



Betriebssysteme

Windows Benutzerkonten und Gruppen

Autor: Prof. Ronny Bodach
Stand 31.05.2024



**HOCHSCHULE
MITTWEIDA**
University of Applied Sciences



Fraunhofer
SIT



Bundeskriminalamt

Agenda

1. Benutzerkonto
2. Gruppen
3. Lightweight Directory Access Protocol
4. Anmeldevorgang

Benutzerkonto

Windows Benutzerverwaltung SID

- Die Benutzerverwaltung auf Windows Betriebssystemen wird mit Hilfe eines Security Identifier, kurz SID realisiert.
- Die SID ist geeignet um jedes System, jeden Benutzer und jede Gruppe dauerhaft zu identifizieren.
- An die SID sind die in Access Control Lists festgelegten Zugriffsrechte und Eigentümer gebunden die auf NTFS Dateisystemen die Benutzerzugriffsverwaltung realisieren.
- Werden Benutzernamen geändert oder gelöscht bleiben deren SID unverändert derjenigen Datei oder demjenigen Verzeichnis zugeordnet.

Beispiel SID

- S-1-5-21-7623811015-3361044348-030300820-1013
- Erläuterung zum Aufbau:
 - S – Kurzzeichen für SID
 - 1 – Revisionsnummer,
 - 5 – Identifizier Authority
 - 21-76.....0300820 – Domäne oder lokales System,
 - 1013 – Benutzer Nummer
(Gruppen von SID's - 500er System, 1000er Benutzer)

0 Null-account Authority
1 World Authority
2 Local Authority
3 Creator Authority
4 Non-unique Authority
5 NT Authority

Benutzerkonten unter Windows

- Benutzerkontoarten
 - Lokal
 - Domain
 - Windows Account
- Art bestimmt
 - Administrator (Person mit Rechteverwaltung)
 - Speicherort von Benutzereinstellungen
 - Anmeldevoraussetzungen

Lokales Benutzerkonto

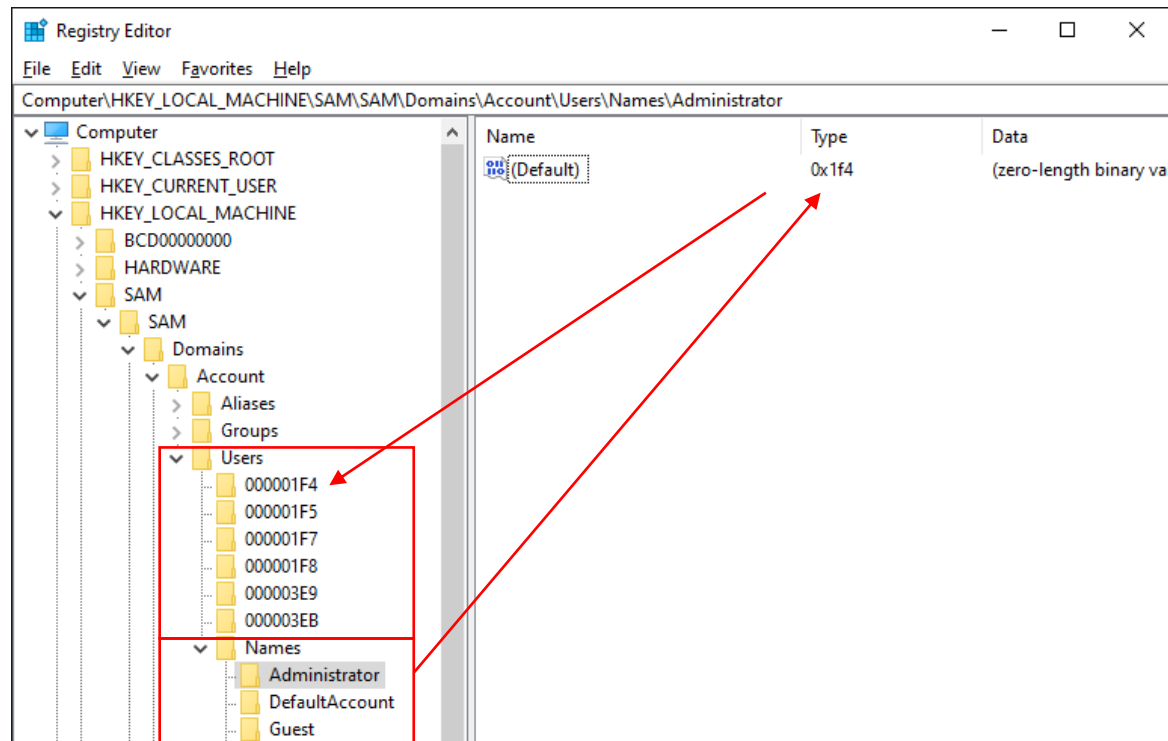
- Bekannt aus Privat-Computer
- Hinterlegt in lokaler Security Account Manager (SAM) Datenbank
- Keine Netzwerkverbindung nötig
- Administriert von lokalen Admin-Benutzerkonto

Lokale Standardkonten

- automatisch bei Installation erstellt
- Lokale Standardbenutzerkonten
 - Administratorkonto (SID S-1-5-LokaleDomäne-500)
 - Gastkonto (SID S-1-5-LokaleDomäne-501)
- Lokale Standardsystemkonten
 - System (S-1-5-18 LocalSystem)
 - Netzwerkdienst (S-1-5-20 NetworkService)
 - Lokaler Dienst (S-1-5-19 NT-Autorität)

Forensisch bedeutsame Registry Informationen Lokales-Konto

- Jeder lokale Nutzer hat Eintrag in der lokalen SAM Datenbank
- Zwei Registry Schlüssel unter:
`\HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users`



Forensisch bedeutsame Registry Informationen Lokales-Konto

- Users Werte

The image shows a Windows Registry Editor window with the following structure:

- Computer > HKEY_LOCAL_MACHINE > SAM > Domains > Account > Users > 00001F4

The right pane shows the following registry values:

Name	Type	Data
(Default)	REG_SZ	(value not set)
F	REG_BINARY	02 00 01 00 00 00 00 2f e4 52 e6 a0 74 cf 01 00 00 ...
ForcePasswordReset	REG_BINARY	
V	REG_BINARY	

The 'Data View' window shows the 'F' value selected, displaying the following data:

Viewer	Summary
Start Offset	0
Position	8
Selection	0
Data Interpreter	
8 bit	16
16 bit	31504
32 bit	352156432
64 bit	129626369658026768
Single	0,00
Double	0,00
Datetime	
WIN SYS 64	ERROR
WIN FILE 64	09.10.2011 14:29:25
UNIX 32	27.02.1981 21:13:52
DOS 32	29.07.1990 17:24:32
OLE 64	30.12.1899 01:00:00
GUID	{14FD7B10-867F-01CC-0000-000000000000...}
ASM 32	adc [ebx-3], bh

The 'Data Interpreter' window shows the following hex data:

