Directoryservices konfigurieren und in Betrieb nehmen

Modul 159

Titel	Directoryservices konfigurieren und in Betrieb nehmen	**Typ**	Kategorie	**Version**	1.7
Thema	Modul 159	**Klasse**	öffentlich	**Freigabe Datum**	14.05.2012
Autor	Janik von Rotz	**Status**	Status		
Ablage/Name	D:\SkyDrive\education\bbzs\4.lehrjahr\sba\Modul159\Modul 159 Directoryservices konfigurieren und in Betrieb nehmen.docx				
Schlüsselwörter					
Kommentare					

Dokumentverlauf

Version	Datum	Autor	Beschreibung der Änderung	Status
1.0	28.04.2012	Janik von Rotz	Erstellen Dokument	In Bearbeitung
1.1	05.05.2012	Janik von Rotz	Freigabe	In Bearbeitung
1.2	07.05.2012	Janik von Rotz	Ergänzen: Sichern von WLANs in einer Active Directory Umgebung	Fertiggestellt
1.4	13.05.2012	Janik von Rotz	Doku erweitert Siehe AD Planung Praxisbeispiel	Fertiggestellt
1.6	14.05.2012	Janik von Rotz	Ergänzen Reverse Lookup Zonen file	Fertiggestellt
1.7	14.05.2012	Janik von Rotz	Überarbeiten Formatierungen	

Referenzierte Dokumente

Nr.	Dok-ID	Titel des Dokumentes / Bemerkungen	Ablage / Link

Lizenz

Inhaltsverzeichnis

1 Directory Systeme

1.1 Vorteile

Vorteile von Acitve Dirctory LDAP basierten Netzen gegenüber Peer to Peer Netzen:

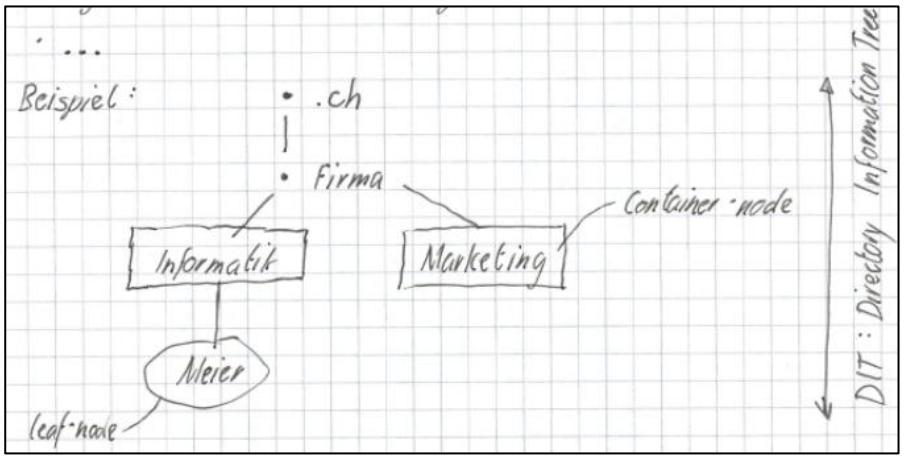
- Zentrale Verwaltung von Benutzern
- Zentrale Verwaltung der Computer
- Zentrale Verwaltung der DNS-Ressource Records, inkl dynamischem DNS
- Zentrale Verwaltung der Zugriffssteuerung auf freigegebene Ressourcen (Dateifreigaben und Drucker)
- Flexible Suche nach Einträgen im DIT
- Aufbau von Singlel Sign On Infrastrukturen
- Verbesserung der Sicherheit durch Gruppenrichtlinien-Objekte

1.2 Hierarchische Datenhaltung

Hierarchische Datenhaltung für:

- Angaben zur Top-Level-Verankerung (DNS
- Angaben zur Organisation (Firma)
- Angaben zur Organisation-Einheit (Organizational Unit = OU)
- Angaben zu Personen
- Angaben zu Computern
- Angaben zu den AD-integrierten DNS-Knoten
- …

Beispiel:



1.3 Gespeicherte Informaionen

- Angaben über Domänen, Organisationseinheiten, Benutzer und Computer in Objekten mit Attributen.
- In AD zudem:
  - DNS RR Records (A, AAAA, PTR, NS, SRV)
  - Gruppenrichtlinien-Obbjekte
  - Drucker, Freigaben

Abbildung 1: Einfacher DIT

1.4 Informationsmodell von LDAP

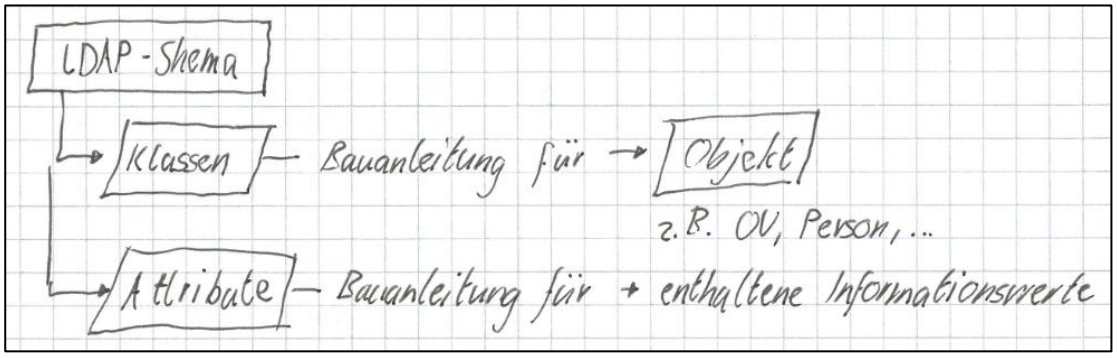


Abbildung 2: Informationsmodell von LDAP

- In der Klasse wird festgelegt, welche Attribute in einem Objekt eingetragen sein müssen der können.
- Im Attribut wird festgelegt, welche Zeichen erlaubt sind, weche Suchoperationen erlaubt sind.
- Der Basis-Teil eines LDAP-Schemas ist normiert (RFC, IANA)
  - Interopralität der verschiedenen LDAP-Implementierungen
- Die Klassen und Attribute werden über OIDs identifiziert.
- Firmen können bei IANA LDAP-Schema-OID-Teilbäume reservieren.

1.5 LDAP Namensmodell

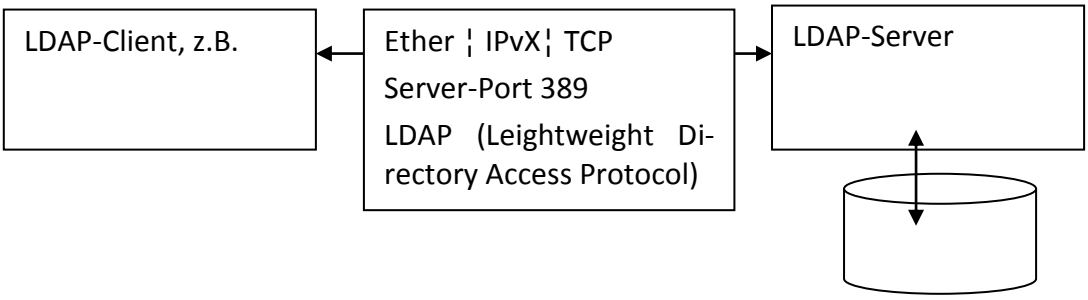
LDAP-objekte z.B. eine OU wird anhand einer Bau-Anleitung, die im LDAP-Schema steht erzeugt.

Diese Objekte, bzw. die Lage der Knoten wird über den DN (Distinguished Name) festgelegt.

Dies ist der vollständige Pfad im LDAP-DIT.

Beispel: dn: CN = Sonja Meier, OU = Sales, …, c = de

1.6 LDAP Client-Server-Architektur



1.7 Besipiel eines DAP-Trees (DIT)

<firma.ldif>

```
dn: cn=Manager, dc=selflinux, dc=de
    cn: Manager
    description: Directory Manager
    description: Verzeichnis-Manager
    objectClass: organizationalRole
    objectclass: top
    roleOccupant: cn=Thomas Bendler,ou=Development,dc=selflinux,dc=de
    roleOccupant: cn=Steffen Dettmer,ou=Development,dc=selflinux,dc=de
dn: o=Selflinux,dc=selflinux,dc=de
    objectclass: top
    objectclass: domain
    objectclass: organization
    o: Selflinux
    l: Hamburg
    postalcode: 21033
    streetadress: Billwiese 22
dn: ou=Development,o=Selflinux,dc=selflinux,dc=de
    objectclass: top
    objectclass: organizationalunit
    ou: Development
dn: ou=Sales,o=Selflinux,dc=selflinux,dc=de
    objectclass: top
    objectclass: organizationalunit
    ou: Sales
dn: ou=Support,o=Selflinux,dc=selflinux,dc=de
    objectclass: top
    objectclass: organizationalunit
    ou: Linux
```

dn: cn=Thomas Bendler,ou=Development,o=selflinux,dc=selflinux,dc=de

objectclass: top
objectclass: person
objectclass: organizationalperson
objectclass: inetorgperson
cn: Thomas Bendler
sn: Bendler
ou: Development
mail:project@selflinux.de
l: Hamburg
postalcode: 21033
streetadress: billwiese 22
telephonenumber: 040-7654321
facsmiletelephonenumber: 040-7654321
userpassword: {CRYPT}saHW9GdxihkGQ

dn: cn=Steffen Dettmer,ou=Development,o=Selflinux,dc=selflinux,dc=de

cn: Steffen Dettmer
sn: Dettmer
ou: Development
mail: steffen@dett.de
telephoneNumber: +49 (30) 1234567
objectClass: person

dn: cn=Sonja Essler,ou=Sales,o=Selflinux,dc=selflinux,dc=de

cn: Sonja Essler
sn: Essler
ou: Sales
mail: sonja@bendler-net.de
telephoneNumber: +49 (30) 1234568
objectClass: person

dn: cn=Thomas Lippert,ou=Support,o=Selflinux,dc=selflinux,dc=de

cn: Thomas Lippert
sn: Lippert
ou: Support
mail: tom@bendler-net.de
telephoneNumber: +49 (30) 1234569
objectClass: person

Diese LDIF-Datei erzeugt auf einem LDAP-Server den folgenden DIT:

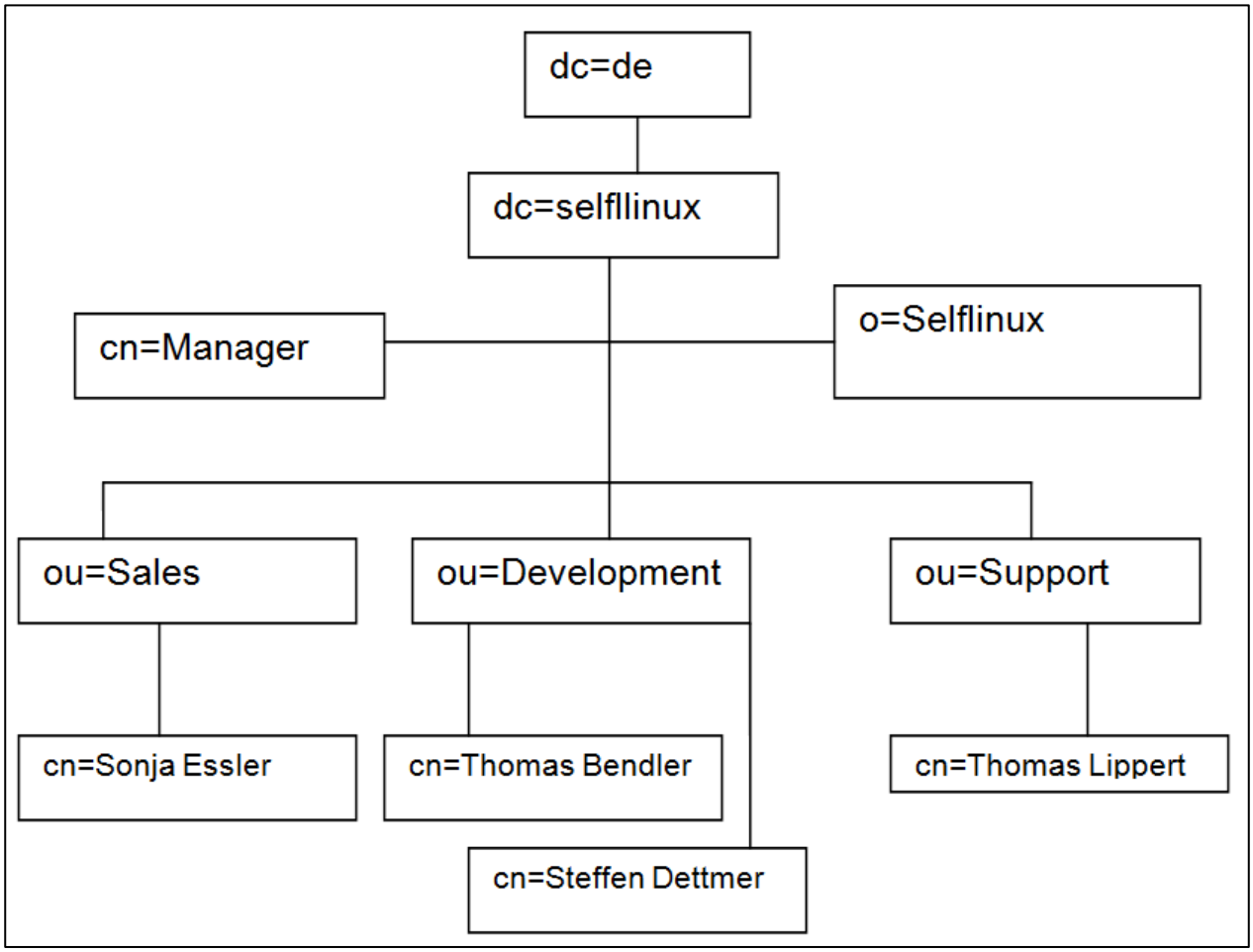


Abbildung 3: LDIF Tree

2 IEEE 802.1x

2.1 Ziele von IEEE 802.1x

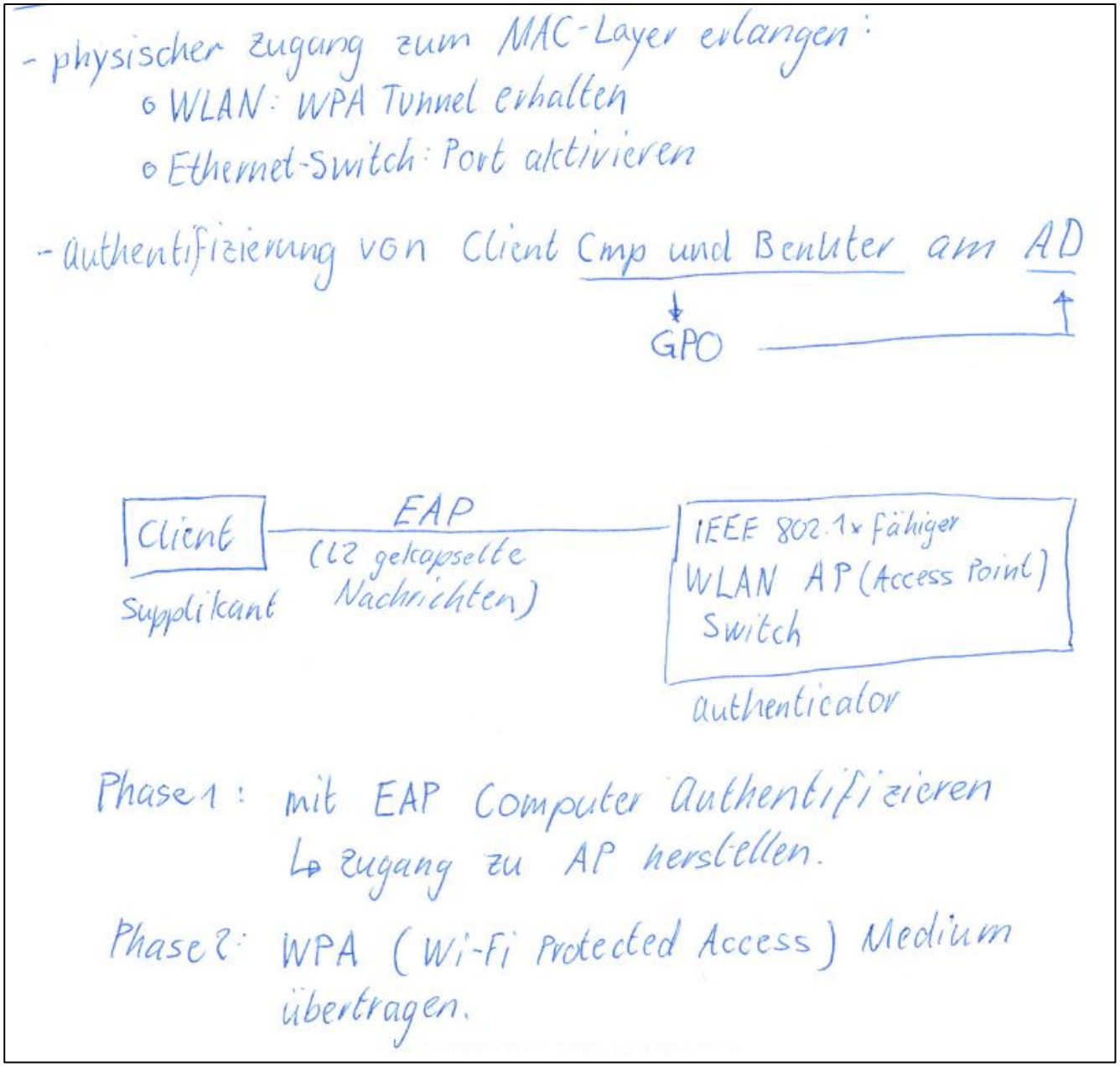


Abbildung 4: Ziele von IEEE 802.1x

2.2 IEEE Authentifizierung nach EAP-TLS

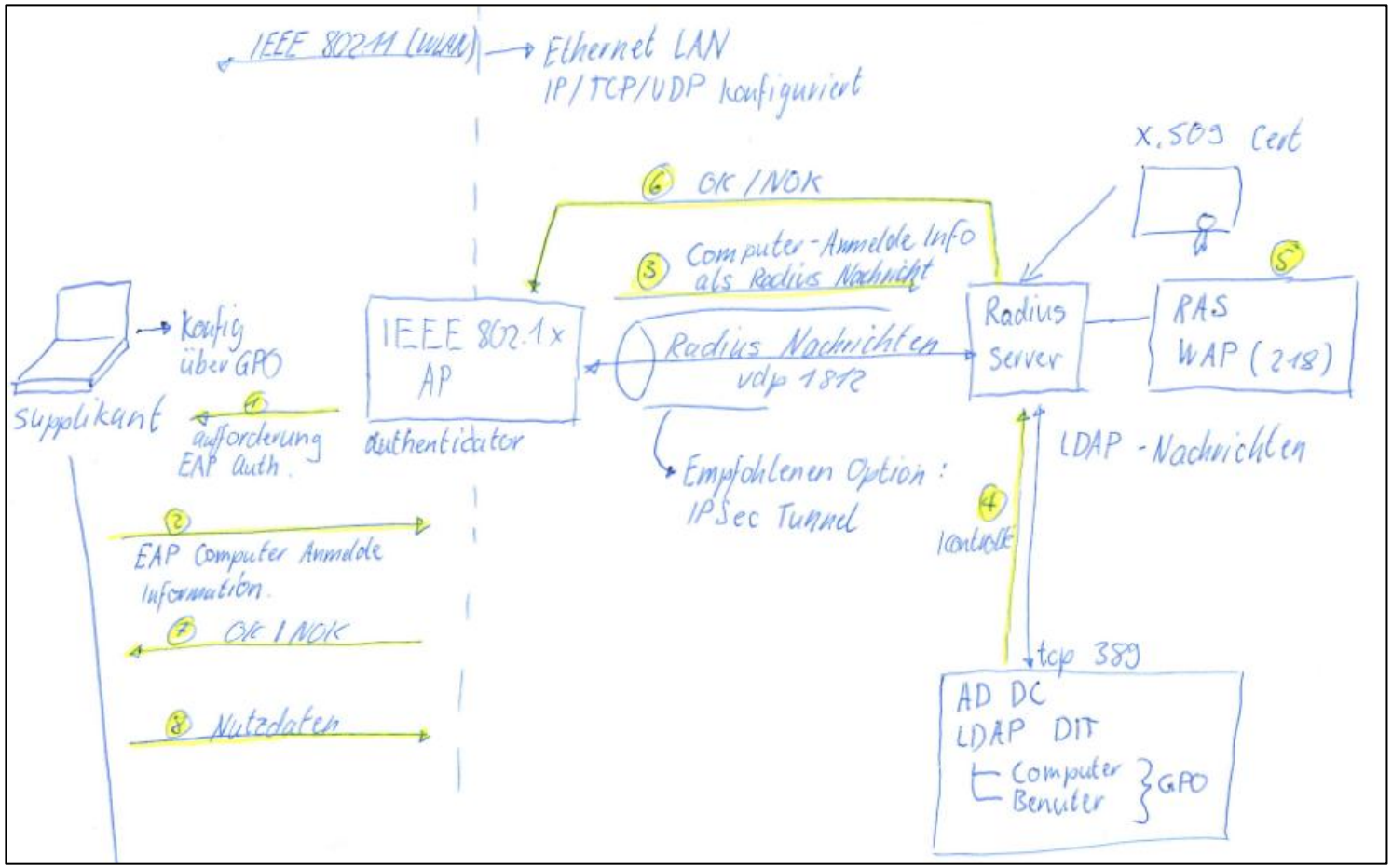


Abbildung 5: IEEE Authentifzierung nach EAP-TLS

Vorteile dieses Verfahrens:

- Computer und Benutzer basierte Authentifizierung anstelle eines bekannten PSK.

2.3 Sichern von WLANs in einer Active Directory Umgebung

2.4 Hauptoptionen

- WPA-PSK (Wi-Fi Protected Access, Pre-shard Key) für sehr kleine Unternehmen und Heimarbeitsplätze
- Kennwortbasierte WLAN-Sicherheit für Unternehmen, die keine Zertifikate verwenden und nicht benötigen
- Zertifikatbasierte WLAN-Sicherheit für Unternehmen, die Zertifikate benötigen und installieren können.

Die Frage, welche der drei Hauptoptionen für eine bestimmte Situation angemessen ist, kann mit Hilfe des folgenden Entscheidungsbaumes entschieden werden.

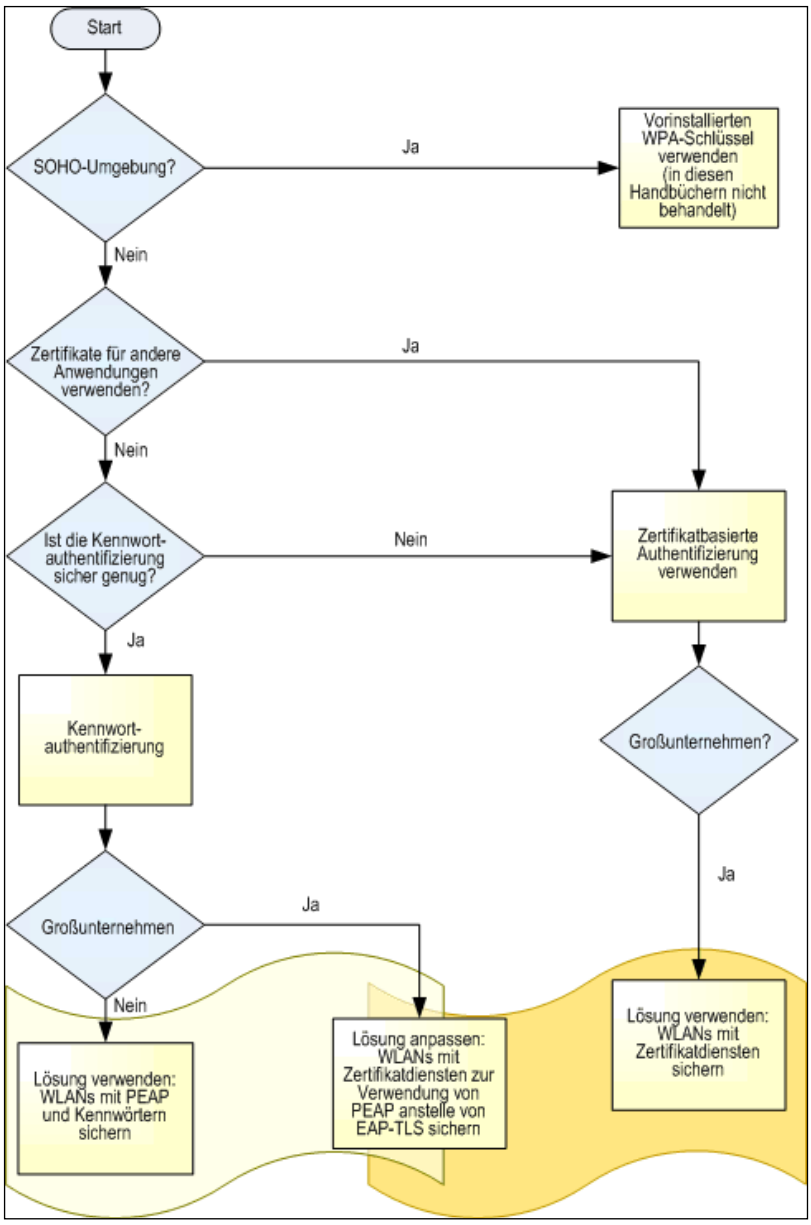


Abbildung 6: Entscheidungsbau WLAN Security

2.5 Argumente für Drahtlos-Netzwerke

Die Vorteile der WLAN-Technologie lassen sich in zwei Kategorien unterteilen: geschäftliche Vorteile und operative Vorteile.

2.5.1 Geschäftliche Hauptvorteile

Die geschäftlichen Vorteile ergeben sich durch die verbesserte Unterstützung von flexiblen Arbeitseisätzen und der dabei erforderlichen Mobilität innerhalb des Unternehmensgebietes.

2.5.2 Operative Vorteile

Die WLAN Technologie kann dazu beitragen, die Kapitalkosten für die Netzwerk-Infrastruktur zu senken.

- Die Kosten der Bereitstellung des Netzwerkzugriffs in Gebäuden werden erheblich verringern.
- Das Netzwerk kann leicht je nach unterschiedlichem Bedarf durch Unternehmensveränderungen bzw. nach Tagesbedarf skaliert werden.
- Kapital muss nicht mehr in die Gebäudeinfrastruktur eingebunden sein; die drahtlose Netzwerkinfrastruktur lässt sich verhältnismässig leicht in ein anderes Gebäude verlegen.

Der entscheidende Vorteil der IEEE 802.1X basierten Netzzugangsvermittlung besteht darin, dass der Netzzugang nur nach erfolgreiche, persönlicher Authentifizierung des Benutzers gewährt wird. Bei einen PSK-basierten Netzzugangsvermittlungen, ist nicht feststellbar, welcher Benutzer die WLAN-Ressourcen verwendet hat.

2.6 Sicherheitsprobleme in WLANs

Bedrohung	Beschreibung der Bedrohung
Lauschangriffe (Offenlegung von Daten)	Das Abhören von übertragenen Daten kann zum Verlust von vertraulichen Daten, ungeschützten Anmeldeinformationen und zu potenziellem Identitätsdiebstahl führen. Außerdem ermöglicht es erfahrenen Eindringlingen, Informationen über Ihre IT-Umgebung zu sammeln, die für einen Angriff auf andere Systeme oder Daten verwendet werden können, die andernfalls nicht anfällig wären.
Abfangen und Ändern übertragener Daten	Wenn ein Angreifer Zugriff auf das Netzwerk hat, kann er einen feindlichen Computer zum Abfangen und Ändern von zwischen zwei legitimen Teilnehmern ausgetauschten Netzwerkdaten einfügen.
Spoofing	Der Zugriff auf ein internes Netzwerk ermöglicht einem Eindringling das Vorgeben scheinbar legitimer Daten auf eine Weise, die von außerhalb des Netzwerks nicht möglich wäre, zum Beispiel eine gespoofte E-Mail-Nachricht. Die meisten Personen (einschließlich Systemadministratoren) neigen dazu, internen Objekten weitaus mehr zu vertrauen als Objekten, die von außerhalb des Unternehmensnetzwerks stammen.
DoS (Denial of Service)	Ein Angreifer kann DoS-Angriffe mit verschiedenen Methoden auslösen. Signalunterbrechungen auf Funkebene können beispielsweise durch so einfache technische Geräte wie eine Mikrowelle ausgelöst werden. Es sind jedoch auch weiter entwickelte Angriffe möglich, die auf die Drahtlosprotokolle niedrigerer Ebene an sich abzielen, sowie weniger komplexe Angriffe, die auf Netzwerke über schlichte Datenüberflutung der WLANs durch wahllosen Datenverkehr abzielen.
Freie Internetbenutzung (oder Diebstahl von Ressourcen)	Ein Eindringling möchte möglicherweise "nur" Ihr Netzwerk als freien Zugriffspunkt für das Internet nutzen. Obwohl sich dies nicht so schädigend wie die anderen Sicherheitsbedrohungen auswirkt, verringert es nicht nur die Verfügbarkeit des Dienstes für die legitimen Benutzer, sondern kann auch Viren und anderen Bedrohungen einschleppen.
Zufällige Sicherheitsbedrohungen	Einige Funktionen von WLANs erhöhen sogar die Bedrohung durch unbeabsichtigte Angriffe. Zum Beispiel könnte ein legitimer Besucher seinen Laptop starten, ohne eine Verbindung mit Ihrem Netzwerk herstellen zu wollen, wird jedoch automatisch mit dem WLAN verbunden. Der Laptop des Besuchers ist jetzt ein potenzieller Zugriffspunkt für Viren auf Ihr Netzwerk. Diese Art von Sicherheitsbedrohung ist lediglich in nicht abgesicherten WLANs ein Problem.
Inoffizielle WLANs	Selbst wenn Ihr Unternehmen offiziell über kein WLAN verfügt, sind Sie dennoch Sicherheitsbedrohungen durch im Netzwerk installierte, nicht verwaltete WLANs ausgesetzt. Von begeisterten Mitarbeitern gekaufte preisgünstige WLAN-Hardware kann unbeabsichtigte Sicherheitslücken im Netzwerk öffnen.

2.7 Effektives Absichern von WLANs

Aufgrund der oben dargestellten Sicherheitsprobleme haben sich führende Netzwerkgeräte-Hersteller und Normenaufsichtsbehörden bemüht sichere Verfahren für WLANs zu entwickeln. Die zur Zeit bekanntesten Alternativen zur Absicherung von WLANs sind:

- Keine WLAN-Technologie verwenden
- Verwenden von WPA-PSK Sicherheit
- Verwenden von VPN-Technologie (speziell des IPSec-Standards) zum Schutz des WLAN-Datenverkehrs
- Verwenden von 802.1X-Authentifizierung und Datenverschlüsselung (WPA mit gemanagtem Key)

2.7.1 Hauptelemente der WLAN-Sicherheit

Der Schutz eines WLANs umfasst drei Hauptelemente:

- Authentifizierung des Client-Computers und Authentifizierung der Person, die eine Verbindung zum Netzwerk herstellt, sodass mit hoher Gewissheit fest steht, wer eine Verbindung zum Netzwerk herzustellen versucht
- Autorisierung der Person oder des Geräts für die Nutzung der Ressourcen im LAN
- Schutz der im Netzwerk übertragenen Daten vor Lauschangriffen und nicht autorisierter Änderung

2.7.2 Authentifizierung für den Zugang zum WLAN

Es muss zwischen persönlicher (auch für Computer gemeint) und unpersönlicher Authentifizierung bzw. Autorisierung zur Erlangung des WLAN-Zugriffs unterschieden werden:

Unpersönliche Authentifizierung/ Autorisierung

WEP und WPA-PSK	Alle ,die WEP-Schlüssel oder den WPA-PSK für ein WLAN kennen, haben grundsätzlich Zugriff auf die WLAN Infrastruktur

Persönliche Authentifizierung/ Autorisierung

IEEE 802.1X	Der Standard IEEE 802.1X basiert auf persönlicher Authentifizierung von Benutzer und Computer gegenüber einem RADIUS-Server, der typischerweise seinerseits auf Daten eines LDAP-DITs operiert.

Verschlüsselung der Datenübertragung

WEP	WEP (Wired Equivalent Protection) hat bekannte kryptologische Mängel und soll aus diesem Grunde für die Verschlüsselung von Daten in Unternehmen nicht mehr angewendet werden.
WPA	WPA kann im Enterprise Mode oder in einem PSK-Mode betrieben werden. Der Enterprise Mode nutzt IEEE 802.1X/EAP und RADIUS für die Authentifizierung, während im PSK-Mode weiterhin 8-63 Zeichen lange pre-shared-Key eingesetzt werden.

2.7.3 Vergleich von verschiedenen Methoden zur WLAN-Sicherheit

Eigenschaft	IEEE 802.1X	WPA-PSK	IPSec
Persönliche Authentifizierung (Benutzerauthentifizierung)	Ja	Nein	Ja, falls Zertifikats- oder Kerberos-Authentifizierung eingesetzt wird
sichere Datenverschlüsselung	Ja	Ja	Ja
Computer-Authentifizierung (2)	Ja Jeder Computer verfügt in einer zertifikatsbasierten Implementierung von IEEE 802.1X über ein eigenes Computer Zertifikat	Nein, alle Computer besitzen den gleichen WAP-PSK	Ja

2.7.3.1 Computer-Authentifizierung

Diese Fähigkeit ist erforderlich, damit die folgenden Windows-Domänenfeatures ordnungsgemäss funktionieren:

- Computer-Gruppenrichtlinienobjekte (GPOs) nach erfolgter Computer-Authentifizierung anwenden
- Servergespeicherte Benutzerprofile
- Benutzeranmeldeskripte und mit Gruppenrichtlinien bereitgestellte Software

Bei IEEE 802.1X wird die Computer-Authentifizierung durch die Installation eines Computerzertifikats ermöglicht.

2.8 802.1X-Authentifizierungsarten in einer Active Directory Gesamtstruktur

2.8.1 EAP/TLS-Authentifizierung

EAP/TLS ist eine Authentifizierungsmethode auf Zertifikatsbasis mit **gegenseitiger** Authentifizierung von Benutzer **und** Computer und einem Radius Server, der gegen entsprechende Einträge im LDAP-DIT der Gesamtstruktur überprüft.

2.8.1.1 Zertifikate

Zertifikate bilden die Grundlage der Infrastruktur öffentlicher Schlüssel (Public Key Infrastruktur). Sie stellen elektronische Ausweise oder Referenzen dar, die von einer Zertifizierungsstelle (Certification Authority, CA) ausgegeben werden und

mit einem Schlüsselpaar verknüpft sind, bestehend aus einem öffentlichen und einem privaten Schlüssel.

Der öffentliche Schlüssel kann in Form eines Zertifikates publiziert werden, der private Schlüssel darf nur dem Antragssteller bekannt sein (z.B. Sicherheit durch Speicherung auf PIN-Code geschützte Smarcard.

Ein Zertifikat ist eine **digital signierte** Sammlung von Informationen mit einem Umfang von etwa 2 bis 3 KByte. Im Normalfall enthält ein Zertifikat Folgendes:

- Informationen zum Benutzer, dem Computer oder dem Netzwerkgerät, **dem der zum ausgestellten Zertifikat gehörige, private Schlüssel gehört**. Der Benutzer, der Computer oder das Netzwerkgerät werden als **Antragssteller** bezeichnet.
- Informationen über die ausstellende Zertifizierungsstelle
- **Den öffentlichen Schlüssel aus dem zum Zertifikat gehörigen Schlüsselpaar**
- Die Namen der digitalen Signatur- und Verschlüsselungsalgorithmen, vom Zertifikat unterstützt werden
- Angaben zur Gültigkeit des Zertifikats und zur Überprüfung des Sperrstatus.

2.8.2 Benötigte Zertifikate für die EAP-TLS Authentifizierung

Ausstellung von Zertifikaten an Benutzer und Computer

Folgende Zertifikate sind zur IEEE 802.1X - EAP/TLS-Authentifzierung von Benutzer und Computer innerhalb einer Active Directory Gesamtstruktur (was das Eidomänen-Modell einschliesst), erforderlich:

Zertifikat für RADIUS-Server

Zur 802.1X Authentifizierung wird die Verwendung des Windows Server 2003-Internetauthentifizierungsdienstes (IAS) als RADIUS-Server empfohlen.

Für den Radius-Server muss ein Computerzertifikat ausgestellt und installiert werden.

Zertifikat für den Zugriffsclient (Supplicant)

Clientcomputer brauchen ein Zertifikat zur 802.1X-EAP/TLS Authentifizierung, wenn der Computer Mitglied einer Gesamtstruktur ist. Dann sind auch die oben erwähten Active Directory Features einsetzbar.

Zertifikat für den Benutzer

Zur Authentifizierung des Benutzers über 802.1X-EAP/TLS benötigt der Benutzer ein Zertifikat.

