuje, a notací Internet Mail, kde je třeba zadat celou e-mailovou adresu včetně adresy poštovního serveru.

Zrušit certifikát

Svůj certifikát smí zrušit každý uživatel, certifikát CA smí zrušit pouze administrátor. Po zvolení této akce se z tabulky certifikátů zruší certifikát vybraný v seznamu certifikátů. Pokud je vybraný certifikát certifikátem CA a uživatel není administrátor, pak je tato funkce nedostupná.

Exportovat certifikát

Tuto akci může provést libovolný uživatel. Objeví je dialogové okno, kde zadá jméno souboru, do kterého chce certifikát uložit. Tato akce je dostupná z hlavního menu nebo kontextového menu v záložce *Certifikáty*.

Obnovit heslo

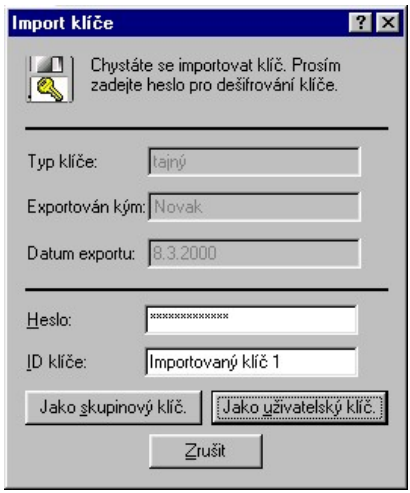
Volba je dostupná pomocí *IW ConfigManageru* pro všechny uživatele ve spolupráci s privilegovanými uživateli. Po zvolení této akce se zobrazí dialogové okno pro zadání hesel dvou ze tří privilegovaných uživatelů a požadovaného uživatelského jména. Pokud budou obě hesla správně zadána, objeví se okno, ve kterém bude vypsáno heslo požadovaného uživatele.

Exportovat klíč nebo sadu klíčů v zašifrované podobě

Akce je dostupná pouze vlastníkovi klíče. Po zvolení této akce bude zobrazeno dialogové okno, ve kterém bude pole pro zadání hesla pro zašifrování výsledného souboru (povolují se jen znaky 32-126 ASCII). Po zadání hesla se objeví dialogové okno, kde uživatel zadá jméno souboru, do kterého chce klíč exportovat. Poté se klíč zašifruje a uloží do tohoto souboru. Tato akce je dostupná z hlavního menu nebo kontextového menu v záložce *Klíče uživatele* či *Klíče skupiny*.

Importovat klíč nebo sadu klíčů v zašifrované podobě

Volba je povolena každému uživateli. Po zvolení této akce se objeví dialogové okno, ve kterém uživatel vybere soubor, ze kterého chce klíč (sadu klíčů) importovat. Poté se zobrazí okno s polem pro zadání hesla pro odšifrování klíče (povolují se jen znaky 32-126 ASCII) a polem pro zadání a ID nového klíče. V případě tajného symetrického klíče je nutno určit, zda půjde o uživatelský nebo skupinový klíč. Importovat skupinový tajný klíč smí ale pouze administrátor, pro běžného uživatele je volba importovat klíč jako skupinový, nedostupná. Po odšifrování se klíč (sada klíčů) importuje s tím, že vlastníkem importovaných klíčů se stane příjemce těchto klíčů. Tato akce je dostupná z hlavního menu nebo kontextového menu v záložce *Klíče uživatele* nebo *Klíče skupiny*.



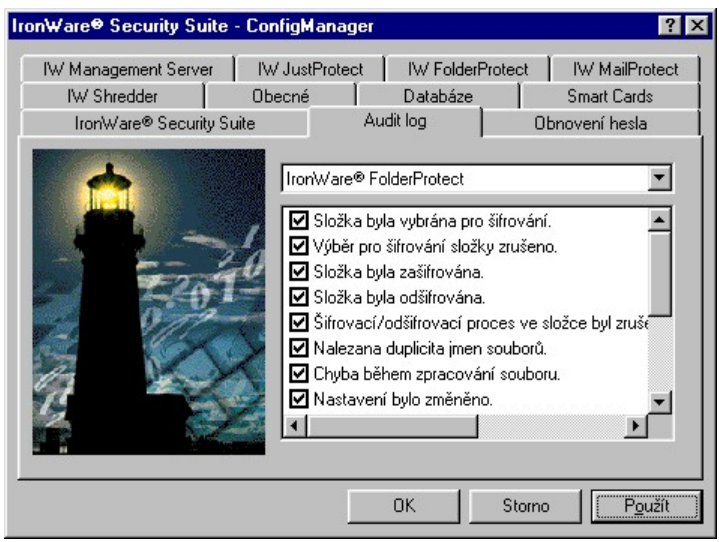
Obr. 77. IW KeyManager - import klíče

• IronWare® AuditLog

IW AuditLog slouží k zaznamenávání činnosti systému IronWare®. Pro zobrazení záznamů *IW AuditLogu* slouží *IW LogViewer*. *IW LogViewer* může spustit kterýkoliv auditor, administrátor i uživatel, ale vymazávat zaznamenané události v IW AuditLogu smí pouze auditoři, ostatní mají možnost záznamy pouze prohlížet.

• Nastavení IW AuditLogu

Nastavení *IW AuditLogu* se provádí v *IW ConfigManageru* v záložce *AuditLog*. K této záložce mají přístup pouze auditoři, na nichž záleží, které události v systému se mají zaznamenávat.



Obr. 78. Audit Log - záložka AuditLog v IW ConfigManageru

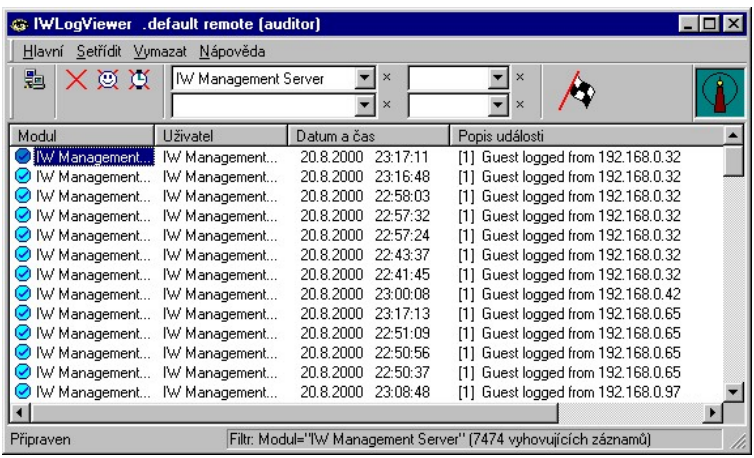
Pomocí výběrového seznamu v horní části záložky může auditor vybírat jednotlivé části IronWare® Security Suite a u nich pak navolit seznam událostí, které se mají zaznamenávat.

• IW LogViewer

IW LogViewer slouží k editaci *AuditLogu*. Umožňuje snadnou orientaci v záznamech *AuditLogu* pro všechny uživatele a zároveň umožňuje auditorům tyto záznamy spravovat.

Při každém přihlášení k IW Management Serveru se provádí mirror (kopírování) serverové databáze na lokální počítač. Pro všechny účty uživatelů zkopírovaných z IW Management Serveru se do Audit Logu vloží záznam o zaktualizování dat uživatelů. V

.



Obr. 79. IW LogViewer – hlavní okno – výpis záznamů

Menu a nástrojová lišta

IW LogViewer je možné ovládat z menu a nástrojové lišty, kde jsou soustředěny funkce pro práci se seznamem zaznamenávaných událostí v systému IronWare® Security Suite. Nástrojová lišta je pomůcka pro rychlé vyvolání nejběžněji používaných akcí.

Obr. 80. IW LogViewer - nástrojová lišta

Menu	Podmenu		Popis
Hlavní	Spusť/zastav načítání		Provede načtení seznamu událostí podle nastavení filtrů.
	Změň PKI server		Umožní přihlášení k jinému PKI. Uzavře komunikaci s právě otevřeným serverem a nechá uživatele přihlásit k jinému.
	Konec		Ukončí práci s IW LogViewerem.
Setřídit	Podle modulu		Seřadí záznamy o událostech, které se staly v systému IronWare® Security Suite, v IW LogVieweru podle modulu, ve kterém nastaly.
	Podle uživatele		Seřadí záznamy o událostech, které se staly v systému IronWare® Security Suite, v IW LogVieweru podle uživatele, který je vyvolal.
	Podle času		Seřadí záznamy o událostech, které se staly v systému IronWare® Security Suite, v IW LogVieweru podle času, kdy k nim došlo.
	Podle popisu		Seřadí záznamy o událostech, které se staly v systému IronWare® Security Suite, v IW LogVieweru podle typu události (přidání klíče, přihlášení uživatele apod.).
Vymazat	Vybraná(é) událost(i)		Pomocí této volby může auditor vymazat záznamy o přesně vybraných událostech.
	Vše od vybraného uživatele		Touto volbou vymaže auditor všechny záznamy, které se týkají událostí vyvolaných určitým uživatelem.
	Vybrané události a starší		Umožňuje auditorovi smazat veškeré záznamy starší, než jím zvolený záznam.
Nápověda	O aplikaci IW LogViewer…		Vyvolá okno s informacemi o IW LogVieweru.

Kromě nástrojů spojených s položkami menu obsahuje panel nástrojů ještě filtry, které umožňují zobrazení jen určitých dat a umožňují tím maximálně snadnou a přehlednou práci s IW LogViewerem.

Pomocí levého horního filtru je možné zobrazovat události jednotlivých modulů. Po kliknutí na šipku se zobrazí seznam modulů, z něhož může uživatel zvolit, který modul jej zajímá. Přeje – li si uživatel filtr naopak vynulovat, stačí kliknout na křížek vedle šipky.

Levý dolní filtr umožní zobrazit události, které vyvolal určitý uživatel. Po kliknutí na šipku se rozbalí seznam uživatelů, ze kterého je možné volit. Přeje – li si uživatel filtr naopak vynulovat, stačí kliknout na křížek vedle šipky.

V pravém horním filtru je možné určit datum nejstaršího zobrazeného záznamu. Po kliknutí na šipku se zobrazí kalendář, pomocí kterého je možné zvolit datum. Přeje – li si uživatel filtr naopak vynulovat, stačí kliknout na křížek vedle šipky.

Při použití současně s předchozím filtrem je možné nastavit časový interval, v němž došlo k událostem, které se mají zobrazit. Samostatně tento filtr umožňuje zvolit datum nejnovějšího zobrazovaného záznamu. Toto datum je možné vložit z klávesnice, nebo z kalendáře, který se zobrazí po kliknutí na šipku. Přeje – li si uživatel filtr naopak vynulovat, stačí kliknout na křížek vedle šipky.

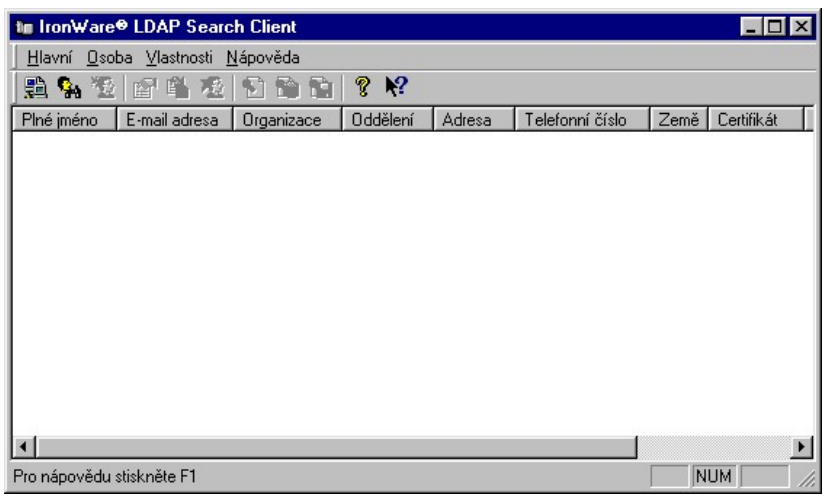
Aby byla práce s IW LogViewerem urychlena, startuje se prázdný. Teprve po stisku tlačítka „*Start nahrávání“* nebo po zadání tohoto příkazu z menu *Zobrazit* se provede načtení záznamů. Zda se log soubor načte celý nebo jen některé jeho položky pak záleží na nastavení filtrů.

Načítání záznamů je možné kdykoliv přerušit stisknutím tlačítka „*Zastavit nahrávání“*. Pokud uživatel načítání přeruší, zobrazí se mu jen ta část logu, která byla načtena před stiskem tlačítka.

• IronWare® LDAP Search Client

IW LDAP Search Client je jedinou volitelnou částí C-PKI. Instaluje se jako součást IronWare® Security Suite – Client. Slouží k získávání informací o uživatelích a jejich certifikátech, jejich zobrazení, uložení do souboru, případně import do PKI. Dovoluje vyhledávání podle různých kritérií. Administrátorům LDAP serverů umožňuje také modifikaci záznamů na serveru, přidávání nových záznamů či mazání existujících.

Program je možné spustit prostřednictvím zástupce *IronWare® LDAP Search Client* v programové skupině *IronWare Security Suite,* nebo prostřednictvím ikony programu *IW Tray* v panelů úloh.



Obr. 81. IW LDAP Search Client – hlavní okno

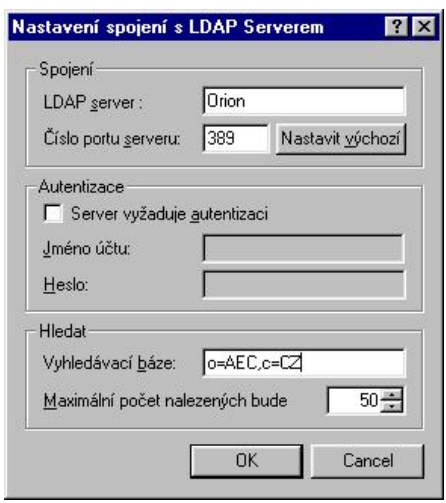
Popis menu programu

Hlavní	*Hledat osobu*	Vyhledání informací o osobě podle zadaných kritérií.
	Nová osoba	Vloží nový záznam do databáze LDAP Serveru.
	Konec	Ukončí program IW LDAP Serch Client.
Osoba	*Vlastnosti*	Zobrazení podrobných informací aktuálního záznamu.
	Modifikovat	Změna informací v databázi (podle oprávnění uživatele) aktuálního záznamu.

	Smazat	Zrušení vybraného záznamu z databáze LDAP Serveru.
	Zobrazit certifikát	Zobrazení certifikátu aktuálně vybraného uživatele.
	Importovat certifikát	Import certifikátu.
	Uložit certifikát	Uložení certifikátu aktuálně vybraného uživatele do souboru.
Vlastnosti	*Nastavení spojení*	Nastavení parametrů spojení s LDAP Serverem.
	Zobrazit	Možnost zobrazení/skrytí panelu nástrojů a stavového řádku.
Nápověda	*Body nápovědy*	Zobrazení témat nápovědy.
	O aplikaci…	Informace o programu.

Volba připojení k LDAP Serveru

Nejprve je nutné nastavit vlastnosti připojení ke zvolenému LDAP Serveru. Dialogové okno *Nastavení spojení s LDAP Serverem* s tímto nastavením je možné vyvolat volbou *Nastavení spojení* v menu *Vlastnosti*, a nebo přímo stiskem klávesové kombinace *Alt+C* či tlačítkem v nástrojové liště.

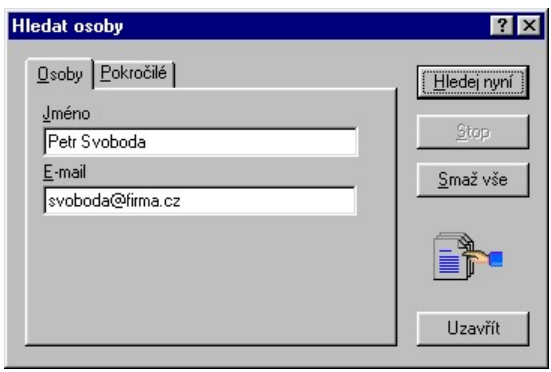


Obr. 82. IW LDAP Search Client - nastavení spojení s LDAP Serverem

Ve skupině *Spojení* je nezbytné nastavit jméno LDAP Serveru, ke kterému se má IW LDAP Search Client připojit, a nebo přímo jeho IP adresu (položka *LDAP server*). V políčku *Číslo portu serveru* pak číslo portu pro připojení ke zvolenému serveru. Tlačítko „*Nastavit výchozí"* provede nastavení výchozí hodnotu čísla portu. Jestliže server vyžaduje autentizaci, pak je třeba vyplnit i políčka *Jméno účtu* a *Heslo*.
Ve skupině *Hledat* je možné v políčku *Vyhledávací báze* změnit databázi, ve které se má vyhledávání provést a v políčku *Maximální počet nalezených bude* lze nastavit maximální počet nalezených záznamů, které budou serverem vráceny.

Jak vyhledávat informace…

Prvním krokem je zadání vyhledávacích parametrů. To lze provést výběrem položky *Hledat osobu* v menu *Hlavní*, tlačítkem v nástrojové liště, nebo stiskem klávesové kombinace *Ctrl+F*. Zobrazí se dialogové okno *Hledat osoby*, které obsahuje dvě záložky. V záložce *Osoby* je políčko *Jméno* pro zadání jména hledané osoby, a políčko *E-mail* pro hledání podle elektronické adresy. Vyhledávání pak probíhá tak, že server vyhledává ve své databázi všechny položky, které začínají zadaným textem.
Druhým způsobem je rozšířené vyhledávání podle zvolených kritérií, které bude použito zvolíte-li záložku *Pokročilé*. Vlastní vyhledávací proces se spustí po stisku tlačítka *Hledej nyní*.



Obr. 83. IW LDAP Search Client - nastavení vyhledávacích kritérií

Obr. 84. IW LDAP Search Client – pokročilé vyhledávání

V průběhu vyhledávání program postupně do hlavního okna vypisuje nalezené záznamy. Po uzavření vyhledávacího dialogového okna lze záznamy prohlížet a v případě odpovídajících administrátorských práv i editovat, mazat a přidávat nové záznamy.

LDAP jednoznačné jméno – jedinečný klíč pro záznam v databázi. Informace o nalezeném uživateli.

• IronWare® Tray

IW Tray je modul, který slouží k rychlému spouštění nainstalovaných modulů IronWare® Security Suite, k šifrování a podepisování ve schránce Windows a v aktuálním okně. Program se spouští automaticky při startu Windows a minimalizuje se do pravé části hlavního panelu, kde zobrazí svoji ikonu.

Obr. 85. IW Tray - zobrazení ikony programu v hlavním panelu

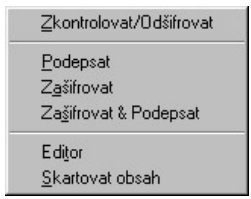
Kliknutím myši na ikonu IW Tray se zobrazí hlavní nabídka programu. V této nabídce se zobrazují odkazy na instalované moduly IronWare® Security Suite, nápovědu, operace s IronWare® MailProtectem a ukončení. Skutečný počet a význam odkazů na moduly IronWare® závisí na druhu vaší instalace. Ostatní položky v nabídce jsou na druhu instalace nezávislé a nemění se.

Obr. 86. IW Tray - příklad nabídky programu

- **Nabídka programu**

IW Clipboard

IW Clipboard slouží k šifrování, dešifrování, podepisování a editaci textu ve schránce Windows. Po použití je možno obsah schránky bezpečně skartovat.



Obr. 87. IW Tray - nabídka IW Clipboard

Zkontrolovat/Odšifrovat – tato volba zkontroluje digitální podpis textu ve schránce a zda je text zašifrovaný. Pokud je tento text zašifrovaný, provede jeho dešifrování. Dešifrovaný text se uloží zpět do schránky, kde je připraven k dalšímu použití. Pokud je text pouze podepsán, z textu odstraní digitální podpis a uloží ho zpět do schránky.

Podepsat – podepíše digitálním podpisem text uložený ve schránce a uloží ho do schránky. Je-li už text podepsaný a chcete jej znovu podepsat, přidá se nový digitální podpis k prvnímu podpisu. Při kontrole podpisu pak mají oba podpisy stejnou váhu a jsou zobrazeny současně. Jestliže je tento text navíc ještě zašifrovaný, a chcete jej znovu podepsat, potom mají digitální podpisy jinou úroveň.

Zašifrovat – zašifruje text ve schránce a uloží ho zpět zašifrovaný. Šifrování probíhá pomocí funkcí IW MailProtectu. Nastavení voleb pro šifrování se provádí prostřednictvím modulu IW ConfigManager. Možnost výběru certifikátů příjemců je nabídnuta po zvolení této nabídky. Následně se pak zašifruje text schránky Windows certifikátem toho pro koho je text určen. Ten si pak může text dešifrovat svým privátním klíčem.

Zašifrovat & Podepsat – zašifruje text schránky a zašifrovanou zprávu podepíše digitálním podpisem a výsledek uloží zpět do schránky. Slučuje dvě funkce IW Clipboardu a to funkci *Zašifrovat* a funkci *Podepsat*.

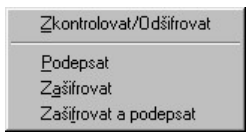
Editor – umožňuje editaci schránky Windows. Po zvolení nabídky se zobrazí editační okno, s textem schránky. Text se dá editovat jako v jednoduchém textovém editoru. Tlačítko *„Obnovit obsah“* v editoru slouží

k aktualizaci obsahu schránky. Schránka Windows se aktualizuje textem, který se zrovna nachází v okně editoru.

Skartovat obsah – tato volba bezpečně vymaže (skartuje) obsah schránky Windows. Schránka je vymazána až po potvrzení volby.

Aktuální okno

Nabídka *„Aktuální okno“* slouží k operacím s aktuálním oknem, ve kterém lze editovat text. Umožňuje text šifrovat, dešifrovat a podepisovat.



Obr. 88. IW Tray - nabídka Aktuální okno

Zkontrolovat/Odšifrovat – tato volba zkontroluje digitální podpis textu v aktuálním okně, a zda je tento text zašifrovaný. Pokud je tento text zašifrovaný, provede jeho dešifrování. Dešifrovaný text se uloží zpět do aktuálního okna, kde je připravený k dalšímu použití. Pokud je text pouze podepsán, pak z textu odstraní digitální podpis a uloží ho zpět do aktuálního okna.

Podepsat - podepíše digitálním podpisem text uložený v aktuálním okně a uloží ho do zpět do aktuálního okna. Je-li už text podepsaný a chcete jej znovu podepsat, přidá se nový digitální podpis k prvnímu podpisu. Při kontrole podpisu pak mají oba digitální podpisy stejnou váhu a jsou zobrazeny současně. Jestliže je tento text navíc ještě zašifrovaný, a chcete jej znovu podepsat, potom mají digitální podpisy jinou úroveň.

