Správa uživatelů a jejich práv

Tato kapitola pokrývá několik oblastí souvisejících s bezpečností provozu **WinBase602**. Popisuje zejména:

- jak lze ve **WinBase602** přidělit jednotlivým uživatelům práva ke čtení a přepisování různých dat a k provádění určitých činností;
- jak se spravují uživatelé a jejich skupiny a jak se udržují hesla uživatelů;
- jak se identifikují uživatelé, ověřuje jejich totožnost a jak fungují digitální podpisy.

Provoz WinBase602 bez bezpečnostních prvků

Zvolit provoz **WinBase602** bez bezpečnostních prvků popsaných v této kapitole má smysl, pokud klient i server pracují na jediném počítači bez možnosti síťového přístupu a k tomuto počítači je fyzicky umožněn přístup pouze jediné osobě.

V takovéto situaci lze pomocí parametru **/L** na příkazové řádce klienta **WinBase602** zabránit zobrazení přihlašovacího dialogu. Uživatel je přihlášen jako anonymní a může se z vlastní iniciativy později přihlásit pod skutečným jménem.

Přístupová práva

Systém přidělování práv jednotlivým uživatelům má za cíl ochránit důvěrná data před vyzrazením, zabránit nepovolaným osobám přepisovat, rušit nebo vkládat data, znemožnit neautorizované změny v návrhu aplikace a vymezit, který uživatel smí provádět které akce - například, které programy smí spustit, které formuláře otevřít, které sestavy vytisknout, které dotazy položit.

Dobrý systém přidělování práv musí splňovat dva (částečně protichůdné) požadavky: umožnit detailní specifikaci práv a jednoduchou správu (přidělování, odebírání) práv.

Ve **WinBase602** lze specifikovat práva zvlášť pro každou tabulku, zvlášť pro každý její sloupec, a je-li to potřeba, pak i zvlášť pro každý záznam.

Jednoduchost správy práv si žádá nástroje, které budou efektivně ovladatelné v situaci, kdy se desítkám (nebo stovkám) uživatelů přidělují práva ke stovkám (nebo tisícům) objektů. **WinBase602** tuto situaci řeší pomocí tzv. *rolí* a *skupin* uživatelů. Autor aplikace přidělí práva rolím (uživatele v aplikaci) a správce provozu aplikace pak jen obsadí uživatele nebo jejich skupiny do těchto rolí.

Kdo může nabývat práv?

Práv může nabýt buď UŽIVATEL, SKUPINA uživatelů nebo ROLE. Členy těchto tří okruhů nazýváme SUBJEKTY PRÁVA. Právo se vždy přiděluje určitému subjektu.

Uživatelé a *skupiny uživatelů* jsou definováni na serveru (a mohou být i sdíleni mezi servery). Jejich existence je nezávislá na aplikacích - v každé aplikaci v jedné databázi vystupují stejní uživatelé a jejich skupiny. Na rozdíl od uživatelů a skupin jsou *role* objekty existujícími *uvnitř* aplikace. V každé aplikaci mohou být definovány jiné role a mimo svoji aplikaci role žádný význam nemá.

Smysl skupin a rolí je v tom, že uživatelé mohou nabývat práv jejich prostřednictvím: když je uživatel *zařazen* do některé skupiny nebo *obsazen* do některé role, pak získává všechna práva přidělená této skupině nebo roli. Do role lze obsadit i skupinu uživatelů: pak práva přidělená roli získají všichni uživatelé zařazeni do této skupiny.

Efektivní práva

Práva, kterými konkrétní uživatel disponuje, budeme nazývat EFEKTIVNÍMI PRÁVY. Uživatel může tedy nabýt efektivních práv dvojím způsobem:

- buď jsou přidělena přímo jemu (jeho vlastní práva);
- anebo je získá prostřednictvím skupin, do nichž náleží, resp. rolí, do kterých je obsazen.

Vzhledem k tomu, že je jednodušší obsadit uživatele do role než mu přidělovat stovky práv, je výhodnější používat ke správě práv druhou cestu.

K čemu lze nabýt práv?

Subjekt může nabývat práv:

- k objektu (např. k definici tabulky, návrhu formuláře, textu programu);
- k datům v celé tabulce (globální práva);
- k datům v určitém záznamu v tabulce (pokud to tabulka umožňuje).

Záleží na návrhu tabulky, zda dovoluje přidělovat práva i k datům v jednotlivých záznamech, nebo pouze globálně ke všem záznamům. V návrháři tabulek lze zvolit jednu z těchto variant.

Práva k záznamům

Většina tabulek nepotřebuje určování detailních práv na úrovni jednotlivých záznamů. Například v tabulce KNIHOVNA určitý uživatel může mít globální právo číst záznamy nebo přepisovat všechny záznamy, ale není zpravidla třeba přidělovat právo číst nebo přepisovat pouze některé záznamy. Naopak v tabulce KORESPONDENCE, v níž záznamy odpovídají dopisům, má smysl přidělit právo přepsat záznam autorovi dopisu, právo číst záznam adresátovi, a tedy specifikovat práva na úrovni jednotlivých záznamů.

Pokud tabulka umožňuje přidělování práv na úrovni jednotlivých záznamů, pak se tato práva sčítají s globálními právy přidělenými k datům v tabulce jako celku. V efektivních

právech k záznamu se proto projeví jak práva k celé tabulce tak i specifická práva k tomuto záznamu. Typicky se určitá základní práva přidělí k datům v celé tabulce (například globální právo číst neutajované sloupce) a další práva se pak přidělují k jednotlivým záznamům (například autor záznamu má právo jej přepsat).

Jakých práv lze nabýt?

Ve vztahu k *záznamu* v tabulce lze získat právo:

- *číst* určité sloupce záznamu;
- *přepsat* určité sloupce záznamu;
- *zrušit* záznam;
- *poskytnout* svá práva dalšímu subjektu (ve **WinBase602** neexistuje právo poskytnout ta práva, která uživatel nemá).

Ve vztahu k celé *tabulce* (tedy ke všem záznamům, které jsou v ní obsaženy) lze získat stejná práva jako k jednotlivým záznamům a navíc právo *vkládat* nové záznamy.

Ve vztahu k *objektu* (tedy například k návrhu tabulky, k formuláři, programu) jsou práva poněkud zjednodušena. Lze získat právo:

- *použít* objekt (například otevřít formulář, spustit program, položit dotaz);
- *změnit* objekt (předefinovat tabulku, upravit návrh formuláře, přidat příkaz do menu);
- *zrušit* objekt;
- *poskytnout* svá práva dalšímu subjektu.

Automaticky přidělovaná práva

Pokud tabulka umožňuje přidělování práv na úrovni jednotlivých záznamů, pak lze specifikovat, jakých práv má automaticky nabýt skupina EVERYBODY k nově vkládaným záznamům: může jít o právo číst nebo přepisovat všechny sloupce nebo právo zrušit záznam. Tato práva může uživatel, který záznam vložil, kdykoli explicitně odebrat.

Subjekty práv

Subjekty práv lze rozdělit na ty, které vznikají automaticky, a ty, které jsou vytvářeny podle potřeby.

Standardní subjekty práv

Bez přičinění uživatele či správce existují v každé databázi určité tzv. STANDARDNÍ SUBJEKTY práv. Jsou to:

- uživatel ANONYMOUS;
- skupiny DB_ADMIN a EVERYBODY;
- role ADMINISTRATOR, SENIOR_USER a JUNIOR_USER v každé aplikaci.

Uživatel pojmenovaný ANONYMOUS (neboli anonymní uživatel) je vyhrazen pro ty uživatele, kteří se přihlásí na server, aniž by uvedli své jméno. Takto přihlášený uživatel nemůže podepisovat záznamy ani certifikovat jiné uživatele.