2.8.3 Ablauf der 802.1X-Authentifizierung in einer Gesamtstruktur

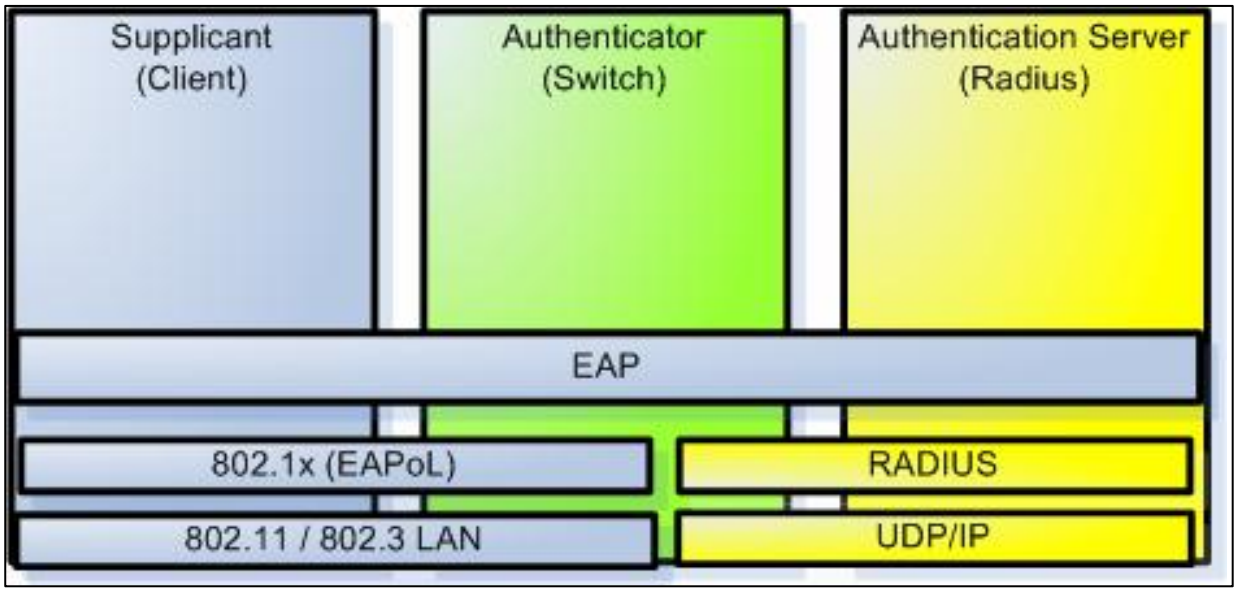


Abbildung 7: Übersichtsdiagramm 802.1x Authentifizierung

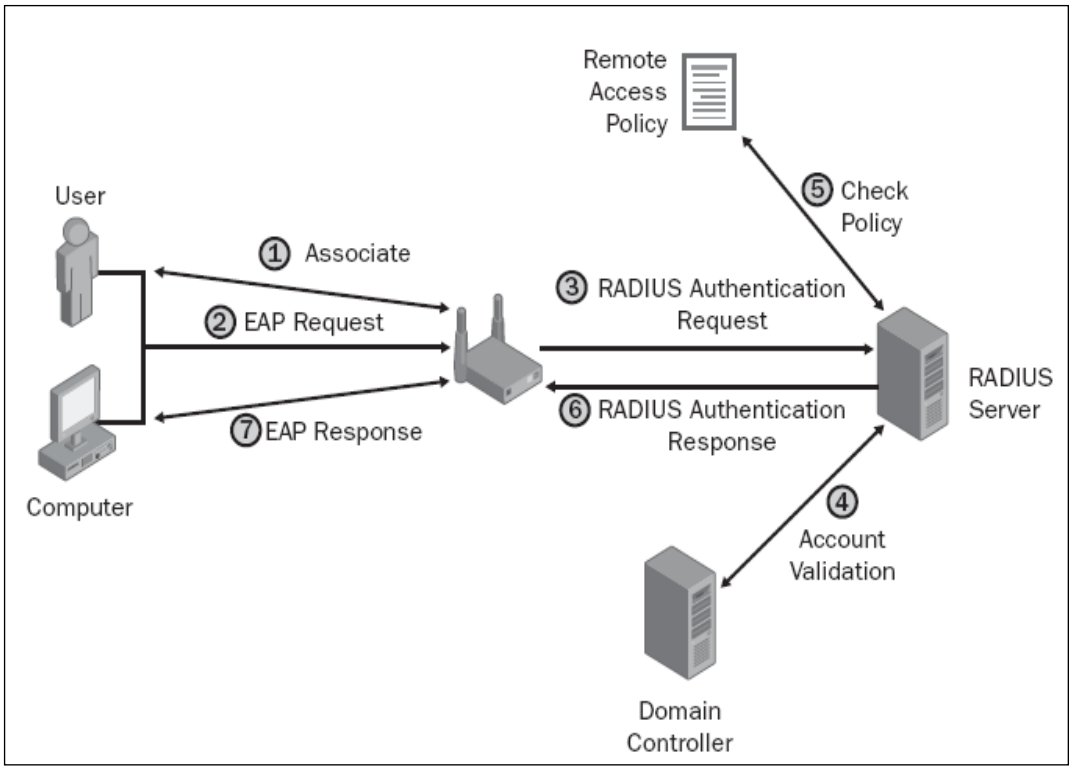


Abbildung 8: Ablauf der Authentifizierung

1. Die Supplicant-Software auf dem Client-Computer versucht, eine Verbindung mit dem IEEE 802.1X –Authenticator (WLAN Access Point) herzustellen. Der Authenticator reagiert mit der Aufforderung zur EAP-Authentifizierung
2. Der Computer gibt seine Anmeldeinformation (die mit seinem privaten Schlüssel signiert ist) an den Authenticator weiter.
3. Der Authenticator übersetzt die EAP-Authentifizierungsnachricht des Computers und in Radius Authentifzierungspakete und leitet diese an den Radius Server weiter.
4. Der Radius Server wendet sich an einen Domänencontroller, um aus dem Antragsteller-Namen die Signatur des gesendeten Zertifikats zu überprüfen.
5. Der IAS Radius Server überprüft anhand der auf dem IAS Radius Server konfigurierten RAS-Richtlinien, ob der im LDAP identifizierte Computer über den Authenticator Zugang erhalten soll
6. Der Radius Server sendet eine RADIUS-Authentifizierungsnachricht mit einer Erfolgs- oder Fehlermeldung an den Authenticator. Im Erfolgsfall wird der Authenticator dem Supplicant einen gemanagten 802.1X-Port öffnen.
7. Der Authenticator sendet sendet dem Supplicant eine EAP-Erfolgs- oder Fehlernachricht.
8. Nun kann der Supplicant seinerseits eine Identifizierung des Radius-Servers vornehmen, da der Radius-Server auch mit einem Zertifikat ausgerüstet ist
   Nun kann der Domänencontroller die Computer-Gruppenrichtlinien-Objekte und anderen Startskripte an den Supplicant senden, aufgrund der Comuter-Identifizierung nun klar geworden ist, welche Computer-Konfigurationseinstellungen zu übertragen sind.
   Wenn dieser Prozess abgeschlossen ist, kann sich der Benutzer mit Hilfe seines Zertifikats anmelden.

2.9 Übersicht Netzzugangsverfahren

2.9.1 Leistungsstufen

Es gibt 3 Leistungsstufen

9. IP-Konfiguration
10. Authentifizierung für MAC-Schicht (Layer 2) Zugang (Optional kann aber Vorraussetung für Leistungsstufe 1 sein).
11. Authentifizierung an einem LDAP Directory System

Layer1	Layer2	Layer3
DHCPv4		
DHCPv6		
IPv6 => Router solicitaion (Erkennen ob Router vorhanden ist)		
Router advertitsement		
	WLAN WPA mit PSK PP Zugang	
	IEEE 802.1 X (MAX- und Diectory-Zugang nach persönlicher Authentifizierung	

2.9.2 L1 DHCPv4

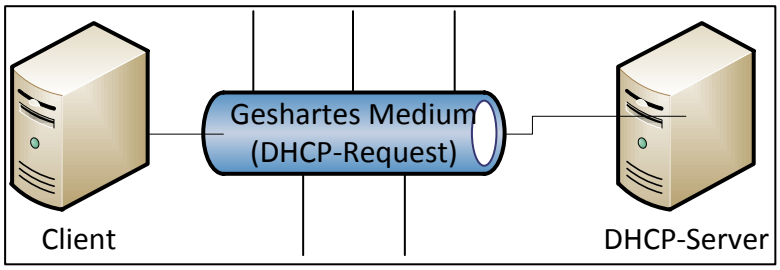


Abbildung 9: DHCP

2.9.3 Verkapselung Packet

Ehternet		
DstMacAdr: BC (Broadcast)	**IP**	
srcMACAdr: Client Mac	destIPAdr: IPBroadcast	**UDP**
	srcIPAdr: 0.0.0.0	

3 Active Directory

3.1 Physische Struktur von Active Directory

3.1.1 Directory-Datenspeicherung und Zugriffsprotokolle

Sämtliche Verzeichnisdaten werden auf jedem Domänencontroller im

- LDAP Directory Information Tree (LDAP-DIT) in der Datei ntds.dit
- und in den Transaktionsprotokollen (schwebende Operationen)

gespeichert.

Zur Einspeicherung und für den Zugriff auf die LDAP-Knoten werden verschiedene Software-Komponenten und Zugriffsprotokolle eingesetzt. Die nachstehende Abbildung gibt dazu einen Überblick.

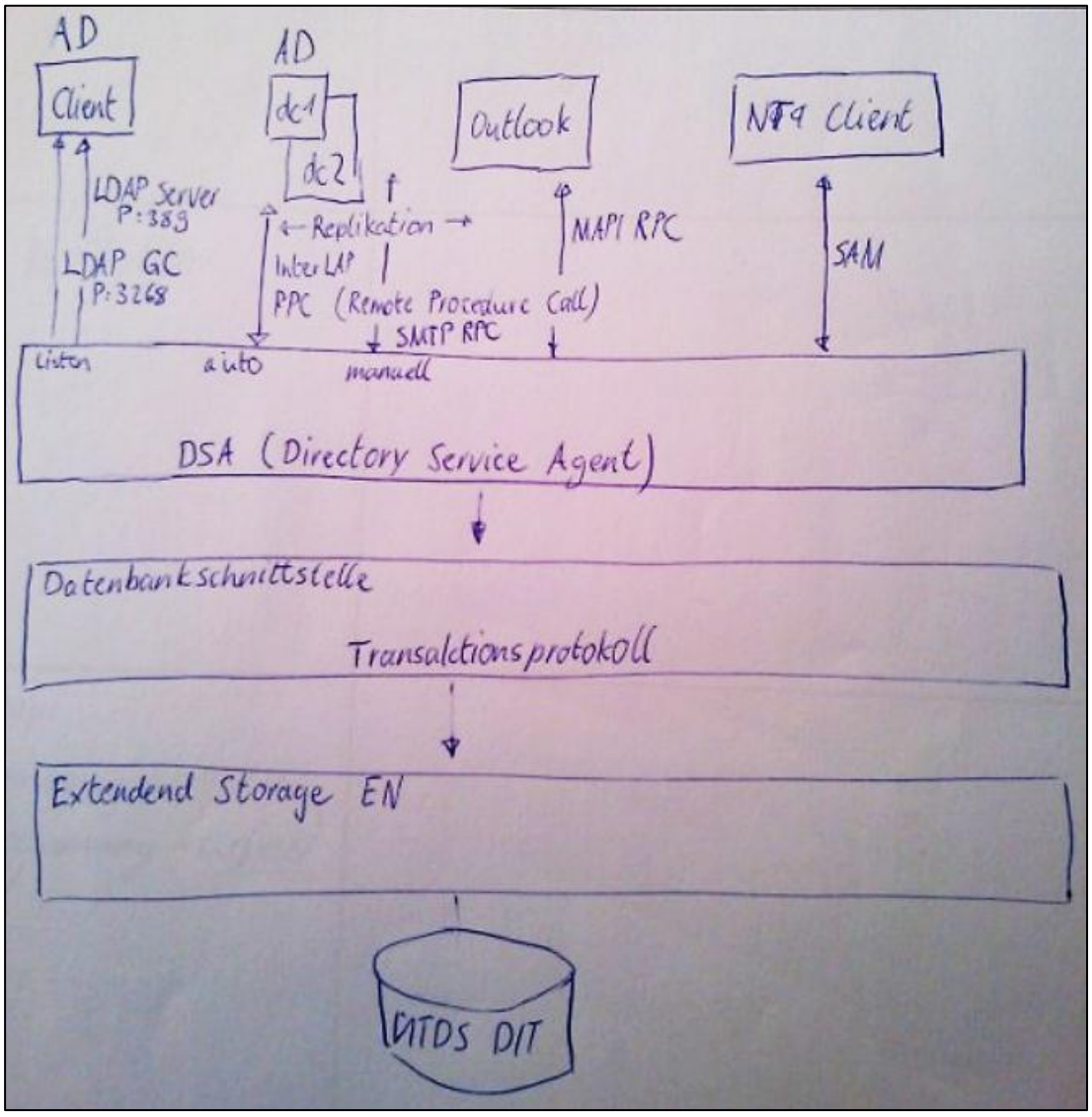


Abbildung 10: Architektur der AD-Directory-Daten Einspeicherung

Auf den LDAP-DIT kann mit den folgenden Protokollen zugegriffen werden:

LDAP	• Client -> LDAP-Protokoll –LDAP-DIT : tcp-Serverport: 389 • Client -> LDAP-Protokoll ->Globaler Katalog (GC): tcp-Serverport: 3268

Replikation	• Gegenseitiger Abgleich des DIT zwischen den DCs.
	• Standort-intern:
	  ○ Automatisch über RPC
	• Standort-übergreifend:
	  ○ Manuell konfigurieren, über SMTP oder RPC
	• (AD-Standort = IP-Teilnetz !!!)
	• Replikation erfolgt im Multimaster-Betrieb

MAPI	• MAPI = Messaging Aplication Programming Interface • (z.B. zur Authentifizierung der Outlook-Benutzer)
SAM	• Security Account Manager • Zur Anbindung von Windows NT Clients • (IP ¦ TCP <- RPC)

Die obengenannten Protokolle verwenden für den Zugriff auf den LDAP-DIT die folgenden Software-Komponenten auf dem Domänencontroller:

DSA **Directory Service Agent**	Liefert die Zugangs-Schnittstellen für die verschiedenen Client-Rollen und die Replikation des DIT.
Datenbank-Zugriffsschicht	Pufferung der Schreib- und Lese-Operationen -> Transaktionsprotokoll
SE **Extensible Storage Engine**	Exklusiver Zugriff auf den DIT

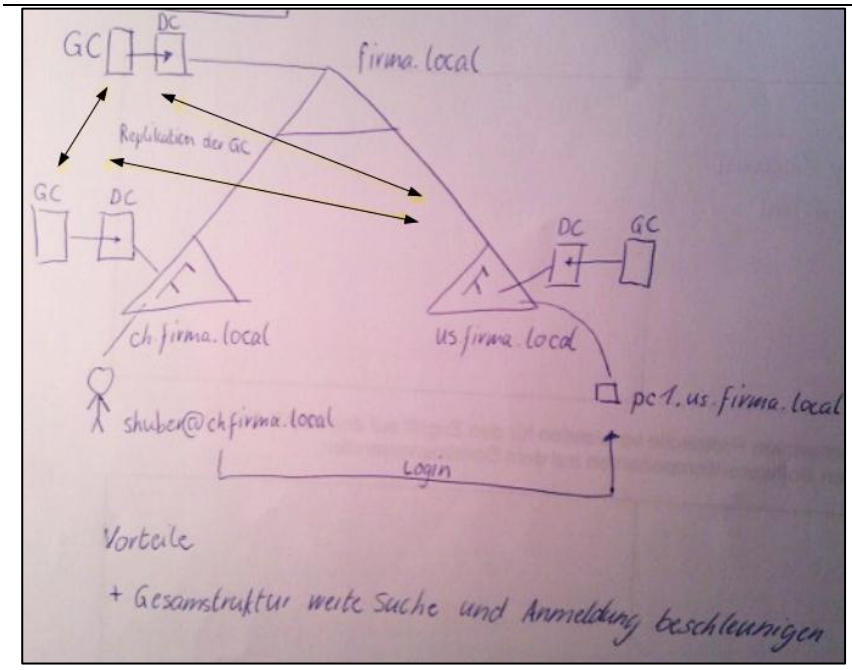


Abbildung 11: Anmeldung des GC

Vorteile: Gesamtstruktur weite Suche und Anmeldung beschleunigen

3.1.2 Domänencontroller

Auf dem Domänencotroller werden die verschiedenen Komponenten des Active Directorys ausgeführt, dazu gehören insbesondere die folgenden Systeme:

Systeme, die auf jedem Domänencontroller aktiv sind:

- Kerberos Key Distribution Center (KDC)
- Active Directory integriertes Domain Name System (DNS)
- LDAP Datenspeicherung und Zugriffs-Schnittstellen
- Directory-Daten Replikationsmechanismus
- Gruppenrichtlinien Objektverwaltung

Systeme, die auf gewissen Domänencontrollern aktiv sind:

- Globaler Katalogserver
- Betriebsmaster-Rollen

3.1.2.1 Globaler Katalogserver

Der globale Katalog ist ein schreibgeschütztes Teilreplikat aller LDAP-DITs in der Domänen-Gesamtstruktrur und enthält:

- alle LDAP-Objekte (Knoten) aller Domänenverzeichnisse der Gesamtstruktur
- aber nur eine Teilmenge der möglichen Attribut-Werte.

Im Schema wird fürr jedes Attribut festgelegt, ob es im globalen Katalog eingespeichert werden soll. Attribute, die im globalen Katalog eingespeichert werden, sind als Elemente des Partial Attribut Sets (PAS) gekennzeichnet. Im MMC-Snap-In für das Active Directory Schema, kann ein Attribut zum PAS hinzugefügt werden.

Im globalen Katalog werden grundsätzlich nur jene Attribute vorgehalten, die häufig nachgefragt werden.

Der globale Katalog hat in einer Domänengesamtstruktur den folgenden Nutzen:

- Beschleunigung der Benutzer-Authentifizierung bei Interdomämen-Anmeldung
- Interdomänenweite Suchvorgänge nach LDAP-Knten (z.B. Drucker) sind bequem möglich.
- Suchvorgänge nach Attributwerden aus dem PAS (Partial Attribut Set) sind schneller als auf dem LDAP-DIT.

3.1.3 Betriebsmaster-Rollen

Bei der Konstruktion des Active Directory Services war man bemüht, einen möglichst grossen Funktionsumfang im Multimasterbetrieb ausführen zu lassen.

3.1.3.1 Multimaster- versus Master- / Slave-Betrieb

Master-/ Slave-Betrieb	Multimaster-Betrieb
Ein Master enthält den Stammdatensatz, die übrigen Server, die für die gleiche Aufgabe zuständig sind, müssen ihre Daten durch einseitige Replikation aktuell halen. Auf den Slaves könen durch den Administrator keine Daten gepflegt werden. Typisches Beispiel: Master- Slave Beziehung bei klassischen DNS-Servern (z.B,. mit BIND).	Im Multimaster Betrieb können Daten auf jedem Server, der den fraglichen Dienst hostet, gepflegt werden. Jeder Server repliziert mit jedem anderen Server. Typische Beispiele: -> siehe unten!