Zašifrovat – zašifruje textový obsah aktuálního okna a uloží ho zpět zašifrovaný. Šifrování probíhá pomocí funkcí IW MailProtectu. Nastavení šifrování se provádí prostřednictvím modulu IW ConfigManager. Možnost výběru certifikátů příjemců je nabídnuta po zvolení této nabídky. Následně se pak zašifruje text aktuálního okna certifikátem toho pro koho je text určen. Ten si pak může text dešifrovat svým privátním klíčem.

Zašifrovat & Podepsat - zašifruje text aktuálního okna a zašifrovanou zprávu podepíše digitálním podpisem a výsledek uloží zpět do aktuálního okna pro další použití. Slučuje dvě funkce a to funkci *Zašifrovat* a funkci *Podepsat*.

Nápověda

Tato volba spustí nápovědu programu IronWare® Tray , kde jsou k dispozici informace o programu IW Tray. V nápovědě jsou i nejčastější dotazy uživatelů a odpovědi na ně (FAQ).

Konec

Program IW Tray se touto volbou po vašem souhlasu ukončí.

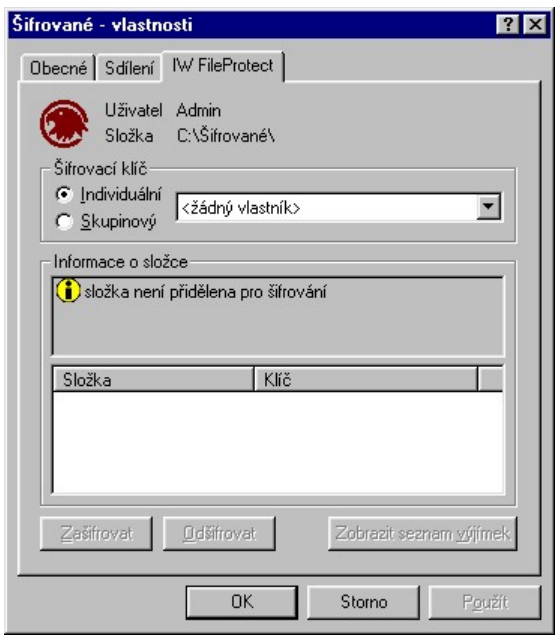
Kontextová nabídka

Program IW Tray umožňuje v kontextové nabídce (na kliknutí pravým tlačítkem myši na soubor) podepsat, zašifrovat, ověřit podpis a dešifrovat libovolný soubor. Umožňuje též oddělený podpis (clear sign) i mnohonásobný podpis.

IronWare® Security Suite Protection

• IW FileProtect - On-line šifrování

Po instalaci modulu IW FileProtect jej uživatelé najdou jako stejnojmennou záložku ve Vlastnostech jakékoliv složky na pevném disku, síťovém disku či výměnném médiu. Zde je možné přidělit tuto složku k šifrování IW FileProtectem výběrem šifrovacího klíče, a tuto složku včetně jejích podsložek zašifrovat. Data mohou být šifrována jak pro jednotlivé uživatele, tak pro skupiny uživatelů, kteří data mohou sdílet, a přitom je nikdo mimo skupinu nemůže použít. Stav podsložek ve složitějších strukturách složek je nejlépe viditelný v kořenové složce celé struktury.



Obr. 89. IW FileProtect – záložka ve Vlastnostech souboru

V horní části záložky se pod hlavičkou *Uživatel* vždy zobrazí jméno aktuálně přihlášeného uživatele. Položka *Složka* znázorňuje kořen struktury složek, v níž se uživatel v daný okamžik nachází.

Pokud uživatel přepíná mezi záložkou IW FileProtect a jinými programy, data na záložce se při každém návratu k IW FileProtect aktualizují. Objeví se okno *Prohledávám složky,* které znamená, že subsystém prochází danou strukturu složek a zjišťuje, zda v ní byly provedeny nějaké změny.

- Je-li složka přidělena pro šifrování IW FileProtectem, nepoužívejte na její mazání IW Shredder a na šifrování IW JustProtect, protože může dojít ke kolizi. Vždy složku nejprve odšifrujte a odpřidělte IW FileProtectem a až potom použijte IW Shredder či IW JustProtect. Toto omezení se netýká IW JustProtect šifrování do EXE souboru. Při použití IW Shredderu i IW JustProtectu totiž dochází k přejmenování zpracovávaných souborů a to VXD Driver modulu IW FileProtect z bezpečnostních důvodů nedovoluje a proto se operace neprovede a končí s chybou. Chyba nepoškozuje data, ale požadovaná akce nejde provést.
- Nešifrujte složky Windows a složky, kde je nainstalován IronWare® Security Suite a IronWare® Management Server (v případě instalace clienta i IW Management Serveru na jednom počítači).
- V průběhu zašifrovávání či odšifrovávání složky IW FileProtectem a současném provádění jiné akce (mazání souborů, přidávání souborů, skartování IW Shredder), které byly spuštěny až v průběhu šifrování na stejném adresáři, může dojít k nekonzistenci dat. V tomto případě se může stát, že se některé soubory nezobrazí a nebude možné s nimi pracovat. Tuto nekonzistenci lze snadno opravit znovuprovedením šifrovacího procesu.

Záložka IW FileProtect obsahuje následující oddíly:

Šifrovací klíč

V tomto poli je možné zvolit šifrovací klíč pro zašifrování zvolených souborů či složek.

- *Individuální* – obsahuje tajné klíče uživatele, a kromě nich dvě speciální položky:

<žádný vlastník>	Vybraná složka není vybrána k šifrování.
<nešifrovat>	Umožňuje nastavit ochranu proti šifrování. Složku s tímto atributem nelze zašifrovat. Funkce je dostupná pouze pro administrátora.

- *Skupinový* – obsahuje sdílené klíče skupin uživatelů, a kromě nich dvě speciální položky:

<žádný vlastník>	Vybraná složka není vybrána k šifrování.
<nešifrovat>	Umožňuje nastavit ochranu proti šifrování. Složku s tímto atributem nelze zašifrovat. Funkce je dostupná pouze pro administrátora.

Volba *Skupinový* je dostupná pouze administrátorům.

Podrobnosti o šifrovacích klíčích a jejich rozdělení jsou uvedeny v kapitole *IW KeyManager*.

Informace o aktuální složce

V horní části tohoto pole *Informace o složce* se zobrazují informační hlášení a ve spodní části pak upřesňující informace o stavu vybrané složky a jejích podsložek. Mohou se objevit následující hlášení:

Složka není přidělena pro šifrování znamená, že daná složka nebyla žádným uživatelem přidělena pro šifrování.
Složka je přidělena pro šifrování, ale není zašifrovaná signalizuje, že složka byla přidělena pro šifrování, byl zvolen klíč, ale vlastní šifrování ještě neproběhlo. Nebo naopak, že proběhlo odšifrování složky, ale už nebyl odňat šifrovací klíč.
Složka je zašifrovaná značí, že složka byla přidělena pro šifrování, byl zvolen klíč a proběhlo vlastní šifrování tímto klíčem.
Složka se nebude šifrovat v této složce bylo některým z administrátorů zakázáno šifrování.

Složka je zašifrovaná starou verzí klíče došlo k přegenerování (regeneration) šifrovacího klíče a složka je stále zašifrována klíčem původním. Složku je nutné přešifrovat (stačí zadat *Encrypt* a složka se přešifruje aktuální verzí klíče).
Složka není přístupná (šifrování bylo přerušeno) složka není přístupná, zašifrování/odšifrování bylo přerušeno.
Integrita struktury složek porušena některá z podsložek byla přidělena k šifrování jiným klíčem (jiným uživatelem) a později odpřidělena, čímž došlo k nekonzistenci. Složku je nutno odšifrovat a odpřidělit a znovu přidělit a zašifrovat.
Šifrovací ovladač je vypnut na záložce IW FileProtect v IW ConfigManageru byla zatržena volba *Vypnout šifrovací ovladač*, která IW FileProtect deaktivuje.
Toto není vrchol složky přidělené pro šifrování složka byla přidělena pro šifrování v rámci nadřazené složky a není ji tudíž možno přidělit pro šifrování.
Složka není plně zašifrovaná při procesu zašifrování nebo odšifrování došlo k chybě nebo byla operace přerušena volbou *Storno*.

Ve spodním poli je znázorněn stav složek zašifrovaných nebo vybraných programem IW FileProtect k šifrování, klíče kterými byly zašifrovány a jména jejich vlastníků. Znázorněna je nejen rodičovská složka, ale i jakékoliv jednotlivě použité složky v rámci dané cesty.

	Významy ikon složek
	Složka je platně zašifrovaná.
	Složka je platně zašifrovaná – zobrazení z nadřazené složky.
	Složka byla přidělena pro šifrování, ale není zašifrovaná.
	Složka byla přidělena pro šifrování, ale není zašifrovaná - zobrazení z nadřazené složky.
	V průběhu zašifrování nebo odšifrování došlo k chybě, operace byla přerušena.
	V průběhu zašifrování nebo odšifrování došlo k chybě, operace byla přerušena - zobrazení z nadřazené složky.
	Zašifrování nebo odšifrování bylo přerušeno u určité složky. Část souborů je zašifrována, část je odšifrována.

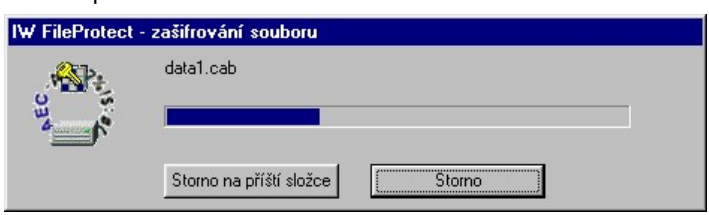
	Zašifrování nebo odšifrování bylo přerušeno u určité složky. Část souborů je zašifrována, část je odšifrována - zobrazení z nadřazené složky.
	Složka je chráněna proti přidělení k šifrování.
	Složka je chráněna proti přidělení k šifrování - zobrazení z nadřazené složky.
	Šifrovací klíč byl přegenerován, složka není zašifrována nově platným klíčem.
	Šifrovací klíč byl přegenerován, složka není zašifrována nově platným klíčem - zobrazení z nadřazené složky.

Vedle každé složky uvedené v informačním poli IW FileProtectu je uveden název klíče, kterým je daná složka zašifrovaná, a vlastník klíče.

	Významy ikon klíčů
	Chráněn proti šifrování.
	Osobní tajný klíč náležející aktuálně přihlášenému uživateli.
	Skupinový tajný klíč, který aktuálně přihlášený uživatel má k dispozici.
	Osobní tajný klíč náležející jinému uživateli.
	Skupinový tajný klíč, který uživatel nevlastní.

Zašifrování složky

Tlačítko „*Zašifrovat*“ umožní zašifrování složky přidělené pro šifrování a všech případných podsložek. V průběhu šifrování se objeví okno se znázorněním průběhu.



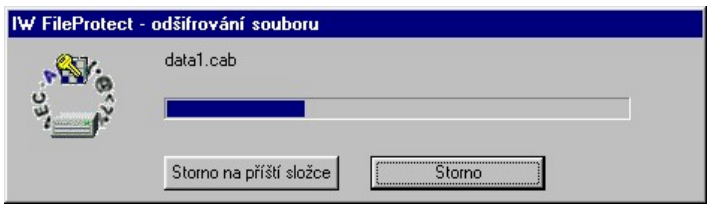
Obr. 90. IW FileProtect – zobrazení procesu šifrování

Storno – okamžitě zruší šifrování

Storno na příští složce – zruší šifrování, jakmile proces dojde k další složce ve struktuře

Odšifrování složky

Tlačítko *Odšifrovat* umožní odšifrování zašifrované složky a případných podsložek. V průběhu odšifrování se objeví okno se znázorněním průběhu:



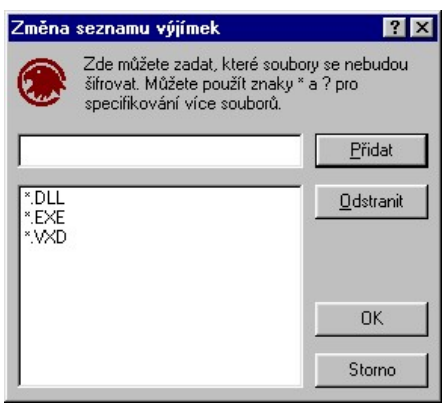
Obr. 91. IW FileProtect – zobrazení procesu odšifrování

Storno – okamžitě zruší šifrování

Storno na příští složce – zruší šifrování, jakmile program dojde k další složce ve struktuře.

Úprava seznamu výjimek

Potřebujete-li nastavit typy souborů, které se z bezpečnostních či jiných důvodů nemají šifrovat (např. EXE, DLL a VXD), pak použijte tlačítko „*Změnit seznam výjimek*“.



Obr. 92. IW FileProtect - vkládání typů souborů vyloučených z šifrování

Přidat – po zadání z řádku přidá typ souboru do seznamu

Odstranit – odstraní označený typ souboru ze seznamu

• Výběr šifrovacích klíčů

• Šifrování složek a souborů osobními tajnými klíči uživatele

Každý uživatel má právo zašifrovat si soubory, které považuje za důvěrné, a které by neměly být přístupné jiným uživatelům. K zašifrování se použije jeho tajný klíč. Takto zašifrovaná data nemůže kromě tohoto autorizovaného uživatele nikdo číst ani modifikovat.

Jak postupovat

V libovolném prohlížeči si zvolte složku, kterou chcete zašifrovat. Klikněte na ni pravým tlačítkem myši a z kontextové nabídky zvolte položku *Vlastnosti*. V zobrazeném okně *Vlastnosti* klikněte na záložku *IW FileProtect*. V poli *Individuální* zvolte jeden ze svých tajných šifrovacích klíčů, případně (máte–li práva administrátora) některý z vámi spravovaných skupinových tajných klíčů. Pokud nemáte práva administrátora, možnost volby ze skupinových tajných klíčů vám není nabídnuta. Program provede přidělení klíče ke složce a v poli *Informace o složce* se objeví informace, že složka je přidělena, ale není zašifrována. Kliknutím na tlačítko *Zašifrovat* dojde k zašifrování dat. Po ukončení šifrování se v poli *Složka / Klíč* objeví příslušná ikona, název složky a úplná cesta a žlutě vyznačený klíč s názvem.

Existuje–li v systému nezašifrovaná složka přidělená k šifrování, jedná se v podstatě o chybový stav. Proto je vhodné a doporučuje se okamžitě po přidělení klíče soubor či složku zašifrovat.

• Šifrování složek a souborů pro skupiny uživatelů

Při práci se sdílenými složkami a klíči je nutné rozlišovat dvě fáze, ve kterých mají rozdílní uživatelé odlišná práva. Přidělovat sdílené složky pro šifrování skupinovým tajným klíčem má právo pouze administrátor, který příslušné klíče spravuje. Zašifrovat je pak může nejen administrátor, ale i kterýkoliv jiný uživatel, který má přidělen daný skupinový tajný klíč. V obou případech je provedené šifrování platné pro celou skupinu. Takto zašifrované sdílené soubory nemá kromě vlastníků daného skupinového tajného klíče možnost nikdo číst ani modifikovat.

Jak přidělit složku k šifrování skupinovým tajným klíčem

Administrátor v libovolném prohlížeči zvolí sdílenou složku, kterou chce zašifrovat. Klikne na ni pravým tlačítkem myši a z kontextového menu zvolí položku *Vlastnosti*. V zobrazeném okně *Vlastnosti* klikne na záložku *IW FileProtect*. V poli *Skupinový* zvolí sdílený šifrovací klíč právě té skupiny uživatelů, pro kterou má být tato složka přístupná. Proběhne přidělení klíče ke složce a v poli *Informace o složce* se objeví informace, že složka je přidělena k šifrování, ale není zašifrována. Kliknutím na tlačítko *Zašifrovat* dojde k zašifrování dat. Po ukončení šifrování se v poli *Složka / Klíč* objeví příslušná ikona, název složky a úplná cesta a žlutě vyznačený klíč s názvem.

Volba šifrovat složku se vztahuje současně i na všechny její podsložky.

- **Šifrování všech složek na disku**

Pokud chcete zašifrovat celou strukturu složek vybraného disku stejným klíčem, je to možné udělat přímo v kořenové složce disku. Při takové operaci se zašifrují veškeré složky a podsložky, které daný disk obsahuje a není třeba šifrovat každou složku zvlášť.

Nedoporučujeme šifrovat složky obsahující programové soubory a soubory nezbytné pro chod operačního systému. Před vlastním šifrováním je důležité rozhodnout, jaká data a z jakých důvodů chcete chránit šifrou. Pokud zvolíte kořen disku C: pro šifrování, IW FileProtect automaticky vyloučí ze šifrování systémové soubory, které kořen tohoto disku běžně obsahuje, a zašifruje pouze jednotlivé složky a jejich podsložky.

Při šifrování IW File Protectem na komprimovaných discích v systému Windows NT může docházet ke kolizím. Proto se šifrování komprimovaných disků nedoporučuje.

- **Přegenerování šifrovacích klíčů**

Pokud je v IW KeyManageru přegenerován šifrovací klíč, ať osobní tajný nebo skupinový tajný, stane se nový (přegenerovaný) klíč ihned aktivním. IW FileProtect vás v takovém případě upozorní, že složka není

zašifrovaná současným platným klíčem. Taková složka je označena a je nutné ji přešifrovat novým klíčem. Stačí pouze kliknout na aktivované tlačítko *Zašifrovat* a program příslušné soubory nebo podsložky v dané složce automaticky přešifruje. Tento proces je pro uživatele transparentní a probíhá tak, že soubory jsou nejprve odšifrovány starým klíčem, a teprve potom zašifrovány pomocí klíče nového. Označení šifrované složky se změní na šedou složku, což signalizuje, že data jsou úspěšně zašifrována.

• Odšifrování osobních složek uživatele

Uživatel se může kdykoliv rozhodnout zbavit svou složku šifrovací ochrany nebo ji zašifrovat klíčem jiným. K odšifrování se použije stejný tajný klíč uživatele, jakým je složka v daném okamžiku zašifrována.

Jak odšifrovat složku zašifrovanou osobním tajným klíčem

V libovolném prohlížeči zvolte složku, kterou chcete odšifrovat. Odšifrování musí být prováděno ze stejného místa struktury složek, odkud bylo provedeno zašifrování, tj. změna musí být prováděna ve složce, ve které se volilo zašifrování, nikoliv v jejích podsložkách. Není možné odšifrovat samostatně soubor, který byl zašifrován v rámci celé složky, v níž se nachází. Klikněte na zvolenou složku pravým tlačítkem myši a z kontextového menu zvolte *Vlastnosti*. V zobrazeném okně *Vlastnosti* klikněte na záložku *IW FileProtect*. V poli *Složka / Klíč* vidíte svoji zašifrovanou složku a klíč, který byl k šifrování použit. Klikněte na tlačítko *Ošifrovat*, které je povelem pro odšifrování dat. Během procesu máte možnost jej přerušit, buď okamžitě nebo u následující složky. Po odšifrování se šedý znak složky změní na červený, a v poli *Informace o složce* se objeví hlášení *Složka je přidělena pro šifrování, ale není zašifrovaná*. Změnou položky ve výběrovém seznamu v poli *Šifrovací klíč / Individuální* ze současného šifrovacího klíče na *<žádný vlastník>* se složka začlení do struktury jako obyčejná složka bez jakýchkoliv modifikací a zmizí z pole *Složka / Klíč.*

Volba odšifrovat složku se vztahuje současně i na všechny její podsložky.

• Zrušení přidělení sdílených složek

Stejně jako přidělit k zašifrování, i zrušit toto přidělení sdílené složky může pouze administrátor, který je správcem skupinových tajných klíčů. Odšifrování se stane automaticky platné i pro ostatní uživatele, kteří používají tento skupinový tajný klíč a mají přístup ke sdílené složce. Na

rozdíl od šifrování, kdy uživatelé náležející do skupiny mají možnost zašifrovat přidělenou složku, možnost odšifrování nespadá mezi jejich práva.

Jak odšifrovat složku zašifrovanou skupinovým tajným klíčem

Administrátor si v libovolném prohlížeči zvolí složku, kterou chce odšifrovat. Odšifrování musí být prováděno ze stejného místa struktury složek, odkud bylo provedeno zašifrování, tj. změna musí být prováděna ve složce, ve které se volilo zašifrování, nikoliv v jejích podsložkách. Není možné odšifrovat samostatně soubor, který byl zašifrován v rámci celé složky, v níž se nachází. Klikněte pravým tlačítkem myši a z kontextového menu zvolte *Vlastnosti*. V zobrazeném okně *Vlastnosti* klikněte na záložku *IW FileProtect*. V poli *Složka / Klíč* vidíte svou zašifrovanou složku a klíč, který byl k šifrování použit. Klikněte na tlačítko *Odšifrovat*, které je povelem pro dešifrování dat. Během procesu máte možnost jej přerušit, buď okamžitě nebo u následující složky. Po odšifrování se šedý znak složky změní na červený, a v poli *Informace o složce* se objeví hlášení *Složka je přidělena k šifrování, ale není zašifrována*. Změňte ve výběrovém seznamu v poli *Šifrovací klíč* současný šifrovací klíč na *<žádný vlastník>*. Složka se tímto začlení do struktury jako obyčejná složka bez jakýchkoliv modifikací, a zmizí z pole *Složka / Klíč.*

Volba odšifrovat složku se vztahuje současně i na všechny její podsložky.

- **Změna šifrovacích klíčů**

Vaše data mohou být zašifrována kterýmkoliv z vašich tajných klíčů, který si zvolíte. Všechny klíče je samozřejmě možné podle potřeby měnit. Záměnu šifrovacích klíčů (na rozdíl od automatické záměny za přegenerovaný klíč) je možné provést pouze v okamžiku, kdy je složka v nezašifrované podobě.

Pokud chcete tedy změnit klíč pro šifrování určité složky, která je v tomto momentě zašifrovaná, je nezbytné data nejprve odšifrovat tlačítkem *Odšifrovat* a odpřidělit (klíč se jménem *<žádný vlastník>*), pak přidělit nový klíč a následně data opět zašifrovat stiskem tlačítka *Zašifrovat*.

• Chování zašifrovaných složek

Přejmenování složek

Pokud dojde k přejmenování zašifrované složky, šifrování dat v této struktuře nebude nijak ovlivněno.

Neautorizovaný uživatel nemá právo přejmenovat zašifrovanou složku, ani vidět zašifrované soubory, které mu nepatří.