Důležité!

Po vytvoření databáze je uživatel ANONYMOUS zařazen ve skupině DB_ADMIN. To znamená, že tento neidentifikovaný uživatel disponuje vzhledem k databázi neomezenými právy. Pokud chcete databázi chránit systémem uživatelských práv, je třeba vytvořit uživatele, který bude pověřen správcováním, zařadit ho do skupiny DB_ADMIN a vyřadit z ní anonymního uživatele.

Skupina EVERYBODY zahrnuje všechny uživatele a žádný uživatel (s výjimkou uživatele ANONYMOUS) z ní nemůže být vyřazen. Každé právo, které této skupině přidělíte, automaticky získají všichni uživatelé.

V každé nově vytvořené (nebo importované) aplikaci automaticky vzniknou výše uvedené standardní role:

- Role ADMINISTRATOR získá všechna práva ke všem objektům a datům v aplikaci. Uživatele obsazeného do standardní role ADMINISTRATOR nazýváme *správce aplikace*.
- Role SENIOR_USER získá práva používat všechny objekty, číst a přepisovat veškerá data (nikoli tedy modifikovat návrh objektů).

Role JUNIOR_USER získá práva používat všechny objekty a číst veškerá data (nikoli tedy modifikovat návrh objektů nebo přepisovat data). Do této role je po vytvoření nebo importu aplikace obsazena skupina EVERYBODY.

Popsaná práva se rolím automaticky přidělují pro všechny nově vytvářené nebo importované objekty v aplikaci. Přidělení práv těmto rolím lze kdykoli změnit. Pokud tyto standardní role nevyhovují povaze aplikace, lze je ignorovat a vytvořit role vlastní. Rušit standardní role je zbytečné.

Práva anonymního uživatele

Anonymní uživatel neudává při přihlašování do systému žádné heslo, proto jako anonymní uživatel může vystupovat kdokoli. Je nutno uvážit, jaký rozsah práv by mu měl příslušet.

Anonymnímu uživateli lze specificky přidělovat práva jako kterémukoli jinému subjektu. Navíc lze rozhodnout, zda anonymní uživatel má mít práva skupiny EVERYBODY, či nikoli.

Zařazení anonymního uživatele do skupiny EVERYBODY je třeba vypnout, pokud jsou skupině EVERYBODY přidělena práva, která nemá získat každá osoba, která zasedne k počítači. Mezi práva skupiny EVERYBODY standardně patří vytváření nových aplikací, tabulek, uživatelů a dalších objektů.

Správce a přístupová práva

Členové skupiny DB_ADMIN automaticky disponují veškerými právy ke všem objektům a datům. Těchto práv nemohou být zbaveni (leda vyřazením z této skupiny). Členy této skupiny nazýváme *správce databáze*.

Správce má také právo kterákoli práva kdykoli komukoli přidělit nebo odebrat.

Fakt, že správce má přístupová práva ke všem datům, skýtá pro něj jistá rizika - může například omylem snadno zrušit tabulku patřící někomu jinému. Pokud se chce chránit proti vlastním omylům, měl by mít dvě logovací jména: jedno patřící do skupiny DB_ADMIN používané pouze pro výkon správcovských pravomocí, a druhé, s omezenými právy, pro běžnou práci s databází.

Ostatní subjekty práv

Uživatelé

Uživatelé definovaní na serveru (kromě standardního uživatele ANONYMOUS) odpovídají osobám, které s databází na serveru pracují. Pokud má systém přidělování práv a ochrany dat fungovat, nemohou se dvě osoby hlásit počítači pod stejným jménem, tedy vystupovat jako jeden uživatel.

Skupiny

Skupiny uživatelů vytváří správce databáze. Skupiny odpovídají množinám osob, které v určité oblasti mají stejná práva. Místo přidělování práv všem uživatelům ve skupině pak stačí přidělit právo skupině jako celku. Například všechny mzdové účetní mohou tvořit skupinu MZ_ÚČETNÍ a tato skupina nabude určitých práv k aplikaci MZDY. Vedoucí mzdové účtárny pak může nabýt ještě jistá dodatečná práva.

Role

Role definuje autor aplikace podle její vnitřní logiky. Nejprve si z požadované funkce aplikace odvodí souvislosti mezi právy: uvědomí si například, že pokud někdo bude mít právo otevřít určitý formulář, musí mít také právo použít definici tabulky, do níž formulář vede, a měl by mít i právo číst data zobrazená ve formuláři. Na základě těchto souvislostí si odvodí role, které uživatel může ve vztahu k aplikaci hrát, tyto role pojmenuje a přidělí jim práva.

Role navržené autorem aplikace jsou obvykle určitým zjemněním standardních rolí. Například ve vztahu k aplikaci obsahující utajená data lze zavést roli UŽIVATEL PROVĚŘENÝ NA ÚROVNI 1, která získá právo číst určitá vybraná data, a roli UŽIVATEL PROVĚŘENÝ NA ÚROVNI 2, která získá právo číst veškerá data. Obdobně na základě okruhů zodpovědnosti lze v aplikaci MAJETEK vytvořit roli UŽIVATEL SPRAVUJÍCÍ NEMOVITOSTI s právem zapisovat do tabulek popisujících nemovitý majetek a roli UŽIVATEL SPRAVUJÍCÍ MOVITÉ VĚCI s právem zapisovat do tabulek popisujících movitý majetek.

Návrh rolí a jejich práva se exportují a importují spolu s aplikací. Práva rolí se tedy zachovají při přenesení aplikace na jiný počítač.

Postup při přidělování práv

Celý systém správy práv byl navržen s cílem maximálně zjednodušit přidělování práv uživatelům. Definice rolí a práva přidělená rolím jsou součástí aplikace. Typická činnost správce aplikace se omezuje na to, že po importování aplikace obsadí do rolí definovaných v aplikaci vhodné uživatele a skupiny uživatelů.

Kdykoli později může majitel práva „poskytovat práva“ poskytnout svá práva dalším subjektům. Manipulaci s právy, skupinami a rolemi lze provádět buď interaktivně způsobem popsaným níže, pomocí SQL příkazů **`GRANT`** a **`REVOKE`** nebo programově pomocí funkcí **`(cd_)GetSet_privils`** a **`(cd_)GetSet_group_role`**.

Zařazování do skupin a obsazování do rolí

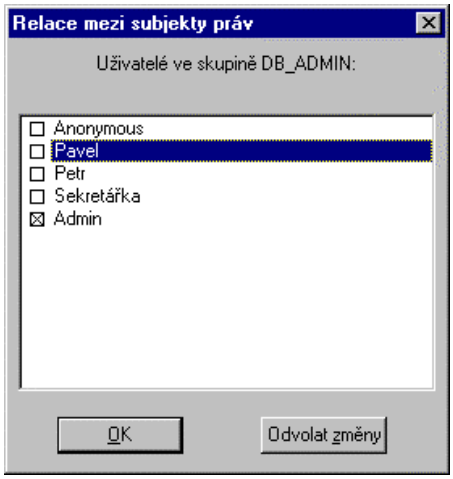
Připomeňme si, že zařazením do skupiny nebo obsazením do role uživatel efektivně získá všechna práva, která byla (nebo budou) této skupině nebo roli přidělena. Proto oprávnění zařazovat resp. obsazovat uživatele musí být omezeno. Platí tato dvě pravidla:

1) Zařazování uživatelů do skupin smí provádět pouze správce databáze (tj. člen skupiny DB_ADMIN).
2) Obsazování uživatelů a skupin do rolí smí provádět:
   - správce databáze,
   - tvůrce aplikace (uživatel, který aplikaci vytvořil nebo importoval),
   - uživatel určený jako správce aplikace (tj. obsazený do role ADMINISTRATOR).

