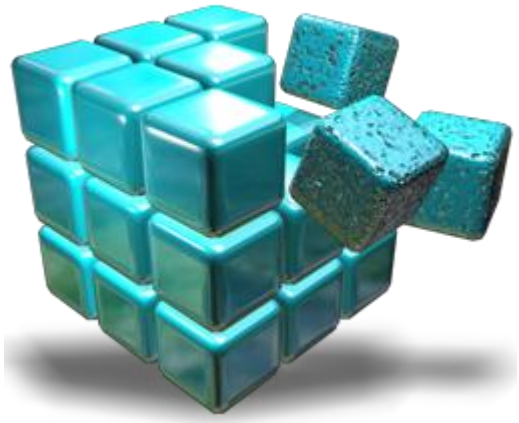


Registre

Spracoval: Ing. Tomáš Domanický

Registre

- Registre fungujú ako hierarchická databáza obsahujúca rôzne systémové, konfiguračné, informačné alebo softvérové nastavenia, ktoré umožňujú fungovanie operačného systému.

- Pri inštalácii nového zariadenia operačný systém najprv priradí zdroje k zariadeniu na základe informácii z registrov a až potom uloží potrebné konfiguračné nastavenia pre dané zariadenie.

Základné pojmy

Security Identifiers (SID)

Systémové účty, užívateľské účty, skupiny užívateľov a iné objekty sa riadia bezpečnostnými zásadami, ktoré určujú Security Identifiers (SID). Vždy, keď operačný systém vytvára bezpečnostné zásady vygeneruje pre ne SID.

- **Local Security Authority (LSA)** v operačnom systéme generuje SID pre lokálnu politiku zabezpečenia a ukladá ich v lokálnej databáze zabezpečenia.
- **Domain Security Authority (DSA)** generuje SID pre politiku zabezpečenia v doméne a ukladá ich do Active Directory. Každý užívateľský účet má SID.
- Príklad skutočného SID: *S-1-5-21-1957994488-706699826-839522115-1219, ale aj S-1-5-18.* ***SID vždy začína písmenom S.***

Základné pojmy

Globally Unique Identifiers (GUID)

- GUID sú čísla, ktoré identifikujú objekty, ako počítače, komponenty programov a iné zariadenia. Tieto objekty majú zvyčajne svoje názvy.
- GUID zostáva unikátne aj vtedy, ak dve zariadenia majú rovnaké mená alebo aj keď ich premenujeme. Všetky GUID majú stále ten istý formát.
- Sú to 16 bytové hexadecimálne čísla usporiadané v skupinách po 8, 4, 4, 4 a 12 číslic oddelených pomlčkou a uzatvorených svorkovou zátvorkou.
- Príklad skutočného GUID: *{21EC2020-3AEA-1069-A2DD-08002B30309D}*, ktoré reprezentuje Ovládací panel.

Základné pojmy

Hexadecimálny zápis (Hexadecimal Notation)

- V oblasti IT technológii desiatková sústava nemá príliš veľa priestoru, nakoľko sa ťažko aplikuje do počítačového systému jednotiek a núl. Binárna (dvojková) sústava je z toho hľadiska vyhovujúca, ale problémom je zložitý prevod medzi dvojkovou a desiatkovou sústavou.
- Riešením je hexadecimálna (šestnástková) sústava, pomocou ktorej je vykonaných 99 % zápisov v registroch. Tie sa potom jednoduchšie konvertujú na binárne.
- Hexadecimálnu sústavu reprezentujú číslice 0 – 9 a písmena A – F.
- Prevod medzi hexadecimálnym a binárnym zápisom je priamy, ale časovo náročný.

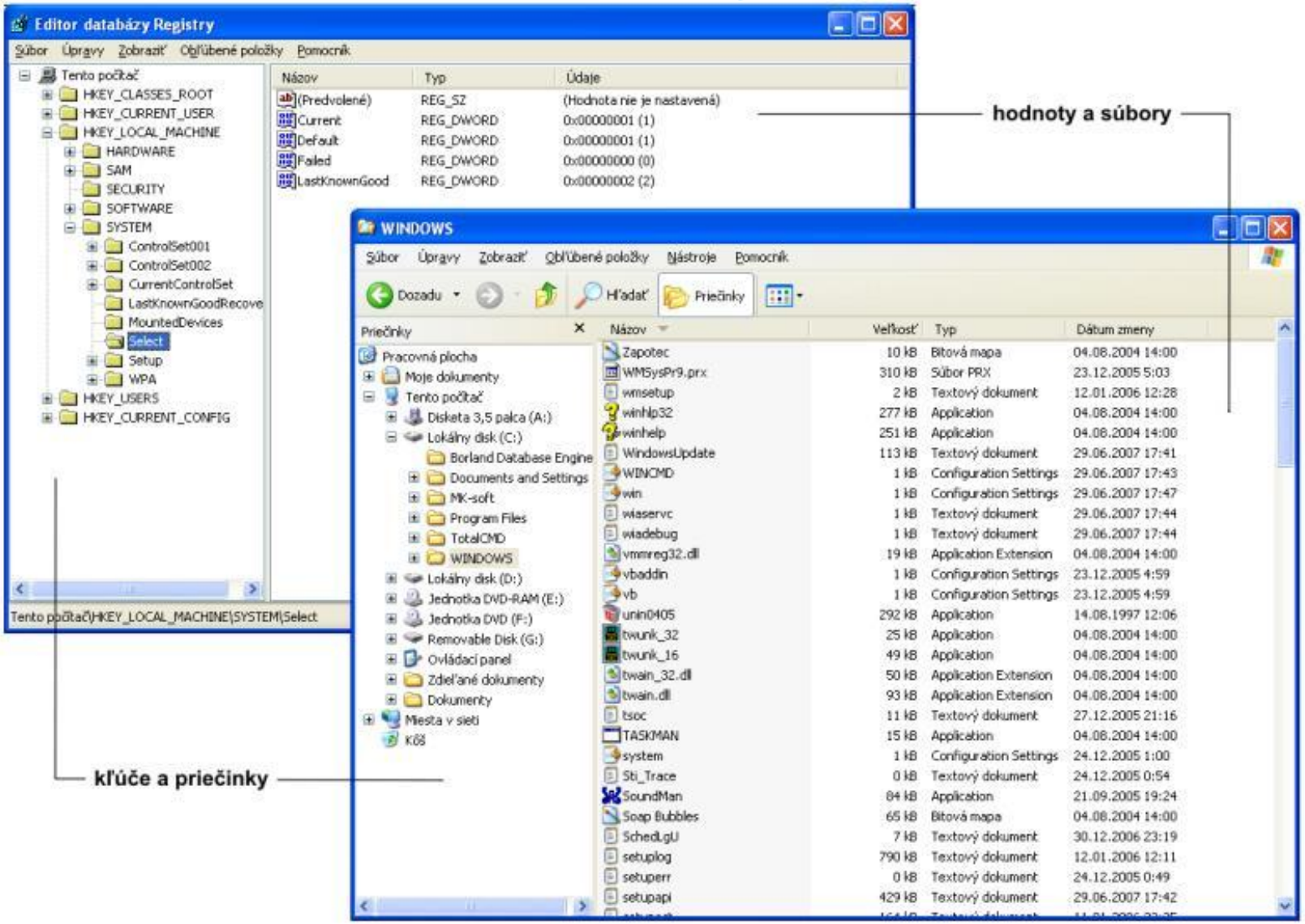
Malá pomôcka – prevod medzi číselnými sústavami

