EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

ZENTRUM FÜR
DATENVERARBEITUNG
(ZDV)

Namenskonzept des Active Directory der Universität Tübingen

Version: 1.1

Autor: Markus Reigl (markus.reigl@uni-tuebingen.de)
Jochen Schmid (jochen.schmid@uni-tuebingen.de)
Benjamin Lang (benjamin.lang@uni-tuebingen.de)

Letzte Revision: 27.05.2019

Änderungshistorie

Autor	Datum	Status	Änderungen/Bemerkungen
Markus Reigl		Entwurf	Erstellung
Markus Reigl	22.06.11	Entwurf	Änderung Gruppentypen Ergänzung der Berechtigungsbezeichner
Markus Reigl	04.10.11	Entwurf	Ergänzung der Berechtigungsbezeichner Korrektur der OU-Namen
Markus Reigl	23.11.11	Entwurf	Ergänzung der Berechtigungsbezeichner
Markus Reigl	30.11.11		Nummerierung der 7. und 8. Stelle im Präfix
Markus Reigl	05.06.14	Final	Diverse Ergänzungen, Terminals und externe Computerobjekte, Gruppennamen Datei-/Ordnerberechtigugnen
Benjamin Lang	27.05.19	Final	Ergänzungen/Änderungen für delegierte OUs

Inhalt

Zweck des Dokuments

Die Universität Tübingen setzt zur Verwaltung von Windows Ressourcen das Microsoft Verzeichnissystem Active Directory (AD) ein. Diese hierarchische Datenbank verlangt für Objektklassen zum Teil global eindeutige Namen. Dieses Dokument regelt verbindlich die Vergabe von Namen für Objekte wie z.B. Computer, Drucker, Gruppen, Richtlinien. Es stellt damit die Grundlage für eine dezentrale Administration der im AD befindlichen Ressourcen der Universität Tübingen dar.

Gültigkeit und Zielgruppe

Dieses Dokument richtet sich an alle Mitarbeiter, Studenten und Wissenschaftler, die Windows Rechner, Drucker und Benutzer im Active Directory der Universität Tübingen administrieren. Die hier definierte Namenskonvention ist für alle Beteiligten **verpflichtend**.

Einleitung

Für die Administration der Microsoft Windows Infrastruktur wird der *Microsoft Active Directory Service* (ADS) eingesetzt. In diesem Verzeichnis werden Objekte in einer hierarchischen Struktur von Containern gespeichert. Bei diesen Containern handelt es sich im Normalfall um *Organisatorische Einheiten* (*Organisational Units*, OUs). Die innerhalb des ADS abgelegten Objekte müssen eindeutige Namen besitzen.

Bei der existierenden dezentralen Administration von Ressourcen ist deshalb ein Namenskonzept notwendig, das ohne aufwändige Abstimmung die Eindeutigkeit der Objektnamen gewährleistet. Dies wird durch ein für jede OU definiertes Präfix erreicht. Administratoren können dezentral Objekte mit diesem Präfix eindeutig benennen.

Weiterhin sei erwähnt, dass das hier vorgestellt Namenskonzept unabhängig von der Windows Infrastruktur und dem ADS angewendet werden kann.

ADS-Struktur

In diesem Kapitel wird die Struktur des ADS erläutert. Das wesentliche Designziel ist es, Verantwortlichkeiten und administrative Aufgaben an die verschiedenen Organisatorischen Einheiten der Universität delegieren zu können.

Im ADS wird primär die administrative Struktur im Hinblick auf die IT abgebildet. Die Modellierung der realen organisatorischen Struktur der Universität steht nicht im Vordergrund, wird aber soweit möglich und sinnvoll berücksichtigt.

Allgemeine Hierarchie

Alle Organisatorischen Einheiten der Uni-Tübingen werden unter der OU „UT“ zusammengefasst. Dies ermöglicht eine spätere Erweiterung um andere Einrichtungen und fasst alle OU’s der Uni-Tübingen in einem Zweig zusammen.

