Süsteemi register (System registry)

Windows XP süsteemi register on süsteemne hierarhiline andmebaas, kus säilitatakse kõiki operatsioonisüsteemi seadeid. Sellise andmebaasi pidamine võimaldab hoida kõigi programmide seadeid n.ö. „ühes kohas“ selle asemel, et kasutada iga programmi kohta eraldi seadistusfaili (näiteks vanemate programmide poolt kasutatud .ini failid).
Samuti võimaldab registri kasutamine kasutada Group Policy'd mis annab administraatorile võimaluse kontrollida nii lokaalse kui ka võrgus oleva arvuti ja erinevate installeeritud programmide seadeid. Lihtsam on ka seadetest varukoopia tegemine, seda siis kas kogu registri sisu eksportimise abil või registrifailide otsese kopeerimise teel. Kuna register loetakse korraga mällu on seal seadete väärtuste lugemine palju kiirem kui näiteks tekstifailist.
Samas toob register kaasa ka uusi probleeme. Näiteks on HKEY_LOCAL_MACHINE võti koos oma alamvõtmetega süsteemi jaoks nii oluline, et väiksemgi viga selle struktuuris võib muuta kogu operatsioonisüsteemi töökõlbmatuks. Tõsi küll sellise olukorra vältimiseks on loodud turvamehhanisme. Halb on ka see, et registrit ei saa dokumenteerida ja kommenteerida nagu tekstipõhiseid seadetefaile. Samuti on vigasaanud registri taastamine küllaltki raske ülesanne, sest tihti puudub sellises olukorras otsene juurdepääs andmetele.

Andmed on registris organiseeritud puu kujulisse struktuuri. Register koosneb:
- Võtmetest (key)
- Andmekirjetest (data entry)

Igal võtmel võib (kuid ei pruugi) olla temaga seotud andmekirjeid ning alamvõtmeid. Kokkukuuluvaid võtmeid ja andmekirjeid, millede jaoks on süsteemis olemas eraldi failid, kuhu neid salvestatakse, nimetatakse sülemiteks (hive). Windows XP registris on järgmised sülemid:

Sülem:	**Sülemiga seotud failid:**
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

http://support.microsoft.com/kb/256986

Sülemitega seotud failid asuvad kataloogides:
- %SystemRoot%\System32\Config\
- %UserProfile%\
- %UserProfile%\Local Settings\Application Data\Microsoft\Windows\

Windows XP registri sisu on võimalik vaadata ja muuta operatsioonisüsteemiga kaasatuleva vahendi „Registry Editor“ (regedit32.exe) abil.

Käivitades Registry Editor'i näeme lokaalses masinas viit registrivõtit:

Registrivõti	Kirjeldus
HKEY_CURRENT_USER	Sisaldab parajasti aktiivse kasutaja n.ö. „isiklikud“ seadeid. Näiteks on siin kirjas kõik Control Panel'i seaded. Tegelikult on tegemist HKEY_USERS võtme alamvõtmega.
HKEY_USERS	Sisaldab kõiki operatsioonisüsteemi sisseloginud kasutajaprofiilide seadeid.
HKEY_LOCAL_MACHINE	Sisaldab konkreetse arvuti seadeid. Kehtib kõigile kasutajatele,
HKEY_CLASSES_ROOT	On HKEY_LOCAL_MACHINE\Software alamvõti. Sisaldab informatsiooni, mille abil „windows exploreriga“ avatud fail avaneb või käivitatakse sobiva programmiga. Põhimõtteliselt seob faililaiendi programmiga, millega vaikimisi sellise laiendiga faile avatakse. Alates Windows 2000'st on see informatsioon nii HKEY_LOCAL_MACHINE kui ka HKEY_CURRENT_USER võtmete all. HKEY_LOCAL_MACHINE\Software\Classes Võti sisaldab informatsiooni, mis käib kõigi kohaliku masina kasutajate kohta samas kui HKEY_CURRENT_USER\Software\Classes võti sisaldab informatsiooni, mis kehtib aktiivse kasutaja kohta ja on tühistab kõigi kasutajat kohta käiva sama seade (kui selline seade on olemas). HKEY_CLASSES_ROOT võti esitab parajasti aktiivse kasutaja ja kõigi kasutajate kohta käiva vastava informatsiooni kombinatsiooni.
HKEY_CURRENT_CONFIG	Sisaldab informatsiooni arvuti riistvara ja sellega seotud seadete kohta.

http://support.microsoft.com/kb/256986

Muudatuste tegemine registrisse

Register on ülioluline osa Windows XP operatsioonisüsteemist, seega tuleb igasuguste muudatustega olla ettevaatlik. Enne muudatuste tegemist on mõistlik teha registrist tagavarakoopia.

