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 ?

Delegation Concepts

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***

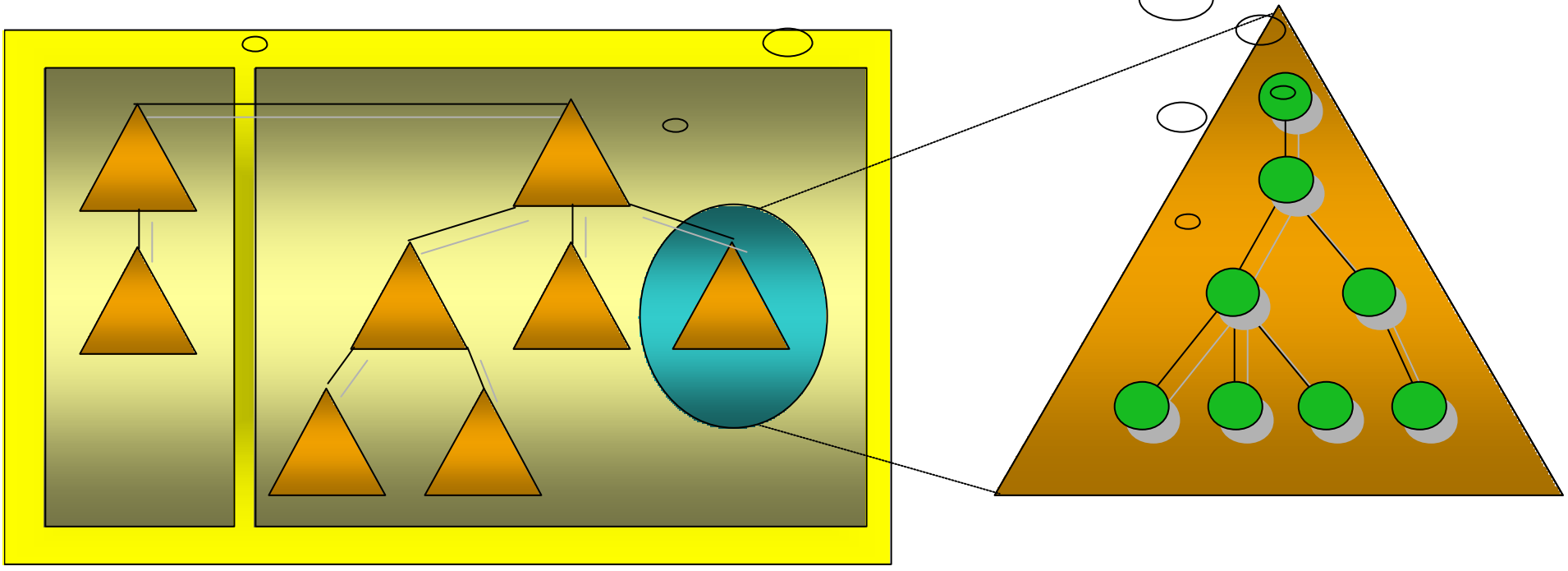
Which object control can be delegated ?

Delegation Concepts (contd.)

Abstract structures to delegate

- Organizational unit (OU)
- Domain
- Forest

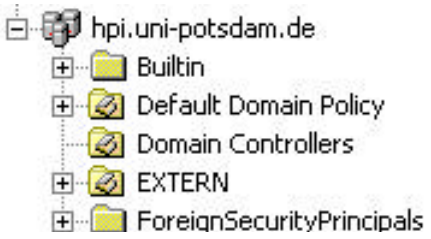
Where to start delegation of control ?