Die Microsoft Standard-OU’s im ADS bleiben in ihrer Form unverändert.

Organistationshierarchie

Das Organisationsmodell der Uni-Tübingen wird auf 4 Ebenen beschränkt. Die Ausprägung der Ebenen unterscheidet sich aber je Fakultät/Bereich, da diese intern nicht homogen strukturiert sind.

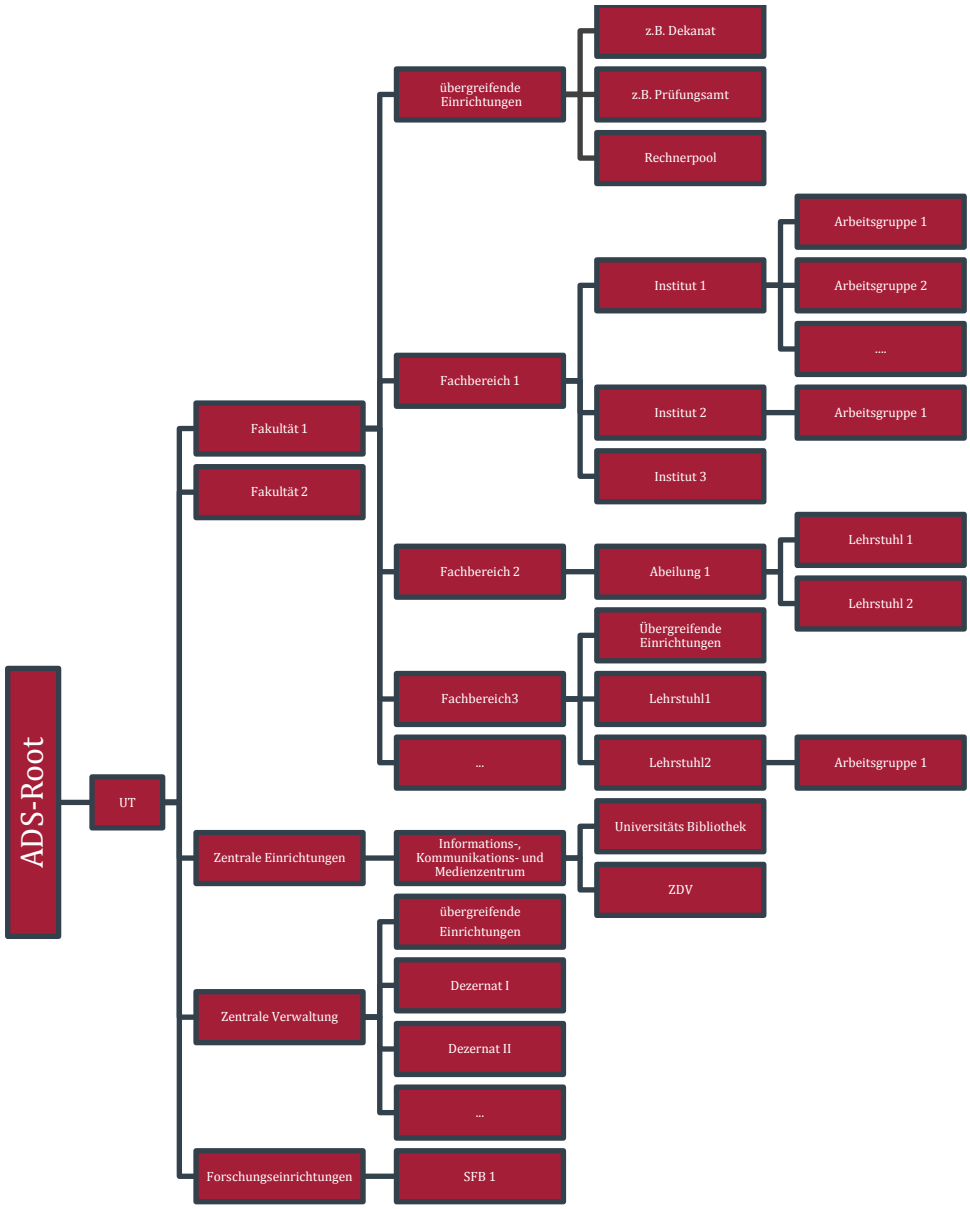

Abb. 1: Beispiel der Organisationstruktur der Uni-Tübingen

Objektverwaltungshierachie

Innerhalb einer Org. Einheit werden die zu verwaltenden Objekte in der folgenden Struktur organisiert. Vom ZDV betreute Computer (Managed Clients) kommen z.B. in die OU „Computers / M“. Von den Org. Einheiten selbst betreute Computer werden in der OU „Computers / D“ verwaltet. Diese Gruppierung erlaubt das Zuordnen unterschiedlicher Richtlinien, das Verteilen von unterschiedlicher Software, etc. Die Org. Einheiten können auf Anfrage eine weitere Unterteilung ihrer „D“ OUs beantragen.

Gruppen für Berechtigungen und Rollen werden in den OUs „Groups / M“ und „Groups / C“ abgelegt.

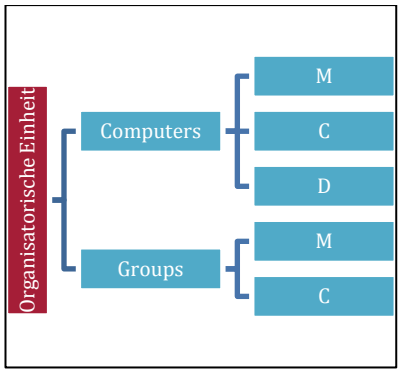

Abb. 2: Objektverwaltungshierarchie einer OU

Gesamtstruktur

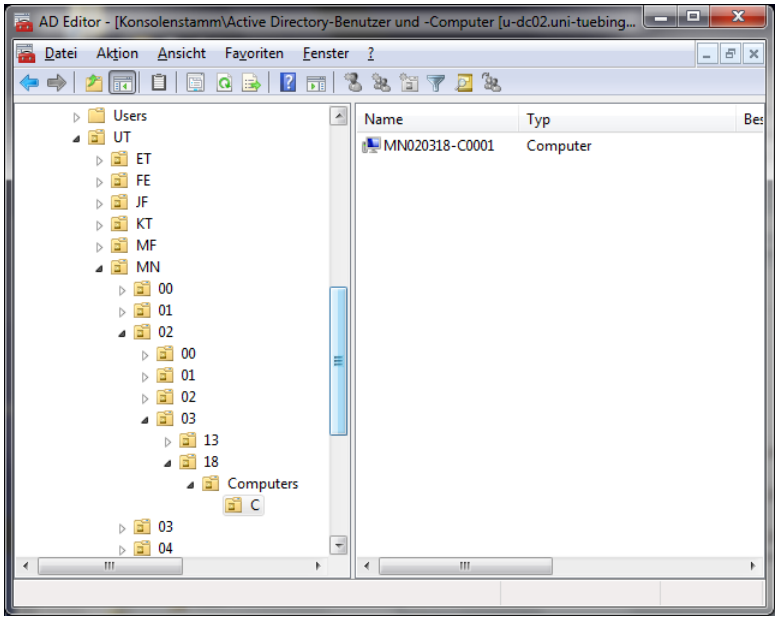

Abb. 3: Auszug der OU Struktur des ADS

Benutzerobjekte

Benutzer werden an von Uni-Tübingen zentral angelegt und automatisch in das ADS importiert. Eine Namensrichtlinie muss an dieser Stelle nicht festgelegt werden.