Bei Active Directory werden die folgenden Kernbereiche im Multimaster-Betrieb auf allen Domäencontrollern betrieben:

- LDAP-DIT
- Acitve Directory integrierte DNS-Zonen

Es gelang nicht, alle Teilaufgaben im Active Directory System Multimaster fähig auszulegen. So müssen bestimmte Aufgaben (Rollen) bestimmten Domäencontrollern zugewiesen werden, bzw. die automatische Zuweisng bei der Installation muss respektiert werden.

Es sind dies die folgendn Rollen, die als Betriebsmaster-Rollen oder FSMO-Rollen (FSMO= Flexible Single Master Operations) bezeichnet werden:

Schemamaster

Gesamtstrukturweite Zuständigkeit

Einziger Domänencontroller in der Gesamtstruktur, der Schreibberechtigung auf den Schema hat..
Ist der erste Domänencontroller der Gesamtstruktur.

Jeder (!) Domänencontroller der Gesamtstruktur besitzt eine schreibgeschützte Kopie de Schemas.

Domänennamenmaster

Gesamtstrukturweite Zuständigkeit

Einziger Domänencontroller in der Gesamtstruktur, der die Berechtigung hat, Domänennamen zu vergeben und zu verwalten.

RID-Master

Domänenweite Zuständigkeit

Verwaltet die Vergabe von relativen IDs (Teil der SID) für die Objekte im LDAP-Verzeichnis der Domäne.
(SID = ID der Domäne + RID)

Infrastrukturmaster

Domänenweite Zuständigkeit

Wird zur Aktualisierung von domänenübergreifenden Verweisen zwischen Gruppen und Benutzern verwendet (universelle Gruppen)

PDC-Emulator

Domänenweite Zuständigkeit

Emuliert die Funktion eines Windows NT Primary Domain Controllers für die Anmeldung am AD.
Wir von Windows NT Workstations benutzt.

3.2 Logische Struktur

3.2.1 Übersicht

Zur logischen Strukturierung eines Active Directory Systems stehen die folgenden Komponenten zur Verfügung

- Partitionen
- Domänenstrukturen
- Domäne
- Standort
- OU

3.2.2 Active Directory System Partitionen

Wie früher schon gezeigt, werden sämtliche Informationen des Active Directory Directory Systems (AD DS) in einer Datenbankdatei auf jedem Domänencontroller gespeichert. Die in der Verzeichnisdatenbank gespeicherten Informationen werden in mehrere logische Partitionen unterteilt. Die jeweils unterschiedliche Informationstypen speicher. Diese Partitionen werden auch als Namenskontexte (Naming Contexts) bezeichnet.

Allen Partionen des AD DS Datenspeichers ist aber gemeinsam, dass die Informationen nach dem LDAP Informations- und Namensmodell eingespeichert werden. So erfolgt die Adressierung eines Benutzerobjektes z.B. durch

CN=Yvonne McKay, OU=Marketing, OU=Miami, DC=SeaFood, DC=com.

Active Directory System Partitionen können mit dem Tool Ldp.exe oder mit dem Snap-In ADSI-Editor untersucht werden.

Der Datenbankspeicher von AD DS ist in folgende Partionen gegliedert:

- Domänenverzeichnispartition (Directory Verz. Part: dc, ou, cn)
- Konfigurationspartition (Standorte, Netzwerk objekte)
- Schemaverzeichnispartition
- Partition des GC (nur bestimmte DCs)
- Anwendungspartition (DNS-Obj bei AD integriertem DNS)

3.2.3 Domänenverzeichnispartition

Enthält:	**Directory-Objekte einer Domäne:** • OUs • Benutzer • Computer
Wird gehostet von	Jedem DC in der Domäne
Kopie für Multimaster-betrieb?	d.h.: „Hostet jeder Domänencontroller eine beschreibbare Kopie im Multimasterbetrieb, oder wird eine Masterkopie von einem Betriebsmaster gehostet? **Multimaster-Betrieb**
Replikation	Standort intern: • Automatisch Standort extern: • Manuell

3.2.4 Schemaverzeichnispartition

Enthält:	**Gesamtstrukturweit gültiges Schema**
Wird gehostet von	Read Write Original • Schema-Master Read Only • Auf jedem DC der Gesamtstruktur
Kopie für Multimaster-betrieb?	d.h.: „Hostet jeder Domänencontroller eine beschreibbare Kopie im Multimasterbetrieb, oder wird eine Masterkopie von einem Betriebsmaster gehostet? **Singlemaster-Betrieb**
Replikation	Gesamtstrukturweit, Konfiguration gemäss 2.1

3.2.5 Partition des globalen Katalogservers

Enthält:	**Alle Objekte der Gesamtstruktur**
Wird gehostet von	Designierten (Rollenbehaftete) DCs
Kopie für Multimaster-betrieb?	d.h.: „Hostet jeder Domänencontroller eine beschreibbare Kopie im Multimasterbetrieb, oder wird eine Masterkopie von einem Betriebsmaster gehostet? **Multimaster-Betrieb**
Replikation	Gesamtstrukturweit, Konfiguration gemäss 2.1

3.2.6 Konfigurationspartition

Enthält:	**Netzwerkobjekte und Standorte Gesamtstrukturweit**
Wird gehostet von	Von allen DCs der Gesamtstruktur
Kopie für Multimaster-betrieb?	d.h.: „Hostet jeder Domänencontroller eine beschreibbare Kopie im Multimasterbetrieb, oder wird eine Masterkopie von einem Betriebsmaster gehostet? **Multimaster-Betrieb**
Replikation	Gesamtstrukturweit, Konfiguration gemäss 2.1

3.2.7 Konfigurationspartition

Enthält:	**Resource-Records (RR) der DNS Zonen für die der DC autorisiert ist. Gilt nur wenn Active Directory ingegriertes DNS vorhanden ist.**
Wird gehostet von	Jedem DC, der zu einer bestimmten Zone gehört.
Kopie für Multimaster-betrieb?	d.h.: „Hostet jeder Domänencontroller eine beschreibbare Kopie im Multimasterbetrieb, oder wird eine Masterkopie von einem Betriebsmaster gehostet? **Multimaster-Betrieb**
Replikation	Gesamtstrukturweit, Konfiguration gemäss 2.1

3.2.8 Domänen

Grundlegende Containter des AD DS

- Grenze für die Replikationen für die Domänenverzeichnis-Parition (~LDAP-DIT)
- Grenze für den Ressourcen-Zugriff, Authentifizierung => Autorisierung gem. DACL (Ressourcen-Zugriffs-Regelung auf der Basis von Sicherheitsgruppen).
- Grenze für Sicherheitsrichtlinien
  - z.B. Passwort- oder Kerberos-Richtlinien
- Grenze für die Vertrauensstellung
  - Vertrauensstellungen werden nur zwischen Domänen eingerichtet

3.2.9 Gesamtstruktur

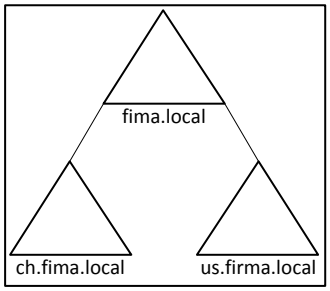


Abbildung 12: Einfaches AD Schema

Gemeinsamkeiten zwischen Domänen sind:

- Chema (RW auf Schema-master, R only auf jeden DC)
- Konfigurationspartition (auf allen DCs der Gesamtstruktur im Multimaster-Betrieb)
- Globaler Katalog (auf designierten DCs in allen Domänen im Multimaster-Betrieb)
- Gesamtstrukturweite Betriebsmaster:
  - Schema- und Domänennamen-Master)

3.2.10 Standorte

Ist ein Container-Objekt (← GPO). Die Definition eines Stao ist gleich bedeutend zu:

- IP-Teilnetz pro Stao
- Replikation zwischen Stao muss manuell eingerichtet werden.

Die Standortverbindung für den operativen Einsatz erfordert in der Regel eine IP in IP (z.B. IPsec) verbindung.

3.2.11 Eigenschaften von Standorten

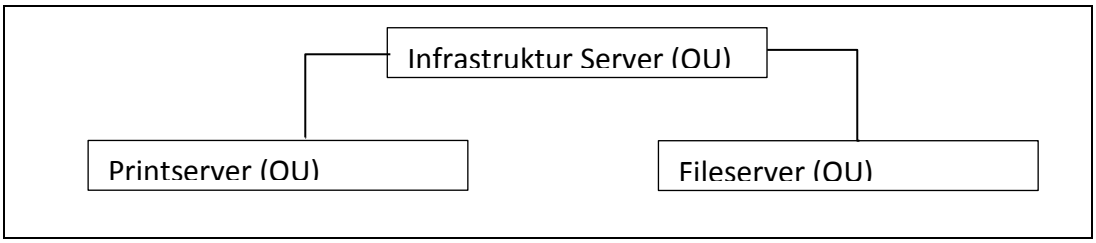
- Enthält ein oder mehrere Netzwerk-Objekte.
- Standortübergreifende Replikation (Verzeichnis Partition, Konfiguration Partition) muss konfiguriert werden.
- In einem Standort können sich Hosts von mehreren Domänen befinden.
- Standort-Zugehörigkeit
    - DC <= Konfig. manuell
    - –Client <= dynamisch, während Boot-Vorgang

3.2.12 Organisationseinheiten

Ist ein Container-Objekt (← GPO)

Strukturierung kann nach verschiedenen Konzepten erfolgen:

- Organisation des Unternehmens
- Funktionale Gliederung z.B. für Server, mobile Clients



(vergl. MSFT Server Security Handbuch mit Vorschlägen zu Sicherheitsrichtlinien, die an die entsprechenden Containter gebunden werden können)