Číselná sústava		
Binárna	Hexadecimálna	Decimálna
0000	0	0
0001	1	1
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	A	10
1011	B	11
1100	C	12
1101	D	13
1110	E	14
1111	F	15

Štruktúra registrov

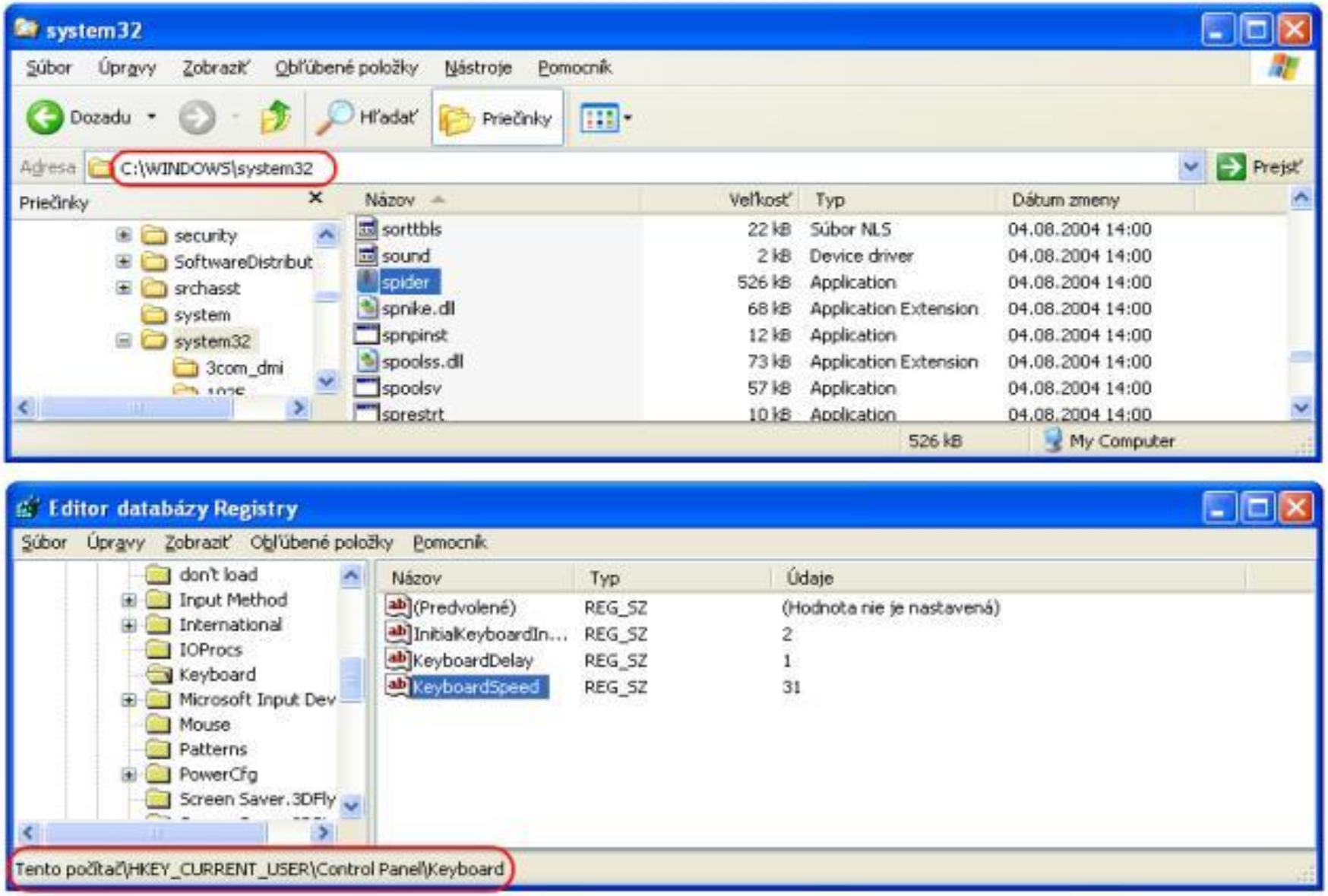
- V Editore databázy Registry v ľavom paneli (panel kľúčov) je vidieť hierarchiu registrov, ktorá je vizuálne podobná systému súborov v ľavom paneli vo Windows Explorery.
- **Kľúče registrov** sú všetky „priečinky“ v paneli kľúčov. Ich hodnoty nájdeme v pravom paneli (panel hodnôt) editora registrov, čo pri porovnaní so systémom súborov predstavuje obsah priečinkov v pravom paneli vo Windows Explorery.
- Všetky disky vo Windows Explorery vidíme pod ikonou Tento počítač, čo je analogický totožné s umiestnením koreňových kľúčov registrov taktiež pod ikonou Tento počítač.