Registrist tagavarakoopia tegemine

1) Käivita regedit32.exe

2) Vali menüüst Fail->Export...
3) Avanenud aknas märgi ära valik „Export range – all“, pane tagavarakoopiale sobiv nimi ning määra ära loodava faili asukoht.
4) Vajuta „Save“

Registrivõtme või andmekirje lisamine

1) Käivita regedit32.exe
2) Vali aknas vasakul olevast puustruktuurist võti, millele soovid lisada alamvõtit või andmekirjet.
3) Vali menüüst Edit -> New ja vastavalt soovile kas „Key“ (võtme lisamiseks) või sobiv kirje andmetüüp (andmekirje lisamiseks). Vastavalt valikule luuakse uus võti või andmekirje, millele tuleb anda sobiv nimi. Andmekirje loomise puhul tuleb peale nime sisestamist sisestada ka kirje väärtus. Seda saab teha tehes kirjel topeltkliki.

Registrivõtme või andmekirje leidmine

1) Käivita regedit32.exe
2) Vali menüüst edit -> find
3) Avanenud aknas märgi ära, kas otsida võtmete, andmekirjete või andmekirjete väärtuste seast. Lisage otsitav fraas ning vajutage „Find“. Peale esimese sobiva vaste leidmist saab liikuda järgmise sobiva vaste juurde vajutades F3.

Registrivõtme või andmekirje muutmine

1) Käivita regedit32.exe
2) Vali sobiv registrivõti või andmekirje
3) Vali menüüst edit->rename (võtme või kirje nime muutmiseks) või edit->modify (kirje väärtuse muutmiseks)

Registrivõtme või andmekirje kustutamine

1) Käivita regedit32.exe
2) Vali sobiv registrivõti või andmekirje
3) Vali menüüst edit->delete

Registrivõtmete eksportimine ja importimine

1) Käivita regedit32.exe
2) Vali registrivõti mida soovid eksportida (koos võtmega eksporditakse kõik selle võtme alamvõtmed ning nende juurde kuuluvad andmekirjed oma väärtustega)
3) Vali menüüst Fail->Export
4) Avanenud aknas kontrolli, et oleks valitud valik „Export range – selected branch“ (tekstiväljal on kirjas ka valitud võti). Anna failile nimi ning vajuta „Save“

1) Käivita regedit32.exe
2) Vali menüüst Fail->Import
3) Avanenud aknast otsi vajalik registrivõtmeid ja andmekirjeid sisaldav fail ning vajuta „open“

Registration Entries (.reg) failid

Faililaiend .reg on Windows XP puhul vaikimisi määratud tähistama Registration Entries tüüpi faile. Tegemist on tekstifailidega, mis sisaldavad kokkulepitud formaadis registrivõtmeid ja andmekirjeid. Süntaks on järgmine:

RegistryEditorVersion
Blank line
[*RegistryPath1*]
"*DataItemName1*"="*DataType1*:*DataValue1*"
„*DataItemName2*"="*DataType2*:*DataValue2*"
Blank line
[*RegistryPath2*]
"*DataItemName3*"="*DataType3*:*DataValue3*"

RegistryEditorVersion - „Windows Registry Editor Version 5.00" kui tegemist on Windows 2000 või XP registrivõtmetega või „REGEDIT4“ kui tegemist on Windows 95 või 98 registrivõtmetega.

[RegistryPath] – Registrivõtme nimi koos tema ülemvõtmete nimedega.