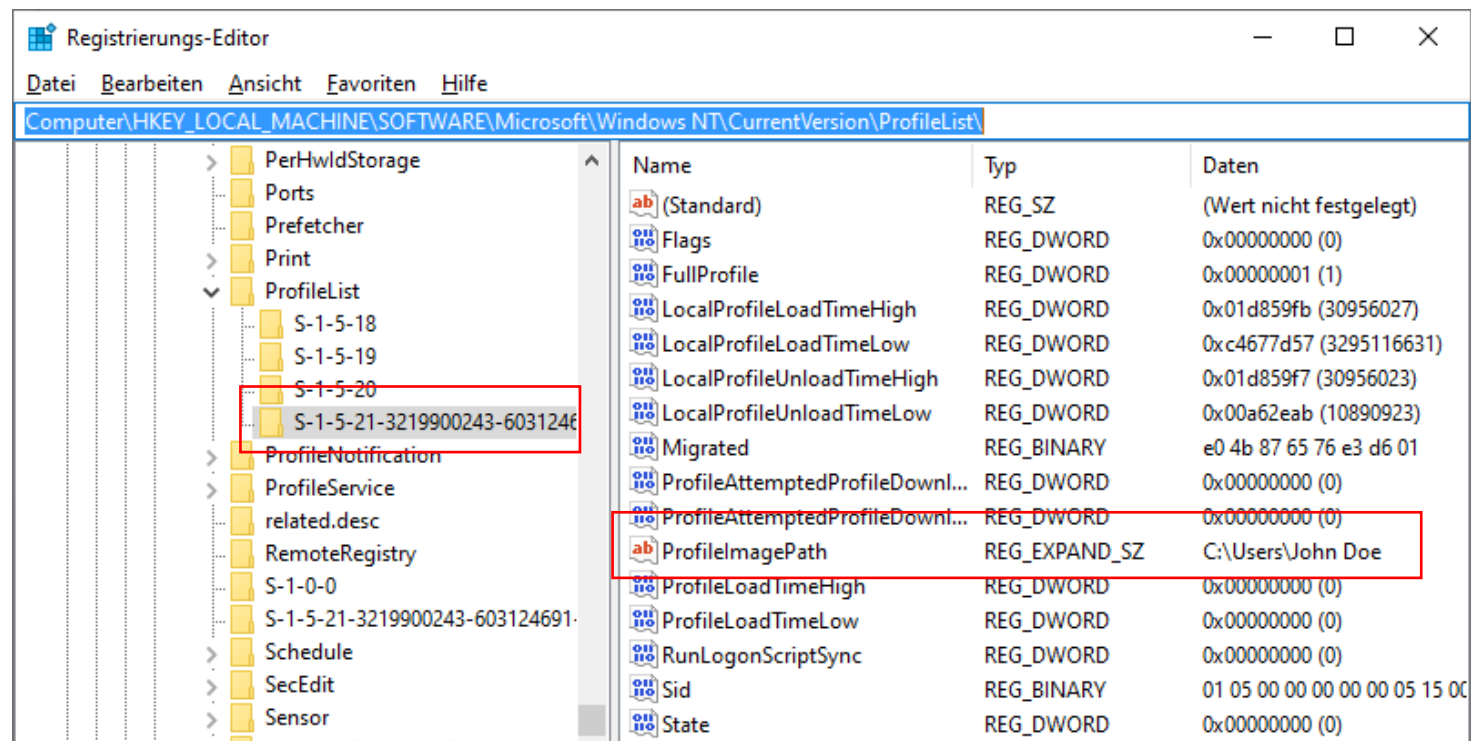
Hex	ASCII
0x00 0200 0100 0000 0000 1078 F014 7F86 CC01{ý.ü.ï.
0x10 0000 0000 0000 0000 6050 918F 9D1E CC01P.ï.
0x20 FFFF FFFF FFFF FF7F A03A 3C2F A81E CC01	yyyyyyyyü :</".ï.
0x30 F401 0000 0107 0000 1002 0000 0000 0000	ð.....
0x40 0000 0C00 0100 0000 0000 0000 0000

Domain-Konto

- Hinterlegt in NTDS.DIT Datenbank des Domaincontrollers
- Anforderung an Netzwerkverbindung hängt von Einstellung auf Domaincontroller ab
- Administriert von Domain-Admin
- Domain-Name
 - steht unter Eingabefeldern
 - Wird vor Benutzername eingeben (getrennt mit \)
Beispiel: HSMW\Benutzername

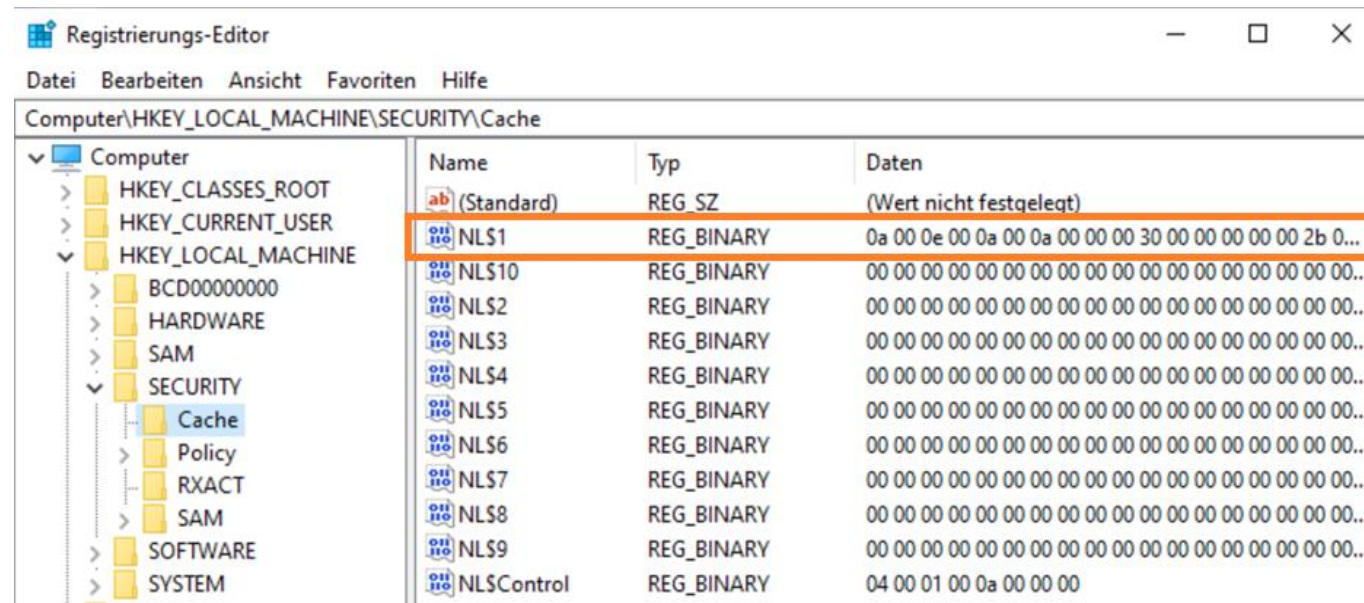
Domain-Konto

- Kein Eintrag in der lokalen SAM Datenbank vorhanden
- Aber, Referenz Eintrag für Benutzer und Profilordner unter:
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList



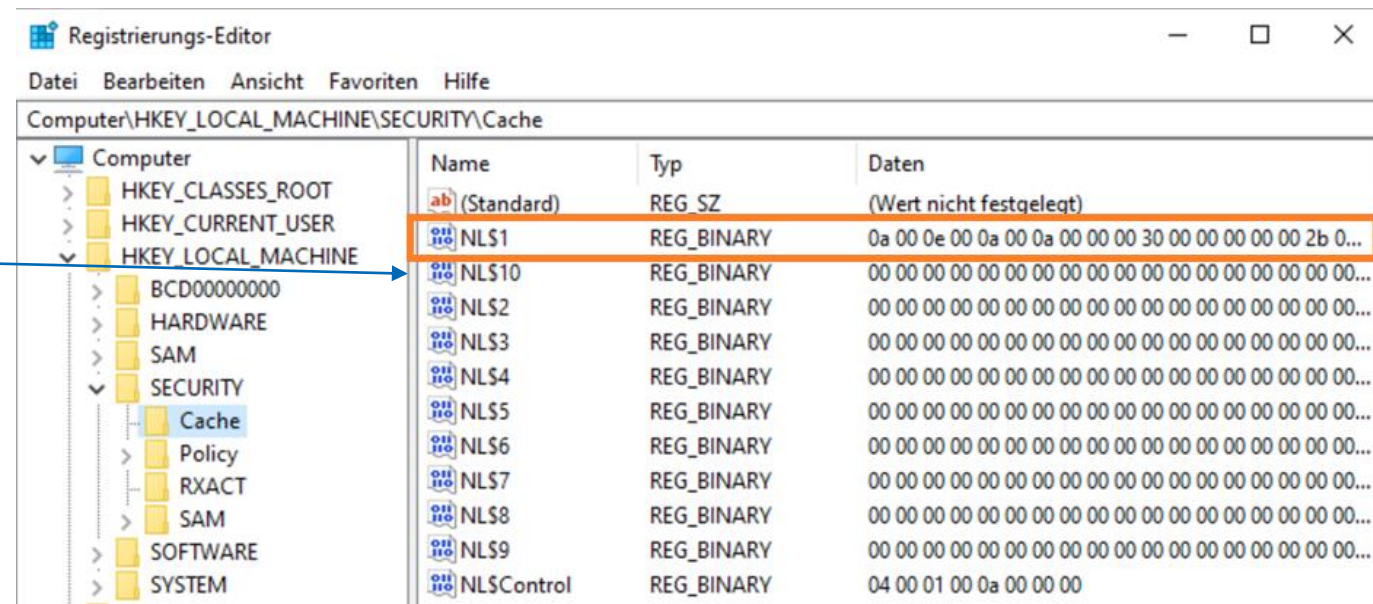
Domain-Konto

- Cached Credentials lokal in SECURITY Registrierung gespeichert
- für lokale Anmeldung ohne Netzwerk
- HKEY_LOCAL_MACHINE\SECURITY\Cache