Před vyřazením některého uživatele ze skupiny DB_ADMIN je nutno dobře uvážit, zda existuje nějaký jiný správce databáze. Databáze by se totiž snadno mohla ocitnout zcela a definitivně bez správce. Proto při každém vyřazování ze skupiny DB_ADMIN se objeví varování:

Uživatel, který sám sebe vyřadí ze skupiny DB_ADMIN, nemůže poté do této skupiny zařadit jiného uživatele, protože tuto akci smí vykonávat pouze správce, a tím již tento uživatel není.

Uživatelé skupiny DB_ADMIN



Označíte-li na řídicím panelu některého uživatele, pak provedením akce **Skupiny** lze zobrazit a editovat seznam skupin, do nichž patří. Naopak označíte-li skupinu, pak provedením akce **Uživatelé** lze zobrazit a editovat seznam uživatelů, kteří do ní patří. Označíte-li roli, lze tlačítky **Uživatelé** resp. **Skupiny** otevřít seznam uživatelů resp. skupin obsazených do role.

Ze skupiny EVERYBODY lze vyřadit pouze anonymního uživatele.

Automaticky přidělovaná práva

Při vzniku tabulek a vkládání záznamů **WinBase602** přiděluje některá práva automaticky.

Pokud uživatel založí tabulku, pak získá k datům ve všech záznamech této tabulky veškerá globální práva, tedy právo číst a přepisovat všechny sloupce, právo vkládat a rušit záznamy a právo poskytovat svá práva dalším subjektům.

Pokud uživatel vloží záznam do tabulky, která umožňuje přidělování práv na úrovni jednotlivých záznamů, pak získá k tomuto záznamu veškerá práva, tedy právo číst a přepisovat jeho sloupce, právo zrušit tento záznam a právo poskytnout práva k tomuto záznamu. Navíc, pokud to je v popisu práv k tabulce specifikováno, může (nebo nemusí) skupina EVERYBODY nabýt některých práv k tomuto záznamu - práva číst nebo přepisovat všechny sloupce nebo práva zrušit tento záznam.

Dále se automaticky přidělují práva standardním rolím podle výše popsaných pravidel.

K systémové tabulce tabulek a tabulce objektů jsou přidělena skupině EVERYBODY tato práva:

- globální právo číst všechny sloupce kromě definice;
- právo vkládat nové záznamy.

K systémové tabulce uživatelů a skupin jsou přidělena tato práva:

- globální právo číst všechny sloupce;
- právo vkládat nové záznamy.

Po vytvoření nového uživatele získá tento uživatel právo editovat svůj popis, a naopak toto právo ztratí jeho tvůrce.

Výjimečné postavení má tabulka klíčů, k níž nemá právo editace ani správce databáze.

Nastavování globálních práv k datům v tabulce

Označíte-li na řídicím panelu některou tabulku, lze provedením akce **Správa tabulky / Práva k datům** otevřít dialog pro nastavování práv k obsahu této tabulky. V takto otevřeném dialogu se nastavují pouze globální práva platná pro všechny záznamy tabulky.

V horní části okna se volí subjekt práva, v dolní části si lze prohlédnout a případně změnit nastavení práv vybraného subjektu práv k označené tabulce. Tlačítky v pravé části můžete kontrolovat (a správce může měnit) zařazení uživatelů ve skupinách, resp. uživatelů a skupin v rolích.

V dolní polovině jsou tři oblasti, kde se kontrolují a nastavují práva. V první oblasti nazvané **Práva k celé tabulce** je trojice označovacích čtverců, které nastavují práva týkající každého záznamu jako celku - vkládání, rušení a poskytování práv. Pod nimi je seznam sloupců, u kterých lze jednotlivě nastavovat práva pro čtení a pro přepis (modifikaci). Pro ulehčení práce s hromadných nastavením jsou po straně tlačítka: **Č+** znamená "vybranému subjektu nastavit právo čtení ke všem sloupcům", **Č-** znamená "... odebrat právo ke čtení všem sloupcům", **P+** znamená " vybranému subjektu nastavit právo přepisu ke všem sloupcům" a **P-** znamená "...odebrat právo přepisu všem sloupcům". Stav práv je okamžitě znázorněn v seznamu před jmény sloupců. První čtverec značí právo číst, druhý právo přepisovat.

Druhá oblast se týká nastavování práv jednotlivých záznamů a je v této chvíli nepřístupná.

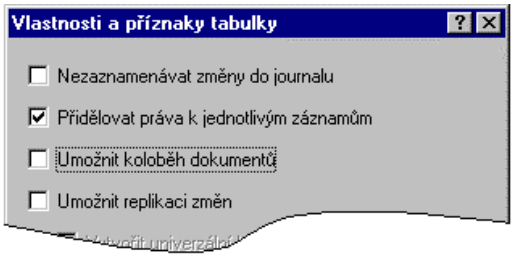
Třetí oblast nazvaná **Efektivní práva** ukazuje (již bez možnosti editace), jaká práva k tabulce reálně přísluší vybranému subjektu práv - kromě přímo přidělených práv se zde berou do úvahy i práva získaná zařazením do skupin či do rolí.

Tlačítkem **Uplatnit práva** můžete navržené změny v nastavení pro vybraný subjekt provést a zároveň zobrazit nový stav efektivních práv. Tlačítkem **OK** se změny provedou také, dialog se navíc zavře.

Nastavování práv k datům v jednotlivých záznamech tabulky

Na možnost nastavovat práva po záznamech je nutné pamatovat již při vytváření tabulky. V dialogovém okně **Vlastnosti a příznaky tabulky** v návrháři tabulek je nutné zatrhnout čtverec **Přidělovat práva k jednotlivým záznamům**.

Příznaky tabulky



Práva k jednotlivým záznamům se nastavují z libovolného formuláře do tabulky. V něm vyberete zvolený záznam a stisknete klávesu F11 nebo tlačítko na liště - tím otevřete dialog pro nastavování práv, v němž bude aktivní i střední oblast označená **Práva k vybranému záznamu**. V ní je vidět absolutní číslo záznamu, na němž stojíte, a máte možnost změnit vybranému subjektu práv jeho práva k tomuto záznamu.

V tomto případě se ve třetí oblasti dialogu, nazvané **Efektivní práva**, ukazují práva k vybranému záznamu. Na tato práva se skládají globální práva k celé tabulce i práva přidělená k záznamu, a to jak práva přidělená zvolenému subjektu, tak i práva přidělená skupinám, do nichž náleží, a rolím, které hraje.