Štruktúra registrov



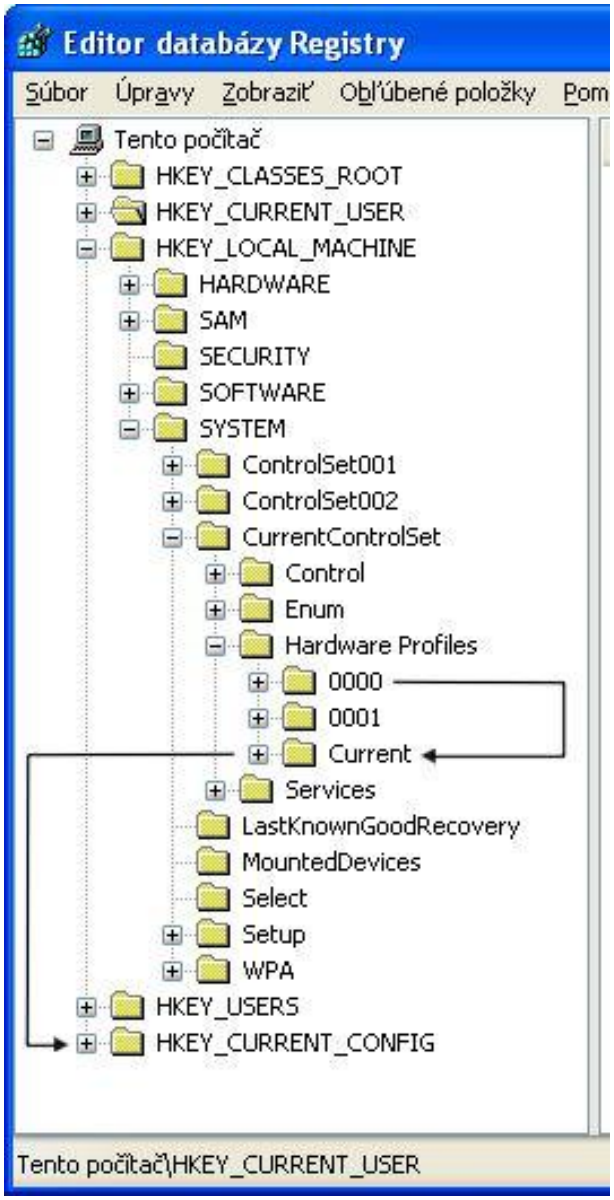
Kľúče

- Editor registrov používa pre ne tie isté ikony ako Windows Explorer pre priečinky.
- Taktiež pre ne platia tie isté pravidlá pomenovávania a vytvárania nových kľúčov t.j. do každého kľúča je možné umiestňovať neobmedzený počet ďalších kľúčov, ale každý s iným názvom.
- Podobnosť so systémom súborov nájdeme aj pri zadávaní cesty ku kľúčom. Cesta C:\Windows\System32\spider.exe odkazuje na súbor nazvaný spider.exe umiestnený na disku C v podpriečinku priečinka Windows s názvom System32. Vetva HKCU\Control Panel\Keyboard\KeyboardSpeed odkazuje na hodnotu nazvanú KeyboardSpeed v koreňovom kľúči HKCU v podkľúči kľúča Control Panel s názvom Keyboard.


system32
Súbor Úpravy Zobraziť Obľúbené položky Nástroje Pomocník
Dozadu
Hľadať
Priečinky
Adresa C:\WINDOWS\system32
Prejsť
Priečinky
security
SoftwareDistribut
srchasst
system
system32
3com_dmi
Názov Veľkosť Typ Dátum zmeny
sorttbls 22 kB Súbor NLS 04.08.2004 14:00
sound 2 kB Device driver 04.08.2004 14:00
spider 526 kB Application 04.08.2004 14:00
spnike.dll 68 kB Application Extension 04.08.2004 14:00
spnpinst 12 kB Application 04.08.2004 14:00
spoolss.dll 73 kB Application Extension 04.08.2004 14:00
spoolsv 57 kB Application 04.08.2004 14:00
sprestrt 10 kB Application 04.08.2004 14:00
526 kB
My Computer
Editor databázy Registry
Súbor Úpravy Zobraziť Obľúbené položky Pomocník
don't load
Input Method
International
IOProcs
Keyboard
Microsoft Input Dev
Mouse
Patterns
PowerCfg
Screen Saver.3DFly
Názov Typ Údaje
(Predvolené) REG_SZ (Hodnota nie je nastavená)
InitialKeyboardIn... REG_SZ 2
KeyboardDelay REG_SZ 1
KeyboardSpeed REG_SZ 31
Tento počítač\HKEY_CURRENT_USER\Control Panel\Keyboard