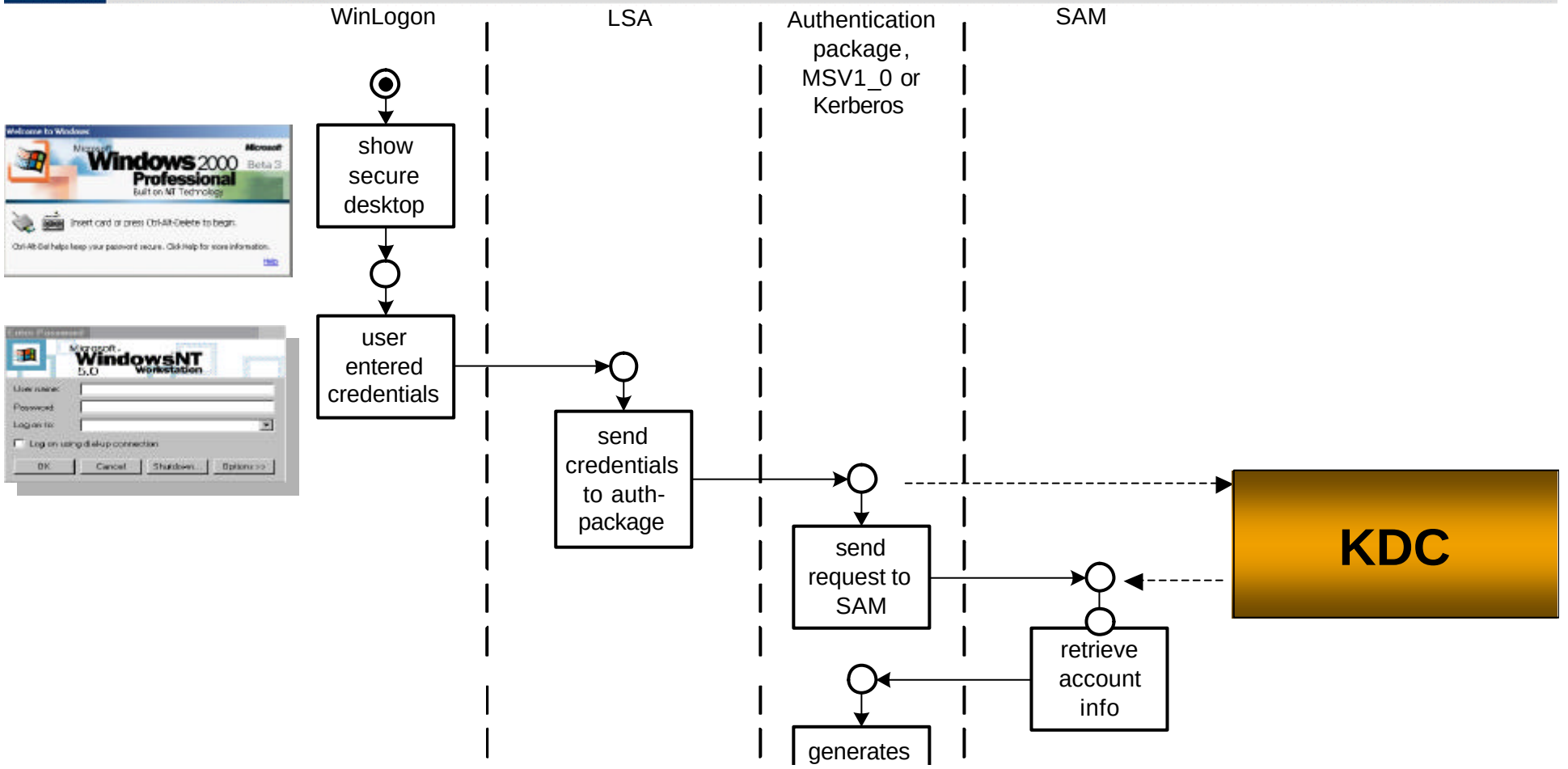
Delegation Concepts (contd.)

- **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	Dabenbanksysteme 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

Access Control Lists

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

Access Control Lists (contd.)