3.3 AD Rechte und Berechtigungen

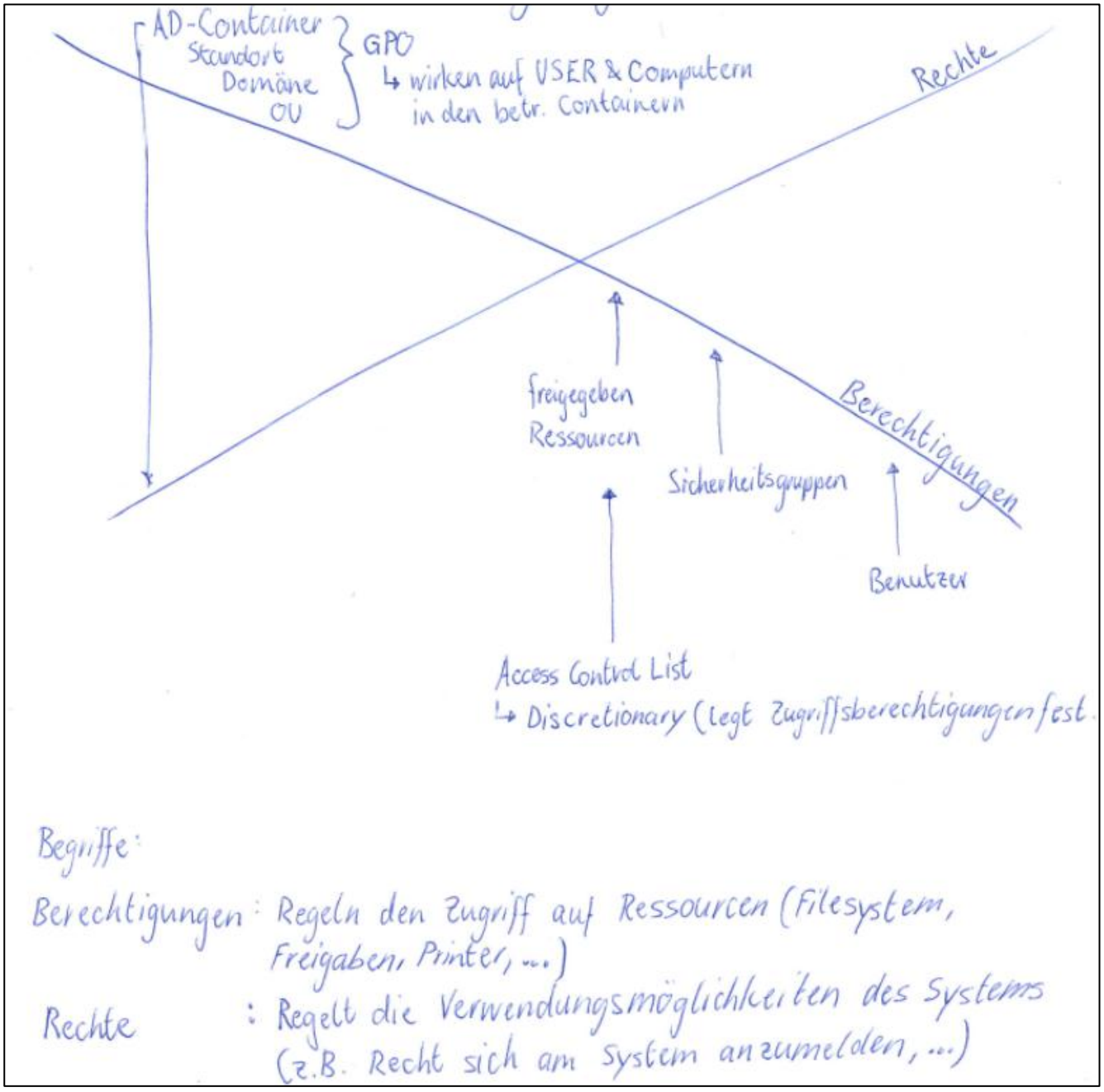


Abbildung 13: AD Rechte und Berechtigungen

3.4 Berechtigungen und Ressourcen Zugriffsplanung

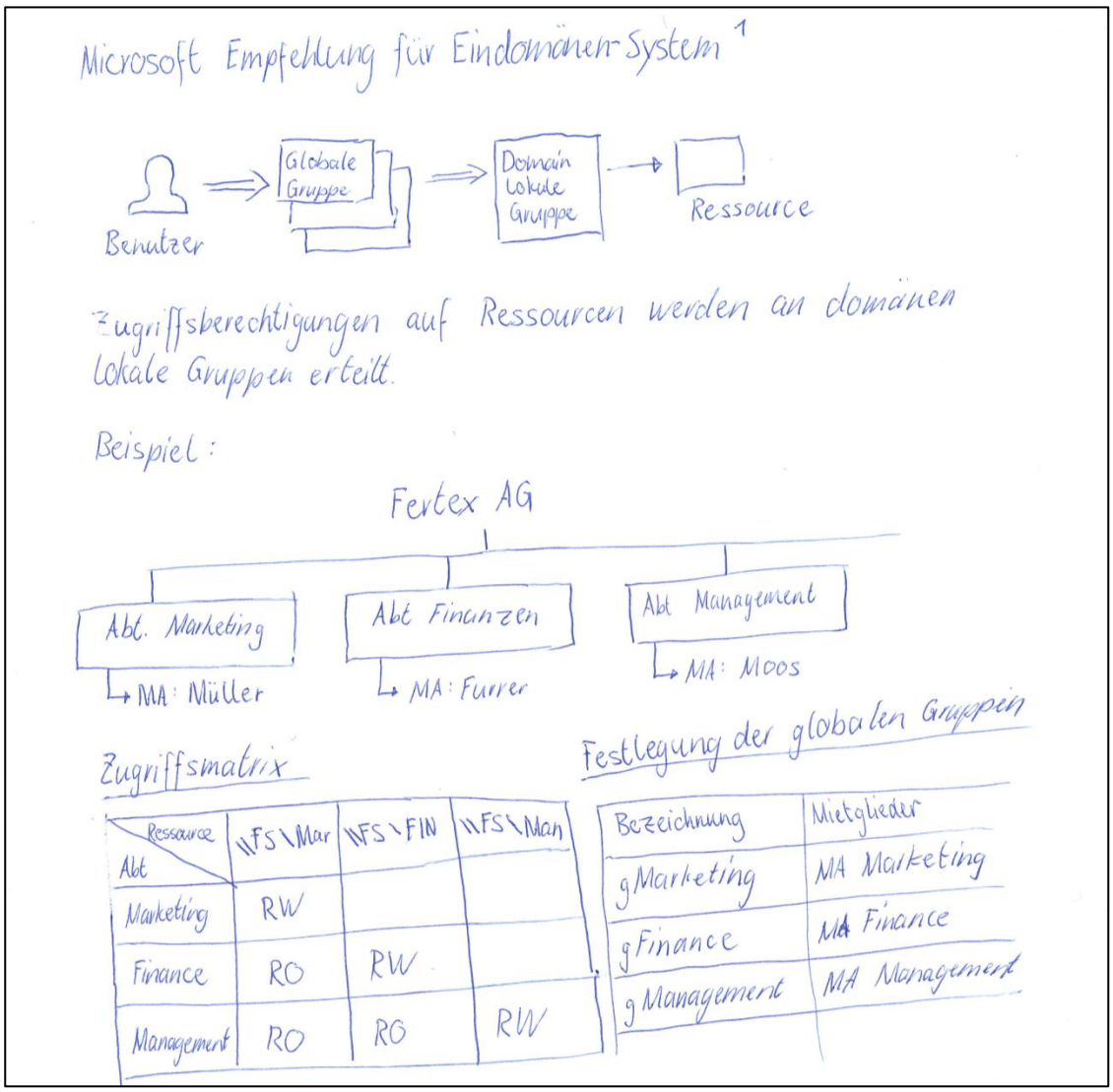


Abbildung 14: Microsoft Empfehlung für Eindomänen-Systeme

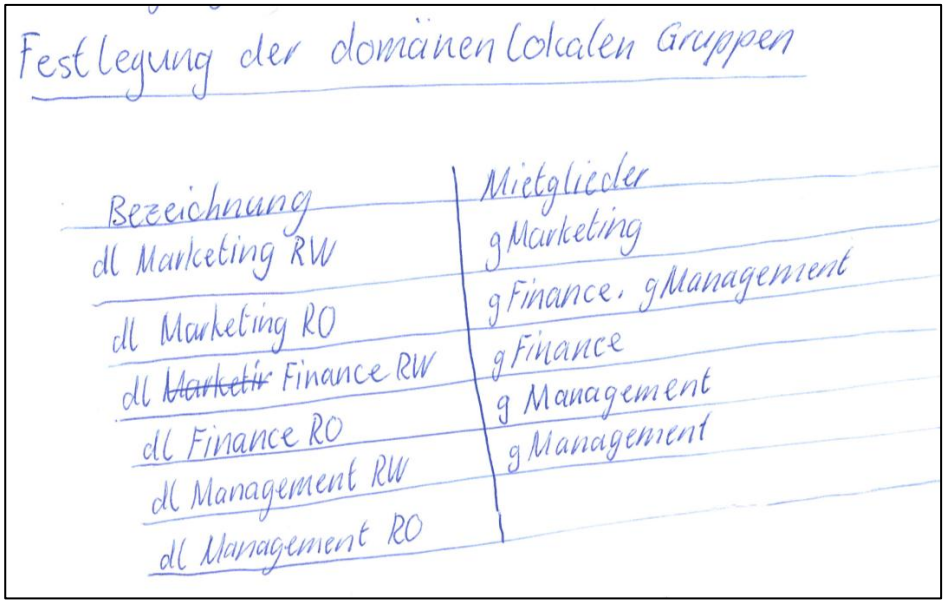


Abbildung 15: Festlegung der domännen lokalen Gruppen

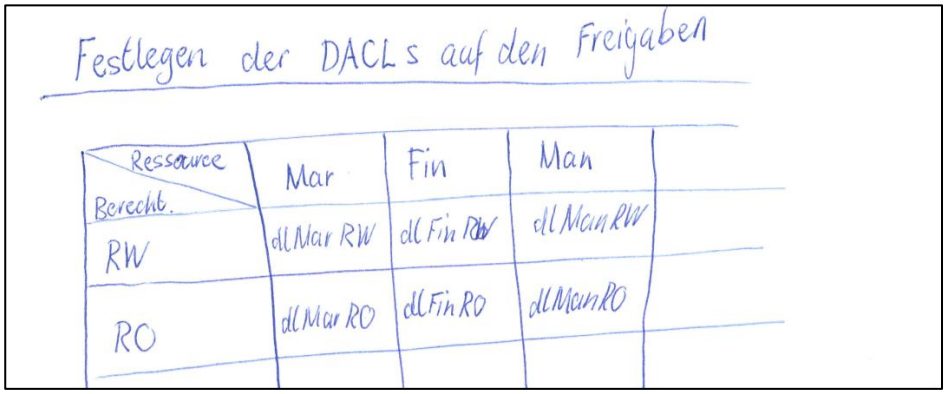


Abbildung 16: Festlegen der DACLs auf den Freigaben

3.5 Zugriffplanung Beispiel

- **Firma:**
  - HUG AG
- **Berechtigungsprinzip**

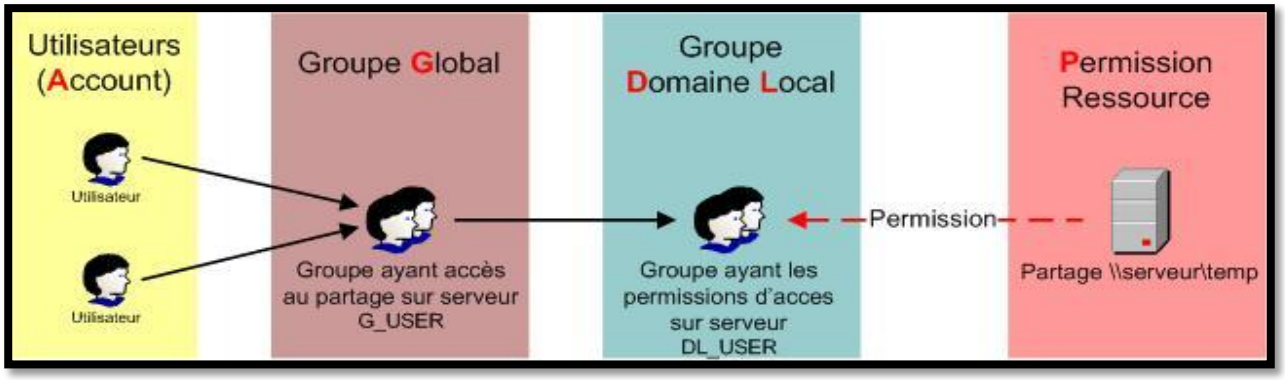


Abbildung 17: AD Berechtigungsprinzip

Abteilungen

Bezeichnung
Management
Einkauf
Verkauf
Logistik
Finance

Zugriffmatrix

	Ressource	**\\FS**			
Abteilung	\\FS\Man	\\FS\Ein	\\FS\Ver	\\FS\Log	\\FS\Fin
Management	RW				
Einkauf	RO	RW	RO		
Verkauf		RO	RW		
Logistik	RO			RW	
Finance		RO	RO		RW

Festlegung der globalen Gruppen

Bezeichnung	**Mitglieder**
gManagement	MA Management
gEinkauf	MA Einkauf
gVerkauf	MA Verkauf
gLogistik	MA Logistik
gFinance	MA Finance

Festlegung der domänen lokalen Gruppen

Bezeichnung	Mitglieder
dlManagementRW	gManagement
dlManagementRO	gEinkauf, gLogistik
dlEinkaufRW	gEinkauf
dlEinkaufRO	gVerkauf, gFinance
dlVerkaufRW	gVerkauf
dlVerkaufRO	gEinkauf, gFinance
dlLogistikRW	gLogistik
dlLogistikRO	
dlFinanceRW	gFinance
dlFinanceRO	

Festlegung der lokalen Gruppen

	Ressource	\\FS\			
Abteilung	\\FS\Man	\\FS\Ein	\\FS\Ver	\\FS\Log	\\FS\Fin
RW	dlManagementRW	dlEinkaufRW	dlVerkaufRW	dlLogistikRW	dlFinanceRW
RO	dlManagementRO	dlEinkaufRO	dlVerkaufRO	-	-

3.6 Gruppenrichtlinien

3.6.1 Allgemeines über Gruppenrichtlinien:

- Der Name kann irreführend sein >> Nach Themen gruppierte Richtlinien.
- Wirken
- Wirken zur Laufzeit als Steuerparameter in der Registry des OS (Teilbaum: Machine / User
- Gruppenrichtlinien wirken auf:
  - Benutzer
  - Computer
- Gruppenrichtlinien werden in Gruppenrichtlinien-Objekte (GPO) im LDAP DIT gespeichert.
- Grupppenrichtlinien-Objekte werden an Container gebunden.

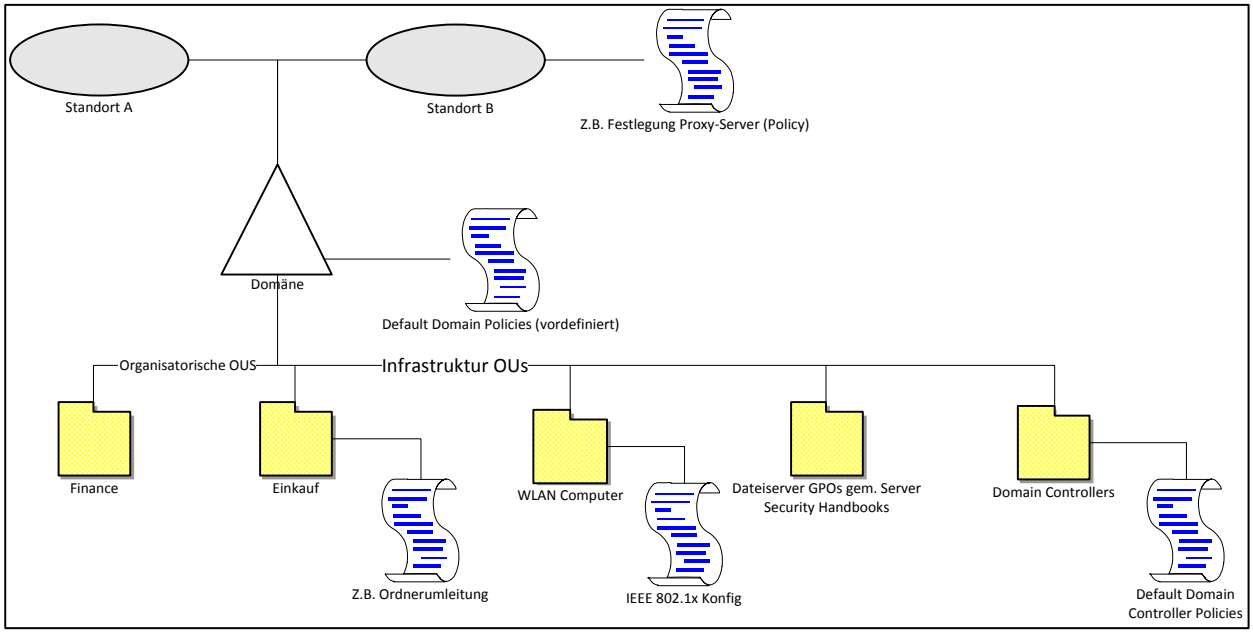


Abbildung 18: Gruppenrichtlinienobjekte

- Dia an einem Container gebundenen GPO wirken auf jene Computer und Benutzer, die sich im betreffenden Container befinden.

3.6.2 Konfigurierbare Einstellungen

- Softwareinstallation / -Verteilung
- Skripte bei:
  - Start / Herunterfahren (Computer)
  - An- / Abmeldung (Benutzer)
- Sicherheitseinstellungen
- Richtlinien für Quality of Service (QoS)
- Administrative Vorlagen (ADM Templates)
- Windows Einstellungen
- Systemsteuerungseinstellungen
- Ordnerumleitung
- Internet Explorer Einstellungen
- Drucker Installation
- Verhindern der Geräte Installation
- Energieverwaltung

4 AD Planung Praxisbeispiel

4.1 Aufgabenstellung

4.1.1 Beschreibung der Situation

Die Firma FERTEX AG ist ein Handelsunternehmung für Futtermittel mit eigener Warenhaltung und Logistik in Sursee (80 Arbeitsplätze) und Aussenstellen in Weinfelden und Lyss (je 30 Arbeitsplätze).

Die FERTEX AG hat die Domäne **<fertex.ch>** im öffentlichen DNS-Namespace bei der Switch registriert und hat vom Provider Cybernet das **IP-Teilnetz <84.10.15.0/ 29>** für die Benutzung in der DMZ in Sursee gemietet.

Das WAN-Interface des Zugangsrouters hat die **IP-Adresse 84.10.1.10/32**.

4.1.2 Netzwerkstruktur

4.1.2.1 Netzwerkstruktur in Sursee

- HSZ mit Active Directory basiertes Netzwerk mit 80 Arbeitsplätzen
- DMZ mit einem BIND-DNS Server und Internet-Dienstserver für http/ HTTPS, SMTP und IMAP.
- WAN: VDSL Anschluss, über ein VDSL-Modem an eine Dreipunkt-Router-Firewall angeschlossen.

Die öffentlichen DNS.-Zonen **<fertex.ch>** und **<0/29.15.10.84.in-addr.arpa>** werden auf dem BIND-NS in der DMZ primär autorisierend gehostet.

Der **zweite autorisierende NS** für diese Zonen befindet sich bei **Cybernet auf**

orca.cybernet.ch.

4.1.2.2 Netzwerkplanung

- Aus Übungsgründen sollen die Masken für die Teilnetze ausserhalb von Oktettgrenzen liegen.
- Im Netzwerkdiagramm sollen auch die erforderlichen Komponenten für die Verbindung der internen RFC 1918 Netzwerke über das Internet und die erforderlichen Protokolle und Tunnel eingezeichnet werden.

4.1.2.3 Netzwerkstruktur in den Aussenstellen in Weinfelden und Lyss

Das Active Directory Netzwerk wird unter Wahrung der Vertraulichkeit und Integrität der Daten und Sicherstellung der Identifikation der Tunnelendpunkte über ein Tunnelprotokoll auf die Aussenstellen ausgedehnt. Benutzer sollen sich am Active Directory auch dann anmelden, wenn die Interstandortverbindung nicht zur Verfügung steht.

Die Aussenstandorte sind mit einem Router-Firewall über eine VDSL-Verbindung mit dem Internet verbunden.

4.1.3 Namensauflösung

- bestmögliche Trennung der intern verwendeten DNS-Zone von vom öffentlichen DNS-Namespace
- bestmögliche Integration des internen DNS in das Active Directory Systgem für Forwad- und Reverse-Lookup Zone
- Weiterleitung der DNS-Queries von internen Clients für externe FQDNs / externe IP-Adressen an einen DNS-Server in der DMZ
- Die öffentliche Forward-Lookup-Zone <fertex.ch> und die öffentliche Reverse-Lookup-Zone für das IP-Teilnetz der DMZ Sursee sollen auf einem DNS-Server in der DMZ Sursee autorisierend gehostet werden
- Für die öffentlichen IP-Teilnetze der Internetzugäne in Weinfelden und Lyss sollen keine Reverse-Lookup-Zonen unterhalten werden, hier genügen die entpsrechenden PTR-Einträge beim Provider.

4.1.3.1 DNS Planung

- Wahl des internen DNS-Domänennamens Server und Zonen, für die diese autorisierend sind.
- Forwarding/ Forwarder – Zuweisung
- Übersichtsdiagramm für Nachrichtenfluss für:
    - Ein Client-PC mach eine FQDN-Anfrage nach einer internen Ressource (z.B. kerberos,
    - bzw. mach eine FQDN-Anfrage für einen externen Host.
    - Am Nachrichtenfluss eintragen, ob Querie rekursiv oder iterativ ist.)
- Lage und Namen der internen und externen Zonendateien einzeichnen.
- Diagramm mit Netz (HSZ, DMZ, WAN) am Stao Sursee:
    - AD integrierte DNS-Server
    - DNS Server in der DMZ
    - FW
- Nachrichtenflüsse
    - <r>
    - <t>
- Vorteile der Lösung mit DNS-Worker-leitung aus Sicher:
    - FW, straffe FW-Regeln für DNS
    - DCs, Entlastung der DCS (müsssen, keine rekursive Queries für Ext, FQDN abarbeiten

4.1.4 Active Directory

- Standorte, Eindomänen Modell, Organisationseinheiten für Benutzer und Computer aus betriebsorganisatorischer Sicht und
- Organisationeinheiten aus Informatik-technischer Sicht
    - (wie im Server Security Handbook in Beispielen gezeigt: **Infrastrukturserver und WLAN-Clients**)
- Visio Diagramm, Trennung der Container-Typen: **Stao, Domäne, OU**
- Sinvolle Anordnung der Container: Stao, Domäne, OU
- Einsatz des OUs für
    - Betriebsorganisatorische Aufteilung
    - Infrastrukturelle Gliederung (für die DCs gibt es bereits eine default OU)
        - Anwendung von Sicherheitsrichtlinien
- Ein Vorteil von AD gegenüber von P2P-Netz:
    - Verbesserung der- und Hostsicherheit mit Gruppenrichtlinien.
- Merkmale von AD Stao

Merkmal	**Bezeichnung**
IP	Besteht aus einem oder mehreren IP-Teilnetzen
AD Domäne	Gehört zu einem oder mehreren Domänen der GS
Repl	Stao-Übergreifende Repl manuell konfigurierbar.

4.2 Planungsarbeiten

4.2.1 Netzwerkplanung (Sursee und Standortverbindungen und Aussenstandorte)

4.2.1.1 IP-Netzwerke

Bezeichnung	Netz-ID
Supernetz für ganzes Intranet	192.168.0.0 /22
Supernetz für Sursee	192.168.0.0 /23
Hauptstandort (Sursee)	192.168.0.0 /24
Nebenstandort (Weinfelden)	192.168.1.0 /25
Nebenstandort (Lyss)	192.168.1.128 /25
DMZ am Standort Sursee	84.10.15.0/ 29

Supernetz: Obwohl es mehrere Teilnetz geben wird, erscheint eine Abdelegierung der reverse Lookup-Zonen im Intranet nicht sonnvoll >> Ganzes Supernetz = eine reverse Lookup-Zone.

4.2.1.2 Netzplanung

Erforderliche Elemente:

- Teilnetze des verteilten Intranets

	Sursee	Lyss	Weinfelden
Supernetz	192.168.0.0 /23		
NW IPadr	192.168.1.0 /24	192.168.1.0 /24	192.168.1.128/25
SN MASK	255.255.254.0	255.255.255.0	255.255.255.128
Kleinste	192.168.0.1	192.168.1.1	192.168.1.129
Grösste IPadr	192.168.0.254	192.168.1.126	192.168.1.254
BC IPadr	192.168.0.255	192.168.1.127	192.168.1.255

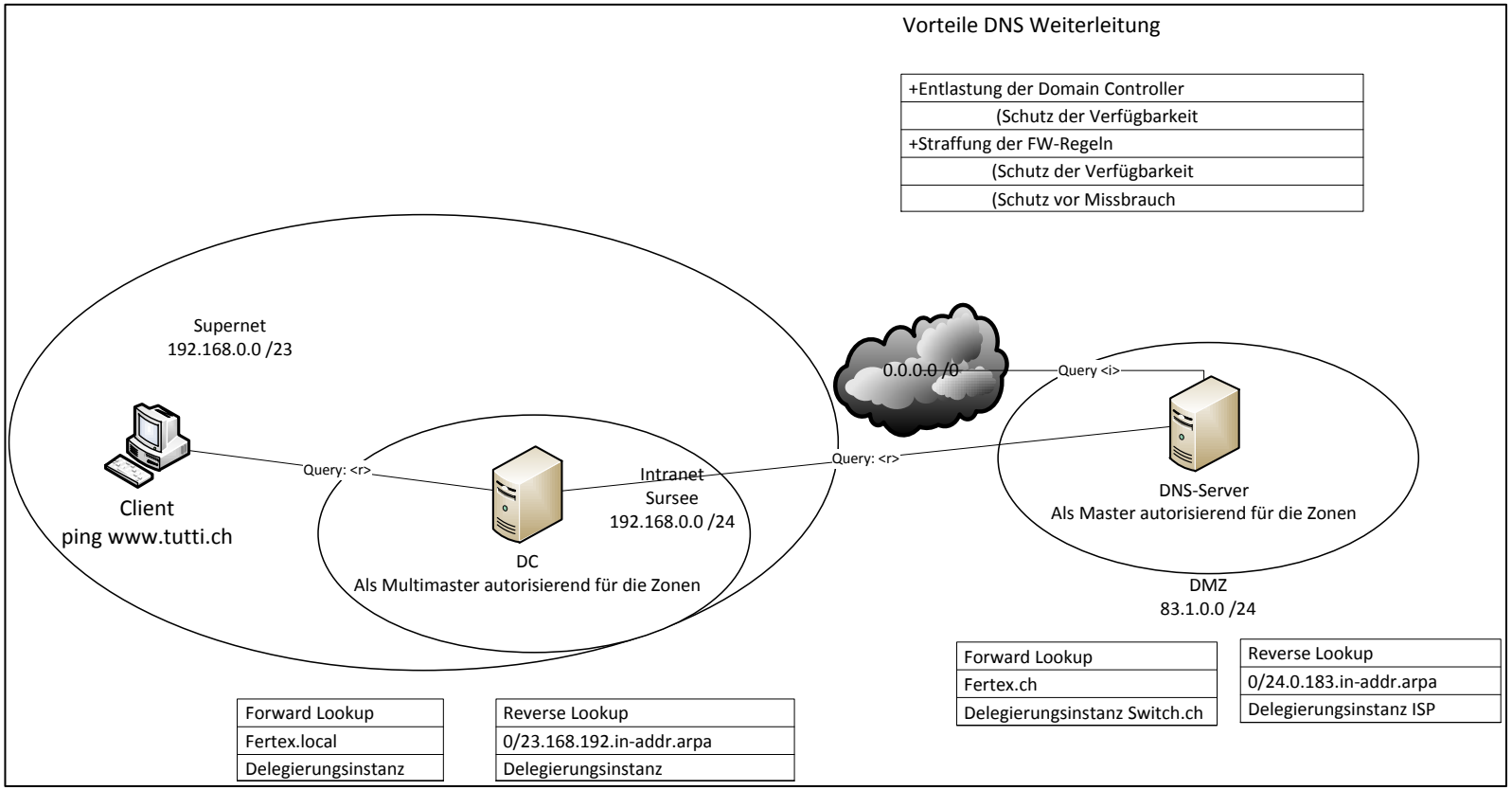
- Zugangsrouter
- Dienste, Protokolle, Tunnels für RFC1918 Net <> 0.0.0.0 /0 <> RFC1918 Netz
- DMZ

4.2.2 DNS-Planung

4.2.2.1 Domänen-Planung

- Intranet: fertex.local
- Extranet: fertex.ch

Bedigungen: max 16 Zeichen wegen NetBIOS und muss eindeutig sein.