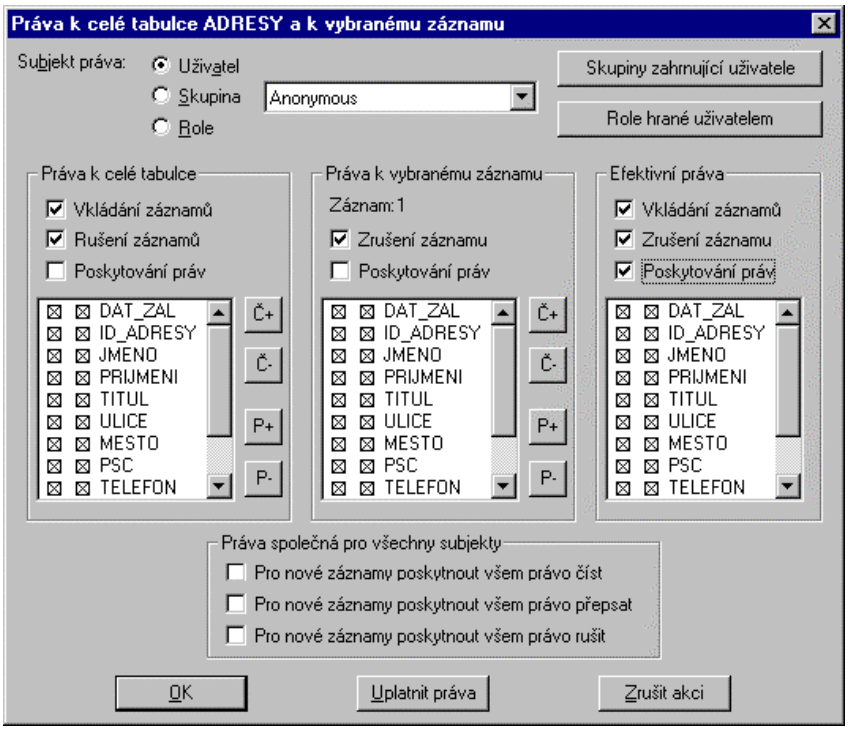
Důsledkem tohoto širokého skládání práv je, že nelze odebrat efektivní právo subjektu k záznamu, pokud:

- toto právo má subjekt přiděleno k celé tabulce;
- toto právo má přidělena skupina, do níž subjekt náleží (k tabulce nebo k záznamu);
- toto právo má přidělena role, kterou subjekt hraje (k tabulce nebo k záznamu).

Nastavení automaticky přidělovaných práv

Skupina označovacích čtverců nazvaná **Práva společná pro všechny subjekty** je aktivní pro tabulky umožňující přidělování práv k jednotlivým záznamům, ať už otevřete dialog pro celou tabulku nebo pro jednotlivý záznam. Specifikuje, jaká práva se automaticky přidělí skupině EVERYBODY pro každý nově vložený záznam. Nastavení v těchto čtvercích je nezávislé na subjektu zvoleném v horní části dialogu.

Práva k datům



Nabývání práv k objektům

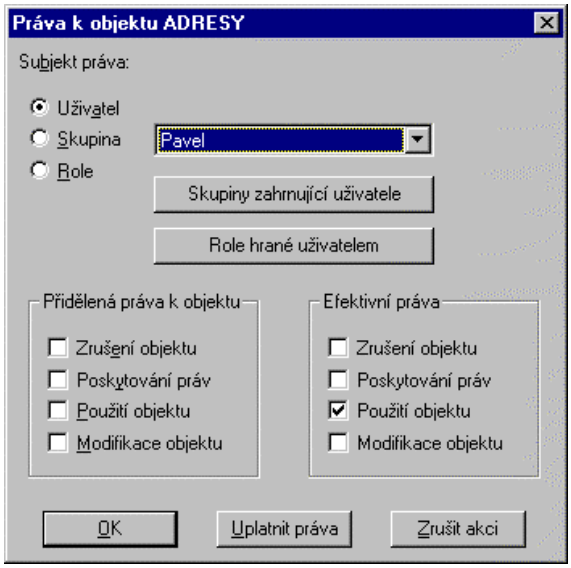
Označíte-li některý z objektů aplikace (včetně tabulek), lze provedením akce **Práva k objektu** otevřít dialog pro nastavování práv k tomuto objektu.

V horní části okna se volí subjekt práva, v dolní části si lze prohlédnout a případně změnit nastavení práv vybraného subjektu práv k označenému objektu aplikace. Tlačítky ve střední části můžete kontrolovat (a správce může měnit) zařazení uživatelů ve skupinách, resp. uživatelů a skupin v rolích.

Skupina označovacích čtverců **Přidělená práva k objektu** ukazuje, která práva má vybraný subjekt práva. Máte-li právo poskytovat práva k tomuto objektu, můžete je zde měnit. Skupina **Efektivní práva** ukazuje (bez možnosti editace), jaká práva k objektu reálně přísluší vybranému subjektu práv - kromě přímo přidělených práv se zde berou do úvahy i práva získaná zařazením do skupin či do rolí.

Tlačítkem **Uplatnit práva** můžete navržené změny v nastavení provést. Tlačítkem **OK** se změny provedou také, dialog se navíc zavře.

Práva uživatele k objektu



K příkladu na obrázku: uživatel Pavel nemá k objektu ADRESY přidělena žádná práva. Skupina EVERYBODY, jejímž je členem, má však přiděleno právo používat objekt - v efektivních právech se proto toto právo objeví. Výsledkem je stav, kdy uživatel Pavel může používat objekt ADRESY. Nemá-li mít Pavel možnost pracovat s objektem ADRESY, musí se odebrat právo používání skupině EVERYBODY.

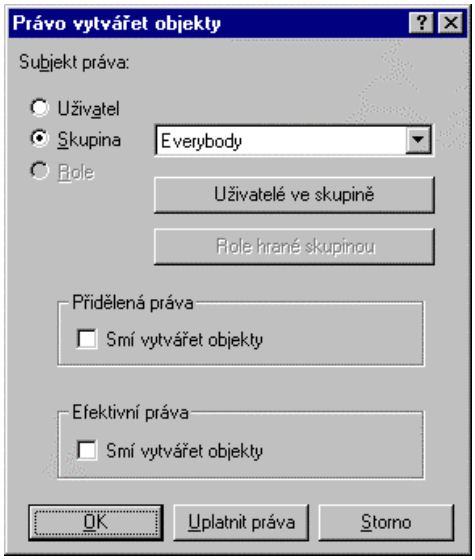
Nastavení práva vytvářet uživatele, aplikace, tabulky a další objekty

Právo vytvářet nové objekty mají ti uživatelé, kteří mají právo vkládat záznamy do systémových tabulek, v nichž jsou tyto objekty uloženy.

Tabulky jsou uloženy v tabulce TABTAB, uživatelé v tabulce USERTAB, aplikace a ostatní objekty (např. formuláře, programy) v tabulce OBJTAB. Standardně má právo vkládat záznamy do těchto tabulek skupina EVERYBODY. Toto právo lze této skupině odebrat a přidělit ho pouze těm uživatelům nebo jejich skupinám, kteří jsou oprávnění importovat, vytvářet nebo modifikovat databázové aplikace resp. zakládat nové uživatele.

Chcete-li nastavit tato práva, pak:

1. otevřete na řídicím panelu ve složce **Systém** položku **Systémové tabulky** a označte zvolenou tabulku;
2. z kontextového popup menu nebo pomocí tlačítka **Správa tabulky** proveďte akci **Práva k datům**;
3. v dialogu odeberte nebo přidělte právo vkládat objekty.



Změna chování práv oproti verzím starším než 5.0

Ve verzích **WinBase602** 4.32 a starších získávala skupina EVERYBODY veškerá práva k objektům vytvářeným anonymním uživatelem a tyto objekty nebylo možno nijak chránit. Od verze 5 tomu již tak není a práva anonymního uživatele fungují stejně jako práva všech ostatních uživatelů.

Od verze 5 již neexistuje uživatel DB_ADMIN, nýbrž skupina tohoto jména, nelze se tedy jako DB_ADMIN přihlašovat. Díky tomu může správcovskými právy k celé databázi disponovat více uživatelů a přitom lze mezi nimi rozlišovat. Pro zjištění, zda přihlášený uživatel patří mezi správce, nelze používat relaci **`Who_am_I="DB_ADMIN"`** a je nutno volat funkci **`(cd_)Am_I_db_admin`**.