Domain-Konto

- Anzahl an maximalen unterschiedlichen Credential (unterschiedliche Domänennutzer) ist abgelegt unter:
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\
- Eintrag CachedLogonsCount
- Datentyp: REG_SZ
- Werte: 0 – 50
- Standard 10

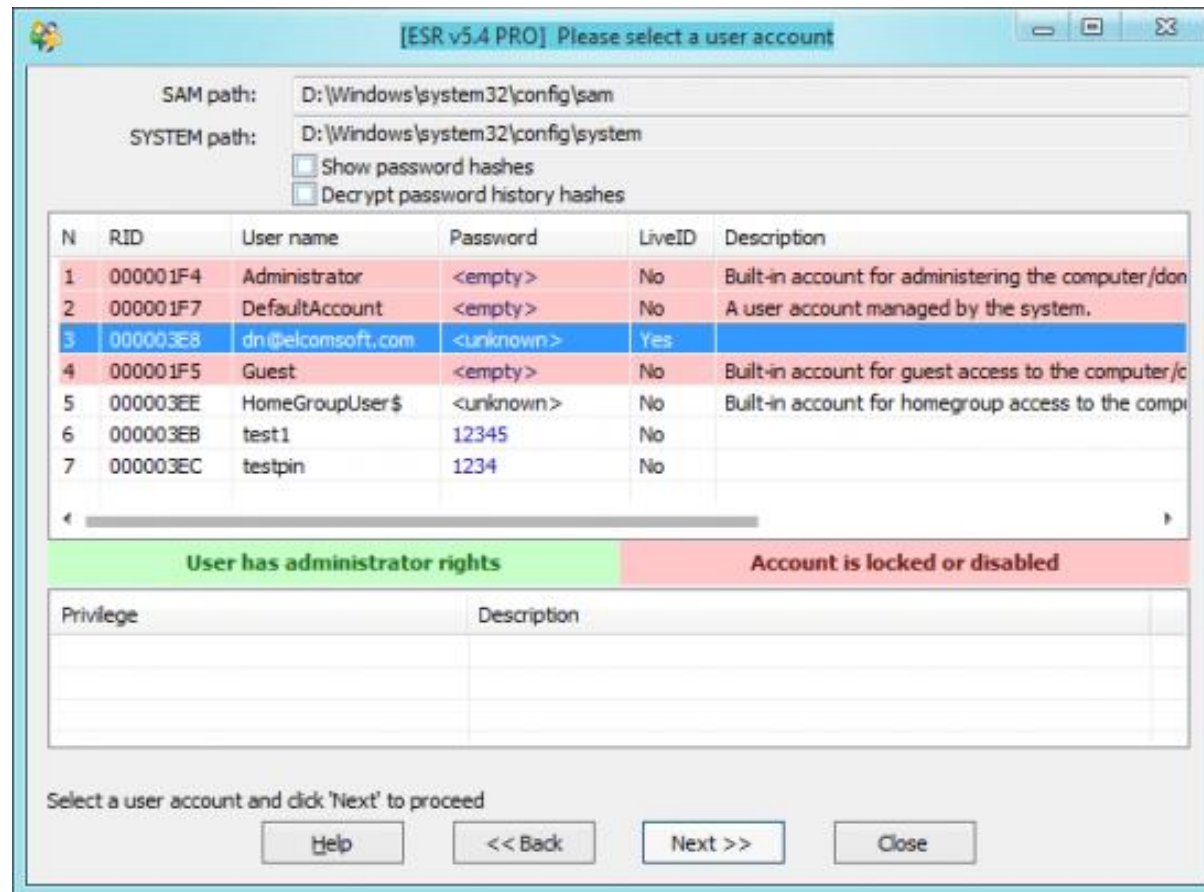


Windows Account

- Anmeldung über Microsoft Account Authentication Server
- Benutzername = E-Mail-Adresse und Passwort
 - Private E-Mail-Adresse
 - Microsoft-E-Mail-Adresse
 - Ehemals LiveID
- Übertragung ist SSL gesichert
- „Remember Login“ speichert verschlüsselten Wert lokal
 - Anmeldung ohne Internetverbindung
- Wert wird gelöscht beim Logout

Windows Account

- Lokaler Wert kann extrahiert und „geknackt“ werden

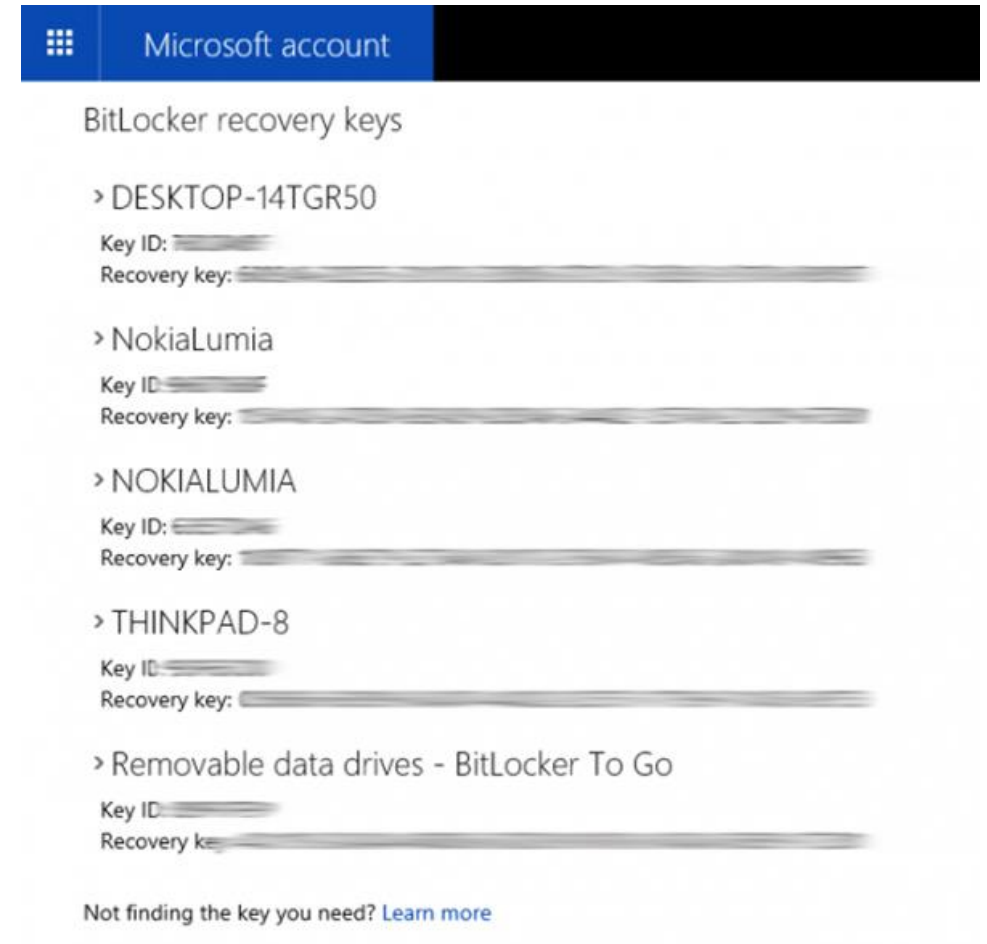


Windows Account

- Windows Account ermöglicht Zugriff auf andere Microsoft-Daten
 - OneNote
 - Teams
 - Bing Search History
 - Hotmail und Outlook.com
 - OneDrive + OneDrive Backups
 - Skype Timeline
 - Reset Protection und Find My Device
 - (Windows Phone und Windows 10 Mobile Backups)
 - Aushebeln der Zwei Faktor Authentifizierung