Aufbau und Benennung der OUs

Struktur der Organisation

Derzeit gibt es für die Uni-Tübingen keine einheitliche Bezeichnung für Fakultäten, Lehrstühle und Institute. Die 2010 vorgenommene Restrukturierung führte zu einem Zusammenschluss der bisherigen Fakultäten. Da die alten Fakultäten, wie z.B. Mathematik, innerhalb der neuen Mathematischen-Naturwissenschaftlichen Fakultät weiterhin eine eigene organisatorische Einheit bilden, werden diese in einer eigenen Ebene der OU-Struktur abgebildet.

Aufbau der Kurzbezeichnung für Organisatorische Einheiten

Der Kurzbezeichner für Org. Einheiten wird aus bis zu 4 Ebenen zusammengesetzt. Jede Ebene wird mit 2 Zeichen abgekürzt. Die Abkürzungen werden ohne

Trennzeichen aneinandergehängt. Die minimale Länge der Bezeichnung ist also 2, die maximale Länge 8 Zeichen.

1. und 2. Stelle: Fakultät, Zentrale Einrichtung, Forschungseinrichtungen

Die Abkürzungen aller Fakultäten und Einrichtungen sind folgendermaßen festgelegt:

ET	Evangelisch-Theologische Fakultät
FE	Forschungseinrichtungen
IT	Islamische Theologie
JF	Juristische Fakultät
KT	Katholisch-Theologische Fakultät
MF	Medizinische Fakultät
MN	Mathematisch-Naturwissenschaftliche Fakultät
PF	Philosophische Fakultät
WS	Wirtschafts- und Sozialwissenschaftliche Fakultät
ZE	Zentrale Einrichtungen
ZV	Zentrale Verwaltung

3. und 4. Stelle: Fachbereich, Dezernat, Fachbereichsübergreifende Einrichtungen

Um möglichst unabhängig von der Benennung zu sein, werden Fachbereich und Dezernate innerhalb einer Fakultät startend mit 01 durchnummeriert. Die Nummer 00 ist immer für zentrale Einrichtungen dieses Bereichs (z.B. Dekanat, Bibliothek, Rechnerpool, etc.) reserviert.

Liste ausgewählter Fachbereiche:

MN	**00**	übergreifende Einrichtungen, Mathematisch-Naturwissensch. Fakultät
	01	Biologie
	02	Chemie
	03	Geowissenschaften
	04	Informatik
	05	Mathematik
	06	Pharmazie und Biochemie
	07	Physik
	08	Psychologie
PF	**00**	übergreifende Einrichtungen, Philosophische Fakultät
	01	Altertums- und Kunstwissenschaften
	02	Asien-Orient-Wissenschaften
	03	Geschichtswissenschaft
	04	Neuphilologie
	05	Philosophie - Rhetorik - Medien
WS	**00**	übergreifende Einrichtungen, Wirtschafts- und Sozialwissens. Fakultät
	01	Sozialwissenschaften
	02	Wirtschaftswissenschaft
ZE	**01**	Baden-Württembergisches Brasilien-Zentrum
	02	Informations-, Kommunikations- und Medienzentrum
	06	Personalrat
ZV	**01**	Dezernat I - Forschung, Strategie, Recht
	02	Dezernat II - Studium, Recht
	03	Dezernat III - Internationale Angelegenheiten
	04	Dezernat IV - Personal, Innere Dienste

	05	Dezernat V - Finanzen
	06	Dezernat VI - Bau, Sicherheit und Umwelt
FE	**01**	SFB 833

5. und 6. Stelle: Abteilung, Seminar, übergreifende Einrichtungen

Abteilungen werden innerhalb eines Fachbereichs/Dezernats durchnummeriert. Die Abteilung „00“ bleibt dabei für übergreifende Einrichtungen des Fachbereichs reserviert.

Folgende Nummern innerhalb der übergreifenden Einrichtungen einer Fakultät sind reserviert:

01	Dekanat / Verwaltung
02	Prüfungsamt
03	Bibliothek / Archiv
04	Fachschaft / Gleichstellung
05	PC-Pool / PC-Labor
09	Emeritiert und i.R.