Změna fungování práv oproti verzím starším než 6.0

Ve starších verzích **WinBase602** získávala skupina EVERYBODY automaticky právo čtení ke každému nově vytvořenému objektu a k datům v každé nové tabulce. Od verze 6.0 získává toto práva pouze role JUNIOR_USER, do níž je skupina EVERYBODY standardně obsazena. Efektivní fungování práv se tím nemění, zjednodušuje se ale hromadné odebrání práva čtení ke všem vytvořeným objektům a datům v aplikaci - stačí vyřadit skupinu EVERYBODY z role JUNIOR_USER.

Uživatelé a jejich správa

Veškerá ochrana databáze před neoprávněnými osobami se opírá o schopnost serveru zjistit, kdo s ním skutečně pracuje. Pokud by se mohl jeden uživatel vydávat za někoho jiného, mohl by například číst data, která mají být před ním utajena, provádět nedovolené změny v databázi nebo provést akce na cizí účet. Klíčovým bodem je proto bezpečné rozpoznání identity uživatele.

Označení uživatele

Každý uživatel **WinBase602** je označen jménem, kterému budeme říkat *logovací jméno*. Logovací jméno uživatel uvádí, kdykoli se přihlašuje na server, a tímto jménem je určena množina práv, kterými bude po přihlášení disponovat. Pro logovací jméno platí stejná pravidla jako pro jména objektů - smí být nejvýše 31 znak dlouhé, nerozlišuje se mezi velkými a malými písmeny. Logovací jména přísluší - jedno k jedné - osobám, které s databází pracují. Výjimkou je logovací jméno standardního uživatele ANONYMOUS, které může využívat kdokoli.

Dále je uživatel popsán doplňujícími informacemi jako občanské jméno a příjmení, identifikační číslo apod. Tyto údaje nemají na práva uživatele žádný vliv, jsou-li však ověřena certifikační autoritou, napomáhají ke ztotožnění logovacího jména s konkrétní osobou (viz dále).

Metoda ověřování identity

Ověřování identity uživatelů je založeno na heslech. Každému uživateli zavedenému v databázi pod svým *logovacím jménem* přísluší *heslo*, které musí uvést, chce-li se pod tímto jménem přihlásit na server.

Bezpečnost hesel

Znalost hesla patřícího k cizímu logovacímu jménu dovoluje proniknout do databáze a využívat práv příslušejících uživateli tohoto jména. Zneužití hesla může uživatel zabránit tím, že:

- volí dostatečně dlouhé heslo (ne jedno slovo, ale celou frázi), neboť narušitel by mohl vyzkoušet všechna slova ze slovníku českého jazyka;
- nevolí jako heslo slova související se svou osobou (jména příbuzných nebo domácích zvířat, místo pobytu o dovolené, název oblíbeného nápoje);
- nepoznamená si heslo nejlépe nikam, případně poznamená si jej na tajné místo v důmyslně zašifrované podobě;
- pravidelně mění své heslo.

Bezpečnostní autorita může stanovit limit na minimální délku hesla a omezit platnost hesel na stanovený počet dní.

Správa hesel ve **WinBase602** se opírá o metodu *one-time-password* z RFC1938. Její vlastnosti lze shrnout takto:

- heslo není nikde v systému zaznamenáno, a to ani v zašifrované podobě;
- heslo se nikdy neposílá po síti, a to ani v zašifrované podobě (neboť síť lze odposlouchávat);
- kód odvozený z hesla, který otevírá uživateli přístup na server, se nedá použít opakovaně;
- analýza programů, které s hesly pracují, ani interních dat uložených na serveru nebo posílaných po síti, nenapomůže ke zlomení hesla.

Relativní nevýhodou této metody je, že heslo lze použít pouze omezený počet krát. Po vyčerpání tohoto počtu, stejně jako po vypršení doby platnosti hesla, si **WinBase602** při přihlašování uživatele vynutí zadání nového hesla.

Správce databáze nemůže zjistit ani změnit cizí heslo. Pokud uživatel své heslo zapomene, neexistuje způsob, jak jej zjistit. V takové situaci lze pouze zrušit uživatelské jméno a založit jej znovu, což ovšem doprovází ztráta všech jeho práv.

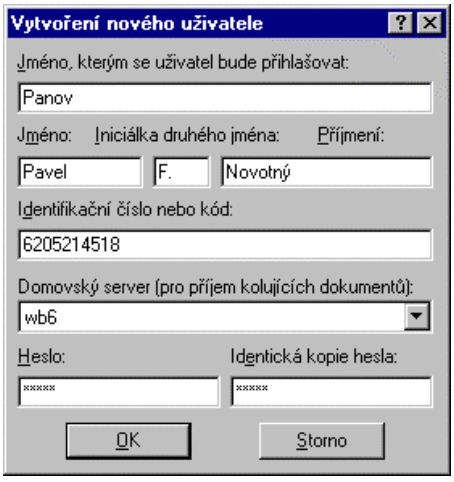
Existuje třída aplikací, jimž by povinnost periodicky měnit heslo přinesla značné komplikace. Jedná se zejména o neinteraktivní klienty **WinBase602** a částečně i přes ActiveX. Pro tyto případy lze použít logovacích jmen začínajících znakem _ (podtržítko). Platnost hesel příslušejících k těmto jménům nikdy nevyprší, za cenu sníženého zabezpečení.

Vytváření nového uživatele

Vytvořit nového uživatele lze buď z řídicího panelu nebo pomocí funkce **`(cd_)Create_user`**. Vytváření nových uživatelů není omezeno pouze na správce, vytvořit uživatele může kdokoliv s výjimkou anonymního uživatele vyřazeného ze skupiny EVERYBODY. Nový uživatel se může nejprve přihlásit jako anonymní a pak vytvořit sebe sama.

Uživatel se vytváří tak, že na řídicím panelu se v levé části vybere server, v jeho systémové složce se zvolí **Uživatelé** a provede se akce **Vytvořit**. V dialogovém okně pak vyplní údaje o uživateli. Vyplnění logovacího jména je nezbytné. Vyplnění hesla je žádoucí z hlediska bezpečnosti. Heslo se zadává dvakrát, jako ochrana proti případným překlepům. Zadání občanského jména, příjmení a identifikačního čísla může být vyžadováno certifikační autoritou. Tyto údaje lze však doplnit až později, před certifikací. Volba domovského serveru se týká pouze koloběhu dokumentů.

Vytvoření nového uživatele

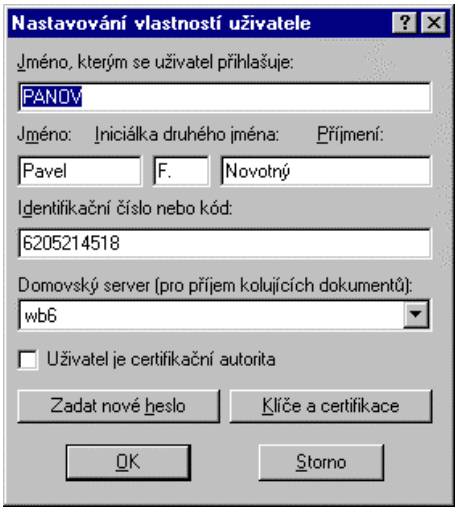


Po vytvoření nového uživatele na serveru se lze pod jeho logovacím jménem přihlašovat. Uživatel může požádat správce databáze o zařazení do skupin, případně správce aplikací o obsazení do rolí nebo o přímé přidělení práv. Může také žádat certifikační autoritu o potvrzení identity (viz dále).

Modifikování údajů o uživateli

Zjistit nebo modifikovat údaje o uživateli lze tak, že se vybere příslušný uživatel a provede se akce **Modifikovat**. Tím se otevře okno popisující uživatele.