Windows Account

- Windows erstellt automatisch BitLocker-Hinterlegungsschlüssel im Microsoft-Konto des Benutzers
- Bei Kenntnis des Passworts Abruf möglich

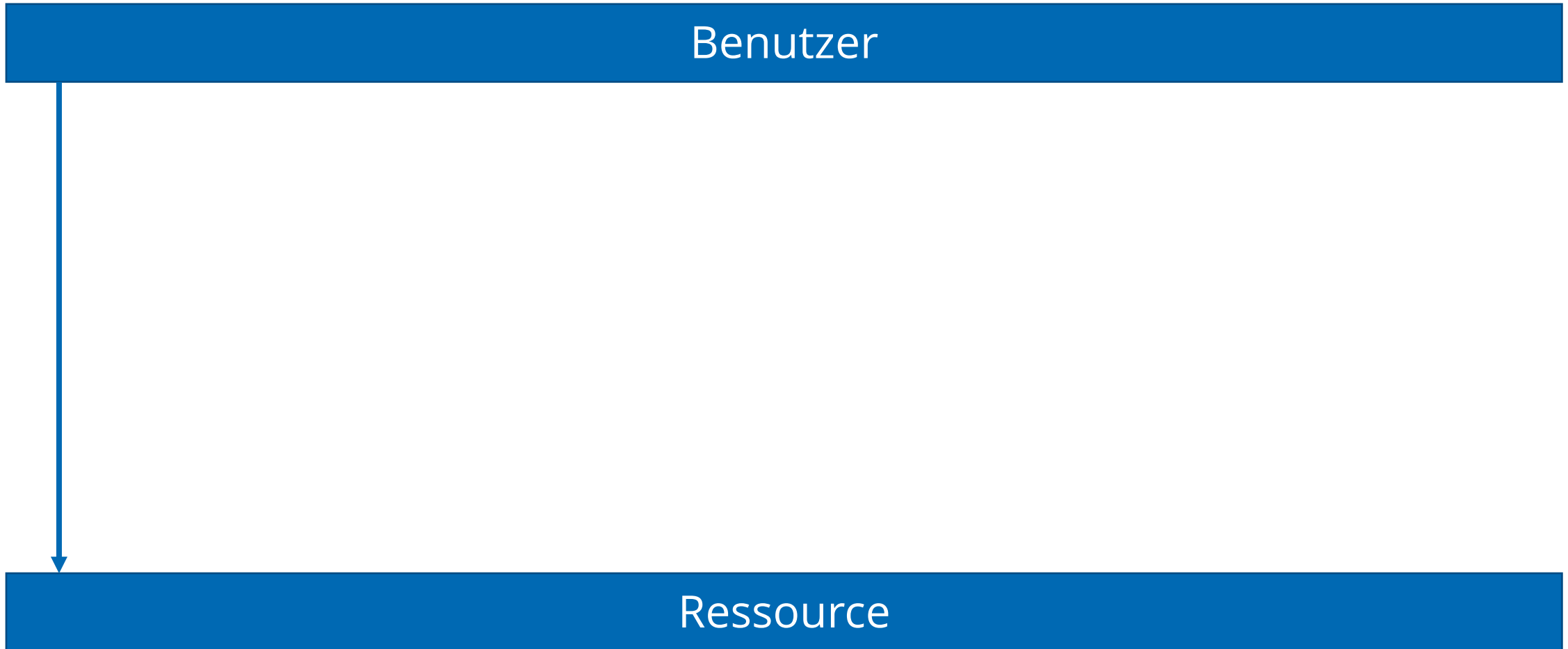


Gruppen

Workgroup

- Bekannt aus Privat-Computer
- Jeder Computer verwaltet sich selbst
- Computer kann eigene Ressourcen in Workgroup teilen
 - Angeschlossener Drucker
 - Netzwerkordner
- Keine Zentrale Verwaltung
- Keine Einheitliche Rechtevergabe
- Hoher administrativer Aufwand

Rechtevergabearten



Direkte Rechtevergabe

- Zuordnung von Ressourcenzugriff für jeden Nutzer einzeln
- Administrativer Aufwand steigt exponentiell mit Benutzer- und Ressourcenanzahl
- Szenario 1:
 - Neuer Netzwerkshare für Vertrieb
 - Alle Vertriebnutzer müssen Netzwerksharezugriff separat zugeordnet bekommen
- Szenario 2:
 - Neuer Nutzer im Vertrieb
 - Nutzer muss allen Ressourcen hinzugeordnet werden



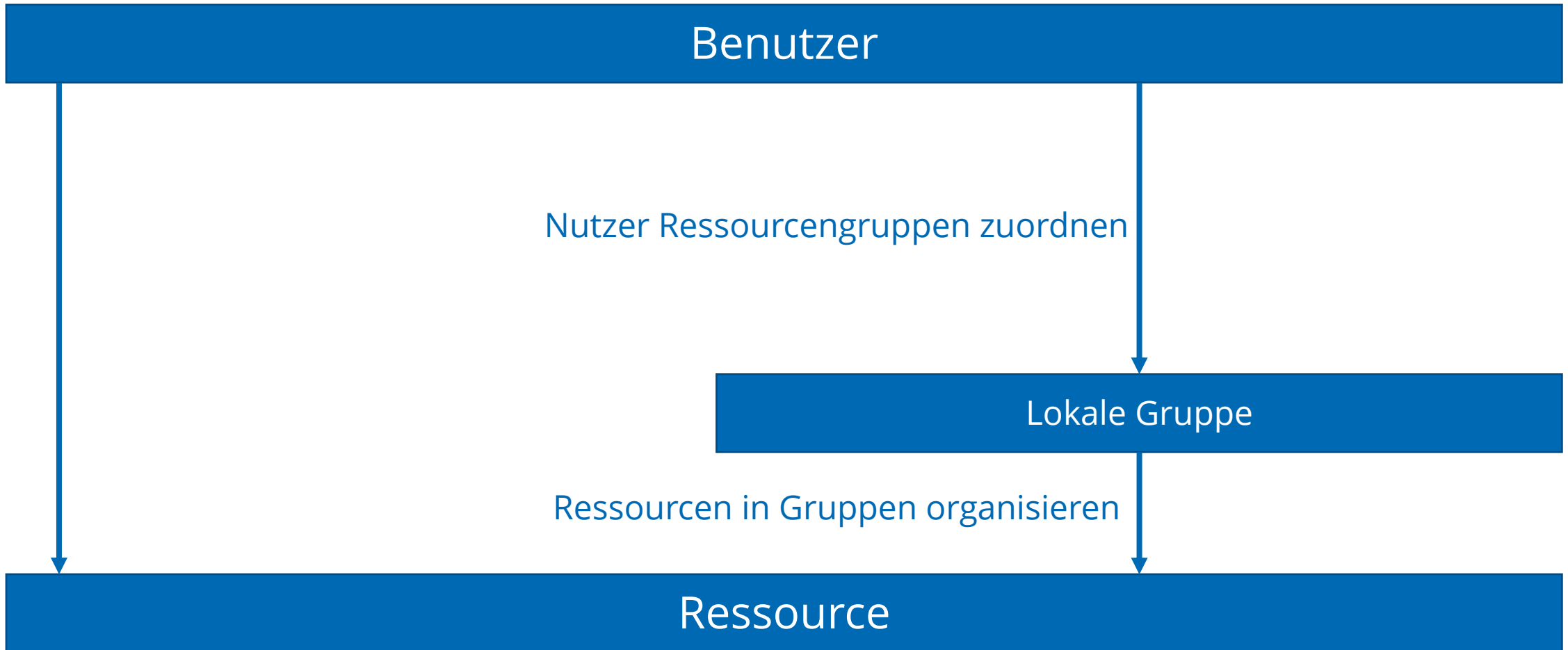
Warum Gruppen?