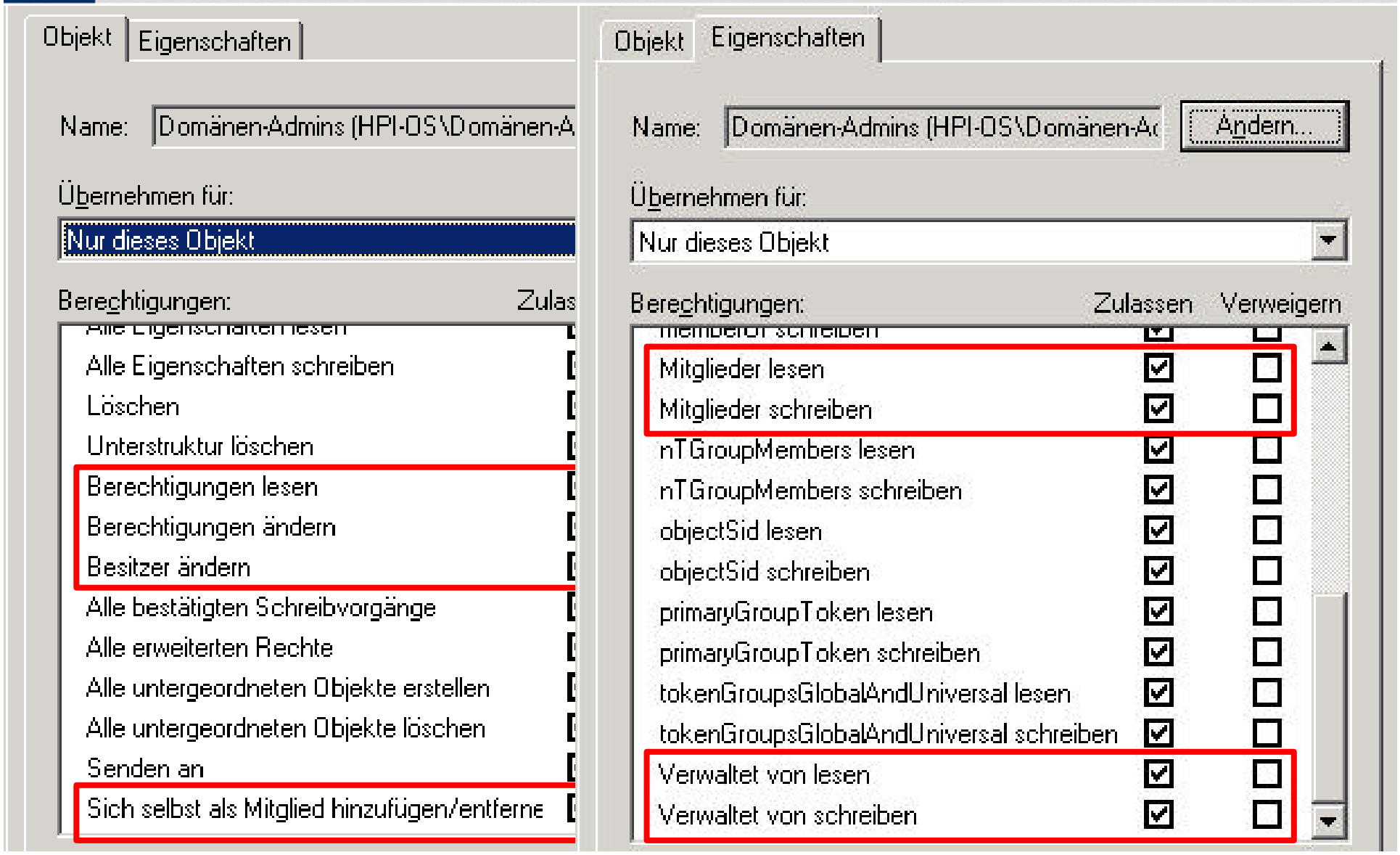
Those permissions can be categorized into