Modifikace uživatele



Přepsat svá jména, identifikační číslo nebo jméno domovského serveru smí uživatel sám nebo správce databáze. Pro ostatní uživatele jsou tyto informace čitelné, ale needitovatelné. Provedení změn v těchto údajích nijak neovlivní práva uživatele.

V tomto dialogu lze uživatele označit jako certifikační autoritu. Toto označení má význam pouze tehdy, pokud je potvrzeno vyšší certifikační autoritou nebo pokud je uživatel vybrán bezpečnostní autoritou jako nejvyšší certifikační autorita (viz *Digitální podpisy a certifikace* dále v této kapitole).

Tlačítkem **Zadat nové heslo** lze otevřít dialogové okno pro zadání nového hesla pro tohoto uživatele. Tuto akci může provést pouze uživatel sám (ani správce databáze nemá tuto možnost).

Tlačítkem **Klíče a certifikace** lze otevřít okno umožňující generování párů klíčů a jejich certifikování. Popis této oblasti je dále v této kapitole.

Provedení libovolné změny v údajích o uživateli (nikoli však změna hesla) se projeví v nově vystavených certifikátech identity, neovlivní však zpětně platnost podpisů dříve vytvořených tímto uživatelem.

Pokud je stejný uživatel zaveden na více serverech, pak je nutno změněné údaje přenést na všechny tyto servery. K tomu lze využít export a import uživatele.

Stejný uživatel na více serverech

Pokud stejný uživatel pracuje na více serverech, pak je žádoucí, aby mohl na všech používat k podepisování stejný klíč. Pokud má být digitální podpis uživatele ověřován na jiných serverech (např. v replikovaných záznamech), pak je dokonce nezbytné, aby na nich existoval tentýž uživatel se stejným klíčem.

Uživatele založený na jednom serveru se na jiný server přenese tak, že se na prvním serveru exportuje do souboru na druhém serveru se importuje.

Přenos uživatele pomocí exportu a importu je nezbytný, pokud uživatel ze serveru A má na serveru B certifikovat jeho totožnost, aby servery mohly zahájit replikační vztahy.

Export / Import uživatelů

Má-li být na jiném serveru totožný uživatel (ve smyslu stejné interní identifikace a stejného klíče), je jedinou cestou export uživatele a na druhém serveru jeho import.

Pamatujte!

Při pokusu vytvořit totožného uživatele akcí **Vytvořit** vznikne uživatel s jinou identifikací. Identifikace uživatele je celosvětově jedinečná.

Chcete-li exportovat uživatele, označte ho na řídicím panelu a proveďte akci **Exportovat**. Na druhém serveru vyberte databázi, označte kategorii **Uživatelé** a proveďte akci **Importovat**.

Uživatele a jejich skupiny lze přenést z jednoho serveru na druhý také hromadně a společně s jejich veřejnými klíči. K tomu slouží v menu ***Nástroje / Server*** příkazy **Export všech uživatelů, skupin a klíčů** a **Import všech uživatelů, skupin a klíčů**. Tato akce se využívá ve dvou případech:

- pokud na dalším serveru chcete pracovat se stejnou množinou uživatelů a ověřovat digitální podpisy vzniklé na prvním serveru;
- pokud přenášíte celý obsah databáze do databáze nové (například při výskytu nespecifických chyb).

Při importu nového uživatele se jeho heslo nastaví na prázdné - heslo ze serveru, z něhož byl uživatel exportován, nelze převzít z důvodu použití mechanismu one-time-password. Při prvním přihlášení si tento uživatel musí zadat nové heslo.

Při importu nových údajů již existujícího uživatele (např. při importu jeho klíčů) se zachová stávající heslo.

Uživatel pro webovské aplikace

Pokud se k serveru přihlašuje **WinBase602 Internet Klient** (na typu nezáleží), používá uživatelské jméno `__WEB` (dvě podtržítka na začátku). Uživatele tohoto jména musí správce vytvořit před prvním pokusem o přihlášení. Zároveň mu přidělí heslo. Přihlásit se jiným jménem z WBIK (jako v dřívějších verzích WBIK) není možné.

Uživatel __WEB musí samozřejmě mít dostatek práv potřebných pro běh aplikace. I toto nastavení je třeba provést před zahájením provozu aplikace, nejsnáze vytvořením správcovské role a obsazením tohoto uživatele do ní.

Běžný klient nemůže toto standardní jméno zneužít, protože je chráněno heslem, bez jehož znalosti je přístup odmítnut.

Digitální podpisy a certifikace identity

V následujících odstavcích budeme směřovat k vysvětlení podstaty a způsobu používání tzv. *digitálních podpisů*, kterými může uživatel **WinBase602** podepisovat dokumenty uložené v databázi. Účel digitálního podpisu je stejný, jako u podpisu na papíře, tedy:

- identifikovat osobu, která dokument podepsala;
- svázat obsah dokumentu s podpisem.

Digitální podpis je implementován tak, aby zajistil, že nelze:

- podpis padělat;
- podepsaný dokument dodatečně pozměnit, aniž by změna byla odhalena;
- po podepsání dokumentu odmítnout autenticitu podpisu, tedy tvrdit, že podpis není můj nebo že jsem podepsal něco jiného;

a to ani při použití administrátorských práv nebo přímého zásahu do databázového souboru.

Pár klíčů

Šifrovací postupy, které umožňují implementovat bezpečné digitální podpisy, jsou založeny na dvojicích klíčů příslušejících uživateli - *veřejném* a *soukromém* klíči. Veřejný klíč každého uživatele je uložen v databázi, je všeobecně znám a je pomocí certifikátu identity spojen s údaji o svém majiteli. Soukromý klíč je uložen na disketě nebo jiném přenosném mediu, je chráněn heslem a je uživatelem pečlivě střežen - vkládá se po počítače pouze při podepisování dokumentů.

Dvojice klíčů dovoluje ověřovat totožnost uživatele podobně jako přetržená fotografie v dobrodružných filmech. Člověk, který přinese druhou polovinu fotografie, je identifikován podobně jako uživatel se soukromým klíčem, který se hodí k veřejnému klíči.

Nejprve se pokusíme vysvětlit, proč používání digitálních podpisů vyžaduje speciální proces ověřování identity zvaný *certifikací*.

Úvodní příběh

Pro pochopení smyslu certifikace identity uvažujme následující scénář:

Pan Josef Semtele nemá rád svoje jméno ani příjmení, a proto se do databáze zavede jako uživatel Boleslav Krumlovský. V databázi si založí aplikaci, v ní vytvoří tabulky a naplní je daty. Tato data jsou perfektně chráněna, nemá k nim přístup nikdo, komu by jejich autor neposkytl oprávnění. Pan Semtele se pokaždé hlásí do databáze jako Krumlovský a vše je v pořádku.

Problémy nastanou, pokud ve firmě pracuje jiný zaměstnanec jménem Krumlovský, který je oprávněn např. schvalovat nákupy výpočetní techniky. K žádankám o nákup připojuje své vyjádření a digitální podpis. Pokud žádanku neoprávněně podepíše pan Semtele (svým pseudonymem Krumlovský), pak nákupčí nemusí poznat, že něco není v pořádku.

Podstata potřeby certifikace

Pokusme se nyní přesně vystihnout, v čem je a v čem není problém:

- databázový server přesně ověřuje přidělení práv jménům uživatelů;
- hesla účinně brání tomu, aby se uživatel přihlásil pod jiným jménem, než jaké si založil;
- není však zajištěno propojení mezi jménem a skutečnou osobou!