Administrátor může přejmenovat všechny zašifrované složky i soubory, a to i soukromé soubory a složky jednotlivých uživatelů.

Viditelnost zašifrovaných dat

Administrátor vidí ve struktuře složek jak jména složek tak i zašifrovaných souborů. Není ovšem schopen číst obsah soukromých souborů jiných uživatelů, protože nevlastní jejich šifrovací klíč.

Uživatel, který nemá práva administrátora a nemá šifrovací klíč ke sdíleným nebo soukromým složkám, má právo vidět pouze strukturu složek zašifrovaných dat. Nevidí však uvnitř žádné soubory, složky se chovají, jako by v nich žádné soubory uloženy nebyly.

• Vkládání, odstraňování a kopírování souborů

Pokud uživatel vloží do zašifrované složky nový soubor, přijme vlastnosti dané složky a automaticky bez zásahu uživatele se zašifruje stejným klíčem. Neautorizovaný uživatel nemá právo vkládat do zašifrované složky nové soubory, v takovém případě mu bude přístup odepřen.

Odstranit soukromé zašifrované složky a soubory má právo pouze jejich vlastník.

Pokud se zašifrovaný soubor či celá složka zkopíruje a vloží do jiné nešifrované struktury složek, šifrovaná data přejímají vlastnosti nové složky a automaticky se odšifrují.

Mazání souborů v zašifrované složce je povoleno vlastníkovi šifrovacího klíče, ale pokud jde opravdu o smazání souboru. Je-li v systému zapnut Koš ve Windows, soubor nebude možno vhodit do koše, protože tak by byla zašifrovaná data odšifrována a prozrazena. Skutečné smazání souboru je povoleno a uživatel obdrží hlášení, že soubor je chráněn proti zápisu.

Přejmenování souborů v zašifrované složce je povoleno pouze vlastníkovi šifrovacího klíče, avšak zašifrovaný soubor není možno přejmenovat na soubor s extenzí, která patří do *seznamu výjimek*.

Stejně tak není možno přejmenovat soubory s extenzí v seznamu vyjímek na jméno souboru s extenzí, která je šifrovaná. Například z *.EXE na *.DOC. Uživatel obdrží hlášení, že soubor je chráněn proti zápisu.

• Označení souborů, které se nemají ve složce zašifrovat

Pokud je uvnitř struktury složek určené k šifrování složka, která se má zachovat v nešifrované podobě, je možné jejímu šifrování zabránit. K tomu je určena funkce *vyřazení ze šifrování.* Právo takto zabránit šifrování souborů má pouze administrátor. Ostatní uživatelé tuto funkci nemají přístupnou.

Jak zakázat šifrování ve složce

Administrátor si v libovolném prohlížeči zvolí kořenovou složku, u které chce zabránit šifrování. Klikne pravým tlačítkem myši a z kontextového menu zvolí *Vlastnosti*. V zobrazeném okně *Vlastnosti* klikne na záložku *IW FileProtect*. Ve výběrovém seznamu v poli *Šifrovací klíč* zvolí možnost <nešifrovat>. V položce *Složka* se objeví ikona složky s modrým R a její cesta, v položce *Klíč* se objeví zpráva, že zvolená složka je *vyřazena ze šifrování*. .

Zákaz šifrování může zrušit pouze osoba, která jej nastavila. Rušení tohoto zákazu se provádí nastavením <*žádný vlastník*> ve výběrovém seznamu v poli *Šifrovací klíč*. Tím se ochrana ze složky odstraní a složka bude dostupná pro šifrování.

• Šifrování na několika úrovních – „obtékání“ složek

Strukturu složek je možné šifrovat na několika úrovních, a kombinovat zde šifrování zadané jednotlivými uživateli i administrátorem.

Pokud je v některých složkách zakázáno šifrování či jsou už šifrované, a zvolí se šifrování nadřazené struktury, data v již přidělených složkách se z nové volby šifrování automaticky vynechají, budou „obtečena“. I v několika úrovňovém šifrování platí, že data jsou dostupná pouze tomu uživateli, který vlastní příslušný šifrovací klíč.

• Systémové požadavky

Proces šifrování probíhá tak, že vybraná data se nejprve zkopírují na nové místo na disku, zašifrují, a pokud šifrování proběhne bez problémů, zkopírovaná data se automaticky odstraní. Pro uživatele je tato operace transparentní. Je implementována z bezpečnostních důvodů, jako zálohový

systém. Při šifrování větších objemů dat musí být proto na disku volné nejméně takové místo, aby jeho velikost odpovídala velikosti největšího souboru určeného k šifrování. Navíc IW FileProtect vyžaduje minimálně 10MB volného místa na disku k jakékoliv své činnosti.

• Záznam o šifrování

Údaje o šifrování každé složky jsou uloženy v souboru *IW Security Descriptor*, který má jméno *IWSECDES.$$$*. V souboru je uvedeno jméno klíče a stav šifrování. Systém se zde rovněž dozví, jestli složka, na kterou se dívá, je rodičovská šifrovaná složka, tj. jestli volba šifrovat byla provedena právě zde a ne v některé podsložce, či v nadřazené složce. Tento soubor je nastaven jako skrytý a lze jej proto číst a editovat pouze v DOSu.

S těmito záznamy je třeba nakládat velice opatrně. Pokud by došlo ke smazání *IW Security Descriptoru*, nebylo by již nikdy možné zašifrovaná data odšifrovat a běžně používat.

• Šifrování výměnných médií

Data je možné chránit nejenom tehdy, pokud jsou uložená na disku, ale také v případě, že jsou vyměňována mezi různými uživateli či přenášena mezi nepropojenými počítači jinou formou, než v rámci sítě. On-line šifrování souborů se dá snadno aplikovat také na výměnná datová média.

Druhy médií vhodných pro šifrování

IW FileProtect umožňuje šifrovat prakticky jakákoliv výměnná média, na kterých se ukládají složky či soubory. Mezi nejběžněji používané patří diskety, ZIP disky, Jazz disky a další.

Postup při šifrování výměnných médií

Zašifrovaná média mohou být určena jak pro vlastní použití dat uživatelem, tak i pro předání osobám, které nevlastní příslušný osobní tajný klíč použitý k zašifrování. Z tohoto důvodu existují rozšířená práva uživatele, který má možnost zašifrovat médium nejenom osobním tajným klíčem, ale i skupinovým tajným klíčem. Druh šifrovacího klíče se potom stanoví podle potřeby.

Menší objemy dat (soubory menší velikosti) je možné přenést na médium a přímo tam zašifrovat tak, jako by byly uložené na disku. U větších objemů dat (velkých souborů) doporučujeme nejprve zašifrovat příslušné médium bez dat, a posléze na něj soubory či složky nakopírovat.

Jak zašifrovat data na výměnném médiu

Vložte do mechaniky výměnné médium, které chcete zašifrovat. V libovolném prohlížeči si najděte kořenovou složku tohoto média, z kontextového menu zvolte *Vlastnosti* a v zobrazeném okně klikněte na záložku *IW FileProtect*. V poli *Šifrovací klíč* zvolte šifrovací klíč, který chcete použít pro šifrování média. Proběhne přidělení klíče ke kořenu média, v poli *Informace o složce* se objeví informace, že složka je přidělena k šifrování, ale není zašifrována. Klikněte na tlačítko *Zašifrovat*, aby došlo k zašifrování média. Po ukončení šifrování se v poli *Složka / Klíč* objeví šedá ikona složky a její cesta, a vedle žlutě vyznačený klíč s názvem. To značí, že operace šifrování proběhla úspěšně. Nyní na takto šifrované médium překopírujte soubory, které chcete chránit a tyto se automaticky zašifrují.

Záznam o zašifrování se přenáší zároveň s médiem. Při šifrování výměnného média se na něj automaticky zapíše i IW Security Descriptor se jménem IWSECDES.$$$. Ten určuje, jakým klíčem je šifrování provedeno. Tento soubor se nesmí smazat! Uložená data by pak nebylo možné odšifrovat a normálně používat.
Bude-li příjemce tohoto média používat pro čtení skupinový tajný klíč v rámci jednoho centrálního PKI, je možno médium přemístit na libovolné místo a do libovolného PC v síti a přilogovat se k PKI s použitím svého jména a hesla. Skupinový tajný klíč bude k dispozici.
Druhá možnost je zašifrovat výměnné médium svým vlastním tajným klíčem. Pak lze toto médium v případě centrálního PKI používat v rámci celé sítě.
Třetí možnost je zašifrovat médium, poslat jej příjemci a současně vyexportovat použitý klíč a také jej (bezpečně) dopravit příjemci. Příjemce pak do svého PKI importuje tento klíč jako osobní (či skupinový) tajný klíč a může zašifrovaná data používat.

- **Konfigurace IW FileProtect**

Jedinou možností nastavení modulu IW FileProtect je vypnutí šifrovacího ovladače. Tuto akci je možné provést v záložce IW FileProtect v IW ConfigManageru. Zaškrtnutím volby *Vypnout šifrovací ovladač* nebudou soubory odšifrovávány ani zašifrovávány. Tato volba slouží především na vytváření archivů v šifrované podobě, tzn. je-li zapnuta tato volba a provedena archivace dat na záložní medium (CD, ZIP, JAZZ...), zůstanou data na tomto médiu šifrovaná i po kopírování. Tato volba je především určena pro vypalování záloh na CD nebo uložení záloh na pásku. Pro jiná výměnná média se doporučuje použít předešlé metody.

V případě použití lokální PKI databáze jsou takto uložená data na záložním médiu čitelná pouze tehdy, nedojde-li k přeinstalování systému IronWare®, nebo pokud se šifrovací klíč, kterým jsou data v archivu šifrována, uloží k pozdějšímu použití pomocí funkce Export.

Obr. 93. IW ConfigManager - záložka IW FileProtect – vypnutí šifrovacího ovladače

• IW FolderProtect - Off-line šifrování

IW FolderProtect je program, který zabezpečuje ochranu dat před neautorizovanými osobami prostřednictvím off-line šifrování dat ve složkách a případně i ve všech jejich podsložkách. Off-line šifrování je funkce, která neprobíhá v reálném čase, nýbrž jednorázově při spuštění nebo vypnutí systému na vašem počítači (případně na vyžádání). Při spuštění počítače se data odšifrují, při vypnutí se naopak zašifrují. Data je samozřejmě možné zašifrovat/odšifrovat ze záložky IW FolderProtect na požádání – automatické šifrování / odšifrování je možné vypnout nebo přerušit.

Modul off-line šifrování s názvem IW FolderProtect umožňuje šifrovat soubory ve vybraných složkách a jejich podsložkách na libovolných lokálních discích. Není možné šifrovat data na vzdálených discích a výměnných médiích. Struktura IW FolderProtect poskytuje podporu více uživatelům, kteří se při startu systému identifikují v IW GINĚ svým přihlašovacím jménem a heslem, přičemž mají různá práva přístupu k jednotlivým složkám a funkcím. Tak může na stejném počítači uchovávat svá tajná data více než jeden uživatel. Data mohou být šifrována pro jednotlivé uživatele stejně dobře jako pro skupiny uživatelů, kteří mohou sdílet tato data, přičemž je nemůže používat nikdo, kdo není členem příslušné skupiny. Po spuštění Windows nebo při přihlášení se jako jiný uživatel se data odšifrují a po dobu běhu systému zůstávají odšifrovaná. Při reloginu nebo ukončení Windows se data aktuálně přihlášeného uživatele zašifrují.

• Konfigurace IW FolderProtectu

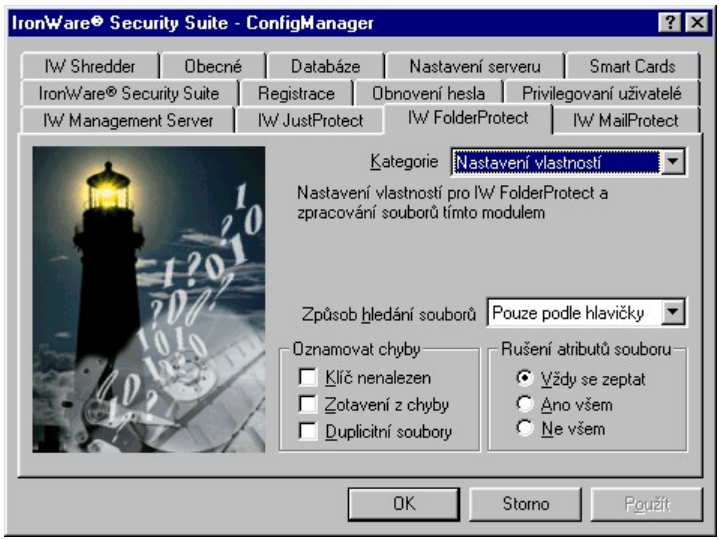
Po instalaci modulu je do skupiny programů IronWare® Security Suite do IW ConfigManageru přidána záložka *IW FolderProtect*. Ta slouží k obecnému nastavení vlastností modulu.

V horní části této záložky je v seznamu *Kategorie* umožněn výběr jedné ze tří položek: *Nastavení vlastností, všechny vybrané složky* a *Soubor s databází.*

Nastavení chování IW FolderProtect

Po výběru kategorie *Nastavení vlastností* je možné provést nastavení chování modulu IW FolderProtect.

Časová prodleva určuje dobu v rozsahu 0-100 sekund, kterou má uživatel k dispozici při startu či vypnutí systému ke zrušení akce *Automaticky zašifrovat*, resp. *Automaticky dešifrovat*. To má samozřejmě význam pouze tehdy, pokud je tato funkce pro danou složku aktivní – viz. záložka *IW FolderProtect - Vlastnosti složky.*



Obr. 94. IW ConfigManager - záložka IW FolderProtect - kategorie Nastavení vlastností

Volba *Způsob hledání souborů* určuje způsob, kterým bude IW FolderProtect při prohledávání složek určovat, zda se v nich vyskytují zašifrované soubory. Způsoby jsou následující:

- *Pouze podle hlavičky*
  Orientuje podle obsahu šifrovaných souborů, které mají speciální formát. Tato metoda je z hlediska vyhledání souborů nejspolehlivější, je však nejpomalejší.
- *Pouze podle přípony*
  Vyhledává soubory prostřednictvím jejich přípony. (IW FolderProtect standardně rozšiřuje název šifrovaných souborů o příponu *.ciphered*, např. *dokument.txt.ciphered*)
- *Podle přípony i hlavičky*
  „Nejpřísnější“ metoda z hlediska označení souboru za šifrovaný, neboť označí soubor jako zašifrovaný pouze v tom případě, že má příponu .ciphered a zároveň i speciální formát.

Použití volby *Pouze podle přípony* je vhodné v případě, že přidělujete k šifrování složky, které obsahují velké množství souborů, jejichž prověření metodou *Pouze podle hlavičky* by trvalo příliš dlouhou dobu. Můžete tak výrazně zkrátit čas potřebný k prohledávání složek. Jako zašifrovaný však může být označen i soubor, který má příponu .ciphered, ovšem není zašifrovaný programem IW FolderProtect či IW JustProtect.

Volba *Pouze podle hlavičky* je při hledání zašifrovaných souborů nejspolehlivější. Její nevýhodou je však větší časová náročnost testovací metody, kterou používá (otevírá každý soubor a kontroluje jeho hlavičku).

Poslední metoda *Podle přípony i hlavičky* je kompromisem mezi časově náročnější metodou *Pouze podle hlavičky* a rychlou, ale ne ve všech případech přesnou *Pouze podle přípony* metodou. Při jejím použití budou na speciální formát obsahu souboru testovány pouze ty soubory, které mají příponu .ciphered.

Vlastní šifrovací proces však k detekci zašifrovaných souborů používá výhradně metodu *Pouze podle hlavičky*, takže nemůže dojít k poškození dat.

Všechny metody jsou optimalizovány, prohledávání složky nepokračuje, pokud již je zřejmý její stav (např. ve složce byl nalezen šifrovaný i nešifrovaný soubor, ve složce přidělené pro šifrování byl nalezen nešifrovaný soubor apod.). To způsobuje, že prohledávání IW FolderProtectu může v rozdílných situacích trvat různě dlouho.

Skupina *Oznamovat chyby* určuje, které chybové stavy budou hlášeny v průběhu šifrování uživateli“:

- *Klíč nenalezen*
  Šifrovací klíč nebyl nalezen.
- *Zotavení z chyby*
  Proces obnovy souborů, který se spouští při startu systému následně po násilném přerušení šifrování (např. výpadkem proudu). Šifrování dat je prováděno způsobem, který zajišťuje, že nemůže dojít ke ztrátě či poškození vašich dat v průběhu šifrování. Chcete-li být informováni o tom, že tato situace nastala, pak zatrhněte tuto volbu.
- *Duplicitní soubory*
  Bude-li políčko s tímto textem zatrhnuto, pak program ohlásí vznik situace, kdy se ve stejné složce vyskytne zašifrovaný soubor, který bude mít po odšifrování stejné jméno jako některý ze souborů, které se v dané složce již vyskytují.

Skupina *Rušení atributů souboru* umožní nastavit způsob reakce šifrovacího systému IW FolderProtectu na situaci, kdy má být zpracován soubor, který má nastaveny atributy *Pouze pro čtení, Skrytý* nebo *Systémový*:

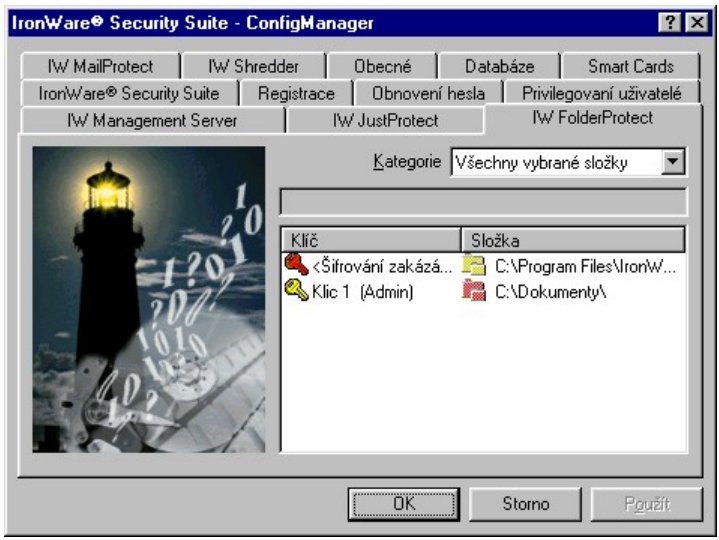
Vždy se zeptat – zobrazí dialogové okno s volbami Ano, Ano pro všechny, Ne, Ne pro všechny. Uživatel tak má možnost určit, jak budou soubory s těmito atributy zpracovány právě běžícím šifrovacím procesem.

Ano všem – globální volba, která vždy automaticky zvolí Ano pro všechny soubory, jichž se akce týká

Ne všem – globální volba, která však vždy zvolí Ne pro všechny.

Zobrazení všech složek přidělených k šifrování

Potřebuje-li uživatel získat rychlý přehled o všech složkách přidělených k šifrování modulem IW FolderProtect, může použít volbu *Všechny vybrané složky* v poli *Kategorie*.



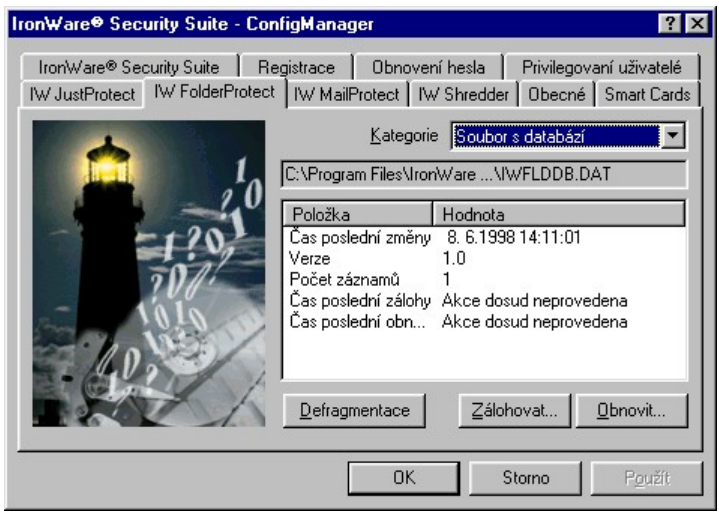
Obr. 95. IW ConfigManager - záložka IW FolderProtect - kategorie Všechny vybrané složky

Po této volbě začne IW FolderProtect prohledávat složky, které jsou vybrány k šifrování a v informativním poli zobrazuje cestu a název právě prověřovaného souboru. Pokud nebyla složka vybraná k šifrování nalezena (byla odstraněna nebo přejmenována), IW FolderProtect tuto složku, po potvrzení volbou *Ano,* odstraní z databáze. Při volbě *Ne* se pak tato složka zobrazuje ve spodní části záložky se speciální ikonou pro neexistující složku. Po dokončení prohledávání je zpřístupněn seznam všech složek, které byly vybrány k šifrování, jim přiřazených klíčů a jmen jejich vlastníků. Použitím pravého tlačítka myši na zvolené složce (nelze provést na složce označené jako neexistující) a po zvolení nabídky *Vlastnosti* v kontextovém menu můžeme na záložce IW FolderProtect nastavovat parametry šifrování zvolené složky – viz. záložka IW FolderProtect.

Správa databáze složek vybraných k šifrování

Po volbě položky *Soubor s databází* ze seznamu *Kategorie* se v záložce zobrazí informace o souboru s databází vybraných složek k šifrování.

Tato položka je dostupná pouze v případě, že přihlášený uživatel má administrátorská práva.



Obr. 96. IW ConfigManager - záložka IW FolderProtect - kategorie Soubor s databází

V horní části části záložky je v informačním políčku zobrazeno jméno souboru s databází. Pod ním jsou informace o této databázi:

Čas poslední změny	Datum a čas poslední změny v databázi.
Verze	Číslo verze databáze.
Počet záznamů	Počet záznamů uložených v databázi.
Čas poslední zálohy	Datum a čas poslední zálohy databáze
Čas poslední obnovy	Datum a čas poslední obnovy databáze ze zálohy.

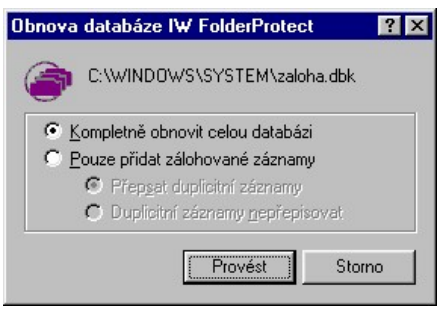
Pro správu databáze slouží tlačítka „*Defragmentace*“, „*Zálohovat…*“ a „Obnovit…“ ve spodní části záložky.