Beispiel:

MN0002: Prüfungsamt der Mathematisch-Naturwissenschaftlichen Fakultät (innerhalt der übergreifenden Eirichtungen)

PF0203: Abteilung Japanologie (03), Asien-Orient-Wissenschaften (02), Philosophische Fakultät (PF)

7. und 8. Stelle: Arbeitsbereiche, Lehrstuhl

Arbeitsbereiche und Lehrstühle werden innerhalb einer Abteilung startend mit „10“ durchnummeriert. Die Bezeichnungen „00“..“09“ bleibt dabei für übergreifende Einrichtungen der Abteilung reserviert. Sind Einrichtungen der 4.Ebene nochmals gruppiert, so kann diese Gruppierung über die Vergabe der Nummern 10, 20, 30, … realisiert werden.

Folgende Nummern innerhalb der übergreifenden Einrichtungen einer Abteilung sind reserviert:

01	Verwaltung
03	Bibliothek
04	Fachschaft
05	PC-Pool
06	(Seminarverwaltung)
09	Emeritiert und i.R.

Beispiele:

WS010503: Bibliothek (03) der Abteilung Sportwissenschaft (05) im Fachbereich Sozialwissenschaften (01) der Wirtschafts- und Sozialwissenschaftlichen Fakultät (WS)

MN010111: Arbeitsbereich „Evolutionsökologie der Tiere“ (11) im Institut für Evolution und Ökologie (01) des Fachbereichs Biologie (01) der Mathematisch-Naturwissenschaftlichen Fakultät (MN)

Präfix einer OU

Für die im Weiteren vorgestellten Objektnamen wird der Präfix der OU, der das Objekt zugeordnet wird, benötigt. Dieses Präfix bildet sich aus der in diesem Abschnitt definierten Kurzbezeichnung der OU und einem nachfolgenden Bindestrich als Trennzeichen.

Beispiele für Präfixe:

WS020003-	Bibliothek der Wirtschaftswissenschaft
MN0203-	Institut für Organische Chemie des Fachbereichs Chemie der Mathematisch-Naturwissenschaftlichen Fakultät

Namenskonzept für Objekte

In diesem Kapitel wird die Vergabe von Namen für die folgenden Objektklassen definiert:

- Computer / Terminals
- Drucker
- Gruppen (insbesondere für den Zugriff auf Ressourcen)
- Gruppenrichtlinien
- Ressourcen (wie Ordnerfreigaben, etc.)

Obwohl im Microsoft ADS Namen nicht nach Groß-/Kleinschreibung unterschieden werden, sollten für ein einheitliches Erscheinungsbild alle Objektnamen mit Großbuchstaben erzeugt werden.

Computerobjekte

Der hier definierte Computernamen wird für die Benennung des Computers innerhalb von Windows und im AD benutzt.

Der Computernamen setzt sich aus dem Präfix der OU, der der Computer zugeordnet wird, und dem Bezeichner zusammen. Der Bezeichner für Clientsysteme besteht aus einem „C“ und einer laufenden Nummer (4-stellig). Serversysteme starten mit einem „S“, Terminals (Thin-Clints, Zero-Clients) starten mit einem „T“. Die laufende Nummer kann beliebig (mit nachfolgenden Nummernbereich) vergeben werden, muss aber innerhalb der OU für die Computer eindeutig sein.

Empfohlen wird die laufende Vergabe von Nummern. Nummern von nicht mehr existierenden Rechnern sollten nicht wieder vergeben werden.

Um Geräte außerhalb des AD konform zu dem hier definierten Namensschema benennen zu können, wird der Nummernkreis 8000-8999 für externe (nicht im AD befindliche Geräte) reserviert. 9000-9999 bleiben ebenso für zukünftige Verwendung reserviert. Der Nummernkreis für Objekte im AD ist also 0001-7999.