4.3 Active Directory-Container-Planung

4.3.1 Active Directory Standorte

Ein Active Directory Standort hat folgende Eigenschaften:

- Ist ein eigenes IP-Teilnetz
- Erfordert manuell konfigurierte Replikation des Acitve Directorys
- Vorhaltung von eigenen Domänencontrollern zur Beschleunigung des Anmeldevorganges und zur Gewährleistung der Verfügbarkeit bei Netzunterbrüchen
- Verbindung der RFC-1918 Standort-IP-Teilnetze durch sichere „IP in IP“-Protokolle

Die Active Directory Standorte liegen auf der Hand: <Sursee>, <Weinfelden> und <Lyss>.

4.3.2 Firmenstruktur bedingte Organisationseinheiten

Grundsätzlich gibt es kein ausschliesslich richtiges Konzept um für eine Firma die Organisationseinheiten zu planen. Es gibt aber viele Gründe, die dafür sprechen, die Firmenorganisation (Abteilungen) in Organisationseinheiten abzubilden.

Demnach werden die, für die für Handelsbetriebe typischen Abteilungen erstellt:

Management, Finanzen, Einkauf, Verkauf, Marketing, Logistik

4.3.3 Technologisch bedingte Organisationseinheiten

Technologisch bedingte Organisationseinheiten dienen dazu, Gruppenrichtlinien zur Verbesserung der Systemsicherheit (MSFT Server Security Handbuch) oder zum Durchsetzen der IEEE 802.1X adaptierten Konfigurationseinstellungen für mobile WLAN-Client im Firmennetz.

Unabhängig davon, ob eine Organisationseinheit Firmenstruktur- oder Technologie-bedingt errichtet wurde, ist Sorge zu tragen, dass in diesen Organisationseinheiten dann auch tatsächlich die entsprechenden Computer und/ oder Benutzer enthalten sind. Andernfalls bleiben die an die Organisationseinheiten gebundenen Gruppenrichtlinien-Objekte ohne Wirkung.

4.4 Sicherheitsgruppenrichtlinienplanung für Ressource-Zugriffsplanung

Im Eindomänenmodell sind dazu die beiden Sicherheitsgruppen-Typen <Globale Gruppe> und <domänenlokale Gruppe> erforderlich.

Globale Gruppen können ineinander verschachtelt werden. Für domänenlokale Gruppen macht dies keinen Sinn, da diese dazu verwendet werden, um den darin enthaltenen Objekten (typsicherweise sind dies globale Gruppen) konkreten Zugriff auf Ressourcen zu erteilen. Demnach sollen in den DACL der Ressourcen lediglich domänenlokale Gruppen eingetragen werden.

Das Verschachtelungsprinzip zur Organisation des Ressourcenzugriffs vom Benutzer bis zu den Ressourcen sieht dann wie folgt aus:

Benutzer -> Globale Gruppe (-> Globale Gruppe) -> domänenlokale Gruppe -> Ressource

4.5 Gruppenrichtlinienplanung für die verschiedenen Container

Nachstehe sind sind einige Beispiele für die Zuweisung von Gruppenrichtlininen aufgeführt:

Name des Gruppenrichtlinien Objektes	GPO wird gebunden an den Container	Wirkt auf die Container-Items	Beabsichtige Wirkung
Proxy_Sursee	Standort: Sursee	Computer am Standort Sursee	Zuweisung eines http-Proxys in der DMZ Sursee
Proxy_Weinfelden	Standort: Weinfelden	Computer am Standort Weinfelden	Zuweisung eines Proxys in der HSZ Weinfelden
Proxy_Lyss	Standort: Lyss	Computer am Standort Lyss	Zuweisung eines Proxy in der HSZ Lyss
IE_Branding	Domäne: Fertex.local	Computer der Domäne fertex.local	Branden des Internet-Explorers auf Firmenlogo
Finance_Folder	OU: Finance	Benutzer in der OU Finance	Zuweisung der Ordner für die Mitarbeiter der Abteilung Finanz
Vergleichbare GPOs für die weiteren Abteilungs-Organisationseinheiten			
Fileservers_Security	OU Fileserver	Fileserver der Domäne fertex.local	Zuweisen von Sicherheitsrichtlinien in Form von GPOs gemäss MSFT Server Security Handbuch
WLAN_IEEE8021X	OU WLANClients	WLAN Clients am Standort Sursee (Fuhrhof: Hubstapler und andere mobile Clients)	Durchsetzen der IEEE 802.1X Konfiguration, optimale Sicherheit in Bezug auf die WLAN-Ressourcenverwendung mit Authentifizierung am Active Directory zu erhalten

5 DNS

5.1 Ablauf der Namensauflösung auf dem Client

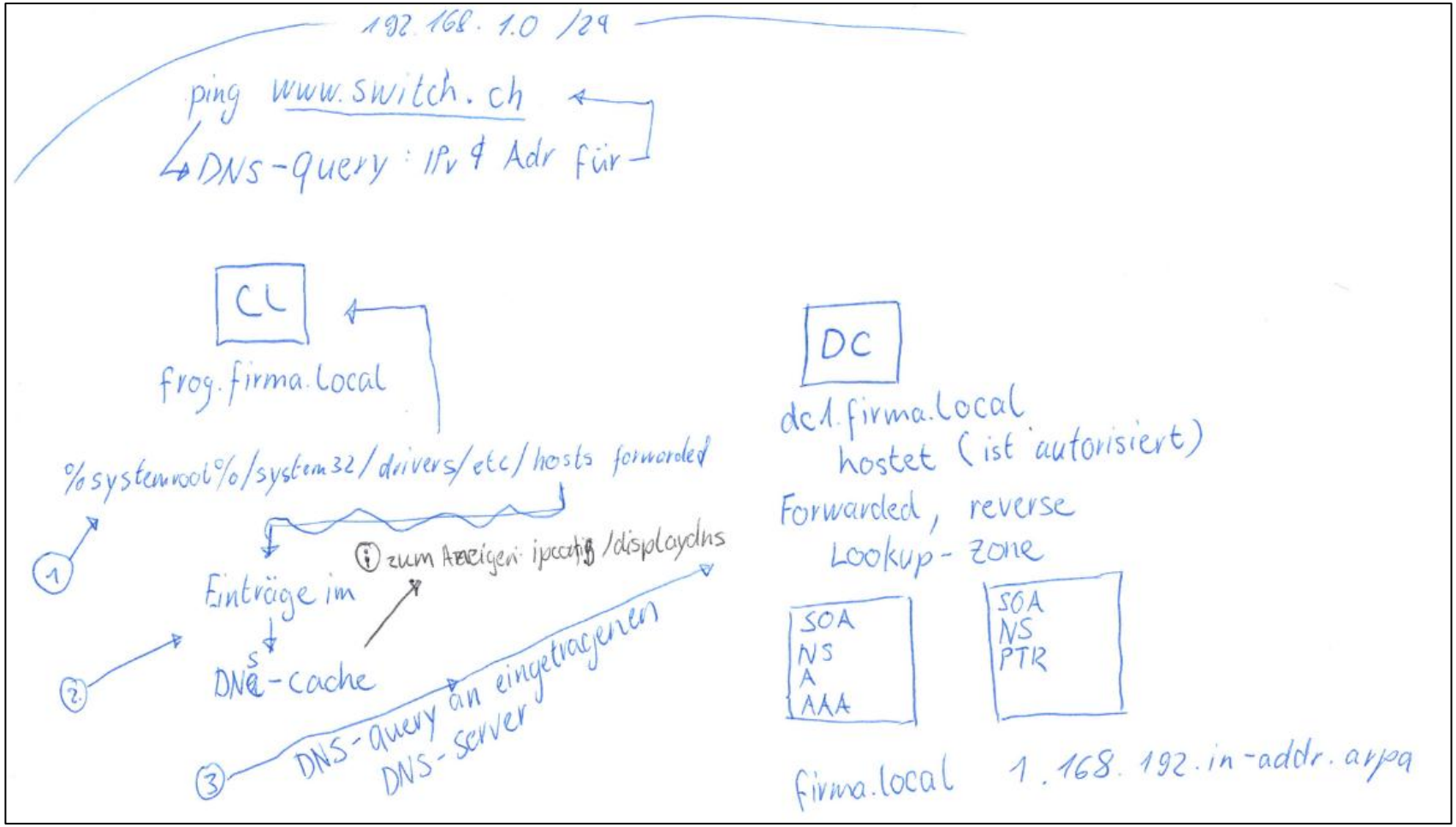


Abbildung 19: Ablauf der Namensauflösung auf dem Client

5.2 Prozess der Namensauflösung

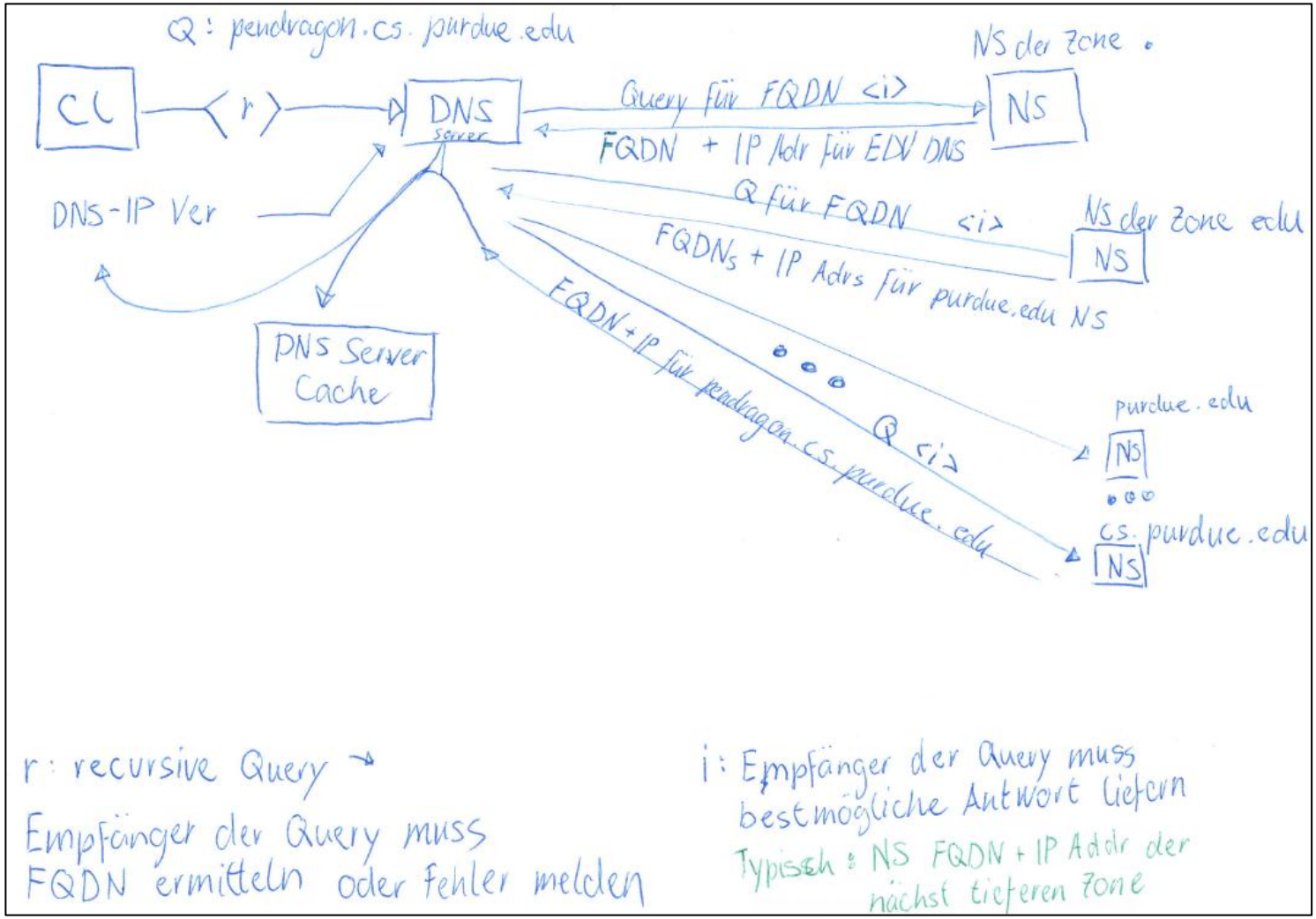


Abbildung 20: Prozess der Namensauflösung

5.3 DNS-Zonen und DNS Domänen

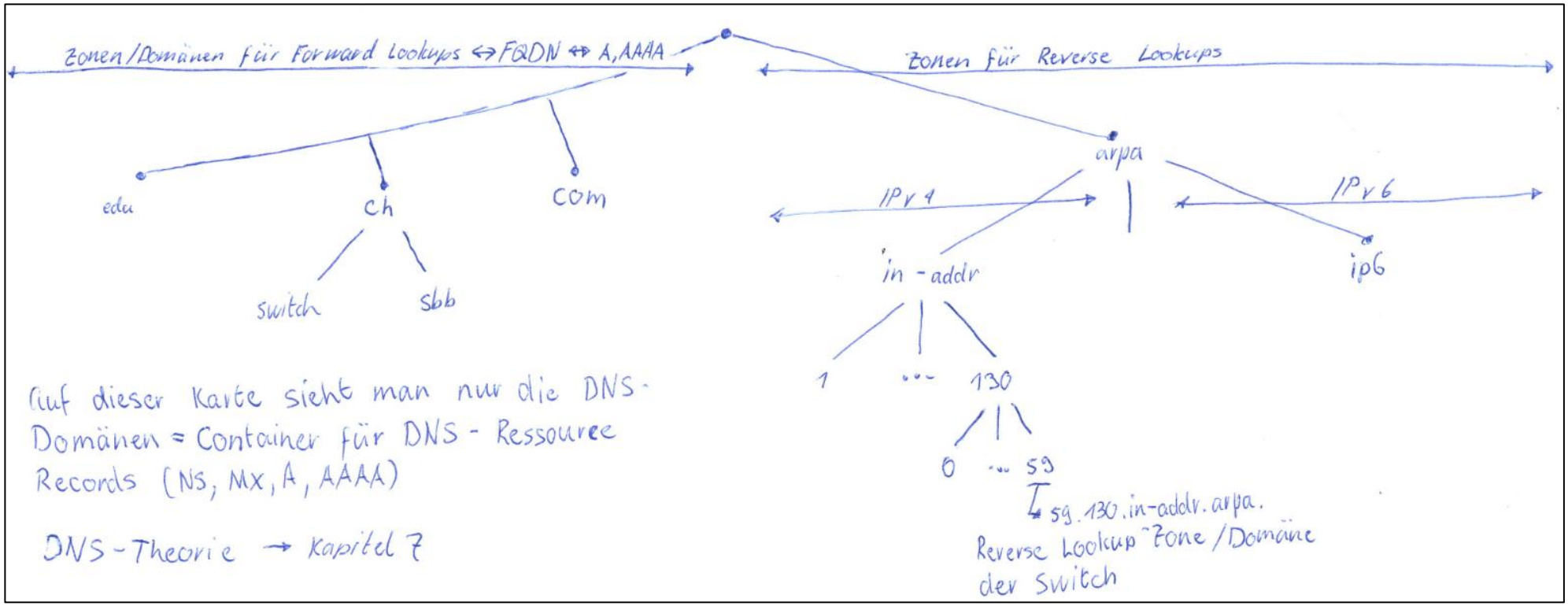


Abbildung 21: DNS-Zonen und DNS Domänen

5.4 Vorteile der Active Direcotry integrierten DNS-Zonen

Die wesentlichen Vorteile einer Active Directory integrierten DNS-zone gegenüber einer Standard DNS-Zone sind:

- Multimaster-Betrieb der DNS-Zonen
- Dynamisches DNS (automatisches Erstellen der A, PTR Records)
- Replikation der DNS Records im Rahmen der AD-Replikation
- Einspeicherung der DNS-Record in der AD-Anwendungspartition