Volba *Defragmentace* odstraní z databáze prázdná místa, která vznikají, když uživatelé ruší přidělení složek pro zašifrování.

Pro případ, kdy dojde k poškození databáze, se doporučuje její pravidelné zálohování, které je možné provést manuálně, nebo tlačítkem „*Zálohovat*“. Pokud bude pro vytvoření zálohy použito příslušné tlačítko, bude zobrazen dotaz na název a umístění souboru s daty aktuální databáze.

Obr. 97. IW ConfigManager – záložka IW FolderProtect – vytváření zálohy databáze

K obnově poškozené databáze slouží tlačítko „*Restore…*“. Objeví se podobný dialog jako při zálohování a po zvolení souboru, ze kterého se má databáze obnovit, je nutné zvolit způsob, jakým se má se zálohou a stávající databází pracovat.



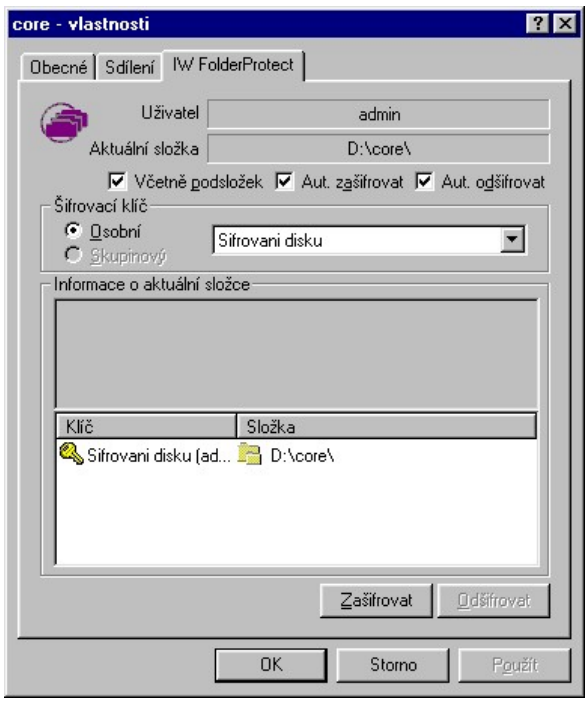
Obr. 117. IW ConfigManager – IW FolderProtect - volba způsobu obnovy databáze

Volba K*ompletně obnovit celou databázi* smaže aktuální databázi a nahradí ji požadovanou zálohou. Bude – li naopak zvoleno *Pouze přidat zálohované záznamy*, bude aktuální databáze zachována a do ní budou vloženy záznamy ze zálohy. Při tomto přístupu je možné položky, které jsou v databázi i v záloze buď ponechat z aktuální databáze (volba *Duplicitní záznamy nepřepisovat*), nebo takovéto položky databáze nahradit odpovídajícími daty ze zálohy (volba *Přepsat duplicitní záznamy*).

Byl–li databázový soubor smazán, IW FolderProtect to zjistí a po varování uživatele vytvoří soubor nový.

• Záložka IW FolderProtect ve Vlastnostech složky

Po nainstalování subsystému *IW FolderProtect* do vašeho počítače je ke standardním záložkám vlastností jednotlivých složek přidána záložka s názvem *IW FolderProtect*. V této záložce je možné nastavit „šifrovací vlastnosti“ této složky, tedy vybrat ji k šifrování, zrušit výběr k šifrování, modifikovat šifrovací parametry této složky atd.



Obr. 98. IW FolderProtect – záložka ve vlastnostech složky

Pole *Uživatel* obsahuje jméno uživatele, který je přihlášen do systému, ať již má nebo nemá přístup k datům dané složky. V políčku *Aktuální složka* je zobrazeno jméno aktuální složky. V době, kdy IW FolderProtect prochází podsložky a hledá zašifrované soubory, je v něm zobrazeno jméno právě testovaného souboru.

Další volbou na záložce je možnost výběru způsobu a úrovně vnoření šifrování :

Včetně podsložek - aktuální složka bude vybrána pro šifrování včetně všech svých podsložek

Automaticky zašifrovat - aplikace provede zašifrování dané složky automaticky při ukončení běhu Windows NT

Automaticky odšifrovat - aplikace provede odšifrování dané složky automaticky při startu Windows NT

K přiřazení šifrovacího klíče slouží přepínač typu vybraného klíče pro šifrování/odšifrování - *Osobní / Skupinový* a výběrový seznam klíčů daného typu ve skupině *Šifrovací klíč*. Výběr složky pro šifrování se provede pouhým výběrem jména klíče v seznamu klíčů. Naopak zrušení výběru složky pro šifrování lze provést výběrem položky <*Nepřiděleno*>. Pro skupinu je i možnost nepovolit výběr dané složky pro šifrování (položka <*Šifrování zakázáno*>).

Zákaz výběru složky pro šifrování smí provést jen administrátor a v takové složce pak není možné šifrovat IW FolderProtectem, dokud její stav administrátor opět nezmění.

Provádět a rušit výběr složky pro šifrování skupinovým tajným klíčem smí jen administrátor. Osobní tajné klíče může libovolně volit či měnit sám uživatel. Samozřejmě pouze z množiny klíčů, které mu patří.

Informace o aktuální složce - informační okno zobrazující informační nebo varovná hlášení, vztahující se k aktuální složce nebo složkám nadřazeným a k činnosti, na kterou je IW FolderProtect nastaven.

Seznam a vysvětlení významu informačních hlášení IW FolderProtect je uveden níže:

- **Hlášení šifrovacího procesu**

Soubor (jméno) má nastaven atribut pouze ke čtení, skrytý nebo systémový. Pokračovat ve zpracování tohoto souboru? Volbou *Ano* (*Ano všem*) bude u souboru resp. souborů atribut odstraněn a soubor bude zašifrován. Pokud zvolíte volbu *Ne, Ne všem,* budou všechny podobné soubory vyňaty ze šifrování
Na disku není dostatek místa k zapsání cílového souboru (jméno). Nastává zejména v případě, že se pokoušíte šifrovat na disketě soubor, který je větší než zbylé volné místo.
Předchozí zašifrovací / odšifrovací proces byl přerušen. Šifrovací proces byl přerušen tlačítkem *„Storno“* nebo chybou systému.

Nalezena duplicita. Soubor (název). Informuje uživatele o situaci, kdy při odšifrování již v dané složce existuje soubor se jménem, jaké bude mít právě odšifrovávaný soubor. Je-li v IW ConfigManageru zapnuta volba *Duplicitní soubory*, pak se objeví toto varovné hlášení a uživateli je nabídnuta možnost přerušení šifrování, přepsání existujícího souboru, a nebo přeskočení odšifrovávání tohoto souboru.
Příprava na zotavení po předchozím přerušeném šifrovacím procesu selhala. Soubor (název). Tato situace může nastat v případě, že některá z aplikací „drží“ pracovní soubor.
Nelze otevřít zdrojový soubor (název). Tato chyba se vyskytne v případě, že se snažíte o šifrování souboru, který aktuálně používá některá běžící aplikace.
Chyba při načtení zdrojového souboru (název). Daný soubor má pravděpodobně otevřená jiná aplikace.
Chyba při zápisu cílového souboru (název). V případě, že jde o disketovou jednotku, nemusí být disketa v mechanice.
Nelze otevřít dočasný soubor (název). Toto chybové hlášení se objeví například při pokusu o šifrování na disketě, která je zajištěná proti zápisu.
Skutečně chcete vybrat *Znovu pro všechny další chyby?* Pokud vyberete ANO, program možná nepůjde zastavit!.

- **Informace o složkách vybraných pro šifrování a přiřazených klíčích**

V tomto okně záložky IW FolderProtect je viditelný seznam složek, vybraných k šifrování, včetně úplné cesty a klíčů, které se k těmto složkám vztahují. Jednotlivé ikony klíčů a složek mají různou podobu. Ikony klíčů a složek jsou uvedeny v následujících tabulkách.

Ikony klíčů, které mohou být složkám přiřazeny	
	Dostupný tajný osobní klíč
	Nedostupný tajný osobní klíč
	Dostupný skupinový tajný klíč
	Nedostupný skupinový tajný klíč
	Rezervovaný klíč. Ve složce, které byl administrátorem přiřazen tento klíč, není povoleno šifrování

Ikony, zachycující stav složky, která byla přid šlena pro šifrování	
	Bez podsložek, obsahuje pouze odšifrované soubory
	Bez podsložek, vyskytují se odšifrované i zašifrované soubory
	Bez podsložek, zcela zašifrovaná
	Bez podsložek, neobsahuje žádné soubory
	Včetně podsložek, s odšifrovanými soubory
	Včetně podsložek, částečně zašifrovaná
	Včetně podsložek, všechny soubory zašifrované
	Včetně podsložek, neobsahuje žádné soubory

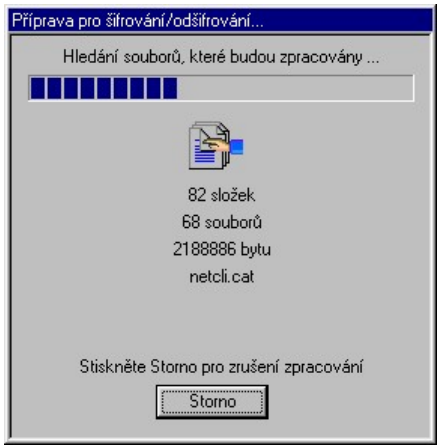
Na spodním okraji záložky se nacházejí dvě funkční tlačítka umožňující spustit šifrování přímo ze záložky IW FolderProtect ve Vlastnostech souboru.

Zašifrovat - po kliknutí na toto tlačítko se soubory v aktuální složce vybrané pro šifrování začnou zašifrovávat vybraným klíčem, a to podle volby, buď včetně podsložek nebo bez nich.

Odšifrovat - po kliknutí na toto tlačítko se soubory v aktuální složce vybrané pro šifrování začnou odšifrovávat, a to podle volby, buď včetně podsložek nebo bez nich.

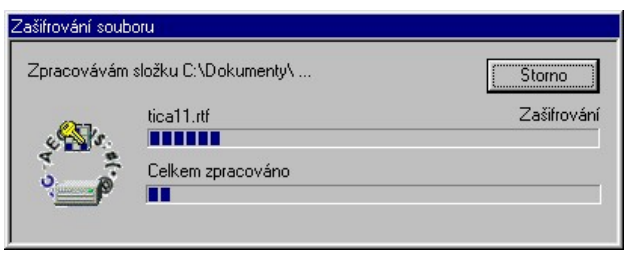
Na záložce jsou dále funkční tlačítka *OK, Storno, Použít* a *Nápověda,* které mají standardní funkci odpovídající prostředí.

Po spuštění šifrovacího procesu se nejprve objeví prohledávací dialogové okno, kdy program zjišťuje celkovou velikost dat, která budou zpracována.



Obr. 99. IW FolderProtect - proces přípravy složky k zašifrování nebo odšifrování

a poté se spustí vlastní šifrovací proces. Oba procesy mohou být kdykoliv přerušeny stiskem tlačítka S*torno*. Jestliže bude toto tlačítko stisknuto již během průběhu přípravného procesu, vlastní šifrovací proces nebude vůbec spuštěn.



Obr. 100. IW FolderProtect - průběh procesu zašifrování složky

Pro případ, že dojde k poškození databáze, je vhodné ji jednou za čas archivovat do zálohy a v případě takové havárie provést obnovení databáze z této zálohy.

Zálohovat databázi je povoleno pouze vcelku, tedy ne pouze pro jednoho uživatele. Obsahuje záznam o datu poslední zálohy.

Obnovovat databázi ze zálohy má právo pouze administrátor. Je to z toho důvodu, že jako jediný je oprávněn k řešení nesrovnalostí.

- **Jak aplikace pracuje**

Zašifrování - datový soubor se zašifruje a přidá se standardní hlavička. Původní soubor se smaže vestavěnou skartovací funkcí. Identifikace klíče: jméno klíče + jméno vlastníka (pokud je sdílená, pak jen jméno klíče). Jestliže se nepodaří soubor smazat, je zobrazeno hlášení uživateli, který je tak o této situaci informován.

Odšifrování - soubory budou normálně odšifrovány a po úspěšném ukončení odšifrování se původní zašifrované soubory smažou. Klíč, kterým byl daný soubor zašifrován, se najde v IW SessionManageru podle hashe klíče, který se nachází v hlavičce každého zašifrovaného souboru.

Důležitou vlastností IW FolderProtect je i to, že použijete-li pravé tlačítko myši k prohlížení vlastností zašifrovaného souboru, objeví se v menu Vlastnosti i záložka IW FolderProtect, ve které naleznete veškeré dostupné informace o zašifrovaném souboru. Jde například o vlastníka souboru, jméno klíče, originální jméno souboru a mnohé další.

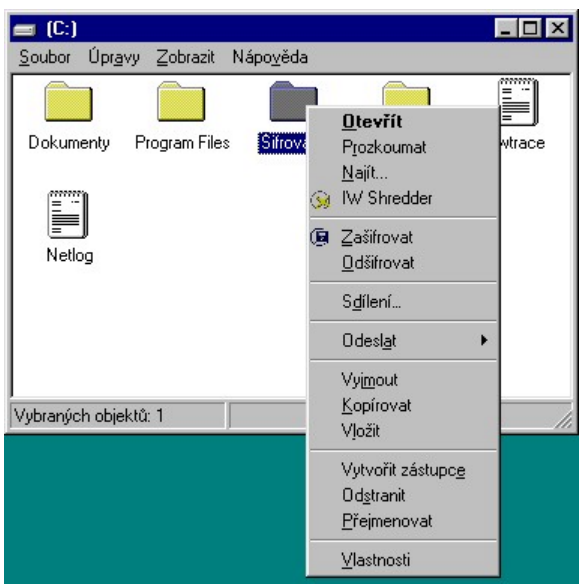
• IW JustProtect

• Základní popis vlastností modulu

Modul šifrování na žádost s názvem IW JustProtect umožňuje šifrovat soubory ve vybraných složkách a složky na libovolných lokálních nebo síťových discích. Data mohou být šifrována jak pro jednotlivé uživatele, tak i pro skupiny uživatelů, kteří data mohou sdílet a přitom je nikdo mimo skupinu nemůže použít. Data mohou být také šifrována do EXE souboru klíčem, který je vytvořen z hesla. Tato data mohou být rozšifrována i mimo instalaci IW Security Suite. Příjemce však musí znát heslo.

• Uživatelské rozhraní IW JustProtect

Šifrování modulem JustProtect je možné vyvolat prostřednictvím položky v lokálním menu souboru nebo složky po stisku pravého tlačítka myši.



Obr. 101. Okno systému Windows s otevřeným kontextovým menu složky

V zobrazeném kontextovém menu jsou přidány položky *Zašifrovat* a *Odšifrovat,* výběrem kterých je zvolena šifrovací akce. Po volbě první z nich se zobrazí okno pro výběr šifrovacího klíče; při volbě druhé možnosti seznam souborů, které budou odšifrovány.

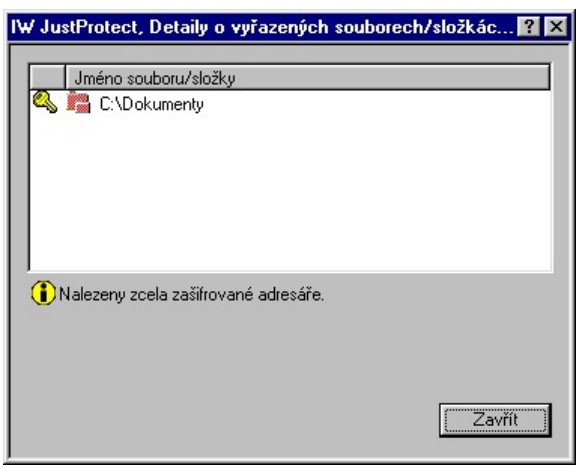
Obr. 102. IW JustProtect - výběr šifrovacího klíče

Obr. 103. IW JustProtect – výběr souborů a složek pro odšifrování

Také je možné označit více souborů a v kontextovém menu tohoto výběru zvolit *Zašifrovat* nebo *Odšifrovat.* JustProtect tyto označené soubory či složky rozdělí podle toho, zda je možné je zašifrovat či odšifrovat. Ty, u kterých je možné příslušnou operaci provést, se vypíší do okna *Jméno souboru / složky.*

Obr. 104. IW JustProtect - okno IW JustProtect v situaci, kdy jsou některé soubory vyňaty ze šifrování

Seznam souborů, u kterých nebylo šifrování provedeno, je dostupný kliknutím na tlačítko *„Zobraz vyřazené…“* (při zašifrování jsou zde např. již zašifrované soubory a při odšifrování nezašifrované či nedostupné soubory). Naleznete zde též zdůvodnění, proč nebylo možné soubory zašifrovat nebo odšifrovat.



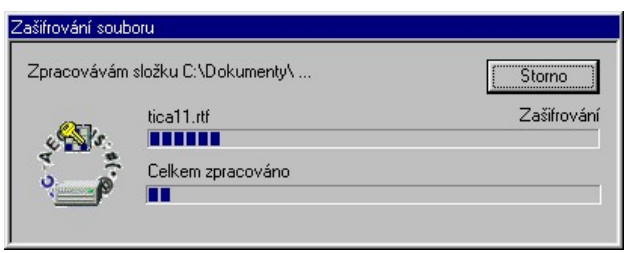
Obr. 105. IW JustProtect - seznam souborů, které byly z nějakého důvodu vyloučeny ze šifrování JustProtectem

V okně pro výběr šifrovacího klíče je nutné určit, jakým způsobem zvolený soubor nebo složku zašifrovat. Je to možné provést jedním z následujících tří způsobů:

- Volba *Osobní klíč* - umožňuje vybrat libovolný tajný klíč aktuálního uživatele, kterým bude zvolený soubor nebo složka zašifrován(a). Bude-li při šifrování složky navíc zvolena volba *Včetně podsložek*, budou tímto klíčem zašifrovány také všechny její podsložky. Data jsou na požádání zašifrována nebo odšifrována a formát dat je kompatibilní s IW FolderProtectem (ne s IW FileProtectem!), takže je možné jednotlivé soubory či složky vzájemně sdílet pro šifrování a odšifrování.
- Volba *Skupinový klíč* – umožňuje administrátorovi vybrat klíč ze seznamu jím spravovaných skupinových tajných klíčů, a ten použít pro šifrování vybraných dat. Bude-li při šifrování složky navíc zvolena volba *Včetně podsložek*, budou tímto klíčem zašifrovány také všechny podsložky zvolené složky. Data jsou na požádání zašifrována a odšifrována a formát dat je kompatibilní s IW FolderProtectem (ne však s IW FileProtectem!), takže i tato data je možné vzájemně sdílet pro šifrování a odšifrování mezi těmito subsystémy.
- Volba *Do souboru EXE* - soubor či struktura složek se zašifruje do tvaru samorozbalovacího souboru s příponou EXE. Uživatel – příjemce je po spuštění takového souboru vyzván k zadání hesla, z něhož je vytvořen kryptografickými metodami šifrovací klíč a soubor či struktura je odšifrována.
- Volbou položky *Přesunout vybrané soubory / složky* dojde v průběhu zašifrování ke smazání původních souborů či složek v otevřeném textu.

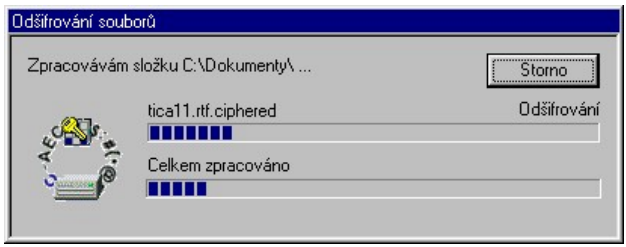
Šifrování osobním nebo skupinovým tajným klíčem

Při zadání a potvrzení volby *Osobní klíč* nebo S*kupinový klíč* tlačítkem *OK* se spustí proces šifrování, jehož průběh je indikován následujícím oknem:



Obr. 106. IW JustProtect - okno zobrazující průběh zašifrovávání souborů

Obdobným způsobem je indikován průběh odšifrovávání souboru nebo složky při zvolení volby *Odšifrovat* v lokálním menu vybrané(ho) složky nebo souboru.



Obr. 107. Okno zobrazující průběh odšifrovávání souborů

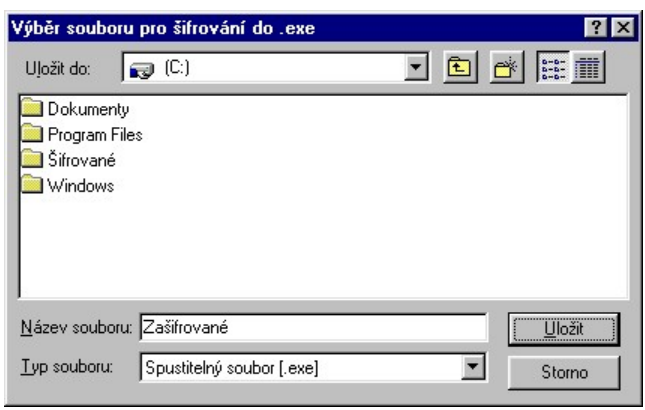
Při šifrování souboru nebo složky do EXE souboru se jedná o vytvoření šifrovaného souboru, kde je ke generování šifrovacího klíče použito zadávané heslo. Tento soubor je zcela nezávislý na systému IronWare® Security Suite. Tato volba je velmi výhodná při zasílání nebo předávání důvěrných dat jiným osobám, které nemusí vlastnit žádný šifrovací program, kde pro odšifrování souboru jim stačí znalost hesla použitého při generování šifrovacího klíče, kterým je soubor zašifrován.

Šifrováni do EXE souboru

Zvolte volbu *Do souboru EXE*.
Vyberte soubor(y) nebo složku(y), který chcete zašifrovat do EXE souboru.

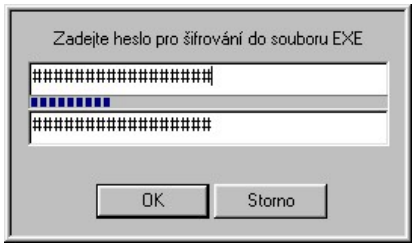
Obr. 108. IW JustProtect - okno se složkou vybranou k zašifrování do EXE souboru

Následně budete vyzváni k zadání jména souboru, do kterého chcete zašifrovaná data uložit, a k zadání složky, do níž má být soubor umístěn.