Kľúče a podkľúče

- Kľúče v registroch sú vzájomne prepojené.
- Napríklad Windows XP ukladá hardwarové profily vo vetve HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\.
- Každý hardwarový profil je podkľúč ####, kde #### je vzrastajúce číslo začínajúce od 0000.
- Podkľúč Current odkazuje na kľúče v aktuálnom hardwarovom profile, a koreňový kľúč HKCC odkazuje na Current ako znázorňuje nasledujúci obrázok


Editor databázy Registry
Súbor Úpravy Zobraziť Obľúbené položky Pom
Tento počítač
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HARDWARE
SAM
SECURITY
SOFTWARE
SYSTEM
ControlSet001
ControlSet002
CurrentControlSet
Control
Enum
Hardware Profiles
0000
0001
Current
Services
LastKnownGoodRecovery
MountedDevices
Select
Setup
WPA
HKEY_USERS
HKEY_CURRENT_CONFIG
Tento počítač\HKEY_CURRENT_USER

Hodnoty

- Každý kľúč musí mať aspoň jednu hodnotu, ale môže ich byť aj viac.
- Hodnotu Default (Predvolené) typu REG_SZ obsahuje každý kľúč.
- Ak kliknutím označíme kľúč na paneli s kľúčmi, na paneli s hodnotami vidíme tri stĺpce, v ktorých sa nachádza:

  • Názov – každá hodnota má názov, pričom sa uplatňujú rovnaké pravidlá pomenovania ako vo Windows Explorery

  • Typ – typ hodnoty určuje typ dát, ktoré obsahuje, napr. hodnota REG_DWORD obsahuje číselný údaj, hodnota REG_SZ – reťazec

  • Údaj – každá hodnota môže byť prázdna, null alebo obsahovať dáta

Typy

- V registroch Windows XP môžeme nájsť nasledujúce typy hodnôt, z ktorých prvé tri REG_SZ, REG_BINARY a REG_DWORD sa používajú na drvivú väčšinu nastavení v registroch.
- **REG_SZ** – textová hodnota. REG_SZ je najčastejším typom údajov v registroch.
- **REG_BINARY** – Binárna hodnota. Editor databázy Registrov zobrazuje údaj binárnej hodnoty v hexadecimálnom zápise, taktiež ho v hexadecimálnom zápise do registrov vkladáme. Príklad binárnej hodnoty :

  REG_BINARY 0x38 0x02 0xCE 0xA9 0x92 0x38 0xD9 0xAB.

Typy

- **REG_DWORD** - Hodnota DWORD (32-bitová). V registroch nájdeme mnoho hodnôt typu REG_DWORD, používajú sa ako Boolean znaky (0 alebo 1, True alebo False, Yes alebo No). Údaj hodnoty môže byť aj 32-bitové číslo bez znamienok v rozsahu od 0 do 4,294,967,295 alebo 32-bitové číslo so znamienkami od -2,147,483,648 do 2,147,483,647. V REG_DWORD môže byť tiež uložený čas v milisekundách (1000 = 1 sekunda). Príklady hodnoty

  REG_DWORD - 0xFE010002, 0x10010100.

Typy

- **REG_DWORD_BIG_ENDIAN** - hodnota DWORD s bytom najvyššieho rádu na prvom mieste. Poradie bytov je opačné ako sú uložené v REG_DWORD. Napríklad číselná hodnota 0x01020304 je uložená v pamäti ako 0x01 0x02 0x03 0x04.

- **REG_DWORD_LITTLE_ENDIAN** - hodnota DWORD s bytom najnižšieho rádu na prvom mieste (opačné poradie bytov). Napríklad číslo 0x01020304 je uložené ako 0x04 0x03 0x02 0x01. Editor databázy Registrov neponúka možnosť vytvoriť hodnotu REG_DWORD_LITTLE_ENDIAN , pretože je identická s hodnotou REG_DWORD.

Typy

- **REG_EXPAND_SZ** - Variable-length text. Hodnota tohto typu zahrňuje premenné. Programy, ktoré používajú tieto hodnoty expandujú premenné pred ich použitím. Napríklad REG_EXPAND_SZ hodnota, ktorá obsahuje %USERPROFILE%\Templates môže byť expandovaná do C:\Documents and Settings\Martin\Templates predtým, než ju program použije.

Typy

- **REG_MULTI_SZ** - binárna hodnota obsahujúca niekoľko reťazcov. Editor databázy Registrov zobrazuje reťazce v riadkoch a umožňuje ich editovanie. V registroch prázdny znak (oxoo) oddeľuje reťazce, a dva prázdne znaky označujú ukončenie reťazcov.
- **REG_RESOURCE_LIST** - zoznam hodnôt REG_FULL_RESOURCE_DESCRIPTION. Editor databázy Registrov zobrazuje tieto hodnoty, ale neumožňuje ich editovanie.

Typy

- **REG_FULL_RESOURCE_DESCRIPTOR** - Zoznam zdrojov zariadení alebo ovládačov pre zariadenia. Tento typ dát je dôležitý pre Plug and Play zariadenia, ale nefiguruje príliš v našej práci s Registrom. Editor databázy Registrov neumožňuje vytváranie hodnôt tohto typu, ale umožňuje ich zobrazenie. Príklad pre túto hodnotu nájdeme vo vetve HKLM\HARDWARE\DESCRIPTION\Description.

- **REG_RESOURCE_REQUIREMENTS_LIST** - zoznam potrebných zdrojov zariadení. Editor databázy Registrov zobrazuje tieto hodnoty, ale neumožňuje ich editovanie.

Typy

- **REG_LINK** - prepojenie. Editor databázy Registrov neumožňuje vytváranie týchto hodnôt
- **REG_NONE** - hodnota nedefinovaného typu.
- **REG_QWORD** - Quadruple-word hodnota (64-bitová). Tento typ je podobný s REG_DWORD ale obsahuje 64 bitov namiesto 32. V Editore databázy Registrov sú tieto hodnoty zobrazené a môžete ich editovať v desiatkovom a hexadecimálnom zápise. Príklad REG_QWORD hodnoty je 0xFE0210010001000l.