5.5 Ablauf von DDNS in einer Windows System-Umgebung

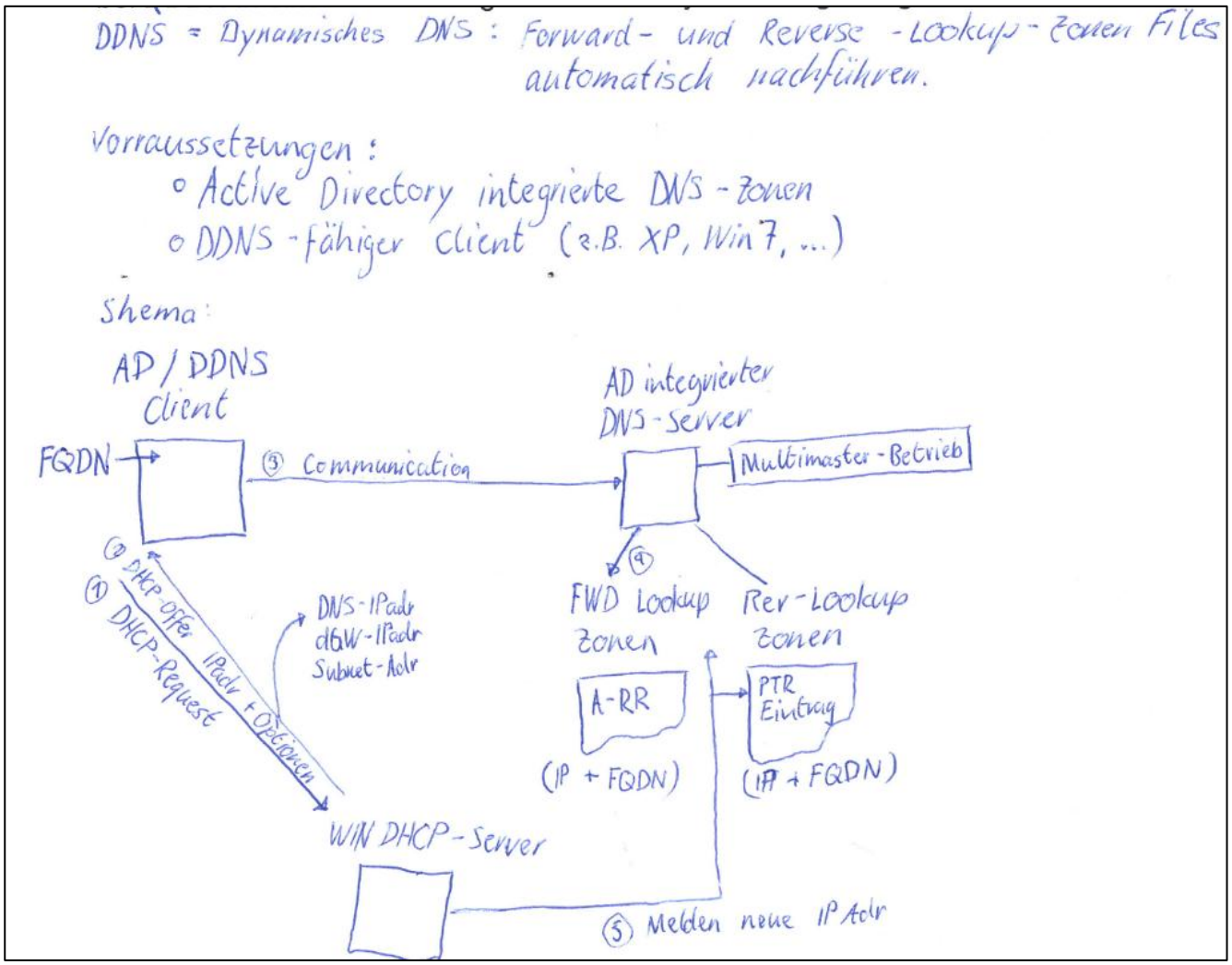


Abbildung 22: Ablauf DDNS in einer Windows System-Umgebung

5.6 Resource-Record Types

RR-Types	Beschreibung	Forward (f) oder Reverse-Lookup (R) Zone
A, AAA	Host-Eintrag	f
MX	Mail-Server	f
SRV	Active Directory Service Komponenten: • LDAP-Server • Global Catalog-Server • Kerberos Server	f
PTR	IPAdr => FQDN	R
SOA	Start of Authority Admin Angaben zur Zonendatei	f, R
NS	Eintrag zur Aufführung eines Nameservers	f, R

5.7 Zonendelegierung, Glue Records

- DNS Zone:
  - Ausschnitt aus dem DNS-Domänen-Baum der einer gemeinsamen Verwaltung untersteht
  - Alle Ressource Records der gleichen Zone werden in einem Zonenfile gespeichert.
- Zonen-Delegierung:
  - Abtreten der Verantwortung für einen Teilbaum an neue Admins
    - RR für die Zonen-Delegierung in der delegierenden Zone

5.8 Beispiel für eine Zonendelegierung

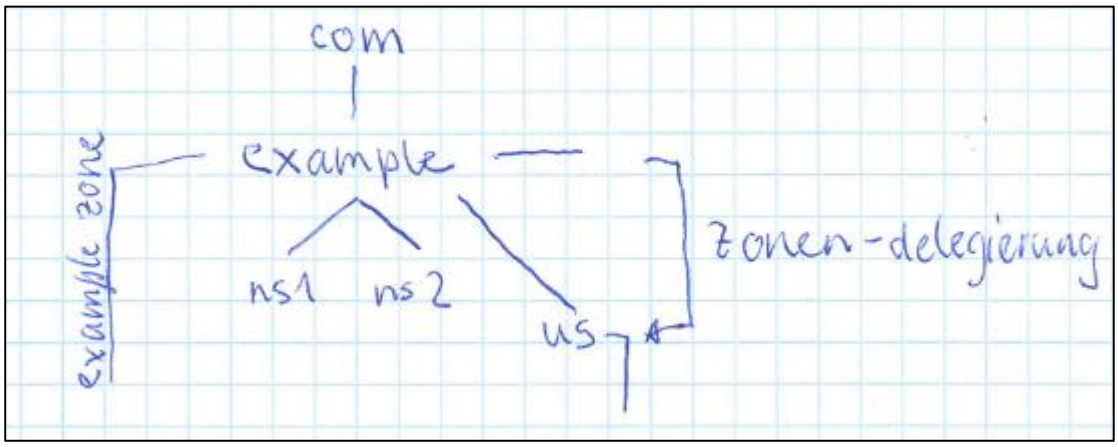


Abbildung 23: Beispiel für eine Zonendelegierung

Vorteile:

- Aufteilung der Administrationsarbeiten
- Erhalt der Performance der DNS-Server

5.9 Aufbau der Zonendatei der delegierenden Zone

Abbildung 24: Aufbau der Zonendatei der delegierenden Zone

5.10 Beispiel Zonendatei „example.com“

```
$ORIGIN example.com.     ; designates the start of this zone file in the namespace
$TTL 1h                  ; default expiration time of all resource records without their own TTL value
example.com.  IN  SOA  ns.example.com. username.example.com. (
              2007120710 ; serial number of this zone file
              1d         ; slave refresh (1 day)
              2h         ; slave retry time in case of a problem (2 hours)
              4w         ; slave expiration time (4 weeks)
              1h         ; maximum caching time in case of failed lookups (1 hour)
              )
example.com.  NS    ns                    ; ns.example.com is a nameserver for example.com
example.com.  NS    ns.somewhere.example. ; ns.somewhere.example is a backup nameserver for example.com
example.com.  MX    10 mail.example.com.  ; mail.example.com is the mailserver for example.com
@             MX    20 mail2.example.com. ; equivalent to above line, "@" represents zone origin
@             MX    50 mail3              ; equivalent to above line, but using a relative host name
example.com.  A     192.0.2.1             ; IPv4 address for example.com
              AAAA  2001:db8:10::1        ; IPv6 address for example.com
ns            A     192.0.2.2             ; IPv4 address for ns.example.com
              AAAA  2001:db8:10::2        ; IPv6 address for ns.example.com
www           CNAME example.com.          ; www.example.com is an alias for example.com
wwwtest       CNAME www                   ; wwwtest.example.com is another alias for www.example.com
mail          A     192.0.2.3             ; IPv4 address for mail.example.com,
                                          ;  any MX record host must be an address record
                                          ; as explained in RFC 2181 (section 10.3)
mail2         A     192.0.2.4             ; IPv4 address for mail2.example.com
mail3         A     192.0.2.5             ; IPv4 address for mail3.example.com
```

Abbildung 25: Beispiel Zonendatei "example.com“

5.11 Beispiel Reverse Zonendatei „23.168.192.IN-ADDR.ARPA.“

IP address =192.168.23.17

Class C base = 192.168.23 ; omits the host address = 17

Reversed Class C base = 23.168.192

Added to IN-ADDR.ARPA domain = 23.168.192.IN-ADDR.ARPA

```
$TTL 2d  ; 172800 seconds
$ORIGIN 23.168.192.IN-ADDR.ARPA.
@              IN      SOA   ns1.example.com. hostmaster.example.com. (
                                2003080800 ; serial number
                                3h         ; refresh
                                15m        ; update retry
                                3w         ; expiry
                                3h         ; minimum
                                )
               IN      NS      ns1.example.com.
               IN      NS      ns2.example.com.
1              IN      PTR     www.example.com. ; qualified name
2              IN      PTR     joe.example.com.
.....
17             IN      PTR     bill.example.com.
.....
74             IN      PTR     fred.example.com.
....
```

Abbildung 26: Beipsiel Reverse Lookup Zone file

5.12 DNS-Zonen und zuständige NS für klassisches DNS

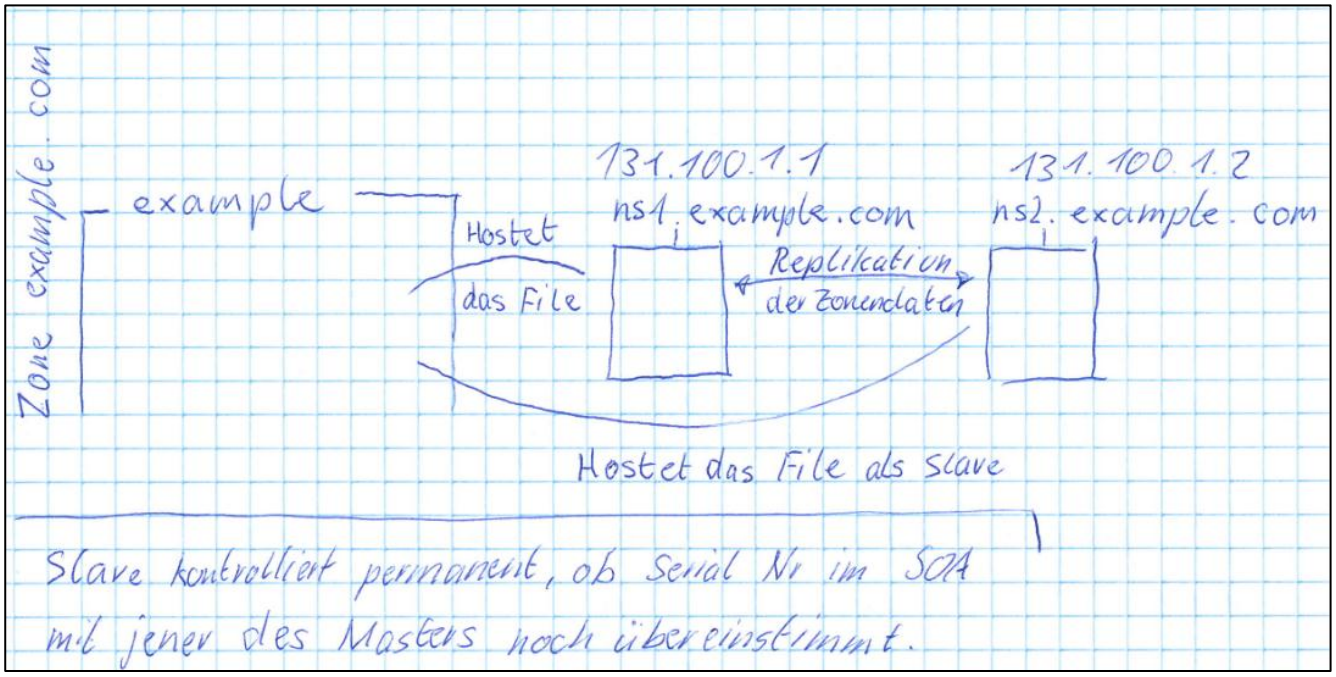


Abbildung 27: DNS-Zonen und zuständige NS für klassisches DNS

5.13 DNS Forwarding

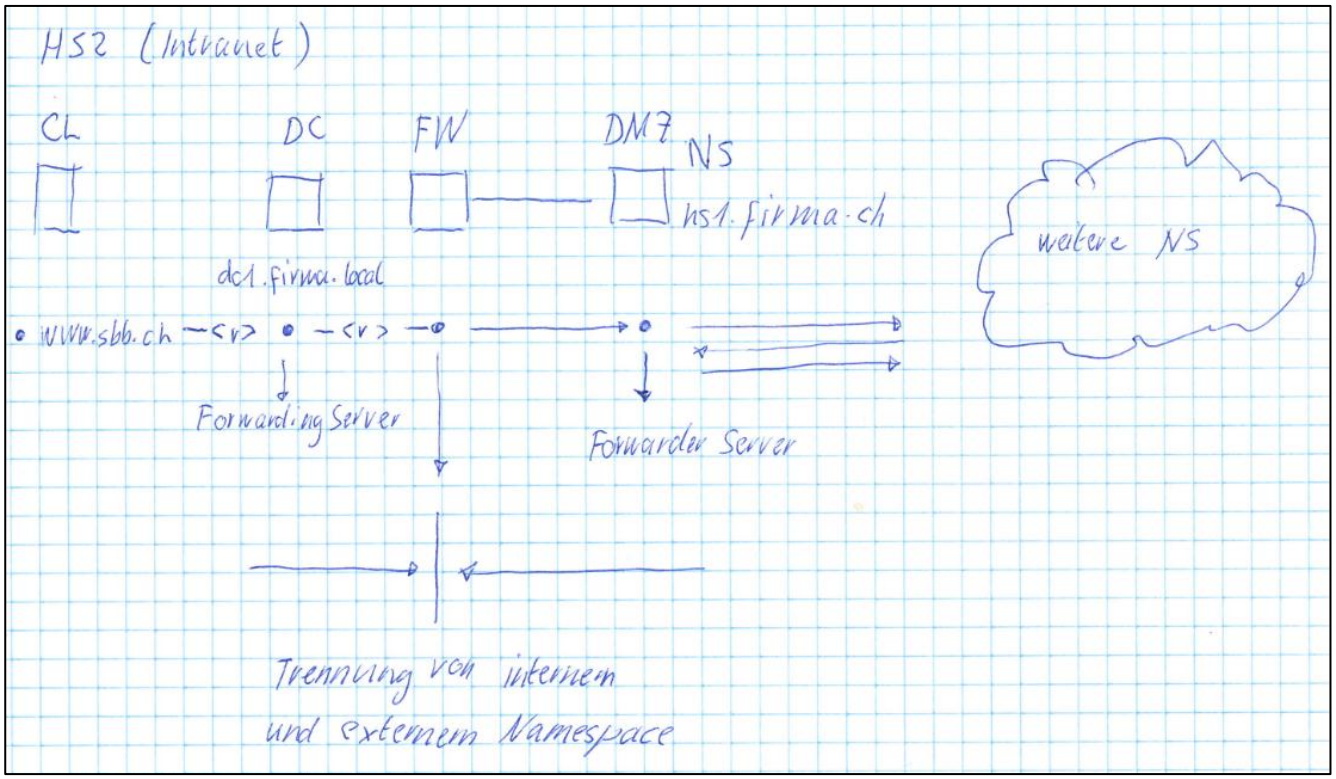


Abbildung 28: DNS Forwarding

5.14 internes und externes DNS mit Zonendelegierung

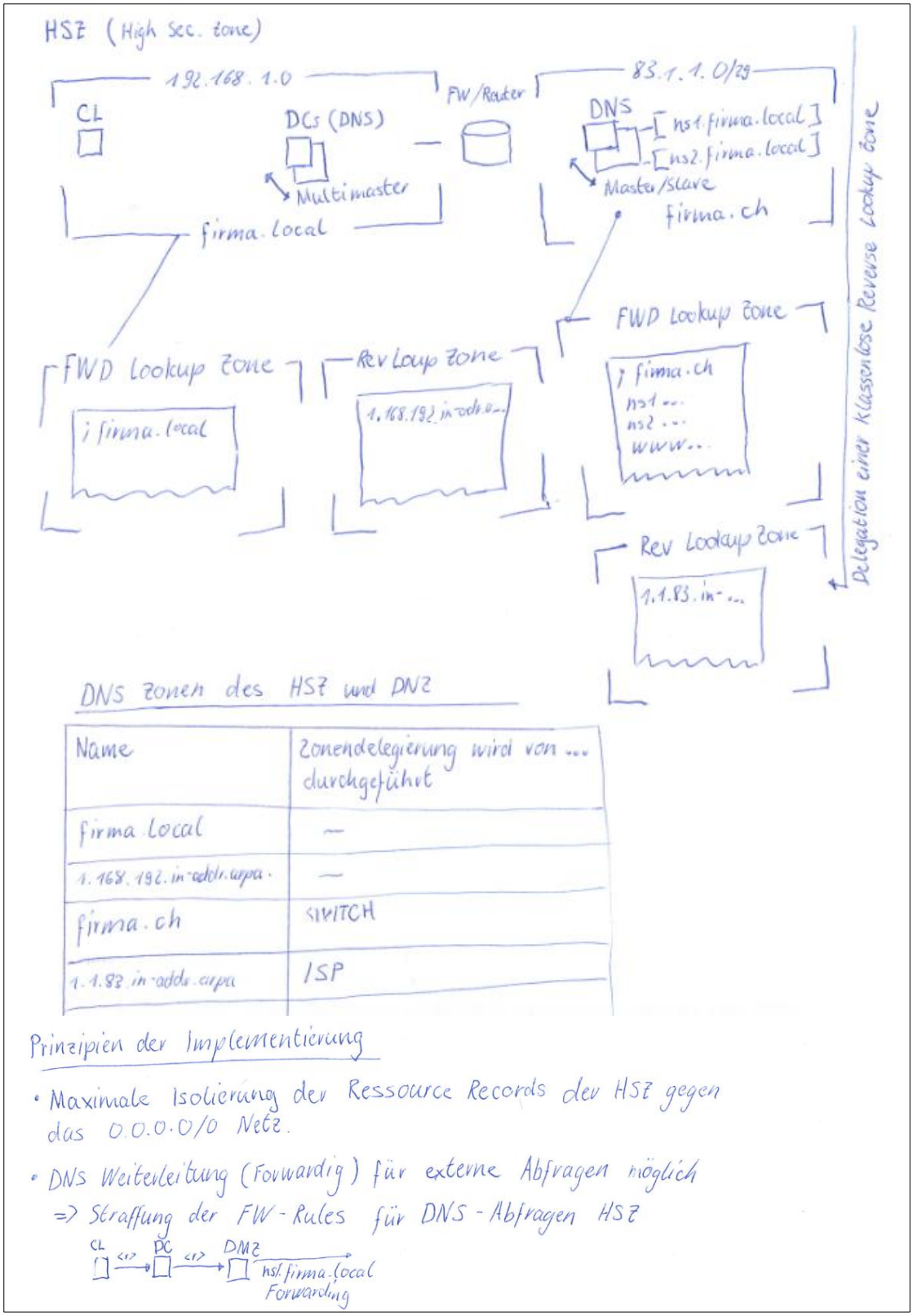


Abbildung 29: Internes und externes DNS mit Zonendelegierung

6 Kerberos V5

Das standardmässig verwendete Authentifizierungsprotokoll von Windows 2000, Windows Server 2003 und Windows XP ist Kerberos. Ältere Betriebssysteme unterstützen Kerberos nicht. Die Implementierung von Kerberos in Windows 2000 ist übereinstimmend mit dem RFC 1510 und kann mit anderen Kerberos V5 Domänen, die ihrerseits gemäss RFC 1510 implementiert sind, kooperieren.