Obr. 109. IW JustProtect - volba názvu a umístění souboru při zašifrovávání do EXE souboru

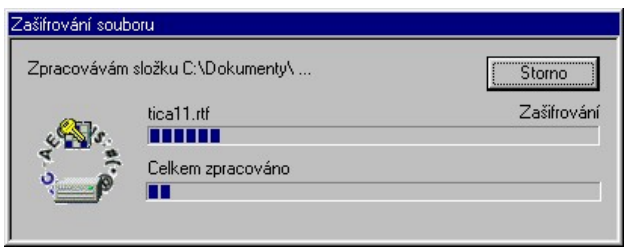
Dále je nutné zadat heslo pro šifrování souboru, které bude sloužit i adresátovi k jeho odšifrování.



Obr. 110. IW JustProtect - zadávání hesla při zašifrovávání do EXE souboru

Po zadání všech potřebných údajů dojde k procesu šifrování, jehož výsledkem je EXE soubor, ve kterém jsou ukryta data v zašifrované podobě. K šifrování do EXE souboru je vždy použit algoritmus CAST.

Byla-li v okně pro výběr šifrování do EXE souboru zatrhnuta volba *Přesunout vybrané soubory/složky,* pak budou všechny původní soubory skartovány stejným postupem jako při šifrování osobním či skupinovým tajným klíčem.



Obr. 111. IW JustProtect - průběh zašifrovávání do EXE souboru

Šifrovat do samorozbalovacího EXE souboru je dovoleno i uživateli, který nemá žádné šifrovací klíče.

- **Informace o událostech v průběhu šifrovacího procesu**

IW JustProtect je schopen detekovat duplicitu při za/odšifrování (při zašifrování již existuje příslušný soubor s koncovkou *.ciphered*, při odšifrování bez ní). Tlačítkem *Přerušit* ukončíme šifrování. Tlačítko *Znovu* nám dává možnost nejprve duplicitní soubor přejmenovat či přesunout, neboť pak se IW JustProtect znovu pokusí o za/odšifrování. Tlačítkem *Ignorovat* se duplicitní soubor přepíše aktuálně šifrovaným souborem.

Seznam chybových a informačních hlášení šifrovacího procesu

Soubor (jméno) má atribut pouze ke čtení, skrytý nebo systémový, pokračovat ve zpracování souboru?
Zvolíte-li *„Ano“*, pak program provede zašifrování i těchto souborů. Pokud zvolíte *„Ne“*, soubor nebude zašifrován.

Na disku není dostatek místa k zapsání cílového souboru (jméno).
Nastává zejména v případě, že se pokoušíte šifrovat na disketě soubor, který je větší než zbylé volné místo.

Předchozí zašifrovací/odšifrovací proces byl přerušen.
Proces byl přerušen tlačítkem „Storno“, nebo došlo k chybě.

Během šifrovacího procesu byla nalezena duplicita vejménech zpracovávaných souborů.
Znamená to, že některý ze zašifrovaných souborů bude mít po odšifrování stejné jméno, jako některý z již existujících souborů.

Příprava na obnovu po předchozí šifrovací chybě selhala.
Program v dané složce nemůže pokračovat.

Nelze otevřít zdrojový soubor (název).
Tato chyba se vyskytne v případě, že se snažíte o šifrování souboru, který aktuálně používá některá běžící aplikace.

Chyba při načtení ze zdrojového souboru (název).

Chyba při zápisu do cílového souboru (název).

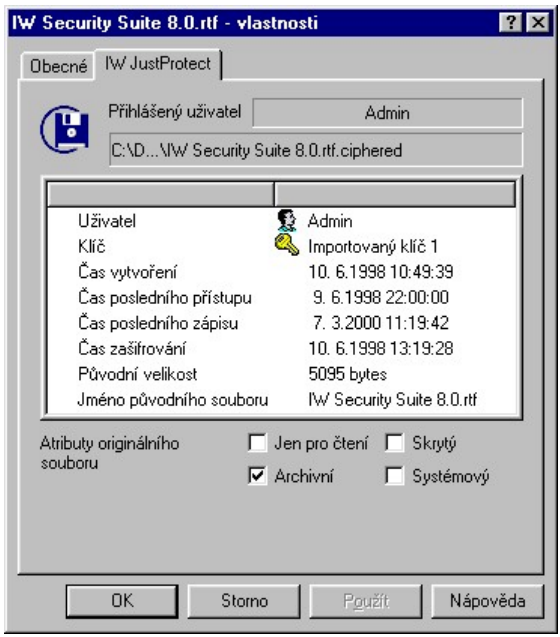
Nelze otevřít dočasný soubor (název). Toto chybové hlášení se objeví například při pokusu o šifrování na disketě, která je zajištěná proti zápisu.

Chcete opravdu zvolit „Znovu“ pro všechny další chyby ?
Program se dotazuje, zda si skutečně přejete automaticky odpovídat volbou *Znovu* pro všechny další chyby. Pokud vyberete ANO a daná chyba se bude periodicky opakovat, pak se může stát, že program nebude moci dokončit práci.

Zobrazení vlastností zašifrovaného souboru

Důležitou vlastností IW JustProtect je i to, že použijete-li pravé tlačítko myši k prohlížení vlastností zašifrovaného souboru či složky, objeví se v menu Vlastnosti i záložka IW JustProtect, ve které naleznete veškeré

dostupné informace o zašifrovaném souboru či složce. Jde například o vlastníka souboru, jméno klíče, původní jméno souboru a mnohé další.



Obr. 112. IW JustProtect – záložka ve Vlastnostech souboru

• IW Shredder

je relativně samostatný bezpečnostní modul, který nevyžaduje ke své činnosti PKI. Je možné jej proto instalovat a provozovat naprosto odděleně.

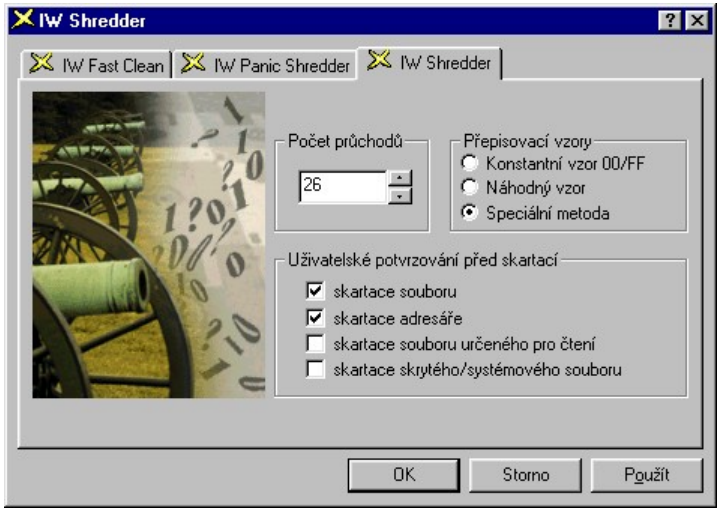
• K čemu slouží IW Shredder?

Úkolem IW Shredderu je bezpečná skartace vašich elektronických dat. Obsahuje další dvě části, kterými jsou *IW Fast Clean* a *IW Panic Shredder*. Navíc po instalaci přibude v programu Průzkumník nebo v jiných souborových manažerech v kontextové nabídce u jména souboru nebo složky volba *IW Shredder*, která umožňuje skartaci souboru nebo složky, či struktury složek, a v kontextové nabídce u písmene disku volba *Disk cleaner* s položkami *Vymazat všechna data, Vymazat volné místo* a *Vymazat celý disk*, slučující obě předchozí volby.

Je-li složka přidělena pro šifrování IW FileProtectem a vyskytují se v ní soubory ze seznamu vyjímek , nepoužívejte na její mazání IW Shredder. Jestliže přesto potřebujete data v této složce skartovat, pak je nutné data odšifrovat a zrušit přidělení této složky.

Po nainstalování modulu je zapotřebí provést nastavení funkcí všech jeho částí. Po spuštění modulu např. zástupcem v menu *Start / Programy / IronWare Security Suite* se otevře okno aplikace se třemi záložkami pojmenovanými IW Shredder, IW Fast Clean a IW Panic Shredder.

- **IW Shredder**



Obr. 113. IW Shredder – nastavení IW Shredderu

Zde se definují obecná nastavení platná pro všechny části aplikace.

V pravé horní části záložky je možné ve skupině *Přepisovací vzory* definovat skartovací znaky. Přepínač *Konstantní vzor 00/FF* přepíše skartované soubory nejprve hodnotou „00“ , a pak „FF“ *, Náhodný vzor* použije pro skartaci náhodně zvolené znaky, *Speciální náhodné znaky* přepíše skartovaná data speciálními znaky pro úplné vymazání disku na fyzické úrovni.

Počet průchodů určuje počet přepisování skartovaného souboru nebo disku skartovacím řetězcem (v rozmezí 1 – 26). Skupina *Uživatelské potvrzování před skartací* definuje akce, u nichž lze zvolit nutnost potvrzení uživatelem před jejich provedením. Jedná se o odstranění souboru, složky, souborů s atributem pouze pro čtení a skrytých a systémových souborů. Po každé provedené změně v nastavení se zpřístupní tlačítko *Použít* , kterým lze konfiguraci ihned aktualizovat.

- **IW Fast Clean**

Obr. 114. IW Shredder – nastavení IW Fast Clean

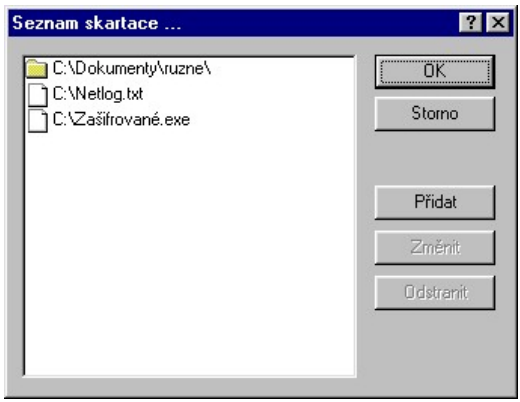
K rychlému odstranění dat na disku počítače podle zvolených kritétií slouží IW Fast Clean.

Skupina *Vyberte opearci* je rozdělena na podskupinu *Diskové operace* , ve které se definují činnosti prohledávající každou diskovou jednotku zvlášť, a na obecnou část, platnou pro celý systém, ve kterém je IW Shredder instalován.

Ve skupině diskových operací je výběrový seznam s disky. Jejich postupnou volbou můžeme definovat pro každý disk zvlášť následující funkce :

- *Skartace .swp and .tmp souborů*
  *Bezpečné s*mazání všech dočasných souborů s příponou .swp a .tmp
- *Skartace koše*
  Bezpečné smazání souborů v odpadkovém koši
- *Skartace volného místa na disku*
  Bezpečné přemazání volného místa na disku

Obecná část obsahuje možnost zadání *Skartovat seznam.* Tato volba zpřístupní tlačítko se symbolem otevírající se složky, po jehož stisknutí máme možnost editovat *Seznam skartace*… .



Obr. 115. IW Shredder – seznam skartace

Tlačítkem *„Přidat“* máme možnost přidat do seznamu buď celou strukturu složek, anebo pouze konkrétní soubory, případně skupinu souborů pomocí zástupných znaků (např. hvězdičková konvence). Další volby v záložce IW Fast Clean umožňují:

- *Skartace historie dokumentů*
  Bezpečné smazání historie dokumentů
- *Skartace run historie*
  Bezpečné smazání historie spuštěných programů z nabídky *Start/Spustit*
- *Skartace cookies*
  Smazání internetových cookies
- *Skartace dočasných souborů*
  Bezpečné smazání dočasných souborů ve složce \TEMP
- *Skartace Inet dočasných souborů*
  Smazání dočasných Internetových souborů

Po každé provedené změně v nastavení se zpřístupní tlačítko *Použít,* kterým můžeme konfiguraci ihned aktualizovat. Tlačítkem *„Skartuj“* pak můžeme spustit provedení skartace.

- **IW Panic Shredder**

Obr. 116. IW Shredder – nastavení IW Panic Shredder

Slouží ke skartaci souborů dle definovaného seznamu prostřednictvím rezidentního modulu IW *Panic Shredder*, který se aktivuje stiskem nadefinované horké klávesy .

Volba zaškrtávacího pole *Používat Panic Shredder* zpřístupní tuto funkci. Rezidentní program je pak při startu systému zaveden do paměti. Tento program lze nahrát do paměti i z příkazové řádky spuštěním ***panicshredder.exe /load***, anebo interaktivně spuštěném modulu ***panicshredder.exe*** a volbou tlačítka *„Zavést“* v dialogovém okně. Odstranění z paměti se provede příkazem ***panicshredder.exe /unload*** nebo volbou tlačítka *„Uvolnit“* v dialogovém okně modulu.

Soubory ke skartaci – umožňuje zadat seznam skartovaných souborů – stejně jako v záložce IW FastClean.

V poli *Aktivační horká klávesa* lze definovat horkou klávesu IW Panic Shredderu, kterou lze spustit skartaci.

IronWare® Security Suite - Communication

• IronWare® MailProtect

IW MailProtect je komunikační program navržený pro bezpečný přenos zpráv a datových souborů pomocí e-mailu v síti Internet, sítích LAN nebo WAN. Použití programu *IW MailProtect* zajišťuje diskrétnost komunikace v rozsahu od běžně zasílaných zpráv přes home banking, až po přenos citlivých obchodních nebo vojenských údajů.

IW MailProtect se skládá ze dvou částí. Jde o IW Tray pro ošetření clipboardu a souborů pomocí kontextového menu a IW MailProtect Plug-in.

IW Tray je nezávislý na používaném e-mailovém programu. V libovolném programu pro posílání zpráv, počínaje CC-mailem, Microsoft Mailem až po Pegasus mail (nebo z libovolné Windows aplikace) můžete zabezpečit svoje data tak, že je vložíte do schránky Windows. Zašifrujete je programem *IW Tray* a pak vložíte zpět do aplikace. Následně může být zpráva odeslána běžným způsobem. Nebo v případě, že máte zatrženu položku *Konvertovat text/soubory do S/MIME formátu* na záložce *IW MailProtect* v IW ConfigManageru, se text ve schránce i připojené soubory uloží do složky zvolené v okně *Adresář*, které se otevírá na téže záložce, v poli *Vždy se ptát při ukládání* jako soubor smime.p7m.

Vlastnosti společné pro IW Tray a IW MailProtect se nastavují na záložce IW MailProtect v IW ConfigManageru.

Obr. 117. IW ConfigManager – nastavení IW MailProtect

Toto záložka slouží k nastavení obecných vlastností *IW MailProtectu*.

Ve výběrovém seznamu *Preferovaný klíč* je uživateli nabídnut seznam jemu dostupných soukromých klíčů, z nichž jeden si uživatel volí pro podepisování zpráv.

Ve výběrovém seznamu *Zašifrování zpráv* vybírá uživatel algoritmus pro šifrování své pošty. K dispozici má pět algoritmů: RC2-40 RC2-128, DES, 3DES, CAST a BLOWFISH. Podrobnosti o jednotlivých algoritmech jsou v kapitole **AEC Šifrovací knihovna**.

Ve výběrovém seznamu *Digitální podpis* volí uživatel mezi hashovacími algoritmy SHA a MD5. Podrobnější informace o těchto hashovacích funkcích jsou v kapitole **AEC Šifrovací knihovna**.

Na této záložce uživatel také rozhoduje, zda se zprávy mají kopírovat do složky „Bezpečné zprávy“, konvertovat text/soubory do S/MIME formátu, ponechávat zprávy po přečtení zašifrované a zda se mají S/MIME přílohy v Microsoft Outlook ukládat na disk.

Tlačítko ve spodní části záložky otevře okno *Adresář*, kde je možné nastavit, kde budou uloženy šifrované zprávy určené k odeslání, a kde budou odšifrované příchozí zprávy.

IW Tray umožňuje také multinásobný podpis souborů. Tímto způsobem může podepsat soubor více něž jeden uživatel. Aby byl multinásobný podpis umožněn, musí být vypnuta konverze do S/MIME. Akci je možné provést i z kontextového menu.

Volba *„Clear sign zapnout“* slouží pro vytváření zvláštního digitálního podpisu, který do podepsaného textu přidá na začátek hlavičku, ale samotný podpis je připojen až na konci textu, který se nachází v otevřené formě. Na rozdíl od klasického podpisu se tento při kontrole podpisu neodstraňuje.

• IronWare® MailProtect Plug-in pro MS Exchange a MS Outlook

Systém IronWare® MailProtect je doplněk do aplikace MS Exchange 5.0 nebo MS Outlook 97, 98 a 2000, tzn. jeho použití a menu jsou zakomponovány do menu zmíněných mail programů. Pracuje se službami Internet Mail a Microsoft Mail.

Konfigurace

Vlastnosti společné pro IW MailProtect Plug-in a IW MailProtect Clipboard se nastavují na záložce *IW MailProtect* v IW ConfigManageru.

Obr. 118. IW ConfigManager - nastavení v záložce IW MailProtect

Tato záložka slouží k nastavení obecných vlastností *IW MailProtectu*.

Ve výběru *Preferovaný klíč* je uživateli nabídnut seznam jemu dostupných *soukromých klíčů*, z nichž jeden si uživatel volí pro podepisování zpráv.

Ve výběrovém seznamu *Zašifrování zprávy* vybírá uživatel algoritmus pro šifrování své pošty. K dispozici má pět algoritmů: RC2-40, RC2-128, DES, 3DES, CAST a BLOWFISH. Podrobnosti o jednotlivých algoritmech jsou v kapitole **AEC Šifrovací knihovna**.

Ve výběrovém seznamu *Digitální podpis* volí uživatel mezi hashovacími algoritmy SHA a MD5. Podrobnější informace o těchto hashovacích funkcích jsou v kapitole **AEC Šifrovací knihovna**.

Na této záložce uživatel také rozhoduje, zda se zprávy mají kopírovat do složky „Bezpečné zprávy“, konvertovat text/soubory do S/MIME formátu, ponechávat zprávy po přečtení zašifrované .

Tlačítko ve spodní části záložky otevře okno *Adresář*, kde je možné nastavit, kde budou uloženy šifrované zprávy určené k odeslání a kde budou odšifrované příchozí zprávy.

Aktivováním položky *Clear sign* přesune IW MailProtect digitální podpis ze zprávy do přílohy. Tento způsob je vhodný, pokud si uživatel není jistý, že adresát(i) používají e-mailové programy kompatibilní se standardem S/MIME.

Menu programu a jejich význam

Po spuštění mail aplikace jsou do panelu nástrojů okna pro psaní zpráv automaticky přidány následující ikony:

 Stisknutím této ikony se zapíná šifrování zpráv. Pro šifrování je použit klíč aktuálního uživatele.

 Touto ikonou se zapíná elektronické podepisování zpráv, podpis slouží pro ověření totožnosti odesílatele.

 Tato ikona zapíná kompresi zpráv před odesláním.

Mimo těchto ikon se po nainstalování IronWare® MailProtect objeví v hlavním okně, v menu Nástroje\Možnosti, záložka IW MailProtect.

Princip výměny klíčů

Pro to, aby mohl komunikační protějšek odšifrovat přijatou zašifrovanou zprávu (zašifrovanou jeho certifikátem), musí mít k dispozici příslušný klíč, k němuž byl certifikát vygenerován. Je zřejmé, že pokud chce uživatel někomu poslat zašifrovanou zprávu musí si nejdříve opatřit certifikát adresáta. Naopak pokud si uživatel přeje, aby mu někdo mohl posílat šifrované zprávy, musí se postarat, aby příslušná osoba měla certifikát, který si vygeneroval k některému ze svých klíčů.

Systém IronWare® MailProtect tento certifikát pošle sám, pokud uživatel pošle osobě nebo osobám, se kterými šifrovaně chce komunikovat, elektronicky podepsaný e-mail.

Pokud má příjemce této zprávy nainstalován bezpečností systém IronWare® MailProtect, pak stačí si tuto zprávu otevřít, aby certifikát byl automaticky přidán do PKI.

Pokud příjemce nemá IronWare® MailProtect, je certifikát obsahující mimo jiné veřejnou část klíče v podepsaném e-mailu stále uložen. Po nainstalování systému stačí tento e-mail znovu otevřít, klíč se automaticky importuje do PKI.

Samozřejmě nejlepší cesta jak získat certifikát komunikačního protějšku je jeho zkopírování z Certifikační autority a jeho import do PKI. Certifikát Certifikační Autority musí být importován jako první a k tomu má právo pouze administrátor PKI. Certifikační autorita je velmi důležitou součástí řešení PKI a self signed certifikáty, bez účasti Certifikační autority na certifikačním procesu, nejsou příliš důvěryhodné.

• IronWare® FTP Client

IW FTP Client je profesionální FTP klient. Byl navržen tak, aby splňoval všechny základní funkce FTP klienta a rozšířil jeho vlastnosti o šifrování a zabezpečení přenášených dat Internetem. Jednou z nejdůležitějších funkcí aplikace IW FTP Client je automatické navazování přerušených přenosů. IW FTP Client obsahuje také jedinečnou funkci souborové fronty, která umožňuje předem připravit přenášené soubory a naplánovat připojení k požadovaným FTP serverům.

IW FTP Client je aplikace, která dovoluje novým uživatelům využívat možnosti FTP služeb bez nezbytnosti hlubších znalostí detailů jeho protokolu. Zjednodušuje používání FTP poskytnutím uživatelsky přívětivého prostředí, namísto poměrně složitého ovládání prostřednictvím příkazové řádky. Jednou z důležitých součástí IW FTP je schopnost shromáždit všechny dostupné informace o souborech a struktuře složek vzdáleného systému, a potom tyto informace prezentovat ve snadno ovladatelném Správci souborů podobném MS Exploreru. Můžete dostat snadné spojení na předdefinovanou síť pouhým dvojitým kliknutím na její jméno. Nejdůležitější vlastností IW FTP je však schopnost zašifrovat a odšifrovat data posílaná prostřednictvím FTP. V následujících sekcích budou detailně popsány nejdůležitější funkce IW FTP Client aplikace.

Systém poskytuje podporu firewallům a je FTP klient aplikací pro Windows Sockets. IW FTP byl navržen tak, aby plně využíval vlastností a schopností Windows, a byl tak snadno pochopitelný a lehce ovladatelný.

Aplikaci IW FTP určitě ocení ti, kteří touží každý den po nových informacích, umístěných v FTP uzlech světové sítě Internetu. Bude také neocenitelnou pomůckou pro ty, které již unavuje zadávání FTP příkazů na příkazové řádce v klasických FTP aplikacích. Hlavním rysem IW FTP jsou zabudované bezpečnostní prvky, tj. možnost posílaná data zašifrovat/odšifrovat a podepisovat. Používáním IW FTP získáváte snadno použitelnou a bezpečnou FTP aplikaci.