- Ziel:
 - gleiche Ressourcenzugriffsrechte (mehrere Nutzer gleiche Rechte)
 - Rechte von Nutzern leichter verwalten
 - Manuelle Arbeit reduzieren (Administrationsaufwand = Kosten)
- Umsetzung:
 - Rechteverwaltung strukturieren
 - Rechteverwaltung vereinheitlichen
 - Benutzer bekommen „Rechtesatz“ (Gruppeneinstellung)
 - Arbeitsrolle bestimmt Rechte

Gruppen

- Beinhalten
 - Ressourcenzugriffsrechte
 - Benutzer
 - Gruppen (Verschachtelung)
- Benutzer können in mehreren Gruppen sein

Rechtevergabearten

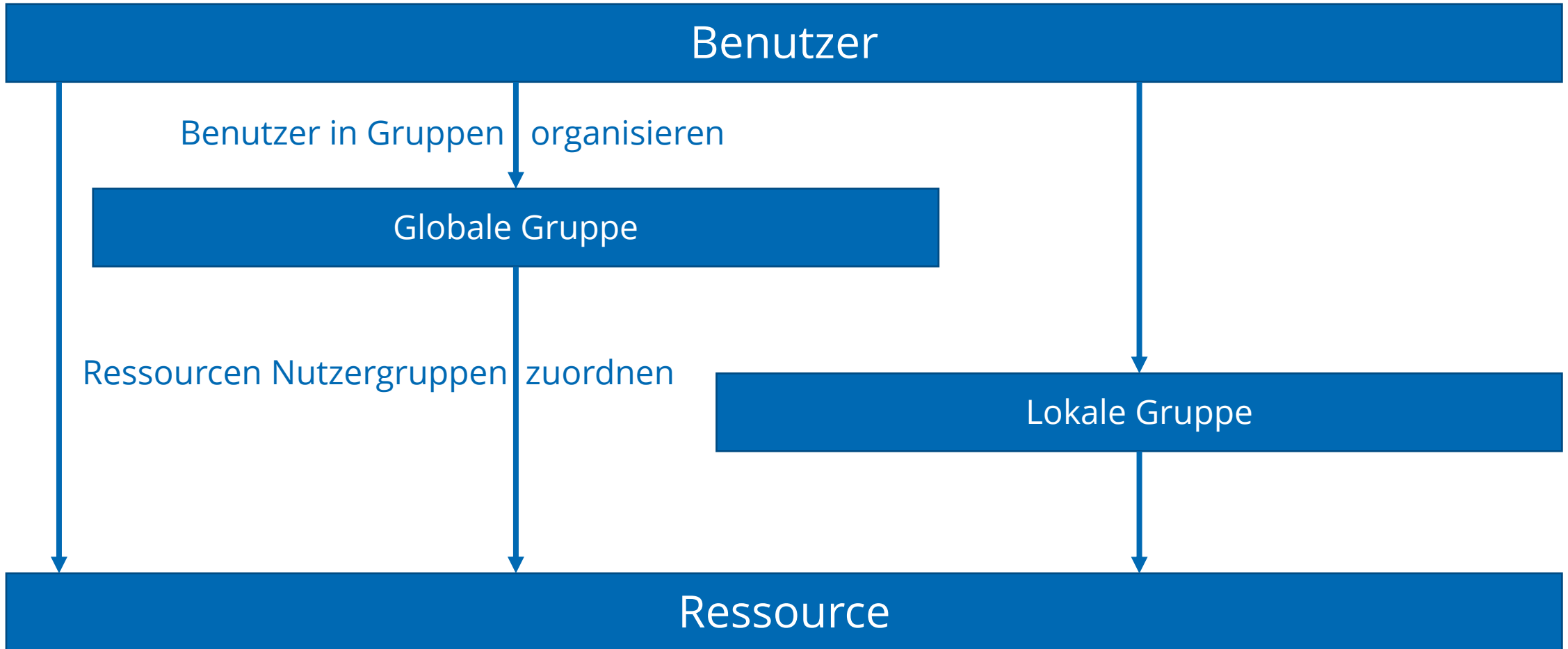


Lokale Gruppen



- Idee:
 - Zusammenfassen von Ressourcen zu Gruppen
 - Beispielsweise:
 - Druckergruppe
 - Scannergruppe
 - Netzwerksharegruppe
 - ...
 - Nutzer werden Gruppen hinzugefügt
- Szenario 1:
 - Neuer Netzwerkshare für Vertrieb
 - lokaler Netzwerksharegruppe hinzufügen
 - Nutzer mit Netzwerkshare-zugriff haben Zugriff auf neuen Share
- Szenario 2:
 - Neuer Nutzer im Vertrieb
 - Nutzer muss allen lokalen Gruppen hinzugefügt werden



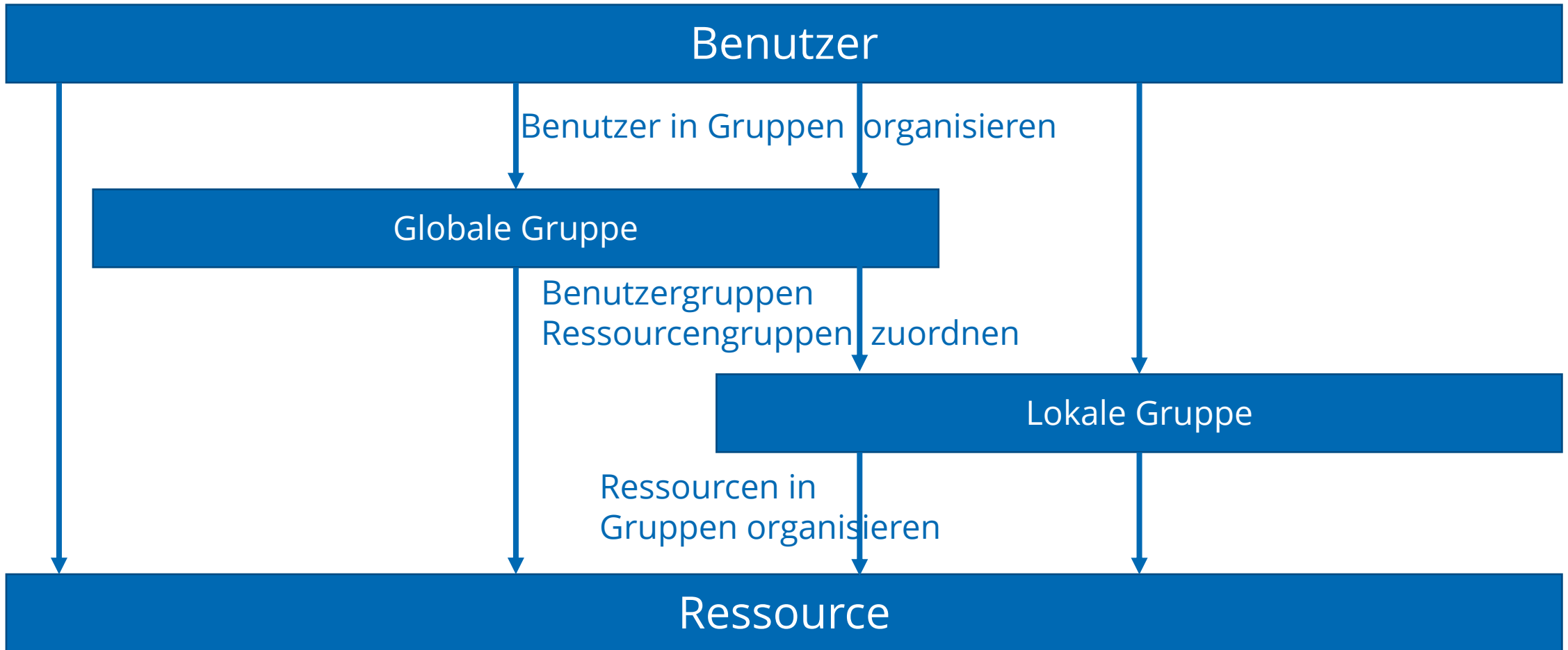
Rechtevergabearten



Globale Gruppen

- Idee:
 - Zusammenfassen von Benutzer zu Gruppen
 - Beispielsweise:
 - Administratorgruppe
 - Vertriebsgruppe
 - Programmierergruppe
 - ...
 - Ressourcen werden Benutzergruppen hinzugefügt
- Szenario 1:
 - Neuer Netzwerkshare für Vertrieb
 - Share muss allen Benutzergruppen zugeordnet werden 
- Szenario 2:
 - Neuer Nutzer im Vertrieb
 - Nutzer muss lediglich Vertriebsgruppe hinzugefügt werden 

