

Autonomy of User Groups in Microsoft Windows

Matthieu-P. Schapranow
André Wendt

Agenda

- Delegation Concepts
- Windows Authentication
- Access Control Lists and Entries
- Demonstration on demand (HPI Interaction example)
- Further possible solutions

Why delegate control ?

Reasons for task delegation

- Organizational structure
- Operational requirements
- Legal requirements
- ...

Autonomy (manage independently)

- *service autonomy*
- *data autonomy*

Isolation (prevent others from)

- *service isolation*
- *data isolation*

Which object
control can be
delegated ?

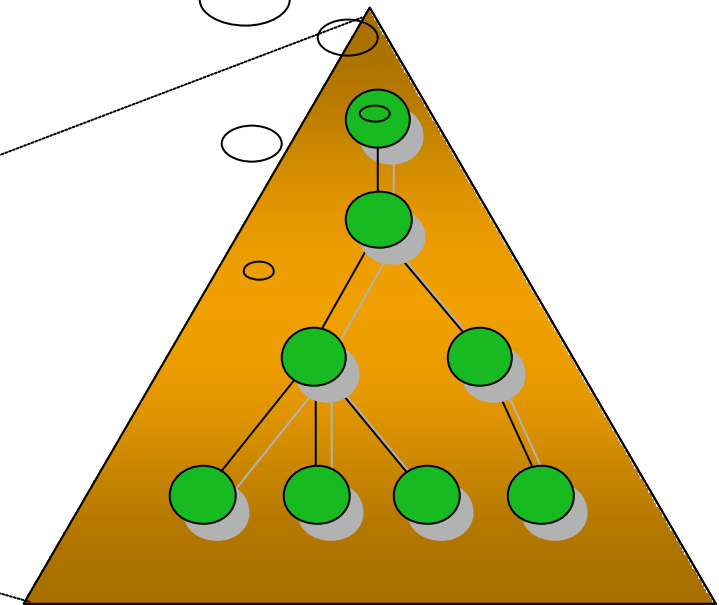
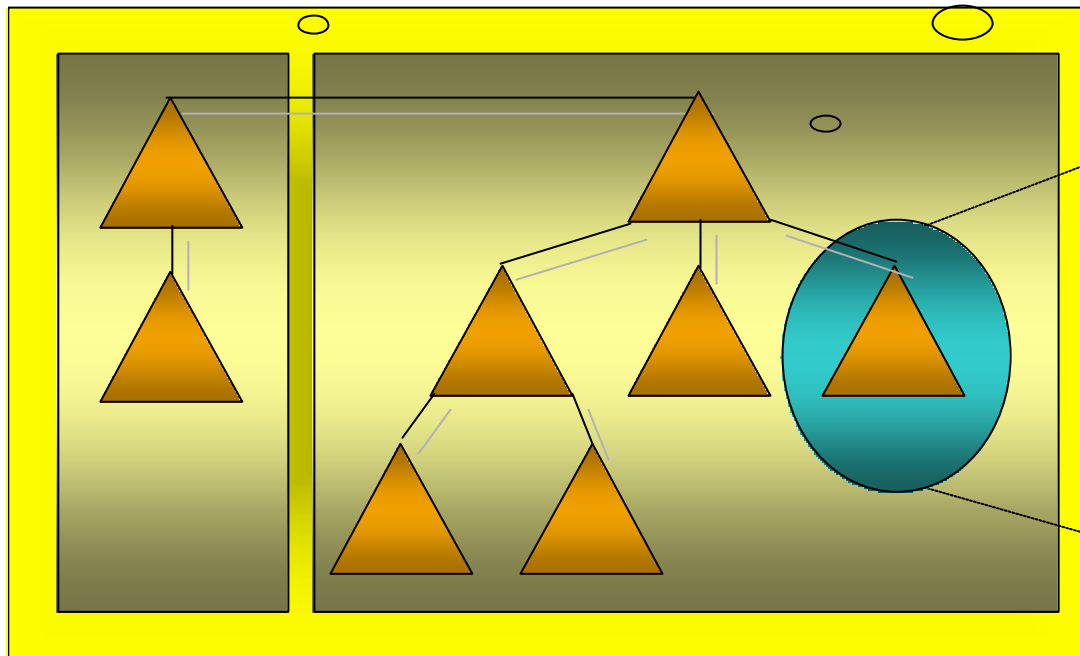
Delegation Concepts (contd.)

Abstract structures to delegate

- Organizational unit (OU)
- Domain
- Forest

Organizational Unit
(Child, Domain)
Domains

Where to start
delegation of control?