Aus Kompatibilitätsgründen sollte der Computername aus nicht mehr als 15 Zeichen bestehen.

Bezeichner	Objekttyp
***C**nnnn*	Clientcomputer (Desktop, Notebook, etc.)
***S**nnnn*	Serversystem
***T**nnnn*	Terminal

Beispiel:

MN010003-C0134	Computer „C0134“ in der Biologiebibliothek (Math. Nat. Fakultät).
ZE0202-S0017	Server „S0017“ im ZDV

Druckerobjekte

Drucker werden analog zu Computern bezeichnet. Der Name eines Druckers setzt sich aus dem Präfix der OU, dem Buchstaben „P“ und einer laufen Nummer (3-stellig) zusammen.

Aus Kompatibilitätsgründen sollte der Druckername aus nicht mehr als 15 Zeichen bestehen.

Gibt es bei einem Drucker für verschiedene Seitenbeschreibungssprachen (PostScript, PCL) dedizierte Queues, so kann dies an den Druckernamen angehängt werden.

Bezeichner	Objekttyp
P*nnn*[PS|PCL]	Drucker

Beispiele:

MN010003-P002 Drucker„P002“ in der Mathem.-Naturwissen. Bibliothek.

ZV03-P319PCL Die PCL-Queue der Druckers „P319“ im Dezernat III

Gruppen

Bei Gruppen werden organisatorische Gruppen und Berechtigungsgruppen unterschieden.

Mit organisatorischen Gruppen werden User in Rollen oder Funktionen eingeordnet. Dies ermöglicht es einem neuen Mitarbeiter, Sachbereiter, etc. sehr einfach die gleichen Rechte zuzuordnen.

Berechtigungsgruppen dienen zur Bündelung der Zugriffe mit unterschiedlichen Berechtigungen auf eine Ressource. Bei jeder Ressource (z.B. ein Dateiordner) wird für jede unterschiedliche Zugriffsberechtigung (full, change, read, add, browse, manage, admin) eine separate Gruppe angelegt und diese mit den entsprechenden Berechtigungen der Ressource zugewiesen. Die organisatorischen Gruppen der Rollen, die auf die Ressource zugreifen müssen, werden in die Berechtigungsgruppe aufgenommen. Im Ausnahmefall können dies auch einzelne Accounts sein. Durch dieses Vorgehen wird an der Ressource nur eine kleine überschaubare Anzahl von Gruppen zugewiesen, die sich im Normalfall nicht mehr ändert und die ganze Verwaltung der Berechtigungen wird über Gruppen im AD vorgenommen. Das Zuweisen einzelner Benutzer direkt auf Ressourcen ist tabu.

Der Name einer Gruppe setzt sich zusammen aus Präfix, Bezeichner und Beschreibung.
Das Präfix wird zugewiesen, falls die Gruppe zu einer OU gehört, bei globalen Gruppen entfällt das Präfix.
Der Bezeichner unterscheidet sich nach Typ der Gruppe (organisatorisch, Berechtigung) und Art der Ressource.

Bezeichner	Gruppe für
gO_	Organisatorische Gruppe (Zusammenfassung von Benutzern einer bestimmten Rolle, Aufgabe, Funktion)
gF_	Datei-/Ordnerberechtigungen
gS_	Freigabe
gP_	Berechtigung für Drucker
gD_	Berechtigungen innerhalb des ADS (Directory)
gG_	Berechtigungen, Zuordnung von Gruppenrichtlinien
gM_	Berechtigung auf Managementobjekte
gE_	Berechtigung für Exchange-Objekte

Die Beschreibung im Teil des Namens der Gruppe kann frei gewählt werden, sollte aber keine Leerzeichen oder Bindestriche enthalten. Der Unterstrich trennt diesen Teil von der folgenden Beschreibung.