Proto potřebujeme mechanismus, který spojení jména a osoby zajistí. Tímto mechanismem je *certifikace*. K záznamu o uživateli na serveru a k jeho veřejnému klíči se dá připojit jeden nebo více tzv. *certifikátů*, které stvrzují, že toto jméno založil skutečně člověk, jehož nacionále jsou u něj uvedeny.

Certifikace identity uživatelů

Certifikace identity uživatelů je proces, při němž pověřená osoba ověřuje a potvrzuje, že údaje o uživateli zaznamenané v databázi souhlasí se skutečnými daty osoby, která o cer-

tifikaci žádá. Certifikace zároveň spojuje údaje o osobě s jejím veřejným klíčem uloženým v databázi. Certifikovaný uživatel může používat digitální podpisy.

Jak a kdo certifikuje identitu?

Certifikát identity smí vystavit pouze důvěryhodná osoba pověřena touto činností. Této osobě se říká *certifikační autorita* (zkráceně CA).

Pro volbu certifikační autority se používají tato pravidla:

- CA by měla osobně znát uživatele, jejichž identitu bude certifikovat;
- CA by neměla mít žádný vlastní zájem na tom, co je obsahem databáze.

V organizacích pracujících s daty citlivými na bezpečnost vykonává funkci CA zvláštní osoba nepověřována jinými úkoly.

Hierarchie certifikačních autorit

První z výše uvedených podmínek je obtížné splnit v organizaci s velkým počtem uživatelů databáze. Proto existuje možnost mít více CA (například v každé divizi firmy jednu) a uspořádat je do hierarchie.

V hierarchii existuje jedna nejvyšší certifikační autorita, která certifikuje identitu CA nižšího stupně a zároveň certifikuje jejich oprávnění vykonávat funkci CA. Tyto CA mohou certifikovat ještě nižší CA. Všechny CA pak mohou certifikovat uživatele podle svého pole působnosti.

Uživatele, který vykonává funkci nejvyšší certifikační autority, určuje funkcionář zvaný *Bezpečnostní autorita*. Nastavení nejvyšší certifikační autority je popsáno v kapitole *Provozní bezpečnost databáze* v tomto manuálu.

Vytvoření páru klíčů

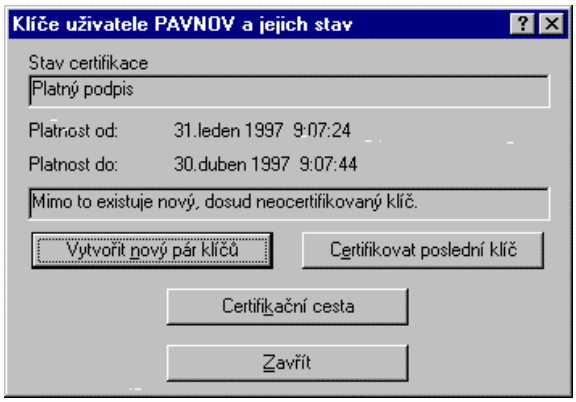
Uživatel, který chce používat digitální podpisy, si nejprve musí vytvořit pár klíčů níže popsaným postupem, a pak si nechá svoji identitu a klíče certifikovat. Postupuje takto:

1. Otevře dialogové okno obsahující údaje o jeho osobě (viz popis správy uživatelů) a případně do něj doplní údaje, které jsou v organizaci pro certifikaci vyžadovány;
2. stiskne tlačítko **Klíče a certifikace** a tím otevře dialogové okno popisující stav jeho klíčů;
3. vloží do mechaniky vlastní disketu pro zaznamenání jeho soukromého klíče;
4. stiskne tlačítko **Vytvořit nový pár klíčů**, tím otevře dialogové okno pro uložení souboru;
5. zvolí umístění souboru se soukromým klíčem a vyplní heslo, které bude chránit jeho klíč;
6. stiskne **OK**.

Tímto postupem se heslem zašifrovaný soukromý klíč uloží na disketu a veřejný klíč zůstane v databázi. Pak uživatel může požádat jemu příslušnou certifikační autoritu o provedení certifikace.

Jak se provádí certifikace klíče uživatele?

Certifikační autorita se přihlásí pod svým jménem, otevře záznam o uživateli, ověří jeho obsah, tlačítkem **Klíče a certifikace** otevře další okno a v něm stiskne tlačítko **Certifikovat poslední klíč**.



Při certifikování zkontroluje nebo zadá datum a čas, do něhož bude certifikát platit. Pak stiskne tlačítko **Certifikuji!**. Poté musí dodat soubor se svým soukromým klíčem a vyplnit jeho ochranné heslo.

Certifikát se vždy vztahuje k určitému klíči. Certifikát přestane platit, pokud:

- uživatel si vygeneruje nový klíč (platnost certifikátu ve vztahu ke starému klíči však zůstává zachována);
- vyprší doba platnosti certifikátu;
- zruší další platnost svého klíče (viz dále).

Uživatel může získat certifikáty od více autorit. Pokud by však další autorita změnila datum nebo čas, do nichž certifikáty platí, zruší tím ostatní certifikáty.

Co musí a co nemusí ověřovat certifikační autorita?

Je-li certifikační autorita požádána o certifikování některého uživatele, ověří:

- zda křestní jméno a příjmení uvedené v záznamu o uživateli je stejné jako jméno a příjmení žádající osoby;
- zda souhlasí dodatečná identifikace uživatele, pokud firemní pravidla tuto identifikaci vyžadují;

- zda nastavení příznaku, že uživatel je certifikační autoritou, odpovídá skutečnosti.

Certifikátor neověřuje, zda:
- osoba žádající o certifikaci skutečně založila uživatele, o jehož certifikaci žádá;
- kdo vlastní soukromý klíč umožňující přístup do databáze pod uživatelovým jménem nebo kdo zná heslo k tomuto klíči;

Uživatel totiž nemůže nic získat tím, že bude žádat o certifikaci jména, které nezaložil, k němuž nevlastní soukromý klíč nebo nezná heslo.

Jak postupovat při vyzrazení soukromého klíče?

Je-li soukromý klíč uživatele vyzrazen, je nutno odvolat jeho certifikáty, jinak by jiná osoba mohla vytvářet falešné podpisy tohoto uživatele.

Uživatel v této situaci požádá některou certifikační autoritu, aby provedla novou certifikaci jeho klíče, a přitom zadala jako okamžik konce platnosti klíče momentální datum a čas. Přitom může využít tlačítko **Zapsat aktuální čas**. Zpětně odvolat platnost klíče nelze.

Digitální podpis

Digitální podpis se ve **WinBase602** vztahuje vždy k obsahu jednoho záznamu, a to buď ke všem jeho sloupcům, nebo pouze k jistému počtu sloupců od začátku záznamu.

Jak umožnit podepisování dokumentů (záznamů)?

Podpis v tabulce

Digitální podpis se v tabulce zaznamenává do zvláštního sloupce typu **Podpis**. Takový sloupec vložíme do návrhu tabulky, jejíž záznamy chceme mít možnost podepisovat.

Digitální podpis hlídá obsah všech sloupců, které jsou v návrhu tabulky *před* ním. Nemá žádný vztah k sloupcům, které následují za ním.

Pokud se v záznamu mají postupně podepisovat jeho části tak, jak se doplňují, lze do návrhu tabulky vložit více sloupců typu **Podpis**. Každý z nich pak hlídá sloupce od prvního až po místo, kde se nachází.

Podpis ve formuláři

V návrhu formuláře odpovídá sloupci typu **Podpis** obvykle složka speciálního druhu *Podpis*. Tato složka obsahuje jméno osoby, která záznam podepsala, stav podpisu a až tři ovládací tlačítka:

Podepsat - zapíše do databáze digitální podpis osoby, která je právě přihlášena;

Prověřit - zjistí a zobrazí aktuální stav podpisu;

Vymazat - smaže podpis.