Rechtevergabearten



Geschachtelte Gruppen

- Idee:
 - Zusammenfassen von Benutzer zu Gruppen
 - Zusammenfassen von Ressourcen zu Gruppen
 - Beispielsweise:
 - Programmierergruppe ist in
 - Druckergruppe
 - Netzwerksharegruppe
 - Websiteeditgruppe
 - Vertriebsgruppe ist in
 - Druckergruppe
 - Kundendatengruppe
- Szenario 1:
 - Neuer Netzwerkshare für Vertrieb
 - Share muss nur Netzwerksharegruppe zugeordnet werden
- Szenario 2:
 - Neuer Nutzer im Vertrieb
 - Nutzer muss lediglich Vertriebsgruppe hinzugefügt werden



Zusammenfassung Gruppentypen

- Lokale Gruppen
 - Fassen Ressourcenrechte zusammen
 - Nur innerhalb einer Domain
- Globale Gruppen
 - Fassen Nutzerrechte zusammen
 - Nur innerhalb einer Domain
- Universelle Gruppen
 - Domainübergreifend (keiner Domain zugeordnet)

Lightweight Directory Access Protocol

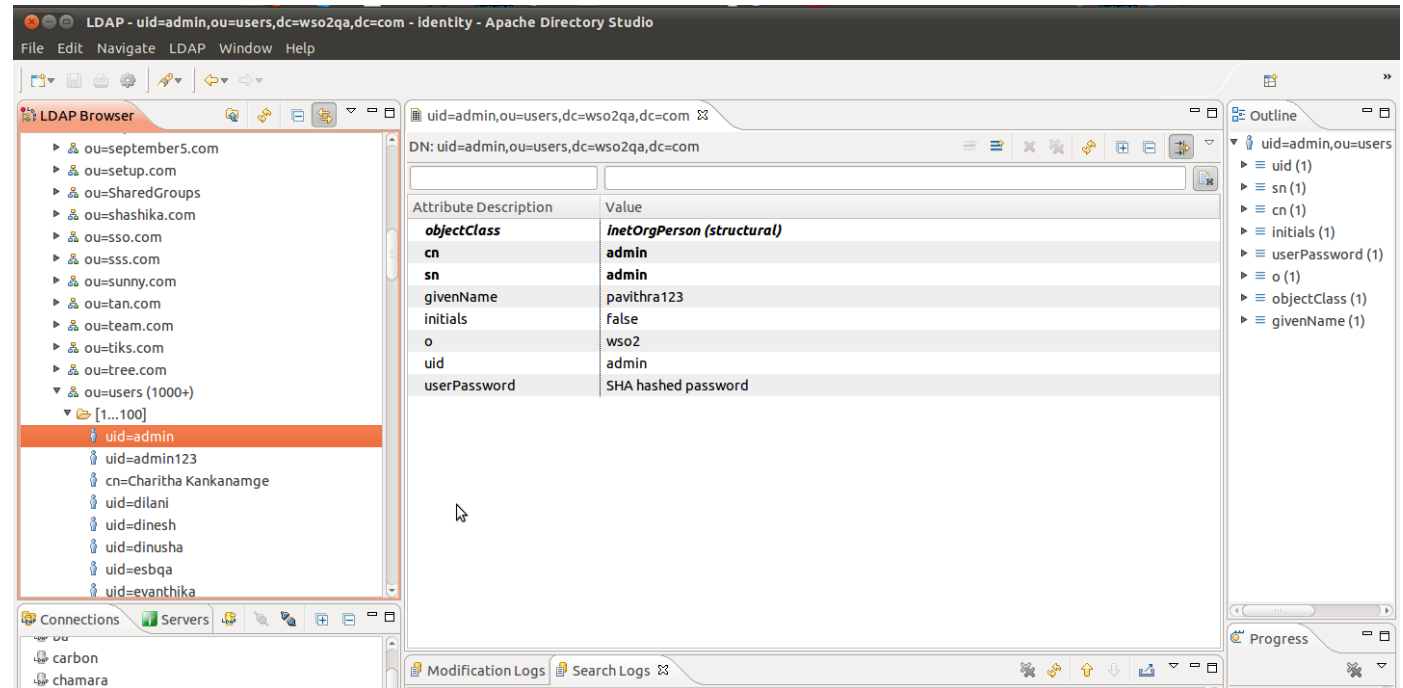
Active Directory Windows

Lightweight Directory Access Protocol

- Leichtgewichtiges Verzeichniszugriffsprotokoll
- Verteilter Verzeichnisdienst („Telefonbuch“)
- Hierarchische Datenbank (Baumstruktur, wie Ordner im Dateisystem)
- Definiert in RFC-4532 (IETF)
- Aufgabe
 - Zentrale Sammlung und Verwaltung von Benutzerdaten
 - Rechte und Hardware werden getrennt
 - Flexibilität für Benutzer
 - Administrativen Aufwand für Admin reduzieren
 - Optimiert auf Lesenden Zugriff (Rechteabfrage, Autorisierung, ...)

Implementierungen von LDAP

- **Active Directory (Microsoft)**
- **Open Directory (Apple)**
- **Open LDAP (Linux)** →
- Apache Directory Studio
- Jxplorer
- FreeIPA
- Samba
- 398 Directory Server (Red Hat)
- OpenDJ
- Zentyal Active Directory
- Oracle Directory Server Enterprise Edition (Oracle)
- eDirectory (Novell)



Domainbegriffe Windows

- Domain (Herrschaftsbereich) → phys. Unternehmen, Standort
 - Replikationsgrenze
 - Sicherheitsgrenze
- Gruppen, Benutzer → phys. Abteilungen
- Gruppenrichtlinie (Group Policy Object - GPO) → phys. Standort
 - Lokale Gruppe (Domain Local Group - DLG)
 - Globale Gruppe (Global Group - GG)
 - Universelle Gruppe (Universal Group - UG)
- Organisationseinheit (Organisation Unit - OU) → phys. Abteilung
- Struktur (Baum), Gesamtstruktur (Wald) → phys. Domaincontroller
- Globaler Katalog
 - 1. Domaincontroller (min. 1 Domaincontroller pro Standort)
 - Datenspeicher für GPOs und andere Objekte
 - Schnittstelle zu anderen Domains

Active Directory Forensik

Speicherung der Gruppenrichtlinien

Ein Gruppenrichtlinien-Objekt (GPO) besteht aus den Komponenten Group Policy Container (GPC) und Group Policy Template (GPT). Ein GPC ist ein Active Directory-Container, welcher GPO-Eigenschaften wie GPO-Status und Versionsinformationen enthält und in der Domänenpartition gespeichert wird.

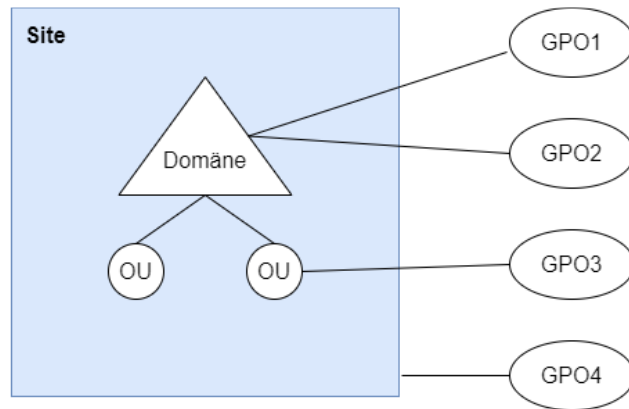
Das GPT wiederum ist ein Dateisystemordner, der sich im Pfad **C:\Windows\SYSVOL\domain\Policies** befindet.

Die GPT-Ordner sind nach den GUIDs der GPOs benannt und besitzen die Unterordner „MACHINE“ und „USER“, die die Computer- und Benutzerkonfiguration repräsentieren.

Im GPT-Ordner einer Gruppenrichtlinie befinden sich verschiedene Dateien und Ordner in verschiedenen Dateiformaten welche die GPO Einstellungen enthalten.

Active Directory Forensik

Ablauf der Anwendung von Gruppenrichtlinien:



GPO-Verlinkung innerhalb der Domänenstruktur

Computerkonfiguration

Anwenden von GPOs

Benutzerkonfiguration



GPO-Hierarchie

Active Directory Forensik

Microsoft Active Directory ist fast wie **das Domain Naming System** eines **Internets** mit domänenbasiertem Grid organisiert. Im AD auf einem Domänen Controller werden Benutzer-, Gruppen- und Computerobjekte gespeichert.