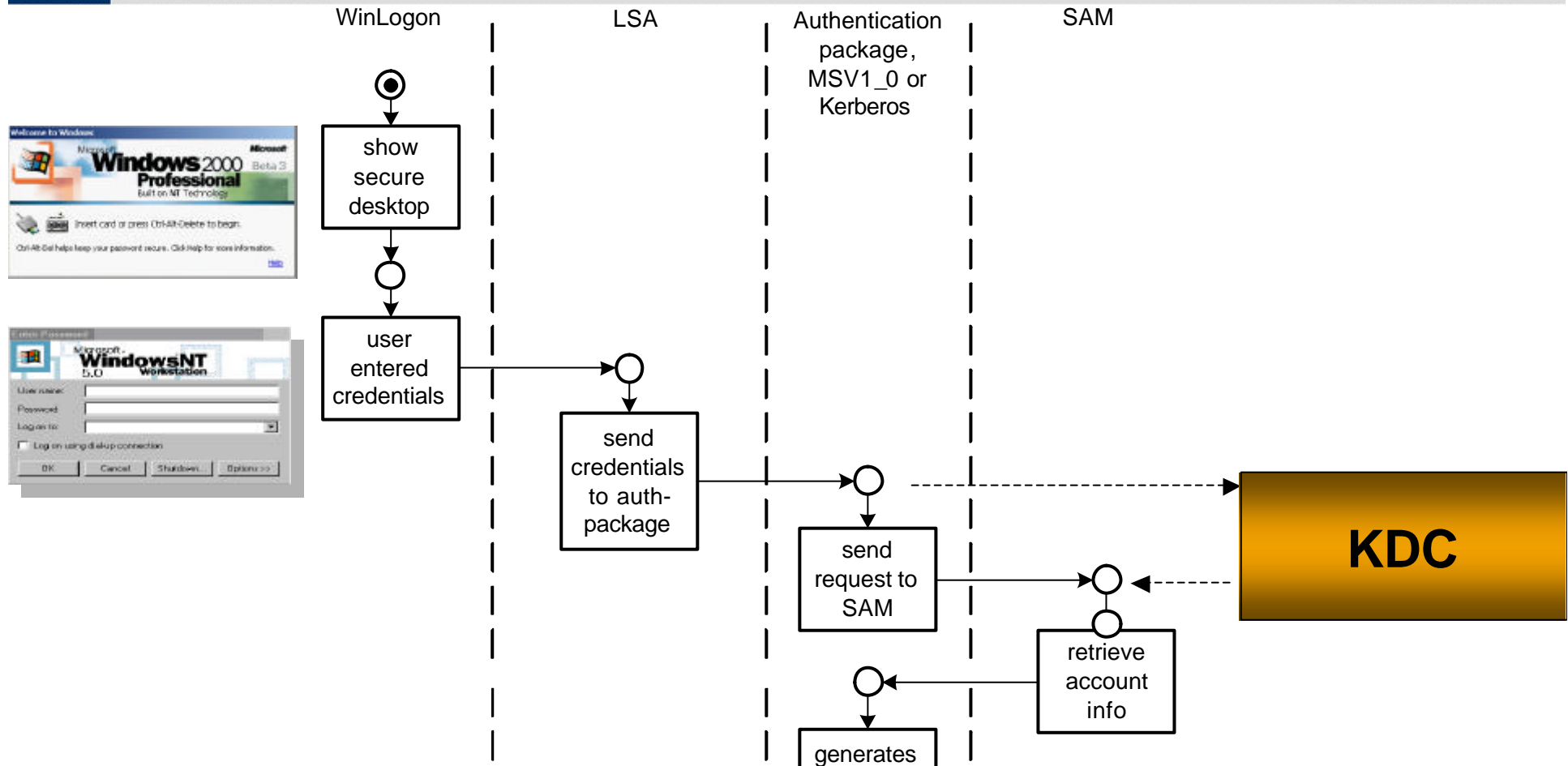
Delegation Concepts (contd.)