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

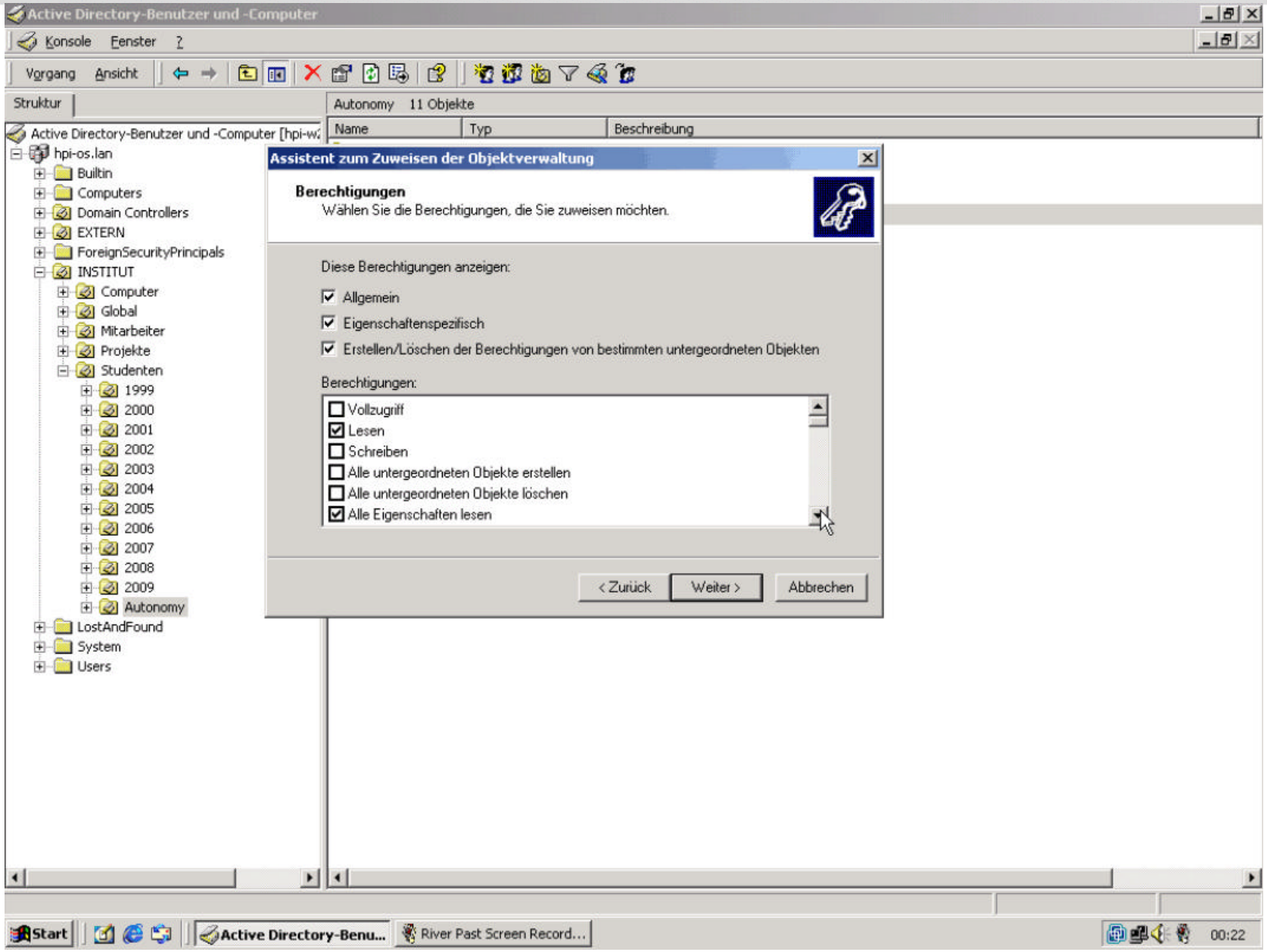
Group object comes with particular permissions:

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

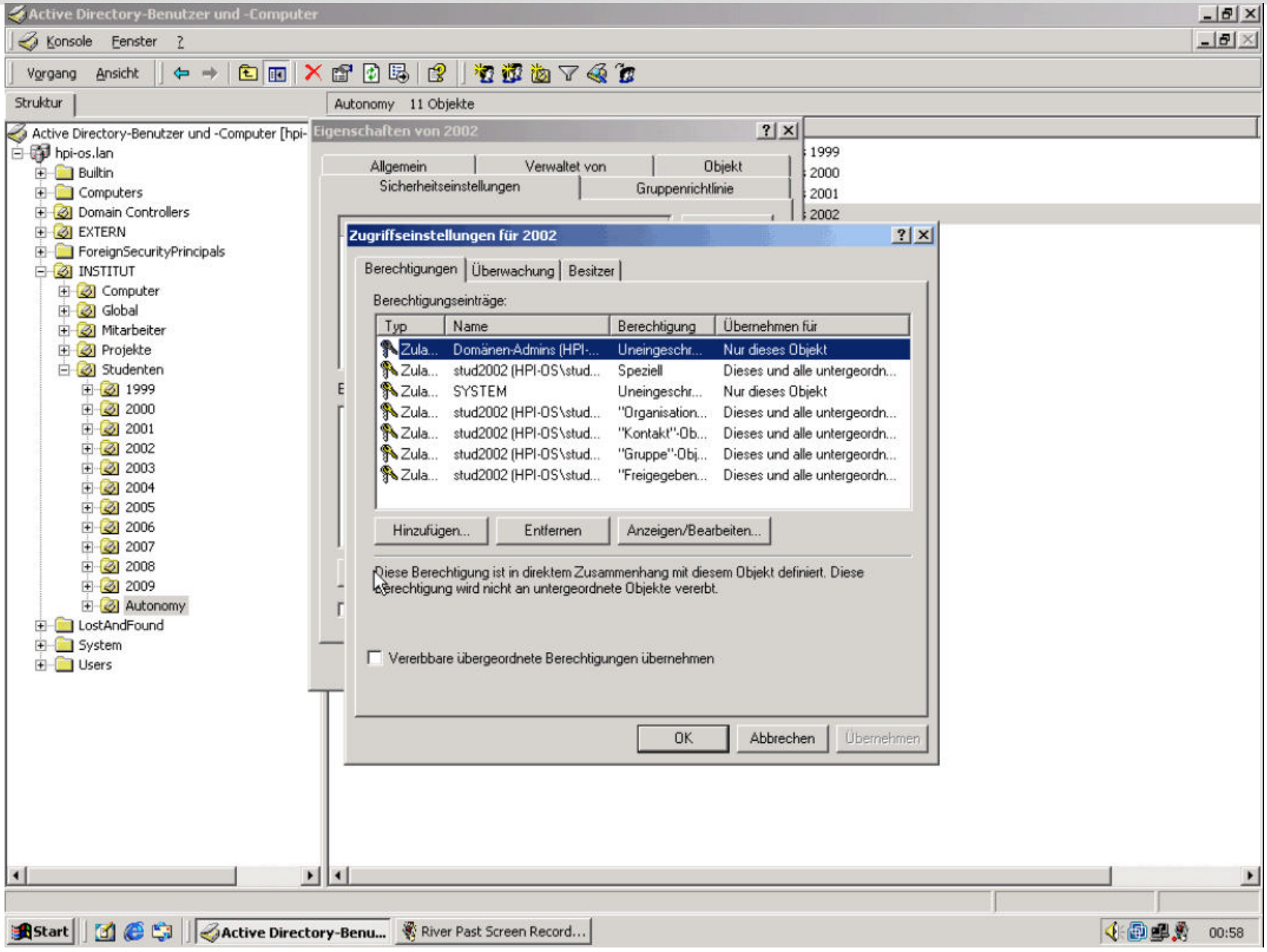
Access Control Entries for Groups



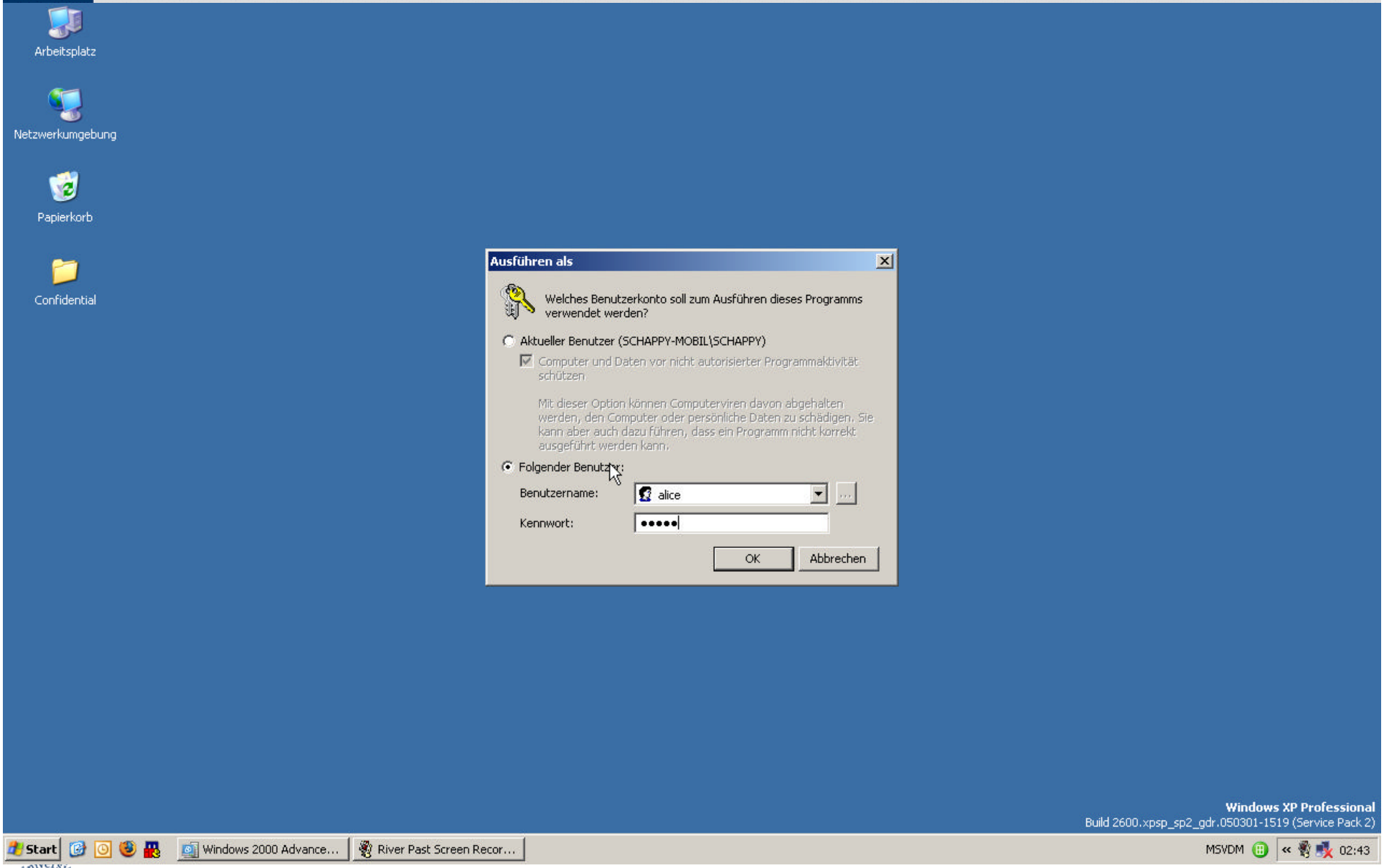
Demonstration on demand (HPI Interaction example)



Demonstration on demand (contd.)



Demonstration on demand (contd.)



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 vs. Cons

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?

Literature

- 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 Corperation, *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)