Speicherort und Dateiname des Microsoft Active Directory

Die Daten von Microsoft Active Directory werden in der **ESE-Datenbankdatei NTDS.DIT (Extensible Storage Engine) gespeichert**. **NTDS.DIT** ist eine Abkürzung für **NT Directory Services** und DIT steht für **Directory Information Tree**.

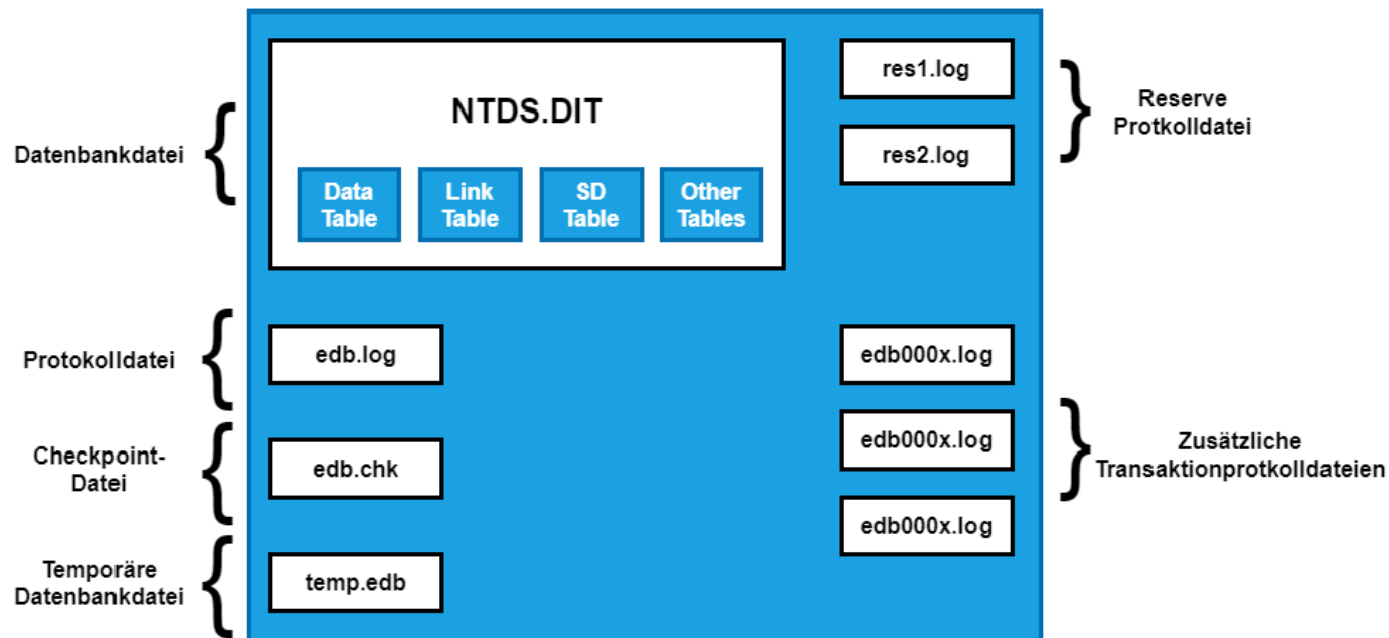
Auf dem Domänenserver sind die beiden Kopien der NTDS.DIT-Datei an zwei geänderten Speicherorten vorhanden:

- **Windir%\NTDS\Ntds.dit**
Diese Datei speichert den Datensatz des Domänencontrollers
- **%SystemRoot%\System32\Ntds.dit**
Diese Datei speichert eine Replika des Datensatz des Domänencontrollers

Active Directory Forensik

Forensische Analyse der NTDS.DIT-Datei

Die physikalische Struktur der Datenspeicherung der NTDS.DIT-Datei besteht aus drei signifikanten Tabellen. *Datentabelle*, *Verknüpfungstabelle*, *Security Descriptor (SD)-Tabelle* und die zugehörigen Protokoll- und temporären Dateien.



Active Directory Forensik

Was kann man bei einer forensischen Untersuchung der NTDS.DIT-Datei analysieren?

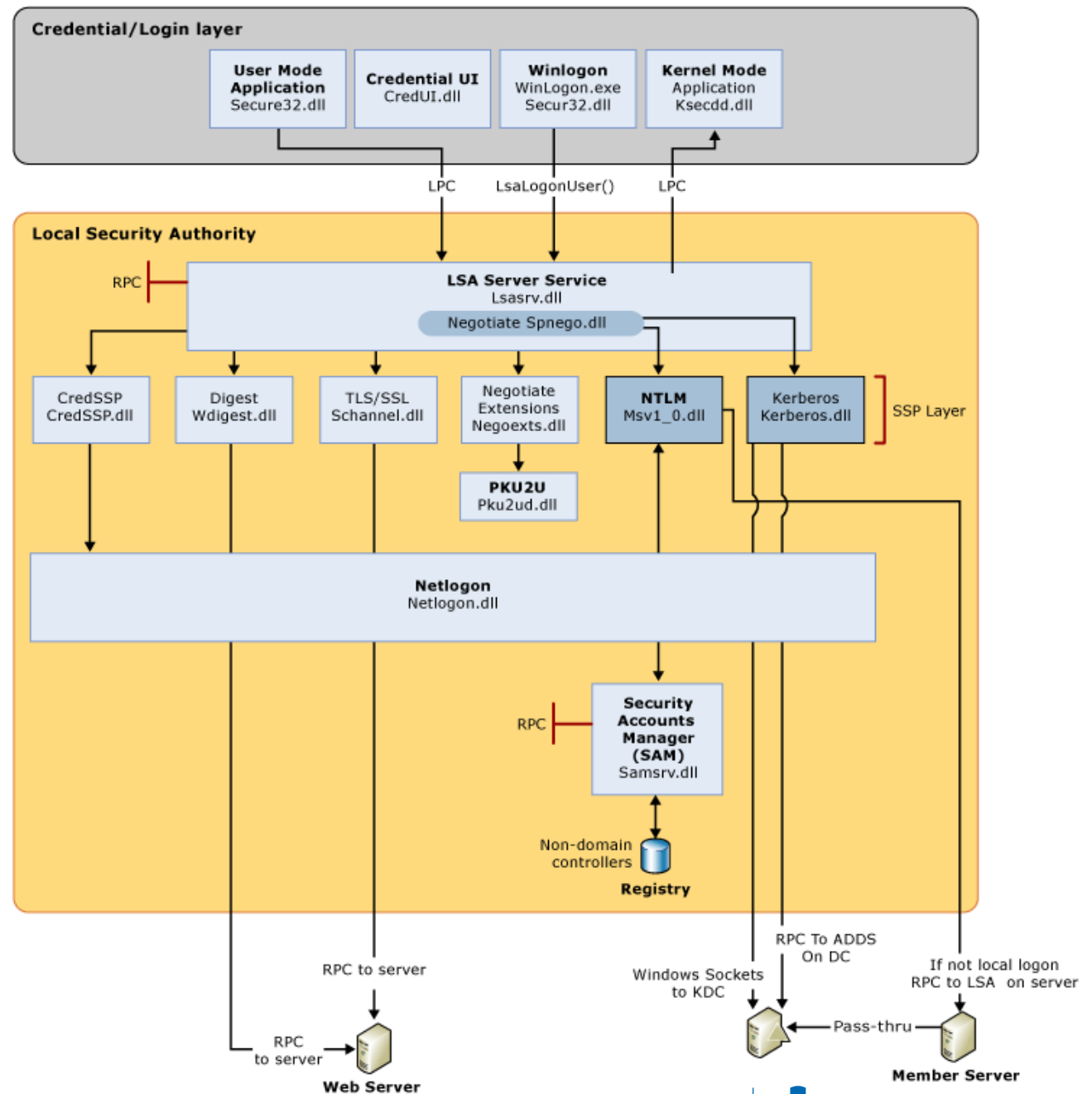
Während einer NTDS.DIT-Analyse kann man Beweise aus den Benutzerkonten der Netzwerk Benutzer und Informationen zu den Computerobjekten auslesen. Die folgenden Informationen beschreiben, welche Art von Beweisen aus dem Active Directory extrahiert werden können:

- Zeitpunkt der letzten Kontoanmeldung
- SID des Benutzers
- Maschine ID der Computer
- Passwort-Hashes
- Gruppenrichtlinien und Berechtigungen (SYSVOL Verzeichnis Domänencontroller)

Anmeldevorgang

Login

- Interaktive Anmeldung (Wissen)
 - Lokale Anmeldung
 - Remote Anmeldung
- Anmeldung mit Smartcard (Wissen + Besitz)
- Biometrische Anmeldung (Biometrie)
- Netzwerkanmeldung (Automatisierung)

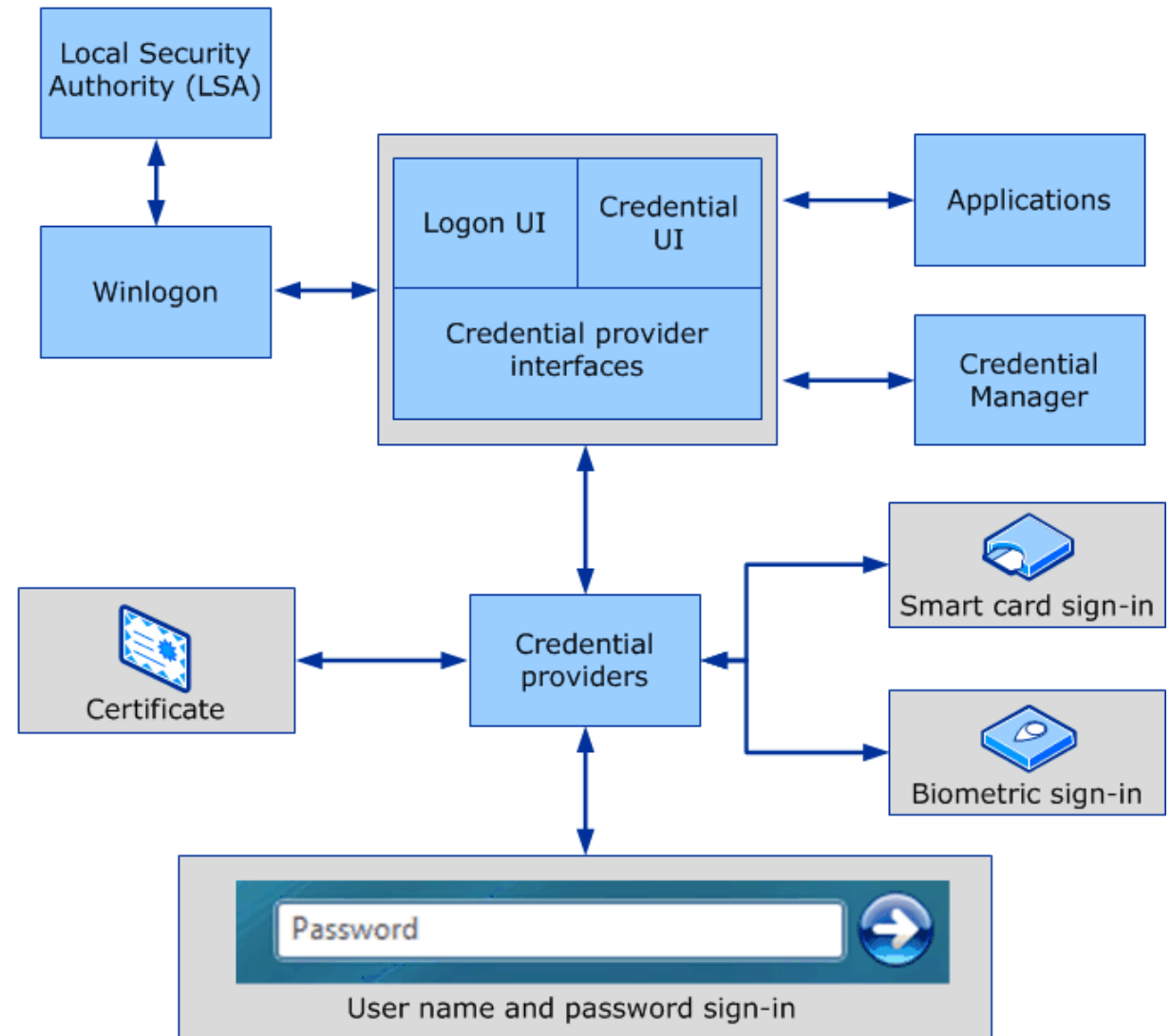


Interaktive Anmeldung

- Physischer Zugriff (wenn lokal)
- Anmeldung über Remote Desktop Service (RDS) (wenn remote)
 - Verwendet Remote Desktop Protocol (RDP)
- Benutzer in lokaler Security Account Manager (SAM) Datenbank hinterlegt
- Netzwerkzugriff nicht erforderlich
- Benutzer meldet sich mit Benutzername und Passwort an
- Benutzer erhält Zugriff auf
 - Lokale Ressourcen
 - Geteilte Netzwerkressourcen
- Anmeldung des Nutzers in Domain wird probiert

Anmeldung mit Smartcards

- Erfordert Kerberos
- Nur mit Domainkonto
- X.509-Zertifikat (PKCS) auf Smartcard
- Private / Public Key Pair auf Smartcard
- Security Chip der Smartcard speichert Private Key
- Freischaltung des Private Keys durch PIN
- Smartcard signiert Aktionen
- Private Key verlässt Smartcard nie



Biometrische Anmeldung

- Nutzbare Biometrische Merkmale
 - Fingerabdruck
 - Iris
 - Gesicht
- Anmeldung vergleicht Messung mit bekannten Samples
- wenn einzig erlaubt Anmeldung, dann Verbindung AD-Controller nötig

Netzwerkanmeldung

- Verwendung erst nach erfolgreicher Anmeldung möglich
 - Benutzerauthentifizierung
 - Dienstauthentifizierung
 - Computerauthentifizierung
- Unsichtbar für Benutzer
- Anmeldung von Netzwerkdiensten und Prozessen während der Nutzung
- Unterstützte Authentifizierungsmethoden
 - Kerberos
 - Zertifikate mit öffentlichen Schlüssel (PKI)
 - Basic Authentication über Secure Socket Layer / Transport Layer Security (SSL / TLS)
 - Digest (Username-Hash und Challenge Response)
 - NT LAN Manager (NTLM) (nur für Abwärtskompatibilität)

Zusammenfassung

Zusammenfassung

Unter Windows gibt es 3 verschiedene Benutzerkontenarten (lokal, Domain, Windowsnetzwerk). Deren Speicherorte und Administration unterscheiden sich.

Gruppen werden zur vereinfachten Rechteverwaltung verwendet. Windows unterscheidet in 3 Gruppentypen (lokal, global, universell). Die übliche Gruppenverschachtelung ist: A-GG-LG-R oder A-GG-GG-UG-LG-R.

LDAP ist ein Protocol zum Austausch von Verzeichnisdienstinformationen. Active Directory ist Microsoft's Implementation von LDAP. Die meistgenutzten Alternativen sind Open Directory von Apple und Open LDAP aus der Linuxwelt.

Es gibt 4 Anmeldevarianten unter Windows. Diese sind: interaktiv, mit Smartcard, biometrisch und Netzwerkanmeldung.

Vielen Dank



**HOCHSCHULE
MITTWEIDA**
University of Applied Sciences

Prof. Ronny Bodach

Hochschule Mittweida | University of Applied Sciences
Technikumplatz 17 | 09648 Mittweida
Fakultät Angewandte Computer- und Biowissenschaften

T +49 (0) 3727 58-1011
F +49 (0) 3727 58-21011
bodach@hs-mittweida.de
www.cb.hs-mittweida.de

Haus 8 | Richard-Stücklen Bau | Raum 8-205
Am Schwanenteich 6b | 09648 Mittweida

Felix Fischer

Hochschule Mittweida | University of Applied Sciences
Technikumplatz 17 | 09648 Mittweida
Fakultät Angewandte Computer- und Biowissenschaften

fische11@hs-mittweida.de
www.cb.hs-mittweida.de

[hs-mittweida.de](https://www.hs-mittweida.de)