Beispiele:

MN0001-gO_Mitarbeiter	Org. Gruppe aller Mitarbeiter im Dekanat Math. Nat. Fakultät
MN0002-gFc_GLW	Gruppe, die Ändern-Berechtigung auf dem Gruppenlaufwerk der Prüfungsamts (MN) hat.

Anmerkung: Für die Struktur der Rechtevergabe siehe „Einsatz von Gruppen zur Vergabe von Berechtigungen“ im Anhang.

Gruppentypen: Organisatorische Gruppen werden im AD vom Typ „Global-Security“ und Berechtigungsgruppen von Typ „Domain local-Security“ angelegt.

Gruppennamen für Datei- / Ordnerberechtigungen

Da eine OU mehrere Shares haben kann, ist der Kurzname der Share im Gruppenname für Datei- und Ordnerberechtigungen mit anzugeben. Der Kurzname eines Gruppenlaufwerks wird den Betreuern bei der Erstellung mitgeteilt. Der Aufbau des Namens einer Berechtigungsgruppe ist:

Prefix-bezeichner_sharename[[_*ordner1*]_*ordner2*]

Bsp:

ZE0202-gFc_GLW	Ändern-Zugriff auf den Hauptordner im Gruppenlaufwerk (GLW) des ZDV (ZE0202)
ZE0201-gFr_GLW_Austausch	Lesen-Zugriff auf den Ordner „\Austausch“ im Gruppenlaufwerk (GLW) der UB (ZE0201)
ZE0201-gFc_IRA_Transfer_In	Ändern-Zugriff auf den Unterordner „\Transfer\In“ in der Share „IRA“ (Projektlaufwerk) der UB (ZE0201)

Abkürzungen für Berechtigungsstufen

Bei der Benennung von Zugriffsgruppen ist im Bezeichner die Berechtigung mit anzugeben. Hierfür sind folgende Kürzel zu benutzen

Zugriff auf	Kürzel	Berechtigung
Datei, Ordner, Freigabe	**f**_	Administration (full access)
	fs_	Full access für Unterverzeichnisse und Dateien, nicht den Ordner selbst.
	l_	Einzelnes Verzeichnis auflisten (list). Das Recht wird NICHT auf Unterordner vererbt.
	b_	alle Verzeichnisse auflisten (browse). Das Recht wird auf Unterordner vererbt.
	r_	Reviewer. Inhalte lesen (read)
	w_	Inhalte erzeugen, aber nicht lesen (write)
	c_	Inhalte verändern (change)
	a_	Autor: neue Dateien erzeugen, eigene Dateien/Ordner schreiben/löschen, alle Dateien lesen
	pa_	Publishing Author: neue Ordner/Dateien erzeugen, eigene Dateien/Ordner schreiben/löschen, alle Dateien lesen
	e_	Editor: neue Dateien erzeugen, alle Dateien schreiben/löschen
	pe_	Publishing Editor: neue Order/Dateien erzeugen, alle Dateien/Ordner schreiben/löschen
	co_	Contributor: neue Dateien erzeugen, nur eigene Dateien ändern/löschen
	d_	Zugriff unterbinden (deny access)
Drucker	**p**_	Drucken und eigene Dokumente verwalten
	m_	Drucker verwalten (manage)
ADS/Directory	**m**_	Gruppen und Computer-Objekte verwalten
	g_	Gruppenmanagement
	c_	Management von Clients und Druckern

Anhang:

Einsatz von Gruppen zur Vergabe von Berechtigungen

Bei der Vergabe von Berechtigungen ist, sofern möglich, immer folgende Struktur anzuwenden:

- Personen/Accounts werden nach ihren Funktionen oder Rollen in organisatorische Gruppen zugeordnet
- Für jede Ressource wird je Zugriffsberechtigung eine Gruppe angelegt, die mit der entsprechenden Berechtigung auf die Ressource zugreifen darf. Beispiel:
  Verändern für Sekretariatsordner → gFc_Sekretariat
  Lesen auf den Ordner der Institutsleitung →gFr_Leitung
- Die organisatorischen Gruppen werden in die Zugriffsgruppen aufgenommen und erhalten so Zugriff auf die Ressourcen.