DataItemName – andmekirje nimi

DataValue – Andmekirje andmetüübile vastavas formaadis väärtus

DataType – Andmekirje andmete tüüp. Võimalikud .reg faili andmetüübid on:

Andmetüüp registris	Andmetüüp .reg failis
REG_BINARY	hexadecimal
REG_DWORD	dword
REG_EXPAND_SZ	hexadecimal(2)
REG_MULTI_SZ	hexadecimal(7)

http://support.microsoft.com/kb/310516

Ülaltoodud viisil kirja pandud .reg fail lisab käivitamisel vastavad võtmed ja andmekirjed registrisse. Samas on võimalik .reg fail kirjutada ka viisil, et käivitamisel vastavad võtmed ja andmekirjed hoopis kustutatakse.

Registrivõtme kustutamiseks tuleb vastava registrivõtme nime ette kirjutada miinusmärk.
Näiteks: [-HKEY_LOCAL_MACHINE\Software\Test]

Andmekirje kustutamiseks tuleb kohe andmekirje nimele järgneva võrdusmärgi taha kirjutada miinusmärk.

Näiteks: "TestValue"=-

Registrivõtmete juurdepääsuõigused

Sarnaselt NTFS failisüsteemile on Windows XP registrivõtmetel juurdepääsuõiguste süsteem, mis reguleerib kasutajale õigusi registrivõtmete suhtes (võtme juures olevaid andmekirjeid loetakse registrivõtmega kokkukuuluvaks, neile eraldi õigusi ei määrata). Kuna register on sarnaselt failisüsteemile ülesehitatud puukujuliselt, siis toimub õiguste määramine ja pärimine täpselt samal viisil kui failisüsteemi juures.

Harjutus

1) Lisage võtmele [HKEY_LOCAL_MACHINE\Software] alamvõti „test“
2) Lisage loodud võtmele andmekirje nimega „kirje1“ väärtusega 1 (andmetüüp DWORD)
3) Eksportige loodud võti faili „key1.reg“
4) Leidke parajasti aktiivsele Windows XP kasutajale kehtivad Notepad'i seaded (vastav võti ja selle juurde kuuluvad andmekirjed). Eksportige need faili „notepad.reg“
5) Kopeerige fail „key1.reg“ faili „key2.reg“. Muutke faili „key2.reg“ faili sisu nii, et käivitades kustutatakse võti „test“ ja andmekirje „kirje1“. Veenduge, et faili käivitamisel vastavad andmed tõesti kustutati.

Group policy

Group Policy on vahend Active Directory arvutite ja kasutajate tsentraalseks haldamiseks. Group Policy abil on võimalik kontrollida süsteemi registri seadeid, tarkvara installeerimist, sisse- ja väljalogimisskripte ning Internet Explorer'i seadeid.

Group Policy seadeid hoitakse Group Policy objektidena (GPO). Üks GPO võib olla seotud (ja seeläbi kehtida) sadadele arvutitele ja kasutajatele. Iga arvuti ja kasutaja kohta saab ühes domeenis eksisteerida ainult üks Group Policy kogum, mis võib koosneda mitmest GPO'st.

Arvutile kehtivad Group Policy seaded laetakse operatsioonisüsteemi üleslaadimisel ning kasutaja kohta käivad seaded siis kui kasutaja sisse logib.

Kuigi Group Policy on peamiselt mõeldud kasutamisesk Ative Directory domeenis saab seda otstarbekalt kasutada ka eraldiseisva arvuti juures piiramaks kasutaja õigusi ning reguleerimaks mõningaid operatsioonisüsteemi seadeid, mille jaoks kasutajaliides puudub.

Group Policy seadete muutmiseks tuleb Windows XP'ga kaasa vaheleht (snap-in) „gpedit.msc“. Vahelehe vasakul pool on näha kohaliku arvuti Group Policy kaks peamist kategooriat:

- Computer Configuration
- User Configuration

Kategooriad jaotuvad mitmeteks alamkategooriateks, millede alla kuuluvad võimalikud valikud (nähtavad vahelehe paremal poolel). Klikkides mõnel valikul ilmub selle detailne kirjeldus ning olek. Valik võib olla ühes kolmest võimalikust olekust:

- Not Configured
- Enabled
- Disabled

Vaikimisi on kõik valikud alguses Not Configured ja kehtib valiku kirjelduses antud vaikimisi olukord. Vastavalt administraatori vajadustele saab valiku kas kinnitada või tühistada. Seda, mis mõlemas olekus toimub saab samuti lugeda valiku kirjeldusest.