Typy

- **REG_QWORD_BIG_ENDIAN** - Quadruple-word hodnota s bitom najvyššieho rádu na prvom mieste. Poradie bytov je opačné ako sú uložené v REG_QWORD.

- **REG_QWORD_LITTLE_ENDIAN** - Quadruple-word hodnota s bitom najnižšieho rádu na prvom mieste (opačné poradie bytov). Tento typ je to isté ako REG_QWORD. Editor databázy Registrov neumožňuje vytvárať hodnoty REG_QWORD_LITTLE_ENDIAN, pretože táto hodnota je identická s hodnotou REG_QWORD.

Organizácia registrov

Ak si otvoríme editor registrov, v ľavom panely pod ikonou *Tento počítač* nájdeme päť koreňových kľúčov (root keys)

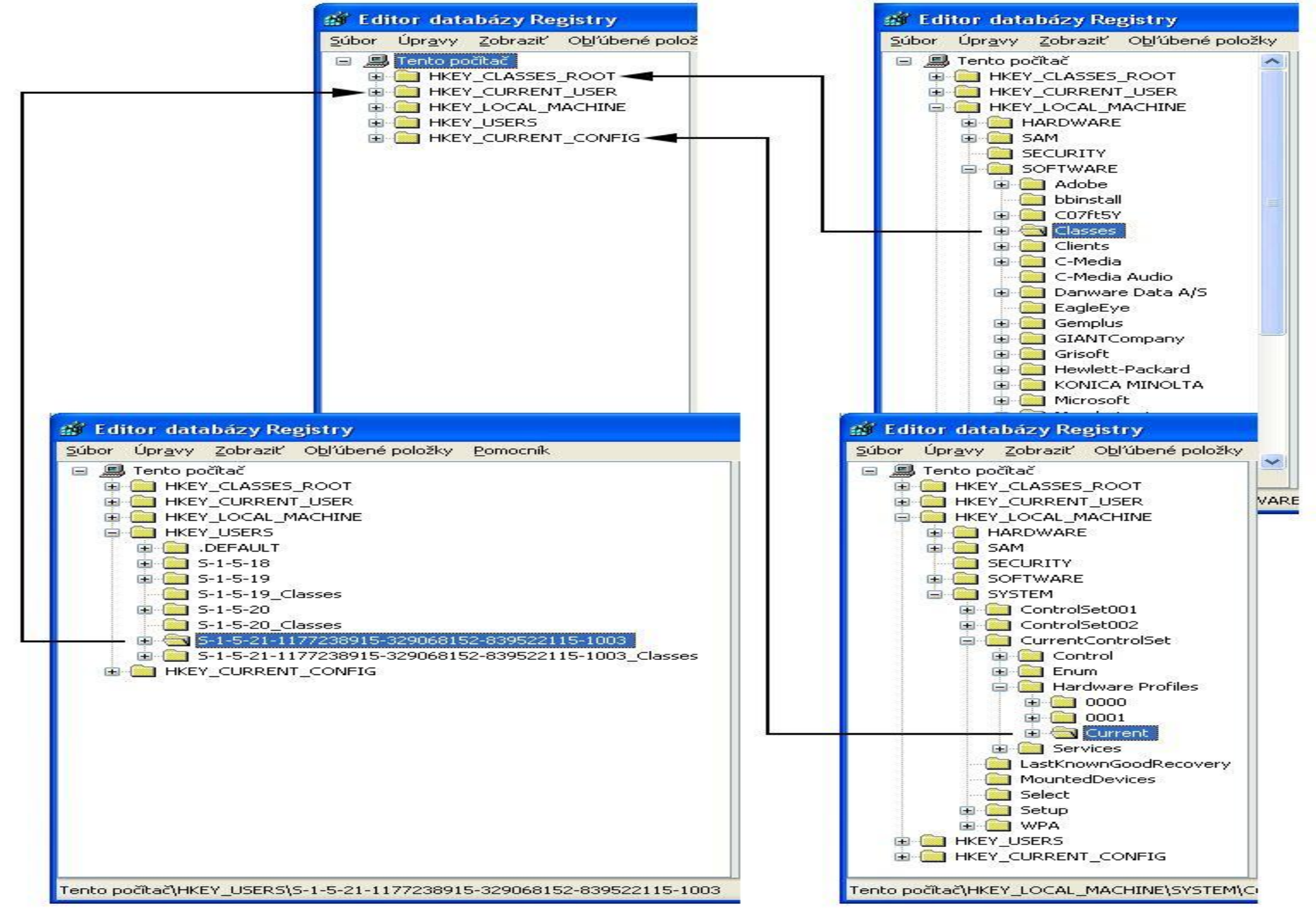
HKEY_CLASSES_ROOT (HKCR), HKEY_CURRENT_USER (HKCU), HKEY_LOCAL_MACHINE (HKLM),

HKEY_USERS (HKU),

HKEY_CURRENT_CONFIG (HKCC).

Organizácia registrov

- Z pohľadu hierarchie sú koreňové kľúče HKLM a HKU dôležitejšie ako ostatné.
- Sú to vlastne jediné skutočné koreňové kľúče uložené na pevnom disku počítača.
- Koreňové kľúče HKCR, HKCU a HKCC len odkazujú na podkľúče koreňových kľúčov HKLM a HKU. HKCU je odkaz k podkľúču HKU. HKCR a HKCC sú odkazy k podkľúčom v HKLM.
- Na obrázku je znázornené prepojenie medzi koreňovými kľúčmi, z čoho je zrejme, že tri koreňové kľúče v registroch sú len odkazy k podkľúčom v HKU a HKLM.