- **Staff OU**
 - ◆ OU per faculty
- **Students OU**
 - ◆ OU per year
- **Extern OU**
 - ◆ Multiple Sub-OUs

 Alexander Heine	Benutzer	Datenbanksysteme SS 05
 alexander.kirscht	Benutzer	Externe Gasthörer Prof.P...
 Amin Halihel	Benutzer	Externe Gasthörer CORB...
 Andre Kloth	Benutzer	
 Andre Neumann	Benutzer	Datenbanksysteme II SS05
 andre.luckow	Benutzer	Externe Gasthörer Prof.P...
 Andrea Schminck	Benutzer	Geoinformationssysteme ...
 Andreas Hertz	Benutzer	IFI 2002
 Andreas Sydow	Benutzer	Datenbanksysteme I SS05
 andreas.havenstein	Benutzer	Externe Gasthörer Prof.P...
 andreas.koehler	Benutzer	Externe Gasthörer Prof.P...
 andreas.schoe	Benutzer	Externe Gasthörer Prof.P...
 Andree Gesche	Benutzer	Datenbanksysteme II SS05
 Anja Schmidt	Benutzer	
 Anna Kovaleva	Benutzer	externe Gasthoerer Prof. ...
 anne.baumgrass	Benutzer	
 Anselm.Kegel	Benutzer	externer Gasthoerer Prof. ...
 armin.schaeper	Benutzer	Externe Gasthörer Prof.P...
 ben.hildebrandt	Benutzer	Externe Gasthoerer Prof. ...
 Benjamin Luepfert	Benutzer	Externe Gasthoerer Prof. ...
 benjamin.richter	Benutzer	Externe Gasthörer Prof.P...
 Bernd Pehlke	Benutzer	Datenbanksysteme SS05
 Bjoern Schuette	Benutzer	
 bjoern.piesker	Benutzer	Externe Gasthoerer Prof. ...
 bjoern.simmrohs	Benutzer	Externe Gasthörer Prof.P...
 carola.fanselow	Benutzer	Externe Gasthörer Prof.P...
 Carolin Lunemann	Benutzer	Geoinformationssysteme ...
 carsten.mohek	Benutzer	Externe Gasthörer Prof. ...
 carsten.reimann	Benutzer	Externe Gasthörer Prof.P...
 Caspar.Wrede	Benutzer	Externe Gasthörer Prof. P...
 chris.gehrmann	Benutzer	Externe Gasthörer Prof.P...
 Christian Bommersbach	Benutzer	
 christian.aethner	Benutzer	Externe Gasthörer Prof.P...
 christian.herrmann	Benutzer	Externe Gasthörer Prof.P...
 christian.loclair	Benutzer	Externe Gasthörer Prof.P...
 christian.pelz	Benutzer	Externe Gasthörer Prof.P...
 christian.schmidt	Benutzer	Externe Gasthörer Prof.P...
 christoph.kling	Benutzer	Externe Gasthörer Prof.P...



Windows Authentication



Static access control

- once a user is logged-on, the Access Token is not changed
- whether access is granted is not determined at the time of access

Active Directory (AD) object permissions

- Windows in general: an attempt to access a securable object is subject to an access check
- same applies to AD objects – AD permissions control who can do what on those objects
- the three default permissions are read, write, and full control
- every AD object has these permissions
- *some may have more (depending on object class)*

Some directory service access rights are:

- read/modify permissions
- read/write all properties
- create/delete all child objects

Those permissions can be categorized into

- **standard and**
- **special permissions**
 - ◆ **validated writes** (validate a property value before writing it)
 - ◆ **“extended rights”** (sets of properties)

Group object comes with particular permissions:

- **read/write group name**
- **read/write groupType**
- **read/write groupAttributes**
- **read/write members**

Access Control Entries for Groups

Objekt Eigenschaften

Name: Domänen-Admins (HPI-OS\Domänen-Admins)

Übernehmen für:
Nur dieses Objekt

Berechtigungen: Zulassen

Berechtigungen:	Zulassen	Verweigern
Alle Eigenschaften lesen	<input type="checkbox"/>	<input type="checkbox"/>
Alle Eigenschaften schreiben	<input type="checkbox"/>	<input type="checkbox"/>
Löschen	<input type="checkbox"/>	<input type="checkbox"/>
Unterstruktur löschen	<input type="checkbox"/>	<input type="checkbox"/>
Berechtigungen lesen	<input type="checkbox"/>	<input type="checkbox"/>
Berechtigungen ändern	<input type="checkbox"/>	<input type="checkbox"/>
Besitzer ändern	<input type="checkbox"/>	<input type="checkbox"/>
Alle bestätigten Schreibvorgänge	<input type="checkbox"/>	<input type="checkbox"/>
Alle erweiterten Rechte	<input type="checkbox"/>	<input type="checkbox"/>
Alle untergeordneten Objekte erstellen	<input type="checkbox"/>	<input type="checkbox"/>
Alle untergeordneten Objekte löschen	<input type="checkbox"/>	<input type="checkbox"/>
Senden an	<input type="checkbox"/>	<input type="checkbox"/>
Sich selbst als Mitglied hinzufügen/entfernen	<input type="checkbox"/>	<input type="checkbox"/>