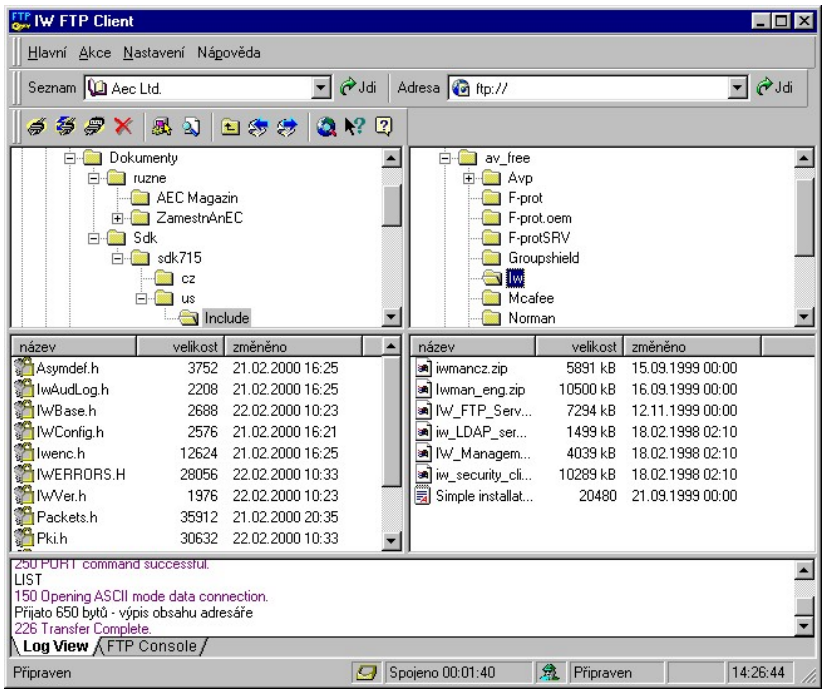
IW FTP Client je součástí IronWare® Security Suite Communication rodiny, která je určena jako univerzální řešení přenosu dat dle časového rozvrhu nebo manuálně prostřednictvím Internetu a FTP protokolu s (v zásadě) libovolnou mírou utajení.

• Nejdůležitější vlastnosti

- program je určen pro systémy Windows 95/98 a Windows NT
- zcela nový FTP engine zaručuje maximální rychlost a minimální spotřebu systémových prostředků
- program podporuje všechny druhy známých FTP serverů (vysoká kompatibilita) a úplnou kolekci FTP příkazů.
- vložená FTP konzola umožňuje zadávání ručních FTP příkazů
- program umožňuje automatické navázání přerušeného přenosu
- program podporuje přenosy celých složek včetně podsložek
- mazání celých složek a podsložek
- podpora drag&drop včetně přenosu z Exploreru (Průzkumníka).
- podpora firewallů a proxy serverů
- podpora pasivního socketu (PASV) RFC 959
- optimalizace pro Windows NT a WinSock 2.0
- unikátní fronta souborů umožňuje přednastavit soubory a servery pro automatický přenos dat
- komfortní, intuitivní ovládání využívající všechny vymoženosti operačního systému Windows
- veškeré události zaznamenány v LOG souborech

• Práce s programem

Následující obrázek vám nabízí rozložení základních ovládacích prvků subsystému IW FTP Client, umožňující snadné ovládání a jeho nastavení. Popis jednotlivých částí následuje.



Obr. 119. IW FTP Client – hlavní okno

• Programová nabídka

Programová nabídka modulu IW FTP Client je tvořena jednotlivými příkazy seskupenými tématicky do skupin. Příkaz je instrukce k proveden í určité činnosti modulu. Většinu obecných příkazů modulu můžete rychle provést pomocí myši tak, že kliknete na požadované tlačítko z nástrojové lišty. Příkazy tvoří skupiny, které jsou umístěny v nabídkách. Některé příkazy provedou požadovanou akci okamžitě, jiné zobrazí dialogové okno, ve kterém pak můžete nastavit požadované volby.

Pokud jste zvolili daný příkaz omylem nebo se příkaz vykonává déle, než jste očekávali, je možné jej přerušit tlačítkem zrušit aktuální příkaz (červený křížek).

Programová nabídka se v modulu IW FTP Client liší v závislosti na nainstalovaných zásuvných modulech (plug-in). Proto prosím pozorně čtěte Nápovědu, aby jste získali přehled, kterého zásuvného modulu se daná nápověda týká. Není-li uveden zásuvný modul (plug-in), pak se jedná o nápovědu platící všeobecně.

- **Menu Hlavní**

Nabídka *Hlavní* nabízí uživateli subsystému IW FTP možnost zobrazit log protokoly, odskoky na asociované programy a vlastní ukončení aplikace.

Otevřít

Toto podmenu nabízí dvě položky:

Nové okno

Příkaz *Nové okno* spustí další IW FTP Client, který, bez ohledu na to, kam je připojen stavajici, nebude připojen nikam.

Kopii aktuálního okna

Příkaz Kopie aktuálního okna spustí IW FTP Clienta a po startu se připojí ke stejnému FTP serveru, k němuž je připojen již aktivní FTP Client. Po připojení je načtena také složka serveru, v níž byl uživatel, když přikaz zadal.

Zobrazit protokol o činnosti

Příkaz *Zobrazit protokol o činnosti* provede otevření **log souboru** ve zvláštním okně. Jedná se o textový soubor (jméno a prohlížeč log souboru lze změnit), ve kterém jsou zaznamenány všechny důležité události v systému, především informace o úspěšném přihlášení se, spojení s FTP serverem, o přenosu dat apod. Každá položka v tomto souboru je opatřena časovým razítkem. Povolení zapisování do *log souboru* najdete v menu *Nastavení - Možnosti* - záložka *Log* . Umístění log souboru lze nastavit v menu *Nastavení - Možnosti* - záložka *Složky a soubory*.

Zobrazit protokol o zabezpečení

Příkaz *Zobrazit protokol o zabezpečení* provede otevření **log souboru** ve zvláštním okně. Jedná se o textový soubor (jméno a prohlížeč log souboru lze změnit), ve kterém jsou zaznamenány všechny důležité události týkající se zabezpečení systému. Každá položka v tomto souboru je opatřena časovým razítkem. Povolení zapisování do *log souboru* najdete v menu *Nastavení - Možnosti* - záložka *Zabezpečení*. Umístění log souboru lze nastavit v menu *Nastavení - Možnosti* - záložka *Složky a soubory*.

WWW Browser

Příkaz *WWW Browser* spustí asociovaný program **WWW prohlížeče** (např. *Microsoft Internet Explorer*), který máte nastavený v menu *Nastavení - Možnosti - záložka Složky a soubory*.

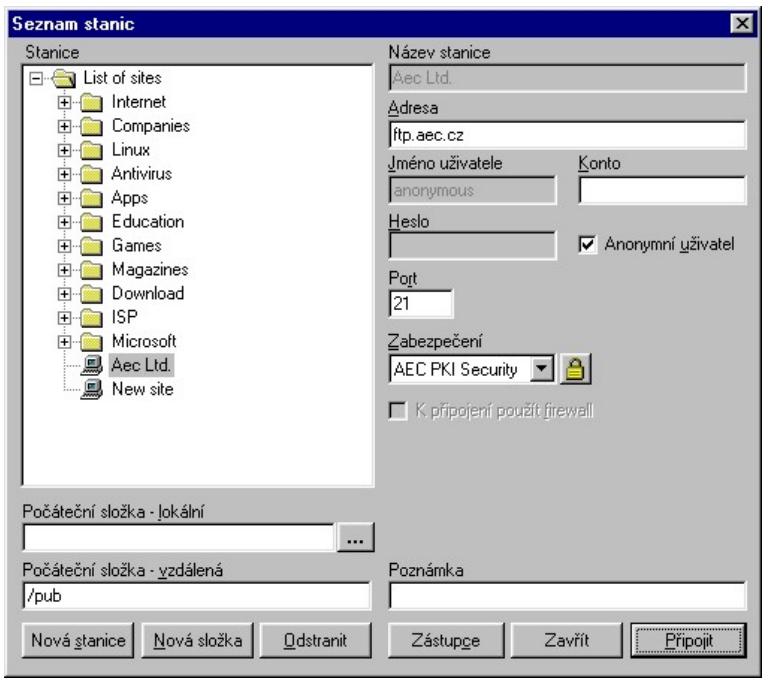
Konec - kliknutím ukončíte program IW FTP Client.

- **Menu Akce**

Nabídka *Akce* umožňuje okamžitě provést všechny operace týkající se událostí - od spuštění přes přerušení až po samotné ukončení akce (události).

- **Připojit**

Kliknutím na tuto volbu dojde k zobrazení dialogového okna, které zobrazí seznam navolených FTP serverů a umožní se připojit na zvolený FTP server.



Obr. 120. IW FTP Client - vytvoření nové položky v seznamu stanic

- **Rychle připojit**

Kliknutím na tuto volbu dojde k zobrazení jednoduchého dialogového okna, které umožní se připojit na zvolený FTP server.

- **Odpojit**

Výběrem této volby dojde k okamžitému rozvázání aktivního spojení na zvolený FTP server. Pokud probíhá přenos souboru, program vyzve k rozhodnutí, zda přerušit stažení přenosu.

- **Přerušit příkaz**

Dojde k přerušení aktuálního příkazu, který je vykonáván.

- **Odeslat soubory**

Máte-li označené nějaké soubory v adresáři lokální stanice a jste-li připojeni k vámi zvolenému FTP serveru kliknutím na tuto volbu dojde k přenosu souboru z aktuální složky lokální stanice do aktuální složky na vzdáleném FTP serveru.

- **Přijmout soubory**

Máte-li vybrané nějaké soubory v adresáři FTP serveru, pak kliknutím na tuto volbu dojde k přenosu souborů z FTP serveru do aktuální složky na lokální stanici.

- **Ruční příjem souboru**

Jste-li připojeni na FTP server, jste vyzváni k zadání cesty a názvu souboru, který chcete přenést na lokální stanici. Nezapomeňte, že všechny použité relativní cesty se vztahují k aktuální složce vzdáleného FTP serveru. Po vyplnění cesty i názvu souboru a kliknutím na tlačítko OK dojde k přenesení zvolného souboru z FTP serveru do aktuální složky na lokální stanici.

- **Ruční odeslání souboru**

Jste-li připojeni na FTP server, jste vyzváni k zadání cesty a názvu souboru, který chcete přenést na vzdálený FTP server. Nezapomeňte, že všechny použité relativní cesty se vztahují k aktuální složce lokální stanice. Po vyplnění cesty i názvu souboru a kliknutím na tlačítko OK dojde k přenesení zvolného souboru z lokální stanice do aktuální složky na vzdálený FTP server

(např. */anonymous/transfer/test.dat* - pak dojde k odeslání souboru *test.dat* z připojeného FTP serveru ftp.aec.cz ze složky *anonymous/transfer*).

- **Zobrazit uvítací hlášení**

Kliknutím otevřete okno, kde dojde k zobrazení posledně přijatého uvítacího hlášení (jedná se o aktuálně, případně naposledy navštíveného FTP serveru).

- **Zobrazit frontu**

Kliknutím otevřete okno, kde dojde k zobrazení aktuální fronty souborů, kterou jste si sami vytvořili.

- **Podrobný výpis složky**

Kliknutím otevřete okno, kde dojde k zobrazení posledně přijatého výpisu naposledy otevřeného adresáře na vzdáleném FTP serveru.

• Menu Nastavení

Nabídka *Nastavení* vám umožní snadno a přesně nakonfigurovat celý systém programu IW FTP Client.

- **Panely nástrojů**

Výběrem této nabídky je vám umožněno modifikovat panely nástrojů v programu IW FTP Client.

K nastavení panelu nástrojů a jeho přizpůsobení uživateli slouží záložky:

Panely nástrojů - definování vzhledu panelu nástrojů na základě přání a potřeb uživatele.

Příkazy - definování vzhledu jednotlivých příkazů z panelu nástrojů na základě přání a potřeb uživatele.

Záložka Panely nástrojů

Výběrem záložky *Panel nástrojů* je vám umožněno modifikovat panely nástrojů v programu IW FTP Client. Objeví se vám dialogové okno, v jehož levé části je zobrazen **seznam** aktuálních a dostupných **panelů nástrojů** (závislé na nainstalovaných zásuvných modulech). Aktivaci panelu (jeho zobrazení v hlavním okně programu IW FTP Client) provedete zaškrtnutím volby u příslušného panelu. Modifikaci vzhledu a chování tlačítek v panelu nástrojů provedete pomocí zatrhnutí voleb:

Zobrazovat popis - po jejím zaškrtnutí se Vám při pohybu myší po ikonách panelů zobrazuje přímo jejich stručný popis.

Vzhled "Cool" - moderní vzhled umožňující alternativní umístění panelu nástrojů.

Velká tlačítka - pokud uživatel dává přednost velkým tlačítkům v panelu nástrojů má možnost tuto vlastnost nastavit zatrhnutím této volby.

Tlačítko *Nový* - přidání nového, uživatelem definovaného panelu nástrojů.

Tlačítko *Výchozí* - po stisknutí tohoto tlačítka se uloží nynější nastavení jako výchozí.

Nastavení panelu nástrojů se ukládá do souboru ftport.ini v hlavním adresáři Windows.

Záložka Příkazy

Záložka *Příkazy* slouží k definování vzhledu jednotlivých příkazů z panelu nástrojů na základě přání a potřeb uživatele.

Můžete zde vybrat kategorii **tlačítek** (danou kategorii panelu nástrojů - liší se nainstalovanými zásuvnými moduly) a následně některé z tlačítek pomocí myši přidat (přetáhnout) do vámi nadefinované tlačítkové lišty. Samozřejmě, že opačný postup (odejmutí požadovaného tlačítka z lišty) je také možný. Po klepnutí myší na některé tlačítko v tomto okně se vám zobrazí jeho popis v sekci *Popis*.

- **Možnosti**

Záložky tohoto menu slouží pro obecné nastavení parametrů programu IW FTP Client, pro uložení cest ke složkám a souborům, nastavení grafických a zvukových parametrů programu, parametrů při startu nebo nastavení Firewall. Najdete zde také definování parametrů pro nastavení zásuvných modulů (plug-in).

Hlavní - nabízí základní modifikace programu IW FTP Client (grafický vzhled oken, formát data, akce na dvojklik myši a co se objeví po startu).

Složky a soubory - slouží k nastavení cest ke složkám včetně názvů souborů k jednotlivým log souborům a k dalším doplňkovým a přidruženým aplikacím.

Zvuky - zde může uživatel určit, zda modul bude či nebude používat zvukové efekty. Dále mu tato záložka usnadňuje správu těchto efektů.

FTP protokol - slouží k předdefinování základních parametrů FTP protokolu.

Firewall - nabízí možnost povolení či zakázání firewallu a jeho obecné nastavení pro připojení a vlastní chod.

Log - kliknutím se nejen zobrazí vlastnosti Log souboru, ale také je možné z této záložky povolit či zakázat logování.

FTP připojení - definice obecných vlastností samotného FTP připojení jako je počet pokusů připojení, doba pro připojení, atd.

ASCII přípony - slouží k definici ASCII přípon, které jsou potřebné k detekci automatického typu přenosu.

FTP konzola - slouží k nadefinování vlastností FTP konzoly.

V případě nainstalovaného zásuvného modulu AEC Security Plug-in:

PKI Zabezpečení - povolení a definování šifrování a komprese přenášených dat v programu IW FTP.

ASCII přípony

Nastavení slouží k definici ASCII přípon, které jsou potřebné k detekci automatického typu přenosu souborů.

ASCII přípona - chcete-li přidat další příponu ASCII vepište ji do kolonky a klikněte na tlačítko *Přidat*. Chcete-li příponu odebrat ze seznamu, označte ji a klikněte na tlačítko *Odstranit*.

Firewall

Záložka *Firewall* slouží k připojení IW FTP klienta k Internetu přes Proxy Server nebo Firewall a nastavení jeho příslušných parametrů.

Používat Firewall - uživatel zatrhne v případě pokud chce přistupovat k Internetu přes Proxy Server nebo Firewall.

Do kolonky *Port* je třeba zadat číslo portu, na kterém pracuje příslušný Proxy server (implicitně **21**)

V sekci *Přihlášení* stanoví uživatel v kolonce *Adresa firewallu* jméno stanice, na které běží Proxy server. K dispozici je také kolonka pro definování přihlašovacího jména uživatele a uživatelského hesla.

V sekci *Typ firewallu* nalezne uživatel čtyři přepínací tlačítka s jednotlivými předvolenými typy Proxy serverů a metod, které používají pro připojení na Internet :

- *SITE adresa* - Proxy server žádá uživatelské jméno a heslo. Nejdříve se uživatel přihlásí na Proxy server a pak teprve je spojení navázáno se vzdáleným počítačem s použitím SITE adresy.

- *USER po přihlášení* - Proxy server žádá jméno uživatele a jeho heslo. Uživatel je přihlášen na Proxy server a spojení se vzdáleným počítačem je navázáno s použitím příkazu USER UserNameOnRemote@RemoteHost.

- *USER bez přihlášení* - Jméno uživatele a jeho heslo se ignorují. USER UsernameOnRemote@RemoteAddress se posílá na Proxy server po úvodním spojení.

- *Proxy OPEN* - žádosti Proxy serveru o uživatelské jméno a heslo jsou ignorovány. OPEN remote_host se posílá Proxy serveru po úvodním spojení.

Příklad:

Například pro proxy server Wingate nebo WinProxy nastavte:

Používat Firewall - zatrhnuto.

Adresa Firewallu - vepište IP stanice, na které je spuštěn Wingate.

V sekci *Typ Firewallu* si vyberte položku *USER bez přihlášení*.

Složky a soubory

V záložce *Složky a soubory* nastavujeme úplnou cestu ke složkám (adresářům), nebo jednotlivým souborům a doplňkovým aplikacím, které je možné spouštět přímo z okna programu IW FTP. K jednoduššímu zadání cesty k souboru využijte tlačítko **„...“** na konci každého vstupního pole.

Popis jednotlivých položek:

Log prohlížeč - uživatel definuje aplikaci, ve které se zobrazují jednotlivé log soubory. Standardně je nastaven zabudovaný prohlížeč, který je součástí programu IW FTP.

Protokol o spojení - uživatel definuje soubor, do kterého se zapisuje detailní protokol o spojení, ukončení spojení, o přihlášení na vyrovnávací FTP server, o přenosu souborů, o spuštění, přerušení a ukončení událostí, atd.

Protokol o zabezpečení - uživatel definuje soubor, do kterého se zapisuje detailní protokol o šifrování a zabezpečovacích funkcích programu IW FTP Client (v případě nainstalovaného zásuvného modulu AEC Security Plug-in).

Výchozí složka pro lokální PC - definice složky lokální stanice, která bude aktivní po spuštění programu IW FTP.

WWW Browser definuje cestu k jakémukoli WWW prohlížeči, který máte nainstalován, a který je potom možné spouštět přímo z okna aplikace IW FTP Client. Zadáním této cesty se stane funkční ikona v panelu nástrojů znázorňující WWW Browser. (např. *Microsoft Internet Explorer*)

Seznam adres stanic - uživatel definuje soubor, do kterého se zapisuje detailní definice parametrů a složek nastavených v seznamu stanic.

FTP protokol

Záložka *FTP protokol* umožňuje předdefinovat obecné vlastnosti FTP protokolu.

Heslo -> Anonymous - do této položky uživatel vepisuje svou e-mail adresu, která bude použita jako heslo v případě použití anonymního přístupu k FTP serveru, vzdálenému počítači (implicitně email@domain.com).

Anonymní konto - položka pro uživatelské jméno v případě anonymního přístupu k FTP serveru (implicitně *anonymous*).

FTP port - číslo FTP portu, na kterém pracuje FTP server (implicitně **21**).

Data Socket Timeout - jde o čas v sekundách potřebný k úspěšnému provedení datových FTP příkazů. Po uplynutí této doby je datový FTP příkaz považován za neúspěšný a program stornuje probíhající krok FTP klienta.

Control Socket Timeout - jde o čas v sekundách potřebný k úspěšnému provedení kontrolních FTP příkazů. Po uplynutí této doby je kontrolních FTP příkaz považován za neúspěšný a program stornuje probíhající krok FTP klienta.

V sekci *Typ přenosu* uživatel definuje pomocí přepínacího tlačítka, jaký typ přenosu souborů zvolit:

- ASCII - lze použít pouze pro textové soubory

- binární - pro všechny soubory kromě textových souborů uložených pod operačním systémem UNIX

- automatický - program rozhodne podle přípony souboru.

V sekci *Velikost bloku* stanoví uživatel velikost bloku v bytech pro **příjem** a **poslání** souborů – při spojení pomocí sítě LAN je možno tuto velikost zvětšit, a tím zrychlit přenos souborů. Doporučená velikost by však neměla přesáhnout 16384 bytů.

Pro přenos dat použít „passive mode"- zatrhnutím této volby bude pro všechny datové přenosy použit **pasivní mód** spojení. V tomto módu vyšle klient serveru příkaz PASV (RFC 967) a provede přímé připojení k serveru na jím zaslaný port. Oproti tomu v případě standardního navazování spojení čeká klient na listen portu na spojení, které zahájí server. Pasivní mód se používá zejména pro připojení přes firewally, které neumožňují zpětné spojení od serveru ke klientovi, nebo pro rychlejší spojení s FTP servery. IW FTP má implementovánu **automatickou detekci** serverů, které pasivní mód nepodporují a při spojení s takovým serverem a zatrhnuté volbě *Pasivní mód* dojde k automatickému dočasnému vypnutí pasivního módu.

Hlavní

Záložka *Hlavní* nabízí základní konfigurace programu IW FTP .

V sekci *Zobrazovat* definujeme vlastnosti okna, ve kterém se systém IW FTP zobrazuje.

Je-li zatrhnuto políčko *Stavový řádek* bude ve spodní části okna IW FTP zobrazen vodorovný pruh - **stavový řádek**. Jsou v něm uvedeny

informace o aktuálním stavu a aktuální čas. Je-li políčko prázdné, stavový řádek se nebude zobrazovat vůbec.

Zatrhnutím políčka *Postupnou výplň* upravuje uživatel vlastnosti záhlaví okna. Je-li zaškrtnuto, záhlaví okna je vyplněno barevným přechodem z černé do modré.

Sekce *Hlavní okno* umožňuje pomocí dvojice přepínacích tlačítek zvolit nastavení velikosti a umístění hlavního okna programu IW FTP Client.

Vybráním tlačítka *Uložit při ukončení* znamená uložení velikosti a umístění okna na obrazovce při správném ukončení IW FTP Client. Při příštím otevření systému IW FTP Client se jeho hlavní okno otevře v takové velikosti a na tom místě, kde jsme ho před ukončením programu zanechali.