Editor databázy Registry
Súbor Úpravy Zobraziť Obľúbené polož
Tento počítač
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS
HKEY_CURRENT_CONFIG
Editor databázy Registry
Súbor Úpravy Zobraziť Obľúbené položky
Tento počítač
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HARDWARE
SAM
SECURITY
SOFTWARE
Adobe
bbinstall
C07ftSY
Classes
Clients
C-Media
C-Media Audio
Danware Data A/S
EagleEye
Gemplus
GIANTCompany
Grisoft
Hewlett-Packard
KONICA MINOLTA
Microsoft
Editor databázy Registry
Súbor Úpravy Zobraziť Obľúbené položky Pomocník
Tento počítač
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS
.DEFAULT
S-1-5-18
S-1-5-19
S-1-5-19_Classes
S-1-5-20
S-1-5-20_Classes
S-1-5-21-1177238915-329068152-839522115-1003
S-1-5-21-1177238915-329068152-839522115-1003_Classes
HKEY_CURRENT_CONFIG
Tento počítač\HKEY_USERS\S-1-5-21-1177238915-329068152-839522115-1003
Editor databázy Registry
Súbor Úpravy Zobraziť Obľúbené položky
Tento počítač
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HARDWARE
SAM
SECURITY
SOFTWARE
SYSTEM
ControlSet001
ControlSet002
CurrentControlSet
Control
Enum
Hardware Profiles
0000
0001
Current
Services
LastKnownGoodRecovery
MountedDevices
Select
Setup
WPA
HKEY_USERS
HKEY_CURRENT_CONFIG
Tento počítač\HKEY_LOCAL_MACHINE\SYSTEM\C

Organizácia registrov

Nastavenia uložené v registroch rozdeľujeme na:

- per–user
- per–computer.

Per–user nastavenia sú špecifické pre užívateľov – uplatňujú sa pre každého prihláseného užívateľa osobitne podľa vlastných užívateľských nastavení. Logický ich preto budeme hľadať v koreňovom kľúči HKCU.

Per–computer nastavenia sa aplikujú pre počítač, čiže pre všetkých prihlásených užívateľov (napr. sieťové nastavenia). Tie zas nájdeme v koreňovom kľúči HKLM.

HKEY_LOCAL_MACHINE

HKLM obsahuje per–computer nastavenia, t.j. nastavenia, ktoré nájdeme v tejto vetve majú vplyv na každého prihláseného užívateľa. HKLM obsahuje nasledujúce podkľúče (všimnite si, že ich názvy sú veľkými písmenami):

- HARDWARE - zahrňuje údaje charakterizujúce hardware ktorý Windows detekuje pri spúšťaní systému. Operačný systém vytvára tento kľúč pri každom spustení a pri vypínaní ho preto neukladá na HDD počítača. Zahrňuje informácie o zariadeniach, ich ovládačoch a s nimi asociovanými zdrojmi.

HKEY_LOCAL_MACHINE

- **SAM** - obsahuje lokálnu databázu zabezpečenia, Security Accounts Manager (SAM). Windows ukladá miestnych užívateľov a skupiny do SAM. Access control list (ACL) tohto kľúča neumožňuje jeho prezeranie dokonca ani administrátorom. SAM je odkaz na kľúč HKLM\SECURITY\SAM.
- **SECURITY** - obsahuje lokálnu databázu zabezpečenia v podkľúči SAM, ako aj ostatné nastavenia zabezpečenia. ACL tohto kľúča taktiež neumožňuje jeho prezeranie ani administrátorom, ale toto oprávnenie môžu získať, ak prevezmú jeho vlastníctvo.

HKEY_LOCAL_MACHINE

- **SOFTWARE** - obsahuje per–computer nastavenia aplikácii, ale mnoho svojich nastavení sem ukladá aj Windows. Vetva pre ukladanie nastavení programov je nasledovne štandardizovaná HKCU\Software\Vendor\Program\Version\. Kde **Vendor** je názov vydavateľa programu, Program je názov programu, a **Version** je číslo verzie programu (často zovšeobecnené na CurrentVersion). HKCR odkaruje na kľúč HKLM\SOFTWARE\Classes.

HKEY_LOCAL_MACHINE

- SYSTEM - obsahuje riadiace nastavenia pre ovládače zariadení a konfiguráciu služieb, z ktorých jedno je aktuálne. Každý podkľúč je riadiace nastavenie nazvané ControlSet###, kde ### je vzrastajúce číslo, ktoré začína od 001.
- Aby sa systém zakaždým spustil správne obsahuje najmenej dve riadiace nastavenia (ControlSet).
- HKLM\SYSTEM\CurrentControlSet je odkaz na ControlSet###. Kľúč HKLM\SYSTEM\Select indikuje ktorý ControlSet### sa používa.

HKEY_USERS

HKU obsahuje najmenej tri podkľúče.

- **DEFAULT** obsahuje per-user nastavenia, ktoré Windows používa pri zobrazení pracovnej plochy pred prihlásením sa užívateľa k PC. Nemýľte si ho však so základným užívateľským profilom, ktorý Windows používa pre vytvorenie nastavení pre užívateľov pri prvom prihlásení sa do systému.

HKEY_USERS

- SID, kde SID je security identifier pre užívateľskú konzolu, obsahuje per–user nastavenia. HKCU je prepojený k tomuto kľúču, ktorý obsahuje nastavenia ako sú nastavenie pracovnej plochy a Ovládacieho panela.
- SID_Classes, kde SID je security identifier pre užívateľskú konzolu, obsahuje per–user triedenie údajov a asociáciu súborov. Obsah kľúčov HKLM\SOFTWARE\Classes a HKU\SID_Classes je prepojený do HKCR.