Mimo to lze do návrhu formuláře nebo sestavy vložit také *hodnotovou složku* svázanou se sloupcem typu **Podpis**. Obsahem této složky je jméno osoby, která záznam podepsala,

a v závorce stav podpisu. Tato složka neumožňuje provádět žádnou ze tří výše uvedených akcí. Využije se kromě sestav i ve standardních formulářích.

Složka Podpis může mít specifikovanou podmínku aktivity. Tato podmínka pak určuje, zda lze v této složce podpis vytvořit. Dříve vytvořený podpis lze prověřovat i tehdy, když podmínka aktivity není splněná.

Podepsat nebo vymazat podpis může pouze ten uživatel, který má ke sloupci typu **Podpis** právo přepisu.

Podpis ve formuláři

Jak probíhá podepisování záznamu?

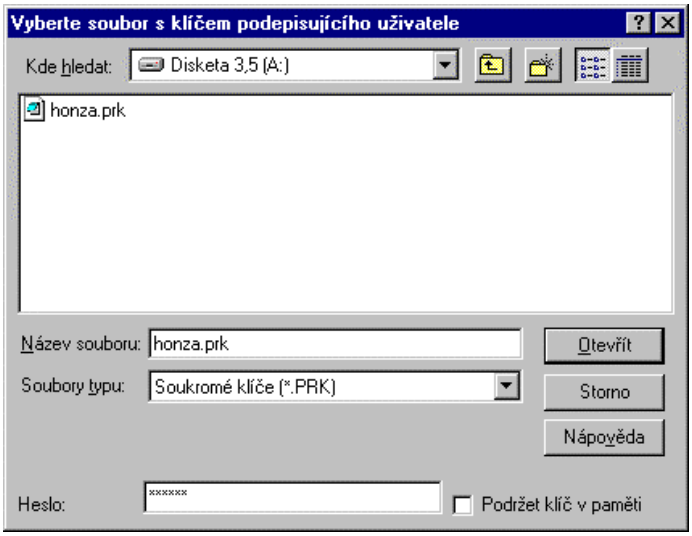
Uživatel může podepisovat dokumenty poté, co si:
1. vytvořil pár klíčů;
2. vyplnil údaje popisující jeho osobu (občanské jméno a příjmení, identifikační číslo);
3. nechal ověřit svou identitu příslušnou certifikační autoritou.

Uživatel podepíše dokument tak, že:
1. vloží do počítače disketu se svým soukromým klíčem;
2. ve formuláři obsahujícím podepisovaný záznam na složce *Podpis* stiskne tlačítko **Podepsat**; tím otevře dialogové okno pro výběr souboru;
3. vybere soubor obsahující jeho aktuální soukromý klíč;
4. vyplní heslo, kterým je klíč chráněn a stiskne **OK**.

Heslo, chránící klíč, je to, které uživatel zadal při generování páru klíčů. Jeho účelem je zabránit zneužití odcizeného klíče. Nemá nic společného s heslem zadávaným při přihlašování se na server **WinBase602**.

Uživatel může v dialogovém okně také zatrhnout požadavek na ponechání klíče v paměti počítače. Pokud je klíč ponechán v paměti, pak při příštím podepisování již nebude nutno vkládat disketu, vybírat soubor ani zadávat heslo, a dokument se podepíše jedním stiskem tlačítka. Heslo zůstane v paměti až do odhlášení se uživatele (nebo ukončení programu).

Výběr souboru se soukromým klíčem



Při podepisování a certifikování se soukromý klíč hledá primárně v adresáři A:\. Pokud chcete tento adresář změnit, můžete specifikovat jiný adresář v souboru WINBASE.INI umístěném v hlavním adresáři ***Windows***, v sekci **`Keys`** v položce **`KeyDir`**, například takto:

```
[Keys]
KeyDir=B:\
```

Stavy digitálního podpisu

Digitální podpis na záznamu se vždy nachází v jednom z osmi stavů:

Není podepsáno - záznam buď dosud nebyl podepsán nebo podpis byl vymazán;

Falešný podpis - podpis byl buď padělán nebo podepsaná zpráva byla nestandardním způsobem pozměněna (například editací databázového souboru);

Změněno po podpisu - některý sloupec záznamu, nacházející se v návrhu tabulky před podpisem, byl korektní cestou přepsán po podepsání záznamu;

Nelze ověřit, neznám uživatele - dokument nese podpis uživatele, který není na tomto serveru znám, proto nelze ověřit, zda je podpis pravý a zda dokument nebyl po podepsání pozměněn;

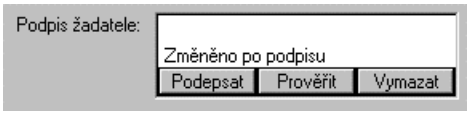
Platný podpis, neověřena identita - podpis je platný, ale není ověřeno, že uživatel, který záznam podepsal, je skutečně tím, za koho se vydává - nemá platné certifikáty identity;

Dokument podepsán po zneplatnění certifikátu - podpis byl vytvořen poté, co již skončila platnost certifikátu ověřujícího identitu podepisující osoby. Pravděpodobně došlo k falešnému podepsání dokumentu pomocí odcizeného soukromého klíče.

Identita ověřena nikoli CA - podpis byl vytvořen uživatelem, jehož identitu uvěřuje jiný uživatel, který k tomu není oprávněn. Výsledek je stejný, jako kdyby identita uživatele nebyla ověřena.

Platný podpis - podpis je platný a uživatel, který jej vytvořil, má platný certifikát identity.

Ukázka stavu podpisu



Nejdůležitější jsou první a poslední stav. Všechny ostatní sdělují, že s podpisem není něco v pořádku.

Prověřování digitálního podpisu

Aktuální stav digitálního podpisu se ukáže až po stisku tlačítka **Prověřit**. Stav, zobrazovaný před stiskem tohoto tlačítka nemusí být platný.

Při prověřování digitálního podpisu se postupuje od podpisu v dokumentu, přes podpis v certifikátu identity podepsavšího uživatele, přes podpisy jeho certifikačních autorit a podpisy v jejich certifikátech, až k vrcholové certifikační autoritě. Žádný článek tohoto řetězu nesmí chybět, jinak se platnost podpisu nedá kladně prověřit.

Stisknete-li tlačítko **Prověřit** spolu s klávesou Shift, otevře se na obrazovce okno obsahující posloupnost jmen certifikačních autorit ověřujících identitu podepsavšího uživatele. Seznam začíná údaji o uživateli a končí údaji o vrcholové certifikační autoritě.

Manipulovat s digitálním podpisem nemůže anonymní uživatel.

Podpisy a změny v údajích o uživateli

Uživatel může kdykoli smazat nebo změnit údaje o sobě v databázi případně si může vygenerovat nové klíče. Po této operaci lze i nadále ověřovat digitální podpisy tohoto uživatele. Uživatel však nemůže podepisovat, dokud si nenechá ocertifikovat nové údaje o své osobě.

Bezpečnost digitálního podpisu

Digitální podpis může úspěšně padělat ten, kdo získá soukromý klíč uživatele a heslo, které jej chrání.

Mimo tuto cestu celosvětově není znám způsob, jak podpis nebo podepsaný dokument padělat. Padělání podpisu není možné ani tehdy, pokud bezezbytku znáte algoritmy použité v pro implementaci podpisu nebo pokud budete volně zasahovat do databázového souboru.

WinBase602 používá princip digitálních podpisů, který byl od objevení v roce 1978 zkoumán nesčetnými vědci a jeví se jako nejbezpečnější ze známých algoritmů.