Je-li vybrána druhá možnost *Zobrazit s def. parametry* znamená to, že okno se vždy zobrazí v předdefinované velikosti a místě dle aktuálního rozlišení, nezávisle na tom v jakém stavu jsme před tím aplikaci ukončili. Tato varianta se nastaví automaticky vždy při přenastavení rozlišení vlastností monitoru v systému počítače.

Při startu otevřít - po spuštění aplikace IW FTP Client dojde k akci, kterou nadefinujete právě v tomto okně. Na výběr jsou možnosti:

Hlavní okno - standardní nastavení. Program je spuštěn bez jakýchkoliv dialogových oken.

Rychlé připojení - po spuštění se otevře zároveň dialogové okno pro rychlé připojení.

Seznam stanic - po spuštění se otevře zároveň dialogové okno *Seznam stanic*, které umožní vybrat nadefinovaný FTP server se všemi parametry a připojit se.

Akce po dvojím kliknutí - jakmile dojde ke dvojímu kliknutí v okně souborů vzdálené nebo lokální stanice na jednom souboru, pak si lze vybrat z těchto akcí, které mohou nastat:

Otevření souboru - lokální soubor je otevřen asociovanou aplikací v rámci operačního systému , vzdálený soubor je nejprve přenesen do adresáře dočasných souborů operačního systému na lokání stanici a až potom otevřen asociovanou aplikací.

Přenos souboru - pokud je aktivní spojení na FTP server, dojde k přenesení souboru ze vzdálené stanice na lokální stanici do právě otevřené složky nebo naopak, dojde k přenesení souboru z lokální stanice na vzdálený FTP server do aktivní složky.

Přidání do fronty - pokud je aktivní spojení na FTP server, pak je vyvoláno dialogové okno pro přidání souboru do fronty souborů. Aktuální parametry - zdrojový soubor, cílová složka, FTP server, přihlášení na FTP server, ... jsou předány do dialogového okna, kde jsou k dispozici

samozřejmě všechny potřebné parametry k úpravě. Kliknutím na *OK* je soubor přidán do fronty.

Žádná akce - dvojí kliknutí je ignorováno a program neprovede žádnou akci.

Kontrolovat jestli je program předvoleným FTP Klientem - program po spuštění provede kontrolu zda IW FTP je předvoleným FTP klientem.

PKI Zabezpečení

Záložka *PKI zabezpečení* umožňuje volbu šifrovacího algoritmu a hashovací funke pro podpis.

V poli *Přihlášený uživatel* je zobrazeno přihlašovací jméno aktuálního uživatele.

Vybrat algoritmus pro šifrování - v tomto oddílu je možno si pomocí přepínacího tlačítka vybrat z pěti metod šifrování (RC2-40, DES, 3DES, Blowfish, CAST).

Vybrat HASH algoritmus pro podepisování - sekce pro volbu jednocestné funkce (MD5 a SHA-1)

Zvuky

Záložka *Zvuky* umožňuje spravovat zvukové efekty aplikace IW FTP.

Zvukové efekty systému povoluje nebo zakazuje uživatel zatrhnutím kolonky *Povolit používání zvuků.*

K určitým událostem programu IW FTP je možné přiřadit zvukové efekty včetně cesty k nim, jejichž seznam uživatel najde v seznamu *Zvuk*. Tlačítkem *Test* má uživatel možnost přehrát si nadefinované zvuky. Zobrazena je i složka se zvukovými nahrávkami pro danou událost. Jednotlivé zvuky musí být ve formátu **wav.**

Log soubor

Okno nastavení vlastností *Log souboru* zobrazí všechny možnosti vzhledu log souboru.

Zatrhnutím kolonky *Povolit zápis do Log souboru* se povoluje nebo zakazuje ukládání informací o průběhu jednotlivých událostí do log souboru. Název a cestu k tomuto log souboru definujeme na záložce *Složky a soubory*.

Pokud je zatrhnuta položka *Mazat Log okno před novým spojením*, pak dojde před spuštěním jakékoliv události vymazáno Log okno.

Jestliže zatrhnete položku *Automaticky zkracovat velikost*, pak lze definovat velikost (v bytech) Log souboru. *Maximální velikost* určuje největší možnou velikost Log souboru. V případě, že je velikost překročena, je

soubor automaticky redukován na velikost souboru, která je definována v kolonce *Zkrácená velikost. Zobrazovat* - definujete počet zobrazovaných řádků v Log okně aplikace IW FTP. Vždy je zobrazeno *n* nadefinovaných posledních řádků z log souboru.

V sekci *Typ zápisu* je k dispozici volba formy zápisu log souboru z hlediska podrobnosti zápisu, k dispozici jsou *Zjednodušený*, *Podrobný* a *Debug*. Jako výchozí hodnota je přednastavena *Podrobný*, který plně vyhovuje standardnímu výpisu funkcí programu IW FTP a vystačuje svým výpisem administrátorům programu IW FTP.

Nevyhovují-li vám barvy okna log souboru, máte možnost nadefinovat svůj vlastní barevný vzhled okna Log souboru v sekci *Barvy* u položek jako je písmo, podklad a čas zápisu události.

Font - možnost změny fontu, řezu a velikosti písma v Log okně.

Ve spodní části okna vlastností log souboru jsou k dispozici informace o umístění a velikosti log souboru.

FTP konzola

Záložka *FTP konzola* slouží k definování vlastností FTP konzoly.

Max. velikost cache paměti - v bajtech maximální velikost paměti pro FTP konzolu.

V sekci *Barvy* máte možnost si určit barevné vlastnosti *Písma* a *Podkladu* FTP konzoly.

Font - po kliknutí se otevře standardní dialogové okno pro výběr fontu, řezu a velikosti písma, které se má zobrazovat ve složce FTP konzoly.

FTP připojení

Na záložce *FTP připojení* jsou k nalezení obecné vlastnosti samotného FTP připojení jako je počet pokusů připojení, doba pro připojení, atd.

V sekci *Připojování* máte možnost nadefinovat v sekundách *Dobu pro připojení*. Jedná se o čas, po který se IW FTP snaží připojit na FTP server, vzdálenou stanici. Kolik pokusů pro připojení po prvním neúspěšném program IW FTP má nastavíte v kolonce *Pokusů*.

Zobrazovat uvítací hlášení - je-li zatrhnuto, pak po úspěšném přihlášení na FTP server aplikace IW FTP oznámí uživateli uvítací hlášení aktuálně připojeného FTP serveru.

Po přihlášení přepnout do složky - chcete-li, aby po úspěšném přihlášení na FTP server se změnila složka vzdáleného FTP serveru, vepište ji zde. Pokud chcete po každém přihlášení specifickou (jinou) složku pro daný FTP server, použijte pro definici složek dialogové okno Seznam stanic.

Potvrzování - tato záložka umožňuje uživateli, výběr varování, která se mu budou zobrazovat.

Uživatel si zde může určit, která varování pokládá za důležitá a chce tudíž, aby se mu zobrazovala, a která naopak zobrazovat nechce.

Dotazovat se na přepsání souborů při odesílání (upload) – upozorní uživatele, že soubor, který odesílá na server, má stejný název jako soubor, který na serveru již existuje, a umožní mu jej přepsat, napojit, nebo zrušit akci.

Dotazovae se na přepsání souborů při příjmu (download) - upozorní uživatele, že soubor, který přijímá, má stejný název jako soubor, který již existuje, a umožní mu jej přepsat, napojit, nebo zrušit akci.

Dotazovat se před vymazáním souboru – uživatel je požádán o potvrzení akce při každém mazání souboru.

Dotazovat se před vymazáním složky – uživatel je požádán o potvrzení akce při každém mazání složky.

Dotazovat se před ukončením spojení – před zrušením spojení je uživatel požádán o potvrzení akce.

Dotazovat se před přerušením přenosu – před přerušením přenosu souboru je požadováno potvrzení tohoto kroku.

Dotazovat se před aut. ověřováním zabezpečených souborů

Varovat při ukončení programu, jestliže fronta obsahuje soubory – pokud se uživatel rozhodne ukončit IW FTP Client a fronta souborů obsahuje ještě nepřenesené položky, je na tuto skutečnost upozorněn a požádán o potvrzení či zrušení akce.

• Menu Nápověda

Nabídka *Nápověda* vám nabídne přehlednou nápovědu, spojí vás na on-line podporu nebo vás informuje o nainstalovaných zásuvných modulech.

Obsah - příkaz, který zobrazí úvodní stránku nápovědy.

Jak používat nápovědu - po stisknutí této nabídky se zobrazí okno sloužící k seznámení se s používáním nápovědy.

Tipy pro práci s programem - po stisknutí této nabídky se zobrazí okno, kde se objeví tip dne, který informuje uživatele o možnostech systému IW FTP. Další tip je možné zobrazit kliknutím na tlačítko *Další tip*.

Technická podpora – Email - kliknutím spustíte svého předvoleného poštovního klienta. Automaticky vepsaná e-mail adresa vám umožní se okamžitě dotázat na vše, co se týká programu IW FTP. Než nám napíšete, prostudujte prosím velmi pečlivě tuto nápovědu.

O aplikaci - po kliknutí se otevře okno, které vás bude informovat o systému

• Panely nástrojů

Oproti IronWare® Security Suite verze 7.0 je zde nový panel nástrojů, který usnadňuje uživateli připojování k různým FTP serverům.

Obr. 121. IW FTP Client - panely nástrojů

tento nástroj se skládá ze dvou částí. První je seznam umožňující výběr FTP stránky z nabídky a druhou část tvoří tlačítko Jdi, které konektuje IW FTP Client na danou adresu.

také tento nástroj má dvě části. Do první se zadává FTP adresa, nebo se pomocí seznamu volí některá z dříve použitých adres. Druhou část tvoří tlačítko Jdi, které provede spojení na danou adresu. Při použití tohoto nástroje je uživatel automaticky přihlášen jako anonymní uživatel.

Aby tento nástroj korektně fungoval je nutné, aby byl nainstalován Internet Explorer verze 4.0 či vyšší.

Připojit – toto tlačítko vyvolá okno *Seznam stanic*, kde je uživateli nabídnut seznam pamatovaných FTP adres, správa těchto adres a možnost připojení ke kterékoliv z nich.

Rychle připojit – tato ikona vyvolá okno *Rychlé připojení*, odkud se uživatel může po zadání patřičných údajů připojit k FTP serveru.

Odpojit – kliknutím na toto tlačítko buď dojde k přerušení aktuálního spojení, nebo (je – li nastaveno) se zobrazí upozornění, že připojení je stále aktivní a zda má opravdu být zrušeno a teprve pak se na přání uživatele přeruší.

Přerušit příkaz – tento příkaz přeruší vykonávání aktuálně prováděného příkazu.

 *Nastavení* – kliknutí vyvolá okno *Nastavení* se všemi záložkami.

 *Prohlížet Log* – příkaz zavolá nastavený editor a otevře v něm log soubor.

 *O úroveň výš* – změní aktuální složku na lokání stanici nebo na serveru o jednu úrověň nahoru.

 *Přijmout označené soubory* – přijme označené soubory ze serveru na lokální stanici.

 *Odeslat označené soubory* – pošle označené soubory z lokální stanice na server.

 *WWW Browser* – spustí zvolený prohlížeč webovských stránek

 *Kontextová nápověda* – tato volba přidá ke kurzoru myši otažník a čeká na určení tématu požadované nápovědy. Poté, má – li toto téma k dispozici, otevře příslušnou stránku nápovědy, pokud nemá téma k dispozici, otevře úvodní stránku se seznamem témat.

 *Obsah nápovědy* – vyvolá úvodní stránku nápovědy se seznamem témat.

- **Okno lokálních složek (vlevo)**

Okno lokálních složek je věrným grafickým obrazem seznamu všech složek vaší lokální stanice (vašeho lokálního PC). Slouží k zobrazení jednotlivých podsložek a souborů vzhledem k vybrané složce. Také slouží k vytvoření, odstranění, přejmenování a přesunu vybrané složky z lokální na vzdálenou stanici a samozřejmě k vlastnímu pohybu mezi jednotlivými složkami na straně lokální stanice. Pokud daná složka obsahuje jakýkoliv soubor, soubory z vybrané složky jsou zobrazeny v okně lokálních souborů.

 Vybranou složkou se rozumí aktuální složka vašeho počítače. K vybrané složce se vztahují veškeré vlastnosti popsané na této stránce nápovědy.

Kliknutí pravým tlačítkem myši na složku vyvolá nabídku těchto příkazů:

Odeslat - odešle vybranou složku včetně podsložek a souborů do aktuální složky na připojeném FTP serveru.

Nová složka - kliknutím vytvoříte novou složku ve vybrané složce na straně lokální stanice. Zároveň je vám automaticky nabídnuto pojmenování této složky.

Odstranit složku - dojde k odstranění vybrané složky včetně všech podsložek a souborů, které ji tvoří.

Změnit složku - do dialogového okna vepište celou cestu včetně disku ke složce (absolutně i relativně), na kterou chcete změnit aktuální složku lokálního počítače.

Přejmenovat složku - po kliknutí je vám nabídnuto přejmenování vybrané složky.

Obnovit - dojde k aktualizování celé struktury lokální stanice.

• Okno lokálních souborů (vlevo dole)

Okno lokálních souborů je věrným grafickým obrazem obsahu vybrané složky lokální stanice. Slouží k zobrazení obsahu vybrané složky (viz Okno lokálních složek). Také je určeno k otevření, zobrazení, odstranění, přejmenování a přesunu vybraného souboru z lokální na vzdálenou stanici.

Vybraným souborem se rozumí označený soubor ve vybrané složce souborů. Označit soubory lze standardním způsobem jako v celém operačním systému Windows:

Kliknutí na jednu položku - označení jednotlivého souboru.

Podržení klávesy CTRL + kliknutí na položku - vybírám, označuji (případně odebírám) soubory.

Podržení klávesy SHIFT + kliknutí na položku - vybereme skupinu souborů.

Kliknutí pravým tlačítkem myši na soubor vyvolá nabídku těchto příkazů:

Odeslat ručně - do dialogového okna vepište název, případně i cestu k souboru (relativní nebo absolutní k vybrané složce), který chcete odeslat z lokální stanice do aktuální složky na připojený FTP server.

Zobrazovat - v nabídce je možné soubory zobrazit jako velké nebo malé ikony nebo jako seznam či detaily.

Seřadit - seřadit soubory lze podle názvu, velikosti i data souboru.

Obnovit - dojde ke znovunatažení (refresh) vybrané složky lokální stanice.

Pokud je vybrán alespoň jeden soubor, pak se nabídka příkazů rozšíří:

Odeslat - odešle vybrané soubory do aktuální složky na FTP serveru.

Přidat do fronty - vybrané soubory jsou nabídnuty k přidání do fronty souborů. Kliknutím je vyvoláno okno Parametry přenosu souboru.

Otevřít - vybraný soubor nebo první ze skupiny vybraných souborů, je otevřen v asociované aplikaci.

Zobrazit - vybraný soubor nebo první ze skupiny vybraných souborů, je zobrazen v prohlížeči souborů.

Odstranit - dojde k odstranění vybraných souborů.

Přejmenovat - po kliknutí je vám nabídnuto přejmenování vybraného souboru.

Vlastnosti - kliknutím se zobrazí okno vlastností vybraného souboru, informující o umístění, velikosti, datu, atributech a názvu souboru.

- **Okno vzdálených složek (vpravo)**

Okno vzdálených složek je věrným grafickým obrazem všech složek vzdálené stanice, FTP serveru. Slouží k zobrazení jednotlivých podsložek a souborů vzhledem k vybrané složce. Také slouží k vytvoření, odstranění, přejmenování a přesunu vybrané složky z FTP serveru na lokální stanici a samozřejmě k vlastnímu pohybu mezi jednotlivými složkami na straně FTP serveru. Pokud daná složka obsahuje jakýkoliv soubor, soubory z vybrané složky jsou zobrazeny v okně vzdálených souborů.

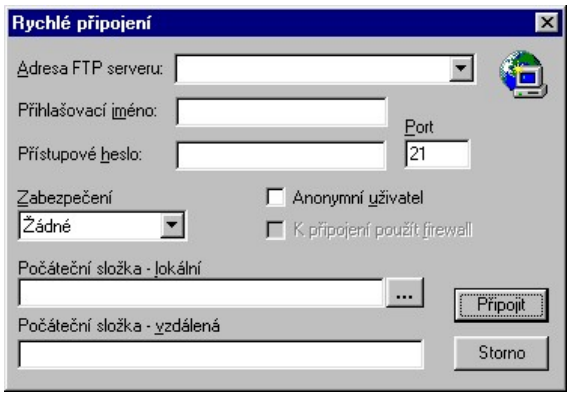
Vybranou složkou se rozumí aktuální složka FTP serveru. K vybrané složce se vztahují veškeré vlastnosti popsané na této stránce nápovědy.

Kliknutí pravým tlačítkem myši na složku vyvolá nabídku příkazů, která je závislá na tom, zda jste připojeni na FTP server či nikoliv.

- **Aplikace není připojena na FTP server**

Připojit - kliknutím na tuto volbu dojde k zobrazení dialogového okna, které zobrazí seznam navolených FTP serverů a umožní se připojit na zvolený FTP server.

Rychle připojit - kliknutím na tuto volbu dojde k zobrazení jednoduchého dialogového okna, které umožní připojit se na zvolený FTP server.



Obr. 122. IW FTP Client – rychlé připojení

- **Aplikace je připojena na FTP server**

Přijmout - odešle vybranou složku včetně podsložek a souborů do aktuální složky na lokální stanici.

Nová složka - kliknutím vytvoříte novou složku ve vybrané složce na straně FTP serveru. Zároveň je Vám automaticky nabídnuto pojmenování této složky.

Odstranit složku - dojde k odstranění vybrané složky včetně všech podsložek a souborů, které ji tvoří.

Změnit složku - do dialogového okna vepište cestu ke složce (relativně či absolutně k aktivní složce), na kterou chcete změnit aktuální složku vzdálené stanice, FTP serveru.

Přejmenovat složku - po kliknutí je vám nabídnuto přejmenování vybrané složky.

Obnovit - dojde ke znovunatažení (refresh) celé struktury FTP serveru, vzdálené stanice.

- **Okno vzdálených souborů (vpravo dole)**

Okno vzdálených souborů je věrným grafickým obrazem obsahu vybrané složky vzdálené stanice. Slouží k zobrazení obsahu vybrané složky (viz okno vzdálených složek). Také je určeno k otevření, zobrazení, odstranění, přejmenování a přesunu vybraného souboru ze vzdálené na lokální stanici.

Vybraným souborem se rozumí označený soubor ve vybrané složce souborů. Označit soubory lze standardním způsobem, jako v celém operačním systému Windows.

Kliknutí na jednu položku - označení jednotlivého souboru.

Podržení klávesy CTRL + kliknutí na položku – kliknutím vybírám, označuji (případně odebírám) soubory.

Podržení klávesy SHIFT + kliknutí na položku - vybereme skupinu souborů.

Kliknutí pravým tlačítkem myši vyvolá nabídku příkazů, která je závislá na tom, zda jste připojeni na FTP server či nikoliv:

- **Aplikace není připojena na FTP server**

Připojit - kliknutím na tuto volbu dojde k zobrazení dialogového okna, které zobrazí seznam navolených FTP serverů a umožní se připojit na zvolený FTP server.

Rychle připojit - kliknutím na tuto volbu dojde k zobrazení jednoduchého dialogového okna, které umožní se připojit na zvolený FTP server.

- **Aplikace je připojena na FTP server**

Přijmout ručně - do dialogového okna vepište název, případně i cestu k souboru (absolutní nebo relativní vzhledem k vybrané složce), který chcete odeslat z FTP serveru do aktuální složky na lokální stanici.

Zobrazovat - v nabídce je možné soubory zobrazit jako velké nebo malé ikony nebo jako seznam či detaily.

Seřadit - seřadit soubory lze podle názvu, velikosti i data souboru.

Obnovit - dojde ke znovunatažení (refresh) vybrané složky vzdálené stanice, FTP serveru

Pokud je vybrán alespoň jeden soubor, pak se nabídka příkazů rozšíří:

Přijmout - odešle vybrané soubory do aktuální složky na lokální stanici.

Přidat do fronty - vybrané soubory jsou nabídnuty k přidání do fronty souborů. Kliknutím je vyvoláno okno s parametry přenosu souboru.

Otevřít - vybraný soubor je přenesen na lokální stanici, a poté je otevřen v asociované aplikaci.

Zobrazit - vybraný soubor nebo první ze skupiny vybraných souborů je přenesen na lokální stanici, a poté je zobrazen v prohlížeči souborů.

Odstranit - dojde k odstranění vybraných souborů.

Přejmenovat - po kliknutí je vám nabídnuto přejmenování vybraného souboru.

Vlastnosti - kliknutím se zobrazí okno vlastností vybraného souboru, informující o umístění, velikosti, datu, atributech a názvu souboru.

• Okno log souboru

V dolní části základního okna je zobrazen aktuální log soubor, do kterého se podrobně zapisují všechny události probíhající v aplikaci IW FTP, takže uživatel má vždy dokonalý přehled, co se kdy v systému stalo. Zobrazit kompletní protokol událostí lze zobrazit pomocí nabídky *Hlavní - Zobrazit protokol o činnosti*.

Log soubor zaznamenává veškeré události a akce spojené s činností subsystému od jeho spuštění, přes aktivaci jednotlivých událostí, vlastní přenos dat až po ukončení aplikace.

Po kliknutí pravým tlačítkem myši v okně *Log soubor* se objeví nabídka *Zobrazit Log soubor* - příkaz provede otevření log souboru ve zvláštním okně. Jedná se o textový soubor (jméno a prohlížeč log souboru lze změnit), ve kterém jsou zaznamenány všechny důležité události v systému, především informace o úspěšném přihlášení se, spojení s FTP serverem, přenosu dat apod. Každá položka v tomto souboru je opatřena časovým razítkem. Povolení zapisování do log souboru najdete v menu *Nastavení - Možnosti*. - záložka *Log*. Umístění log souboru lze nastavit v menu *Nastavení - Možnosti* - záložka *Složky a Soubory*. Vlastnosti Log souboru viz níže.

Vymazat Log okno - příkaz provede vymazání okna Log souboru. Vlastní Log soubor zůstává samozřejmě zachován.

Vlastnosti - kliknutím zobrazíte vlastnosti log souboru.

Povolit, případně zakázat zapisování do log souboru lze v nastavení subsystému IW FTP v záložce *Log*.

Vlastní cestu k protokolu o činnosti (log souboru) lze nadefinovat v menu *Nastavení - Možnosti* - záložka *Složky a soubory*.

• Okno FTP konzola

Okno FTP konzola je na jedné ze dvou záložek ve spodní části aplikace IW FTP. FTP konzola slouží k přímému posílání FTP příkazů na vzdálený FTP server, a proto je pro její plné využití nutná znalost FTP.