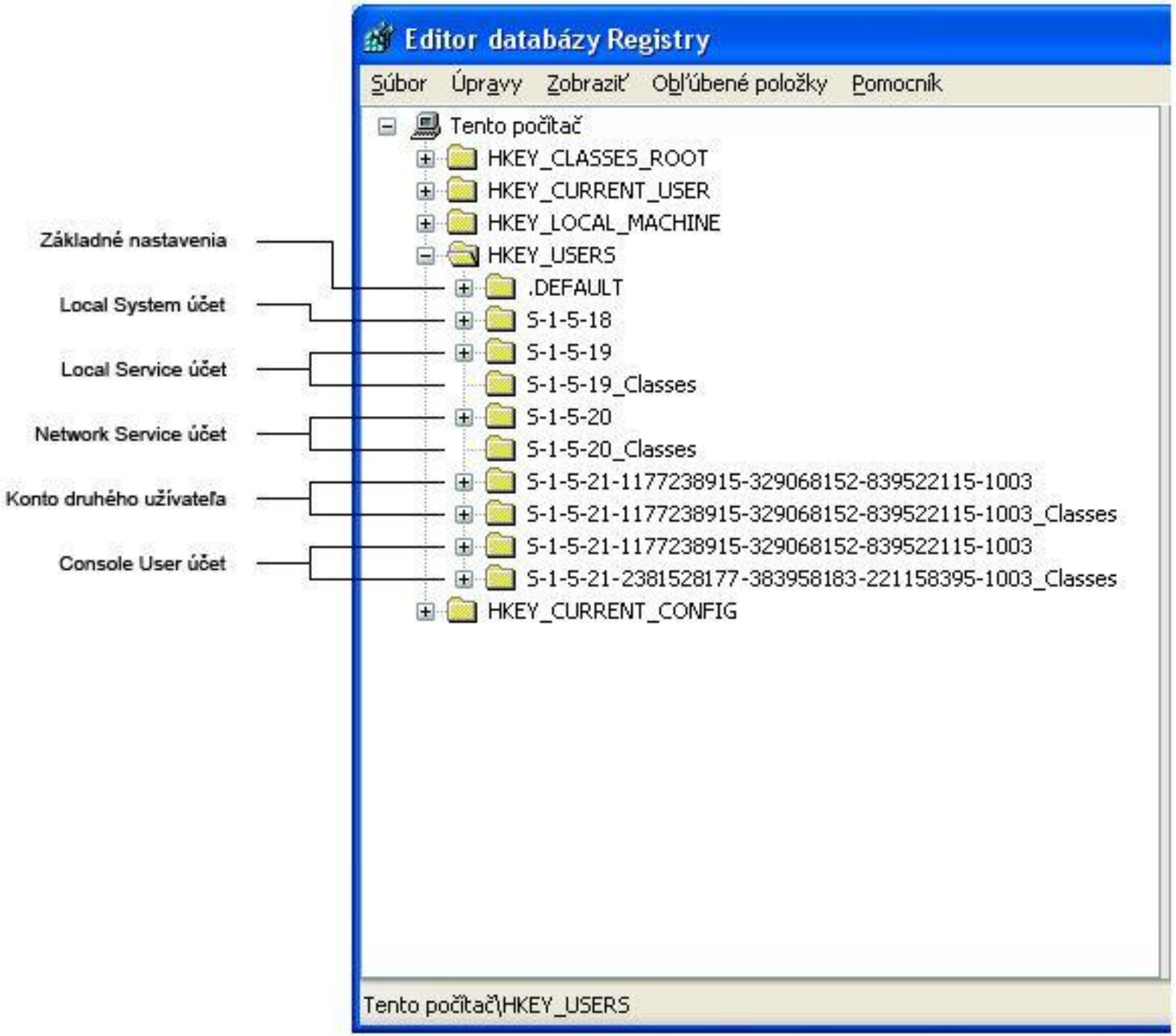
HKEY_USERS

V HKU sa vždy nachádzajú tieto SID:

S-1-5-18 je SID pre LocalSystem účet. Windows XP zavedie tento užívateľský profil ak bežia programy alebo služby pod LocalSystem účtom.

S-1-5-19 je SID pre LocalService účet. Service Control Manager používa tento účet pre zavedenie lokálnych služieb, ktoré sa nespúšťajú pod LocalSystem účtom.

S-1-5-20 je SID pre NetworkService účet. Service Control Manager používa tento účet pre zavedenie sieťových služieb ktoré sa nespúšťajú pod LocalSystem účtom.


Editor databázy Registry
Súbor Úpravy Zobraziť Obľúbené položky Pomocník
Tento počítač
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS
.DEFAULT
S-1-5-18
S-1-5-19
S-1-5-19_Classes
S-1-5-20
S-1-5-20_Classes
S-1-5-21-1177238915-329068152-839522115-1003
S-1-5-21-1177238915-329068152-839522115-1003_Classes
S-1-5-21-1177238915-329068152-839522115-1003
S-1-5-21-2381528177-383958183-221158395-1003_Classes
HKEY_CURRENT_CONFIG
Tento počítač\HKEY_USERS
Základné nastavenia
Local System účet
Local Service účet
Network Service účet
Konto druhého užívateľa
Console User účet

HKEY_CURRENT_USER

HKCU v tomto koreňovom kľúči sa nachádza užívateľská konzola s per–user nastaveniami. Je prepojený s HKU\SID, kde SID je Security Identifier pre užívateľskú konzolu. Táto vetva zahŕňa premenné, nastavenia pracovnej plochy, sieťové pripojenia, tlačiarne a preferencie aplikácii.