Group Policy'ga seotud failid asuvad kataloogis:
C:\WINDOWS\system32\GroupPolicy

See kataloog sisaldab kolme alamkataloogi:

- **Adm** – Sisaldab seadete malle (.adm failid), mis on Group Policy'st valitavad.
- **Machine** - Sisaldab „registry.pol“ faili, mis sisaldab Group Policy Computer Configuration alajaotuse aktiivseid valikuid esindavaid registriseadeid. Need seaded lisatakse süsteemi registrisse operatsioonisüsteemi alglaadimisel. Kui arvutile on läbi Group Policy seatud algkäivitus või sulgemisskripte, siis on need selle kataloogi alamkataloogis „Scripts“.
- **User Folder** - Sisaldab „registry.pol“ faili, mis sisaldab Group Policy User Configuration ajajaotuse aktiivseid valikuid esindavaid registriseadeid. Need seaded lisatakse süsteemi registrisse kui kasutaja sisse logib. Kui arvutile on läbi Group Policy seatud algkäivitus või sulgemisskripte, siis on need selle kataloogi alamkataloogis „Scripts“. Lisaks sisaldab alamkataloog „Microsoft\IEAK“ registirvõtmeid, mis vastavad Group Policy alamjaotuse „\User Configuration\Windows Settings\Internet Explorer Maintenance“ all tehtud valikutele.

Lisaks on ülalmainitud kataloogis veel „GPT.ini“ fail, mis sisaldab informatsiooni lisatud mallide kohta.

Group Policy seadeid kontrollitakse ja vajadusel lisatakse registrisse automaatselt iga 90 minuti järel ning loomulikult ka siis kui toimub operatsioonisüsteemi algkäivitus ja kasutaja sissselogimine.

GPedit.msc kasutamine

Kõige lihtsam on Group Policy vahelehte kätte saada käivitades START->Run kirjutada tekstialasse „gpedit.msc“ ning vajutada „Run“
Nagu juba öeldud on valikud jaotatud kahte suurde ossa. Kuna otsida pole valikute seast võimalik tuleb sobiva seade leidmiseks teada selle täpset asukohta või otsida võimalikku sobivat seadet alajaotuste järgi.
Kui sobiv seade on leitud tuleb sellel hiirega teha topeltkõps ja avanenud aknast valida sobiv seade olek. Samas aknas on võimalik „Explain“ vahelehelt lugeda seade kohta käivat pikemat selgitust.
On võimalik olukord, kus Computer Configuration'i ja User Configuration'i all on sama seade. Sellisel juhul kehtib reegel, et Computer Configuration'i all olev seade on tähtsam kui User Configuration'i all olev seade v.a. juhul kui Computer Configuration'i all olev seade on olekus „Not Configured“

Valik Group Policy seadeid

Machine configuration\Administrative templates\System
*Turn off Autoplay
Enabled {not configured} - Keelab CD-de ja DVD-de automaatse käivitamise.

Machine configuration\Administrative templates\System\logon
*Don't display the Getting Started welcome screen at logon
Enabled {not configured} – Ei kuvata uutele kasutajatele mõeldud Windows'i kasutusõpetust.

Machine configuration\Administrative templates\System\Remote assistance
*Solicited Remote Assistance
Disabled {Not configured} – Keelav sissetulevad Remote Assistance ühendused.
*Offer Remote Assistance
Disabled {Not configured} – Keelab väljaminevad Remote Assistance ühendused.

Machine configuration\Administrative templates\System\system restore
*Turn off System Restore
Enabled {Not configured} – Keerab kinni System Restore teenuse
*Turn off Configuration
Enabled {Not configured} – Ei luba System Restore vahelehel seadeid muuta.