Objekt Eigenschaften

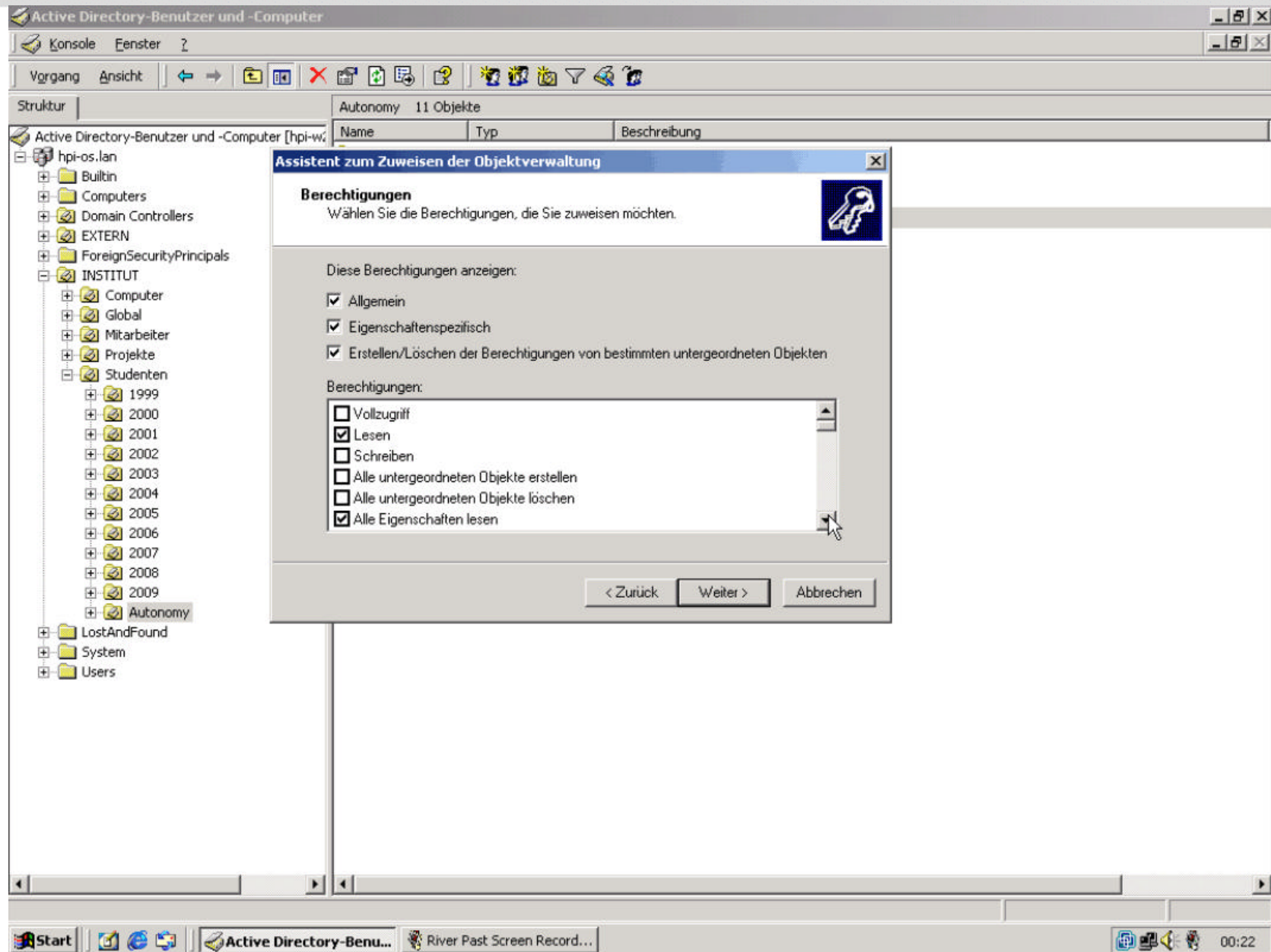
Name: Domänen-Admins (HPI-OS\Domänen-Admins) Andern...

Übernehmen für:
Nur dieses Objekt

Berechtigungen: Zulassen Verweigern

Berechtigungen:	Zulassen	Verweigern
memberof schreiben	<input type="checkbox"/>	<input type="checkbox"/>
Mitglieder lesen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Mitglieder schreiben	<input checked="" type="checkbox"/>	<input type="checkbox"/>
nTGroupMembers lesen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
nTGroupMembers schreiben	<input checked="" type="checkbox"/>	<input type="checkbox"/>
objectSid lesen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
objectSid schreiben	<input checked="" type="checkbox"/>	<input type="checkbox"/>
primaryGroupToken lesen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
primaryGroupToken schreiben	<input checked="" type="checkbox"/>	<input type="checkbox"/>
tokenGroupsGlobalAndUniversal lesen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
tokenGroupsGlobalAndUniversal schreiben	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Verwaltet von lesen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Verwaltet von schreiben	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Demonstration on demand (HPI Interaction example)



Demonstration on demand (contd.)