- **AppEvents** - asociácia zvukov k udalostiam vo Windowse.

- **Console** - zahrňuje dáta zo subsystému konzoly, kompletný znakový mód aplikácii zahrňujúc MS–DOS command prompt. Okrem toho môže obsahovať podkľúče pre určité inštrukcie okien aplikácii.

HKEY_CURRENT_USER

- **Control Panel** - zahrňuje komunikáciu, miestne nastavenia a vzhľad pracovnej plochy. Väčšina týchto nastavení sa prevádza cez Ovládací panel. Ale môžeme tu nastaviť množstvo užitočných nastavení, ktoré nie sú prístupné cez užívateľské rozhranie.
- **Environment** - údaje premenných prostredia nastavené užívateľmi. Každá hodnota asociuje premenné s reťazcom ktorý Windows dosadzuje do premenných.
- **Identities** - každý podkľúč je samostatná identita. Čo umožňuje viacerým užívateľom používať jedeného mailového klienta. Tiež je potrebný pre nastavenia užívateľských profilov vo Windowse, ktorých nastavenia sú v tomto kľúči oddelené.

HKEY_CURRENT_USER

- **Keyboard Layout** - informácie o nainštalovanom rozložení klávesnice.
- **Network** - informácie o namapovaných sieťových diskoch. Každý podkľúč je namapovaný sieťový disk ku ktorému sa Windows pripojí zakaždým, keď sa užívateľ prihlási do systému. Názvy podkľúčov sú písmená diskov ku ktorým sú namapované.
- **Printers** - užívateľské nastavenia pre tlačiarne.
- **Software** - per–user nastavenia pre aplikácie, ale mnoho svojich nastavení sem ukladá aj Windows. Štandard ukladania nastavení programov v tejto vetve je zhodný s HKCU\Softvare opísanom vyššie.
- **Volatile Environment** - definované premenné prostredia, pri prihlásení užívateľa do systému.

HKEY_CLASSES_ROOT

Tento najväčší koreňový kľúč umožňuje podstatne ovplyvniť správanie sa operačného systému. Z pohľadu editácie je preto jeden z najzaujímavejších. HKCR obsahuje dva typy nastavení:

- **Asociácia súborov** - asociuje rozličné typy súborov s programami, ktoré ich vedia otvoriť, vytlačiť alebo editovať.
- **Class Registrations** (triedenie údajov) - pre objekty Component Object Model (COM).

- **Programy** môžu nastavovať per-computer a per-user asociáciu súborov. (rôzny užívatelia na tom istom PC môžu mať rozdielne asociované súbory).
- **Užívatelia** na tom istom počítači môžu používať dva rozdielne programy na editovanie toho istého súboru bez toho, aby ich to vzájomne obmedzovalo.
- **Per-user** asociácia súborov a class registrations sú uložené v užívateľskom profile. Sú preto zavedené pri prihlásení užívateľa z ktoréhokoľvek počítača ak je použitý roaming užívateľský profil.
- **Administrátori** môžu obmedziť užívateľom prístup do HKLM\SOFTWARE\Classes bez toho, aby im znemožnili vykonávať zmeny HKCU\Software\Classes. To umožňuje neobmedzovať schopnosť užívateľov meniť asociáciu súborov a zároveň zvýšiť bezpečnostnú politiku v registroch.
- Každý kľúč vytvorený v HKCR, je systémom v skutočnosti vytvorený v HKLM\SOFTWARE\Classes.

HKEY_CURRENT_CONFIG

- HKCC je prepojenie na konfiguračné údaje v aktuálnom hardwarovom profile, ku kľúču

  HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current.
- Na druhej strane, Current je prepojenie ku kľúču HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\####, kde #### je narastajúce číslo začínajúce od 0000.

Podregistre databázy Registry (Hive Files)

Registre Windows sú fyzický organizovane v podregistroch (Hive), čo sú binárne súbory (hive files). Windows z dôvodu zvýšenia stability a funkčnosti systému pri zlyhaní inštalácie programov, výpadku prúdu a následnom poškodený dát na HDD a pod. vytvára pre tieto súbory ďalšie podporné súbory v ktorých sú uložené záložné kópie hive files. To v prípade potreby umožňuje systému nabootovať aj použitím dát z tejto zálohy. Použitie záložných súborov nám Winodws oznámi dialógovým oknom. Niektoré súbory potrebné pre chod systému boli obnovené zo záložnej kópie. Obnovenie bolo úspešné.

Podregistre databázy Registry (Hive Files)

- **Hive files** nájdeme len v dvoch „skutočných“ koreňových kľúčoch: HKLM a HKU. Vieme, že všetky ostatné koreňové kľúče sú len prepojenia k týmto dvom.
- **Podporné súbory** aj samotné hive files sú uložené v %SYSTEMROOT%\System32\config. Nie sú tam však súbory pre HKU, tie sú v priečinku užívateľského profilu.
- **Hive files** sú charakteristické tým, že ich názvy nemajú žiadnu príponu. Prípony ich podporných súborov nájdeme v nasledujúcej tabuľke.

Prípony Hive files	
Prípona	**Popis**
žiadna	Hive files
.alt	Prípona sa už vo Windows XP nepoužíva. Používa ju Windows 2000
.log	Loguje zmeny v hive files.
.sav	Záložná kópia hive files.

Podporné súbory podregistrov databázy Registry	
Podregistre databázy Registry	**Podporné súbory**
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\System	System, System.alt, System.log, System.sav
HKEY_CURRENT_CONFIG	System, System.alt, System.log, System.sav, Ntuser.dat, Ntuser.dat.log
HKEY_USERS\DEFAULT	Default, Default.log, Default.sav

Koniec