Machine configuration\Administrative templates\System\user profiles
*Delete cached copies of roaming profiles
Enabled {Not configured} – Allalaetud võrguprofiilid kustutatakse kui kasutaja välja logib.
*Only allow local user profiles
Enabled {Not configured} – Lubatud on ainult kohalikud profiilid.

Machine configuration\Administrative templates\Windows components\Internet explorer
*Make proxy settings per-machine (rather than per-user)
Enabled {Not configured} – Internet Exploreri proxi seaded on kõigile masina kasutajatele samad.
*Disable Automatic Install of Internet Explorer components
Enabled {Not configured} – Internet Explorer'i komponente ei installeerita automaatselt.

Machine configuration\Administrative templates\Windows components\windows installer
*Turn off creation of System Restore Checkpoints
Enabled {Not configured} – System Restore Checkpointe enam ei looda.

Machine configuration\Administrative templates\Windows components\windows messenger
*Do not allow Windows Messenger to be run
Enabled {Not configured} – Windows Messenger'i ei saa käivitada.
*Do not automatically start Windows Messenger initially
Enabled {Not configured} – Windows Messenger'i ei käivitata kui kasutaja sisse logib.

Machine configuration\Administrative templates\Windows components\windows update
*Allow Automatic Updates immediate installation
Enabled {Not Configured} – Automaatselt allalaetud operatsioonisüsteemi täiendusi võib kohe installeerida.

Machine configuration\Windows settings\Security settings\local policies\security options
*Devices: Allowed to format and eject removable media
Administrators and Interactive Users {Administrators} – kasutajad, kes tohivad formateerida lisaseadmeid (Näiteks USB pulki)
*Interactive logon: Do not display last user name
Enabled {Disabled} – Viimasena sisselogitud kasutaja nime ei näidata
*Interactive logon: Do not require CTRL+ALT+DEL
Enabled {Disabled} – Sisselogimisel ei pea kõigepealt ctrl-alt-del vajutama
*Interactive logon: Number of previous logons to cache (in case domain controller is not available)
0 logons {10} – ei peeta meeles ühegi viimase kasutaja logiandmeid.

User configuration\Administrative Templates\control panel
*Force classic Control Panel Style
Enabled {Not configured} – Control Panel'it näidatakse klassikalises stiilis.

User configuration\Administrative Templates\control panel\add or remove programs
*Remove Add or Remove Programs
Enabled {Not configured} – kasutajale ei kuvata Add or Remove vahelehte.

User configuration\Administrative Templates\control panel\printers
*Browse the network to find printers
Enabled {Not configured} – kasutaja ei saa võrgust printereid otsida
*Prevent deletion of printers
Enabled {Not configured} – kasutaja ei saa printereid kustutada

User configuration\Administrative Templates\desktop
*Prohibit user from changing My Documents path
Enabled {Not configured} – Kasutaja ei saa My Documents asukohta muuta

User configuration\Administrative Templates\desktop\active desktop
*Disable Active Desktop
Enabled {Not configured} – Active Desktop'i ei saa kasutada.

User configuration\Administrative Templates\network\network connections
*Prohibit access to properties of components of a LAN connection
Enabled {Not configured} – kasutaja ei pääse juurde võrguseadetele

User configuration\Administrative Templates\Start menu and taskbar
*Remove links and access to Windows Update
Enabled {Not Configured} – kasutajale ei kuvata Windows Update linki
*Add Logoff to the Start Menu
Enabled {Not configured} – Start menüüs kuvatakse LogOff valikut
*Clear history of recently opened documents on exit
Enabled {Not configured} – ei jäeta meelde viimati avatud dokumente
*Turn off personalized menus
Enabled {Not configured} – personaliseeritud menüüsid ei kasutata
*Force classic Start Menu
Enabled {Not configured} – Start menüüd näidatakse klassikalises stiilis.
*Do not display any custom toolbars in the taskbar
Enabled {Not configured} – Kasutaja ei saa taskbar'ile lisada oma menüüsid.

User configuration\Administrative Templates\system\CntrAltDel options
*Remove Lock Computer
Enabled {Not configured} – kasutaja ei saa arvtit lukustada
*Remove Change Password
Enabled {Not configured} – kasutaja ei saa parooli muuta