Není možné současně pracovat v Log okně a v FTP konzole. Pokud pracujete s FTP konzolou, nedochází k její synchronizaci s oknem vzdálených souborů a oknem vzdálených složek! Je ale možné navázat příkazy v FTP konzole na již otevřený FTP server.

Kliknutím pravého tlačítka v okně FTP konzoly:

Vymazat okno konzoly - příkaz vymaže okno FTP konzoly.

Vlastnosti - kliknutím spustíte dialogové okno vlastností FTP konzoly.

Některé standardní FTP příkazy používané programem IW FTP, všechny používané příkazy zobrazíte zadáním příkazu help :

open ftp_server - otevře spojení na FTP server ftp_server .

bye - uzavře spojení na aktivní FTP server.

user ‚uživatel' - jméno uživatele ‚uživatel', kterým se přihlašujete na daný FTP server.

pass heslo - heslo jména uživatele heslo, kterým se přihlašujete na daný FTP server, vzdálenou stanici.

cd - změna složky na vzdáleném FTP serveru se známými parametry.

ls - vylistování aktuální složky FTP serveru.

pwd - informace o aktuální složce FTP serveru.

delete ‚jméno_souboru' - smazání souboru ‚jméno_souboru' ze vzdáleného FTP serveru.

• Stavový řádek

Stavový řádek, který je umístěn ve spodní části IW FTP Client, obsahuje následující informace o událostech probíhajících v modulu IW FTP Client:

Ikona fronty souborů - zobrazuje stav fronty souborů pro příjem a odeslání (prázdná nebo naplněna alespoň jedním souborem).

Informace o aktuálním FTP spojení - informuje, zda je připojen lokální počítač na vzdálený FTP server a dobu připojení či není.

Ikona uživatele - grafické zobrazení "typu" připojeného uživatele. Program identifikuje, zda jste se přihlásil jako host nebo jste byl FTP serverem autentizován, zda používáte IW FTP Server atd.

Informace o aktuálně prováděném FTP příkazu - pokud program provádí FTP příkaz, je zobrazena informace *Pracuje* a zároveň čas prováděné operace. Pokud program čeká na FTP příkaz od klienta, pak je zobrazena informace *Připraven*.

Pokud program provádí jakýkoliv FTP příkaz, není schopen provádět další příkazy zadané uživatelem.

Informace o aktuálním času lokálního počítače - zobrazení aktuálního času počítače.

• Odeslání šifrovaného souboru

V nabídce pamatovaných adres je možné si pro jednotlivé adresy určit, zda bude či nebude používán při komunikaci se serverem některý z prvků bezpečnosti nabízený IW FTP Clientem. Pokud si uživatel přeje použít některý z bezpečnostních prvků, nastaví v poli *Zabezpečení* volbu *AEC C-PKI Security*. Poté se vedle pole objeví ikona  . Kliknutím na tuto ikonu se otevře okno *C-PKI Protection*.

V poli *Jméno stránky* je napsáno jméno stránky (FTP serveru), k níž se nastavení vztahuje.

V sekci *On-line zabezpečení* je možné povolit či zakázat používání šifrovaného tunelu pro dané spojení mezi IW FTP Clientem a IW FTP Serverem. Pro šifrované spojení je nutné navolit certifikát serveru a soukromý klíč patřící uživateli.

V sekci *Off-line zabezpečení* má uživatel možnost použít šifrování, podepisování nebo kompresi, může povolit nebo zakázat automatické rozšifrování přijímaných souborů a zobrazení dialogu před každým přenosem. Pro šifrování je nutné vybrat některý z certifikátů příjemce a pro podepisování soukromý klíč. Toto nastavení slouží pro posílání souborů mezi dvěma uživateli přes anonymní FTP server. Jeden z nich pošle na předem smluvenou adresu soubor(y) a druhý si je na daném místě vyzvedne. Pokud je soubor podepsaný, umožňuje to příjemci ověřit si kromě odesilatele také neporušenost tohoto souboru. Šifrování zabrání ostatním uživatelům v přístupu k datům, která jsou v posílaných souborech umístěna, a komprese slouží ke kompenzaci nárustu velikosti souboru při operacích zajišťujících bezpečnost. Aby si adresát mohl soubory stahovat a uvést je do původního stavu musí mít IW FTP Client.

- **Přijetí šifrovaného souboru**

Při přijetí zašifrovaného souboru, který je určen pro vás, je soubor automaticky odšifrován a o podpisu (je-li) je vydáno potvrzení, je-li platný či nikoliv. Stejně tak platnost podpisu potvrzuje neporušenost souboru.

- **Navázání šifrovaného tunelu a autentizace**

Autentizované spojení mezi klientem a serverem, zabezpečené šifrovaným tunelem se ustaví, pokud je zaškrtnuta volba *Použít šifrovaný tunel* v nastavení stanice a/nebo je-li tato funkce vyžadována nastavením účtu na straně serveru. Takové spojení je možné pouze mezi IW FTP Clientem a IW FTP Serverem. Ustavení autentizovaného spojení a šifrovaného tunelu je indikováno ikonou v dolním stavovém řádku.

• Nejčastější problémy a jejich řešení

Nenajdete-li zde odpověď na svou otázku, projděte prosím pozorně Nápovědu. Další Otázky a odpovědi najdete také na WWW stránce http://www.aec.cz, případně pošlete svůj dotaz na e-mail adresu support@aec cz.

OTÁZKA:

Jak nastavit telefonické připojení sítě?

ODPOVĚĎ:

Pro správný běh modulu je nutné, abyste měli na svém počítači nainstalovaný TCP/IP protokol (přenos prostřednictvím FTP není bez tohoto protokolu možný). Přistupujete-li navíc k Internetu prostřednictvím telefonní linky, musíte mít ještě připojený a správně nakonfigurovaný modem a telefonické připojení sítě.

Ve složce *Tento počítač* zvolíme *Ovládací panely* a v nich ikonu *Přidat nebo ubrat programy*. Přepneme se do záložky *Systém*. Zvolíme položku *Komunikace* a v ní musíme zatrhnout *Telefonické připojení sítě*. Instalaci zahájíme stiskem tlačítka *OK* a po jejím úspěšném ukončení jsme vyzváni k restartu počítače.

Dále musíme vytvořit nové telefonické připojení (složka *Tento počítač* - *Telefonické připojení* - *Vytvořit nové připojení*). Po zahájení tvorby nového připojení zadáme název volaného počítače (pod tímto názvem se vám vytvoří nové telefonické připojení) a vybereme ze seznamu modemů používaný modem. Stiskem tlačítka *Další* se posuneme do dalšího okna, kde zadáme UTO a telefonní číslo k ISP a vybereme směrové číslo země (Česká republika 420). Vytváření dokončíme stiskem tlačítka *Dokončit*.

Takto vytvořené připojení je nutné ještě správně nakonfigurovat. To provedeme tak, že klikneme pravým tlačítkem myši na ikonu právě vytvořeného telefonického připojení ve složce *Telefonické připojení sítě* a ze zobrazeného kontextového menu zvolíme položku *Vlastnosti*. Máme zde možnost nakonfigurovat jak modem, tak i ve složce *Typy serverů* i nastavení TCP/IP. Informace potřebné k nastavení typu serverů a TCP/IP získáte od svého poskytovatele Internetu.

OTÁZKA:

Jak nainstalovat TCP/IP protokol?

ODPOVĚĎ:

Pro správný běh subsystému je nutné, abyste měli na svém počítači nainstalovaný TCP/IP protokol (přenos prostřednictvím FTP není bez tohoto protokolu možný). Přistupujete-li navíc k Internetu prostřednictvím telefonní linky, musíte mít ještě připojený a správně nakonfigurovaný modem a telefonické připojení sítě.

Ve složce *Tento počítač* zvolíme *Ovládací panely* a v nich *Síť*. Není-li v okně s názvem *Následující součásti sítě jsou nainstalovány:* vypsán protokol TCP/IP, musíme ho přidat. Provedeme to stiskem tlačítka *Přidat* v záložce *Konfigurace* okna *Síť*. Vybereme druh síťové součásti, který chceme instalovat - tedy *protokol* a opět stiskneme tlačítko *Přidat*. Zvolíme nejprve výrobce, od kterého chceme protokol instalovat - *Microsoft* a z dostupných síťových protokolů zvolíme TCP/IP. Instalace je zahájena stiskem tlačítka *OK*. Po dokončení instalace a restartu počítače je protokol připraven k použití.

OTÁZKA:

Jak nainstalovat modem?

ODPOVĚĎ:

Po připojení modemu na sériový port počítače a zapnutí modemu můžeme nainstalovat ovladače potřebné k jeho správné funkci. Ve složce *Tento počítač* zvolíme *Ovládací panely* a v nich *Přidat nový hardware*. Tím se spustí průvodce přidáváním hardware, který vám pomůže nainstalovat buď standardní ovladač ze systému Windows nebo vybrat ze seznamu alternativních ovladačů případně nainstalovat ovladač z diskety dodávané výrobcem modemu. Stejného výsledku dosáhneme po kliknutí na *Přidat* ve složce *Modemy*, kterou také najdeme ve složce *Ovládací panely*.

OTÁZKA:

Kde najít další informace o produktu, případně nové verze modulu IW FTP Client?

ODPOVĚĎ:

Nové verze modulu IW FTP Client budou umístěny na našem WWW serveru, FTP serveru AEC a jejích partnerů. Můžete také samozřejmě zaslat své dotazy na e-mail adresu support@aec.cz

Klíče – Klíčová infrastruktura plně pracuje s PKI.

Šifrovaný tunel – je používán pro bezpečné navázání šifrovaného spojení mezi IW FTP Clientem a Serverem a mezi FTP ovládací konzolou a FTP serverem.

Audit log – logy pro komunikační programy jsou nezávislé na PKI.

• Použití šifrovaného tunelu a autentizace

Pro zajištění bezpečnosti při přihlašování uživatele na FTP server je možno použít autentizace pomocí certifikátu/soukromého klíče.

A. K bezpečné autentizaci uživatele pomocí certfikátu/soukromého klíče je nutno vykonat následující kroky pro nastavení klientské aplikace.

Jako klientskou aplikaci je nutno použít IW FTP Client.

A.1. Nastavení programu **IW FTP Client**

1. Pomocí IW KeyManageru vygenerujte soukromý klíč uživatele.

2. Vyexportujte certifikát uživatele z vygenerovaného soukromého klíče. Tento certifikát předejte administrátorovi serveru nebo pokud jste administrátor, naimportujte jej do PKI IW FTP Serveru.

3. Naimportujte do Vašeho PKI certifikát serveru, který získáte od administrátora IW FTP Serveru.

4. V menu *Akce - Připojit* - záložka *Stanice* vyberte "Certifikát serveru pro autentizaci" a „Soukromý klíč pro autentizaci“

Použitá terminologie

V tomto článku si vysvětlíme základní pojmy a termíny používané v tomto dokumentu nebo související s bezpečností přenosu informací.

Autentizace

je proces ověření totožnosti někoho nebo něčeho. Autentizace je kritická pro čestný a důvěryhodný průběh komunikací. Je to proces, pomocí něhož jedna strana (ověřovatel) získává ujištění, že identita druhé strany (žadatel, prokazující strana) je ta, jaká je deklarována. Cílem je zabránit záměně stran. Nejčastější technikou je, že ověřující strana prověří správnost zprávy, která demonstruje, že žadatel vlastní tajemství, které je asociováno se správnou stranou.

Elektronický podpis

verifikuje obsah zprávy a identitu podpisující strany. Dává zároveň záruky v tom směru, že aktuální dokument byl zaslán konkrétní vysílající stranou (a kterou). Tato vlastnost je známá jako nepopiratelnost. Ke generování podpisu je používána bezpečná matematická funkce (hashovací funkce) a neexistuje způsob (pro třetí stranu), jak využít digitální podpis z jednoho dokumentu k podepsání jiného dokumentu. Nejmenší změna v podepsaném dokumentu zapříčiní, že proces verifikace podpisu neproběhne.

Hashovací funkce

je matematická funkce, která má za vstup řetězec znaků proměnlivé délky, a tento přetváří na výstupní řetězec pevné délky (obvykle 128 či 160 bitů), kterému se také říká hodnota hashe. Je výpočetně obtížné (prakticky neuskutečnitelné) nalézt dvě různé zprávy s toutéž hodnotou hashe.

Komprese

slouží pro zmenšení velikosti posílané zprávy a tím ke zkrácení doby nutné pro přenos. Komprese se provádí před zašifrováním přenášených dat.

Kryptografický protokol

je sdílený algoritmus definovaný posloupností kroků, které precizují aktivity vyžadované na dvou či více entitách s cílem dosáhnout určitého bezpečnostního cíle. Tento algoritmus využívá kryptologické transformace (někdy se používá i pojem autentizační protokol či protokol typu výzva-odpověď). Účelem (cílem) kryptografických protokolů bývá: autentizace účastníků protokolu, utvoření dohody o kryptografickém klíči, výměna těchto klíčů apod.

Šifrování

je založeno na dvou komponentách - šifrovacím algoritmu a klíči.

Šifrovací algoritmus

je matematická funkce, která převádí srozumitelný text (otevřený text) na nesrozumitelný šifrovaný text. K zašifrování otevřeného textu používají šifrovací algoritmy jako vstup klíč. Jak klíč, tak použitá funkce, jsou kritické pro šifrování. V současné době se používají dvě základní třídy šifrovacích algoritmů: symetrické a asymetrické.

Symetrické šifrovací algoritmy

používají tentýž klíč jak pro šifrování, tak i pro dešifrování (při dešifrování je použita inverzní funkce). Hlavním problémem kryptografie využívající symetrické šifry je klíčové hospodářství (generování, přenos a uchovávání kryptografických klíčů). Všechny klíče zde musí zůstat utajeny, aby bylo zajištěno, že třetí neoprávněná strana nemůže použít klíč k dešifrování tajných zpráv. V systémech s velkým počtem uživatelů je problematika distribuce klíčů (pokud využíváme pouze prostředky na bázi symetrických šifer) velmi obtížně řešitelný problém.

Asymetrické šifrovací algoritmy (systémy s veřejným klíčem)

používají pro šifrování a dešifrování vždy různé části klíče. Jedna část klíče se nazývá veřejným klíčem (ten je součástí certifikátu), druhá soukromým klíčem. Obvykle první z těchto klíčů je zveřejněn pro někoho, kdo ho použije k zašifrování dat pro konkrétního příjemce, zatímco druhý klíč je tímto příjemcem utajován. Výsledkem je vytvoření bezpečné cesty pro výměnu kryptografických klíčů (např. pro symetrické šifrování). Veřejné klíče musí být asociovány se svými uživateli důvěryhodnou vhodně autentizovanou cestou. Systémy s veřejným klíčem jsou význačně pomalejší než symetrické šifry. Z hlediska svých unikátních vlastností tvoří však jejich vhodný doplněk. Jsou zejména používány k přenosu klíčů, k vytváření digitálních podpisů, jsou vhodným prostředkem při konstruování řady kryptografických protokolů.

Šifrovací klíč

můžeme chápat jako konstantu, kterou používá šifrovací algoritmus při šifrování dat. Počet možných klíčů každého algoritmu závisí na počtu bitů klíče.

Soukromý klíč

je utajovaná část klíčové dvojice systému s veřejným klíčem. Slouží k dešifrování zpráv zašifrovaných veřejným klíčem. Používá se také pro vytvoření podpisu zprávy, která bude posílána. Podpis lze ověřit veřejným klíčem vysílající strany.

Veřejný klíč

musí být k dispozici straně, která zasílá zprávu majiteli klíče. Klíč slouží k zašifrování této zprávy. Zpráva je pak dešifrována soukromým klíčem.

Digitální certifikát

označuje vlastníka veřejného klíče. Dovoluje verifikaci tvrzení, že daný veřejný klíč patří skutečně danému jedinci. Certifikáty pomáhají chránit se před možností, že někdo falzifikuje klíč s cílem vydávat se za někoho jiného. Ve své nejjednodušší podobě obsahují certifikáty veřejný klíč a jméno. Tak, jak jsou certifikáty obecně užívány, obsahují rovněž:

- dobu vypršení platnosti
- jméno certifikující autority, která vydala certifikát
- pořadové číslo
- nejdůležitější je digitální podpis vydavatele certifikátu

Nejrozšířenější akceptovaný formát pro certifikáty je definován mezinárodní normou X.509. Tyto certifikáty mohou být pak čteny či psány libovolnou aplikací vytvořenou ve shodě s X.509.

Certifikační autorita

je důvěryhodná třetí strana, která podepisuje uživatelův veřejný klíč a jeho jméno (případně další doplňkové údaje jako doba platnosti) svým soukromým klíčem. Certifikát lze ověřit veřejným klíčem certifikační autority. Pokud chtějí nyní dva partneři spolu komunikovat, mohou se vzájemně autentizovat ověřením digitálního podpisu druhé strany veřejným klíčem partnera a posléze ověřením partnerova veřejného klíče verifikací digitálního podpisu certifikátu užitím veřejného klíče certifikační autority. Stačí pak důvěřovat veřejnému klíči certifikační autority. Tímto způsobem je redukován počet veřejných klíčů, kterým každý z uživatelů musí důvěřovat. Při větším počtu uživatelů jedna certifikační autorita nestačí. Veřejný klíč jedné certifikační autority může být certifikován jinou certifikační autoritou. Vytvářejí se tak sítě certifikačních autorit, které mohou mít různou hierarchickou strukturu.

- **AEC šifrovací knihovna**

Algoritmy používané v bezpečnostních knihovnách AEC Security Plug-in:

Pro šifrování dat - přenášených informací

- RC2-40
- RC2-128
- DES
- 3DES
- Blowfish
- CAST

Pro výměnu klíčů

- ELLIPT
- RSA (mimo USA)
- DSA
- Diffie - Hellman

Pro podpis zprávy

- SHA
- MD5

Jsou použity algoritmy blokových šifer v módu CFB (cipher feedback). Zpracovávají blok otevřeného textu v délce 64 bitů.

Symetrické kryptosystémy

Jsou použity algoritmy blokových šifer v módu CFB (cipher feedback).Zpracovávají blok otevřeného textu v délce 64 bitů.

DES

patří mezi kryptografické standardy (USA). Klíč má délku 56 bitů. Bezpečnost při použití tohoto algoritmu je vysoká, rychlost je úměrná bezpečnosti. Tento algoritmus je používán spíše z důvodů kompatibility s dalšími šifrovacími systémy.

3DES

zesílená varianta kryptografického standartu. Využívá dvojnásobně dlouhý klíč, tj. 112 bitů. Algoritmus DES je použit třikrát, v prvním a třetím

kroku šifruje (pomocí první části klíče), v druhém kroku dešifruje (pomocí druhé části klíče).

Blowfish

je moderní algoritmus s proměnnou délkou klíče (32 - 448 bitů). V systému IronWare® Communication je použita délka klíče 128 bitů. Koeficient bezpečnosti a rychlosti je velmi vysoký. Blowfish byl navržen a publikován v roce 1993 Bruce Schneierem (mezinárodně uznávanou autoritou v oboru kryptografie).

RC2-40

je bloková symetrická šifra s proměnnou délkou (zde max. 40 znaků). Tato šifra je v IronWare® Security Suite použita z důvodu kompatibility s dalšími šifrovacími systémy.

CAST

navržený autory Carlisle Adams a Stafford Taverns, je moderní algoritmus (bloková šifra s délkou bloku 64 bitů). Počet bitů klíče je 128 bitů. Jeho design je velmi podobný algoritmu Blowfish, obsahuje S- boxy závislé na klíči, dále neinvertibilní funkci f a má strukturu Feistelovy šifry. CAST je patentován firmou Entrust Technologies, která ho však postoupila pro volné užití.

Asymetrické kryptosystémy

RSA

algoritmus pro výměnu klíčů a tvorbu elektronického podpisu patřící mezi nepsané standardy. Využívá klíče 320-2400 bitů dlouhé. Jedná se o patentovanou (1977) metodu americké společnosti RSA Data Security Inc. Bezpečnost RSA je založena na skutečnosti, že je obtížné rozložit velká čísla (z nichž každé je součinem dvou velkých prvočísel).

DSA

Je americká norma pro digitální podpis vydaná NIST. Vychází z El-Gamalovy varianty pro podpis ve schematu opírajícím se o obtížnost řešení úlohy diskrétního logaritmu. Její varianta platná v současné době používá prvočíselné pole délky 1024 bitů, soukromý klíč vytvořený tímto algoritmem má délku 160 bitů.

ELLIPT

metoda eliptických křivek - algoritmus implementovaný přímo společností AEC, spol. s r.o. - patří mezi velmi perspektivní algoritmy. Jeho bezpečnost (při stejné délce klíče) je podstatně vyšší než bezpečnost algoritmu RSA. Modulární aritmetika je zde nahrazena aritmetikou budovanou na základě operací s body na eliptické křivce. Rozhodujícím kryptologickým parametrem je počet bodů příslušné eliptické křivky, který je přibližně 2^n (je-li při generování parametrů použito prvočíslo Prime n). Při zachování stejné úrovně bezpečnosti mají eliptické kryptosystémy výrazně kratší délku klíče.

Diffie - Hellman

nejrychlejší algoritmus používaný pro výměnu veřejných klíčů. Použité prvočíslo má délku 1024 bitů.

Hashovací funkce

SHA

hashovací funkce odpovídající normě FIPS PUB 180-1.Vytvoří 160 bitů dlouhý kontrolní hash. Tento hash je při vytváření digitálního podpisu (autentizaci) zašifrován pomocí soukromého klíče asymetrického algoritmu (RSA či ELLIPT).

MD5

je hashovací funkce, vytvářející hash o délce 128 bitů ze zprávy libovolné délky.

Technická podpora

Pokud máte dotaz k libovolnému produktu naší firmy, postupujte následovně:

Prostudujte příslušný soubor manuálu, projděte si příslušné položky nápovědy daného produktu, která je jeho součástí. Pokud zde nenajdete dostačující odpovědi, pokuste se (máte - li možnost) získat informace na elektronických systémech, například WWW stránkách naší firmy.

Pokud se vám přesto nepodaří problém vyřešit, informace o podpoře produktů můžete získat u autora aplikace (viz. kontaktní adresa).

Volejte na telefonickou podporu produktu firmu AEC spol. s r.o.

AEC spol. s r.o.
Bayerova 30
Brno 602 00

Tel.: ++420-(0)5-41235466
Fax : ++420-(0)5-41235038

Hot line: ++420-(0)5-41235268

E-mail: **support@aec.cz**
WWW: **http://www.aec.cz**
WWW: **http://www.aec-security.com**