The screenshot shows the Active Directory console with the 'Eigenschaften von 2002' dialog box open. The 'Zugriffseinstellungen für 2002' sub-dialog is active, displaying a table of permissions for the '2002' object.

Typ	Name	Berechtigung	Übernehmen für
...	Zula... Domänen-Admins (HPI-...	Uneingeschr...	Nur dieses Objekt
...	Zula... stud2002 (HPI-OS\stud...	Speziell	Dieses und alle untergeordn...
...	Zula... SYSTEM	Uneingeschr...	Nur dieses Objekt
...	Zula... stud2002 (HPI-OS\stud...	"Organisation...	Dieses und alle untergeordn...
...	Zula... stud2002 (HPI-OS\stud...	"Kontakt"-Ob...	Dieses und alle untergeordn...
...	Zula... stud2002 (HPI-OS\stud...	"Gruppe"-Obj...	Dieses und alle untergeordn...
...	Zula... stud2002 (HPI-OS\stud...	"Freigegeben...	Dieses und alle untergeordn...

Buttons: Hinzufügen..., Entfernen, Anzeigen/Bearbeiten...

Vererbare übergeordnete Berechtigungen übernehmen

Buttons: OK, Abbrechen, Übernehmen

Demonstration on demand (contd.)

The screenshot shows a Windows XP desktop with a blue background. On the left side, there are four desktop icons: 'Arbeitsplatz', 'Netzwerkumgebung', 'Papierkorb', and 'Confidential'. In the center, a dialog box titled 'Ausführen als' is open. The dialog box contains the following text and controls:

Ausführen als

Welches Benutzerkonto soll zum Ausführen dieses Programms verwendet werden?

Aktueller Benutzer (SCHAPPY-MOBIL\SCHAPPY)

Computer und Daten vor nicht autorisierter Programmaktivität schützen

Mit dieser Option können Computerviren davon abgehalten werden, den Computer oder persönliche Daten zu beschädigen. Sie kann aber auch dazu führen, dass ein Programm nicht korrekt ausgeführt werden kann.

Folgender Benutzer:

Benutzername:

Kennwort:

OK Abbrechen

At the bottom of the desktop, the taskbar shows the Start button, several application icons, and the system tray with the text 'Windows XP Professional Build 2600.xpsp_sp2_gdr.050301-1519 (Service Pack 2)', 'MSVDM', and the time '02:43'.

Further ways to access the AD

- **access and administration of groups via webserver**
 - ◆ PHP-/ASP scripts
 - ◆ Requires access to AD for webserver process
 - ◆ Poses high security risk
- **application programs written for that particular task**
 - ◆ More effort
 - ◆ Security issues
 - ◆ Batch scripts
 - ◆ VB scripts

Pros:

- Fine granular (more than rwx)
- Simple way to delegate control
- Transparent and scalable

Cons:

- Single-sign-on credential
- Replicas need time (transitional trusts)
- Abandoned Groups (Large Numbers of ACEs in ACLs Impair Directory Service Performance)

Thank you for the attention!

Any questions?

- Addison-Wesley, *Inside Active Directory*, 2002
- Arkills, Brian and Wilper, Ross. *Overview of Active Directory Security*. June 4, 2002. (<http://windows.stanford.edu/Public/Security/ADSecurityOverview.htm>)
- Baur, Ralph. *Windows 2000 – Active Directory*. Microsoft GmbH. November 8, 1999.
- Hillman, Mary. *Best Practices for Delegating Active Directory Administration*. Microsoft Corporation, November 24, 2003.
- Meyer, Karl-Heinz et al. *Securing the Windows Plattform*. Presentation, Microsoft Corporation & HP Services, March 29, 2004
- Microsoft Corporation, *Windows NT 5.0 Operating System – Using the Delegation of Control Wizard, Beta 2 Technical Walkthrough*, July 1998
- Microsoft GmbH, *Microsoft Windows Server 2003, Active Directory – technische Übersicht*, July 2002
- Microsoft Technet, *Design Considerations for Delegation of Administration in Active Directory*, June 2005.
(<http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/plan/addeladm.mspx>)