Bemerke: In keinem Fall werden Personen direkt auf Ressourcen zugewiesen (einzige Ausnahme: Persönliche Ordner)

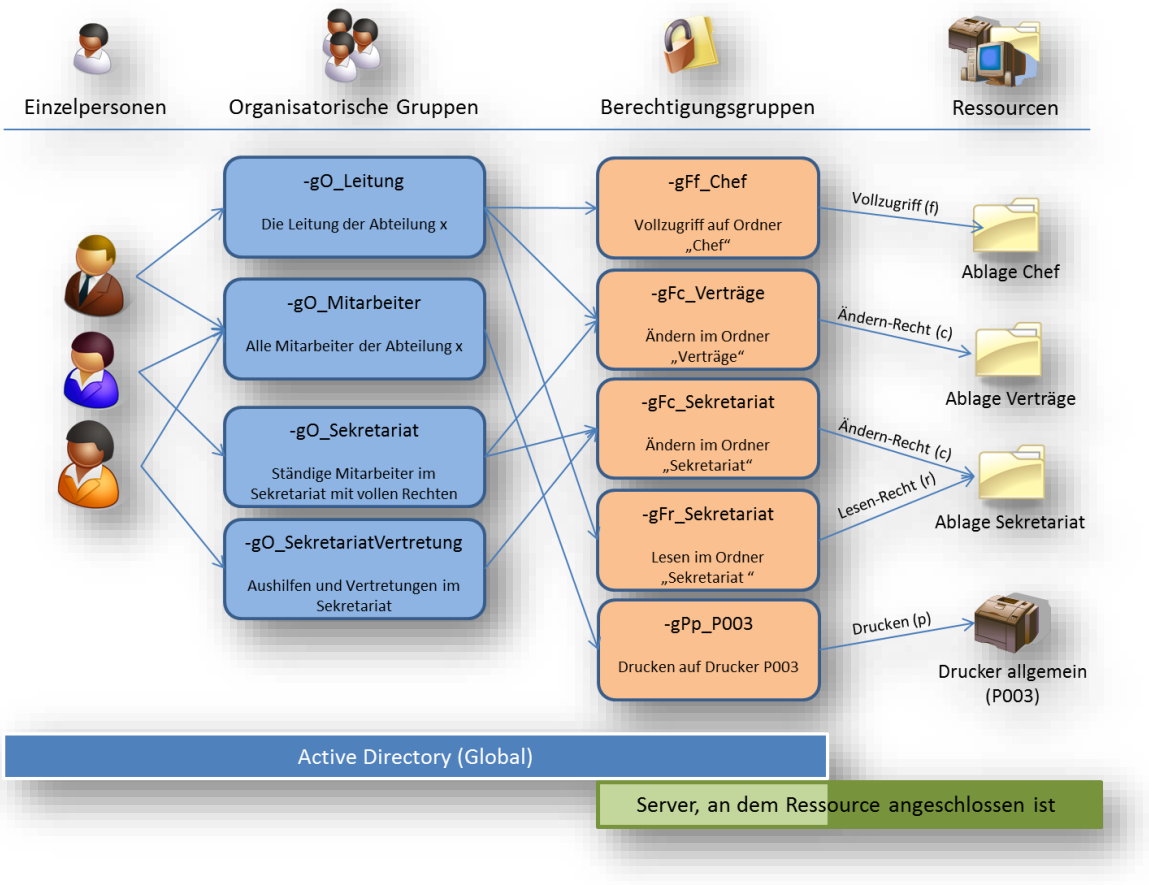

Abb. 4: Gruppenstruktur für die Rechtevergabe