6.1 Wichtige Merkmale von Kerberos V5

Gegenseitige Authentifizierung (im Gegensatz zu PPP CHAP)

Kerberos erlaubt es dem Clienten, den Server zu identifizieren, und erlaubt es, dass Server sich gegenseitig identifizieren können. Die Identifikation des Clienten an einem Server ist natürlich weiterhin auch möglich.

Sichere Übertragung der Authentifizierungsdaten über das Netzwerk

Kerberos Mitteilungen sind mit einer Reihe von Verschlüsselungs-Schlüsseln verschlüsselt. Damit soll sichergestellt werden, dass niemand sich mit einem fremden Client-Ticket oder mit anderen Daten eine Kerberos Mitteilung ausspähen oder beeinflussen kann.

Wie bei den bekannten Authentifizierungsverfahren CHAP, MS-CHAP, MS-CHAPv2 und den EAPs (PEAP, EAP-MD5 CHAP, EAP-TLS), die vornehmlich über PPP, PPPoE, PPPoATM oder mit der Port Authentifizierung IEEE 802.1X gegen Radius-Server eingesetzt werden, gilt das Prinzip:

Das Passwort wird niemals übertragen

(eine gute Beschreibung der oben erwähnten Authentifizierungsverfahren findet man z.B. im TCP/IP-Buch)

Single-Sign On

Innerhalb eines Active Directory Forest (Active Directory Gesamtstruktur , vergl. AD Buch Seite 63) kann ein Benutzer nach erfolgter Authentifzierung bei seiner Stammdomäne auf Ressourcen in anderen Domänen zugreifen (für die er die entsprechende Berechtigung hat), ohne sich bei der jeweiligen Domäne erneut authentifizieren zu müssen.

Der Begriff „Single Sing On“ wird bekanntlich auch in anderer Weise, nämlich in dem Sinne, dass gewisse Applikationen den Zugriff auf dem vom Active Directory Service Ticket (ST) basieren lassen und keine eigene Authentifizierung durchführen. Das z.B. vom MS SQL Server her bekannt.

Schutz vor Wiederverwendung von gesendeten Authentifzierungsdaten

Kerberos minimiert die Möglichkeiten dafür, dass jemand ein Kerberos Authtentifizierungs-Paket auffangen und wiederverwenden kann. Dies wird dadurch erreicht, dass in die Authentifizierungsdaten ein Zeitstempel eingearbeitet wird.

Der eingearbeitete Zeitstempel vermittelt dadurch Schutz, weil für Berechnen von Schlüsselteilen, die für eine Neuanmeldung erforderlich sind, Zeit benötigt wird und nach dem Verstreichen einer gewissen Zeit die aufgefangenen Authentifizierungsdaten insgesamt nicht mehr verwendet werden können.

Standardmässig müssen für Windows 2000 und Windows 2003 alle Uhren innerhalb einer Bandbreite von fünf Minuten liegen, damit die Kerberos Authentifizierung angewendet werden kann Sonst wertet das Key Distribution Center (KDC) den Authentifizierungsversuch als eine Reply-Attacke mit einem aufgefangen Kerberos Authentifizierungspaket.

In der Schweiz bieten sich als Time-Server die folgenden Hosts an: time.ethz.ch oder swisstime.ethz.ch. Unter Windows 2000 und 2003 Server und XP kann die Zeitsynchronisation mit dem Toll W32time.exe durchgeführt werden.

Delegierte Authentifizierung

Windows Dienste personifiziert Clients wenn diese in ihrem Namen auf Ressourcen zugreifen.

Delegierte Authentifizierung liegt vor, wenn ein Netzwerkdienst die Anforderung eines Benutzers annimmt und aufgrund der vermuteten Identität dieses Benutzers eine neue Verbindung mit einem zweiten Netzwerkdienst initiiert., z.B. eine Datenbank basierte Anwendung und der Benutzerkennung auf die Datenbank selber zugreift.

Delegierte Authentifizierung ist sinnvoll für mehrstufige Anwendungen, die Single Sign-on-Funktionalitäten über mehrere Softwaren und Computer hinweg einsetzen. Domänencontroller sind beispielsweise automatisch für Delegierungszwecke vertraut. Wenn Sie das Verschlüsselnde Dateisystem (Encrypting File System, EFS) auf einem Dateiserver verwenden, muss dieser Server für Delegierungszwecke vertraut sein, um verschlüsselte Dateien im Namen der Benutzer speichern zu können.

Delegierte Authentifizierung erweist sich ausserdem als nützlich für Programme, bei denen die Internetinformationsdienste (Internet Information Services, IIS) die Webbenutzeroberfläche zu einer Datenbank zur Verfügung stellen, die auf einem anderen Computer ausgeführt wird, z. B. Microsoft Outlook® Web Access (OWA) in Microsoft Exchange Server, oder für Seiten zur Unterstützung von Webregistrierungen für Unternehmens-Zertifizierungsstellen, wenn diese auf einem separaten Webserver eingerichtet sind.

Kerberos V5 ist ein Industrie-Standard Protocol

Kerberos V5 ist in einem RFC geregelt und gilt in der IT-Industrie als akzeptierter Standard. Das erleichtert die Interoperabilität der Systeme, z.B. SAMBA gegen Active Directory.

Folge der allgemeinen Einhaltung des Kerberos-Standard ist

Interoperabilität

Von Windows System aus kann Authentifizierung auf UNIX-Realms (Realm ist der von den Kerberos-Entwicklern verwendete Begriff für ein Benutzerverwaltungsgebiet, was in Windows in dieser Beziehung dem Begriff „Domäne“ entspricht.

Ticket caching

Nachdem ein Benutzer vom KDC eine Service Ticket (ST) erhalten hat, wird es im perönlichen Service Ticket Cache gespeichert. Damit reduziert sich die Anzahl erforderlichen KDC-Zugriffe auf den DC. Innerhalb der Lebenszeit des Servide Ticket kann das Client System für den Benutzer das gecachte Service Ticket vorweisen.

Hinweis:

Der Ticket Cache kann mit dem Kommandozeilen-Tool Klist.exe oder dem graphischen Tool Kerbtray.exe angezeigt werden. Diese beiden Tools befinden sich bei den Resource Kit Utilities.

6.2 Die Komponenten von Kerberos V5

Die folgenden vier Komponenten werden für die Authentifizierung zwischen Windows 2000-/ XP – Clients und Windows 2000/ 2003 Domänencontrollern benötigt:

6.2.1 Key distribution center (KDC) – Schlüsselverteilungs-Zentrum

Das ist der Netzwerk-Service, der Benutzer und Computer mit dem Ticket-Granting Ticket und mit dem Service Ticket versorgt. Das KDC führt den Austausch der gemeinsamen Geheimnisse zwischen Benutzer und Server durch, wenn sich ein Benutzer und der Server gegenseitig authentifizieren. Der KDC umfasst zwei Dienstleistungen:

den Authentifizierungs-Service (AS)

den Ticket-Granting-Service (TGS), Ticket-Berechtigungs-Service

Die Nachrichten, die zwischen Anmeldeclient und AS bzw. TGS ausgetauscht werden, sind mit KRB_AS oder KRB_TGS bezeichnet. Diese Bezeichnungen werden von Ethereal verwendet.

Der Authentifizierungs-Service führt für die Benutzerin die anfängliche Authentifizierung an der Domäne durch und rüstet den Benutzer mit einem Ticket **Granting Tickt (TGT)** aus.

Immer, wenn ein Benutzer einen Netzwerk-Service anfordert (z.B. Zugriff auf eine Ordner-Freigabe) muss er dem Ticket-Granting-Service sein Ticket Granting Ticket vorweisen.

Der Ticket Granting Service rüstet dann den User bei Bedarf mit einem Service Ticket für die Authentifizierung beim gewünschten Netzwerk-Service aus. In Windows 2000/ 2003 Domänen läuft der KDC auf allen Domänen-Controllern (vergl. entsprechende _kerberos SRV-Resource Records in der Active Directory integrierten DNS-Foreward Lookup Zone der betreffenden Domäne.

6.2.2 Das Ticket Granting Ticket

Das Ticket Granting Ticket wird dem Benutzer ausgehändigt, wenn er sich an der Domäne anmeldet. Das Ticket Granting Ticket ist zugleich auch ein Service Ticket, aber nur für die Benutzung des KDCs. Wenn immer ein Benutzer ein Service Ticket verlangt, muss er dem KDC sein Ticket Granting Ticket vorweisen, damit der KDC feststellen kann, ob der Benutzer bereits an der Domäne authentifiziert worden ist.

Für die Realisierung von zusätzlicher Sicherheit, kontrolliert der KDC vor jeder Ausstellung eines Service Tickets, ob der Account des Benutzers noch gültig ist. Damit wird verhindert, dass jemand, dessen Account während einer Sitzung deaktiviert worden ist, weiterhin auf Ressourcen im Netzwerk zugreifen kann. Wenn der Account eines Benutzers deaktiviert (oder gar gelöscht) wurde, stellt der KDC keine neuen Service Tickets mehr für diesen Benutzer aus.

6.2.3 Service Ticket

Wird vom Benutzer vorgewiesen, wenn immer er auf ein sicherbares Objekt (Netzwerk-Ressource, für die eine DACL= Discretionary Access Control List existiert) zugreift. Der Benutzer hat das Service Ticket, wie oben beschrieben, durch Präsentieren seines TGT vom KDC erhalten.

Das Service Ticket enthält Informationen über den Service/ oder die Ressource für den das Ticket ausgestellt wurde und über den Benutzer, der das Ticket vorweisen muss.

Diese Information wird verwendet damit der angeforderte Service weiss, dass der Benutzer im Netzwerk authentifiziert worden ist. Im Service Ticket sind die SID des Benutzers sowie die SIDs für jene Gruppen, denen der Benutzer angehört, abgespeichert.

Damit kann der angeforderte Service durch Vergleich mit seiner DACL feststellen, ob der Benutzer für den Zugriff auf da sicherbare Objekt berechtigt ist.

Das Service Ticket ist verschlüsselt. Dies geschieht durch die Aushandlung eines gemeinsamen Session Keys zwischen KDC und Ressourcen-Betriebssystem. Das Service Ticket wird mit dem gemeinsamen Session-Key verschlüsselt. Dies stellt sicher, dass es sich beim Lieferanten der Ressource wirklich noch um den richtigen Computer handelt, denn nur dieser kann die Verschlüsselung des Service Tickets rückgängig machen.

6.2.4 Referral ticket - Empfehlungs- oder Überweisungs-Ticket

Mit diesem Ticket stellt der KDC ein Ticket aus, mit dem ein Benutzer bei eine anderen Domäne empfohlen (referral = Empfehlung) wird. Dieses Ticket wird immer dann ausgestellt, wenn eine Benutzerin auf ein sicherbares Objekt (Ressource) auf einem Computer einer anderen Domäne der Gesamtstruktur zugreifen will.

Dieses referral Ticket dient dann in der anderen Domäne als Ticket Granting Ticket. Dieses Ticket ist mit einem Interdomänenschlüssel veschlüsselt. Dieser Interdomänen-Schlüssel wird bei der Einrichtung der transitiven und beidseitigen Vertrauensstellung zwischen den Domänen der Gesamtstruktur erzeugt.

6.3 Ablauf zum Erwerb eines Ticket Granting Tickets (TGT)

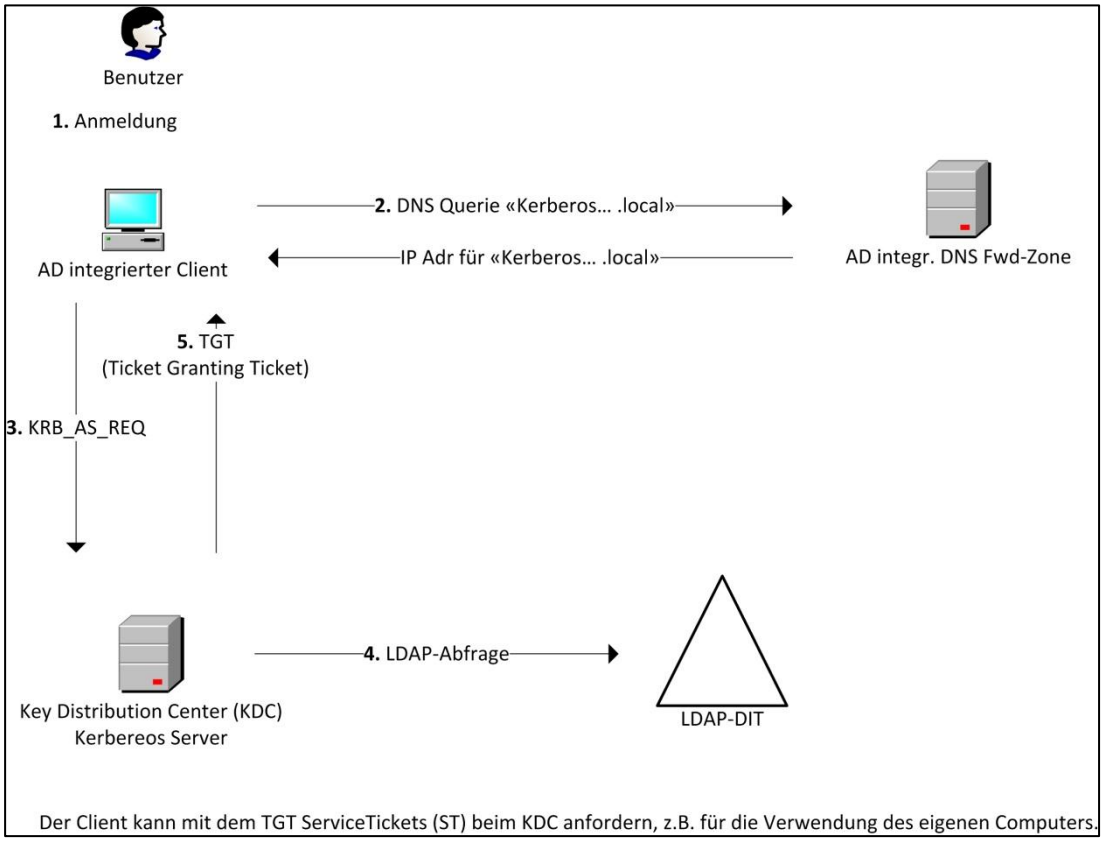


Abbildung 30: Ablauf zum Erwerb eines Ticket Granting Ticket (Shema 1)

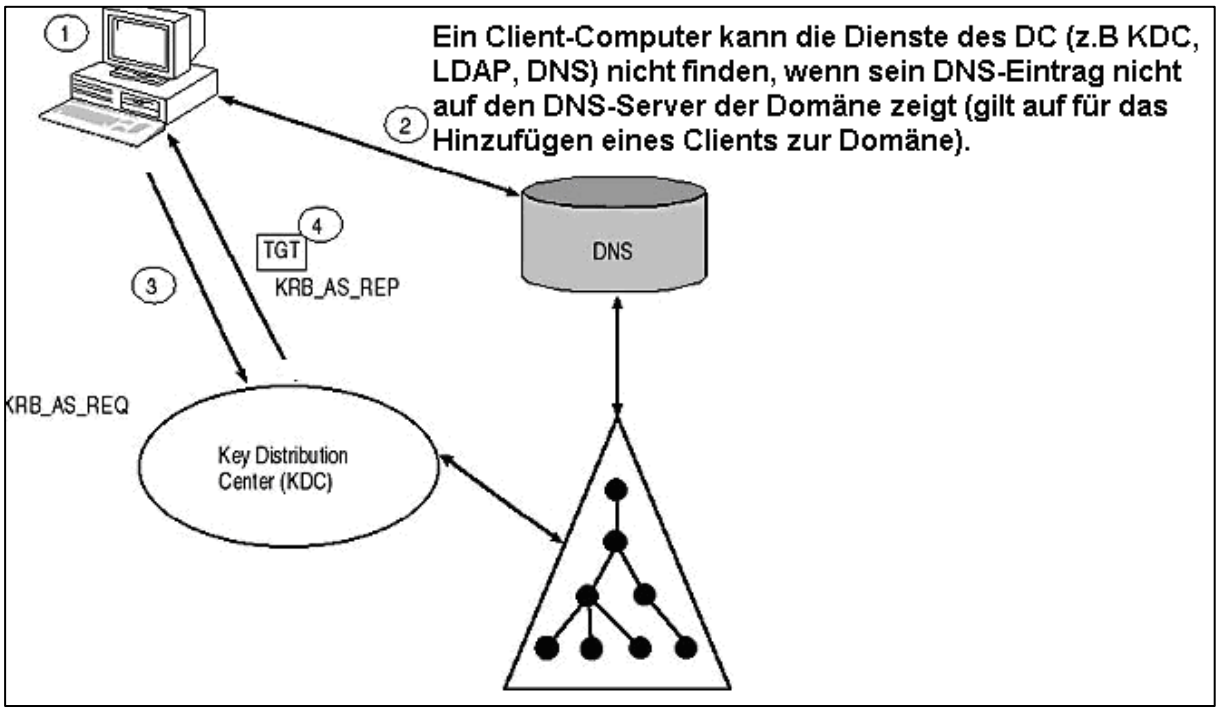


Abbildung 31: Ablauf zum Erwerb eines Ticket Granting Ticket (Shema 2)

Der Client/ Server Authentification Exchange beginnt damit, dass der Benutzer seinen Benutzernamen, das Kennwort und die Domäne in das Windows Logon-Fenster eingibt.

1. Der Client-Computer muss dann die IP-Adresse eines KDCs der Domäne finden. Dafür sendet der DNS-Resolver des Clients eine Anfrage nach einem _kerberos-SRV-Eintrag im Forward-Lookup-Zonenfile des AD-DNS-Servers-
2. Als nächstes sendet der Client-Rechner nun einen Kerberos Authentification Service Request (KRB_AS_REQ –Message) an den Domänenkontroller, dessen Adresse der Client von einem SRV-Eintrag auf dem DNS-Server bezogen hat. Die Konto-Informationen und die aktuelle Rechnerzeit werden mit einem gemeinsamen Schlüssel verschlüsselt.
3. Zum Schluss authentifiziert der Authentifizierungs-Service auf dem DC den Benutzer gegen Einträge im LDAP-DIT. Der KDC generiert dann ein Ticket Granting Ticket (TGT) für den Benutzer. Das TGT wird dem Benutzer dann mit einer Authentification Service Response (KRB_AS_REP) mitgeteilt.

6.4 Vorgang zum Erwerb eines Service Tickets für den Zugriff auf den lokalen Computer

Nachdem der Benutzer mit einem gültigen TGT ausgerüstet worden ist, benötigt er ein Service Ticket für die Benutzung des eigenen Client Computers.

Zweck dieses Vorganges ist es, den Zugriff des lokal angemeldeten Benutzers auf die lokal vorhandenen Ressourcen gemäss ACL zu ermöglichen.

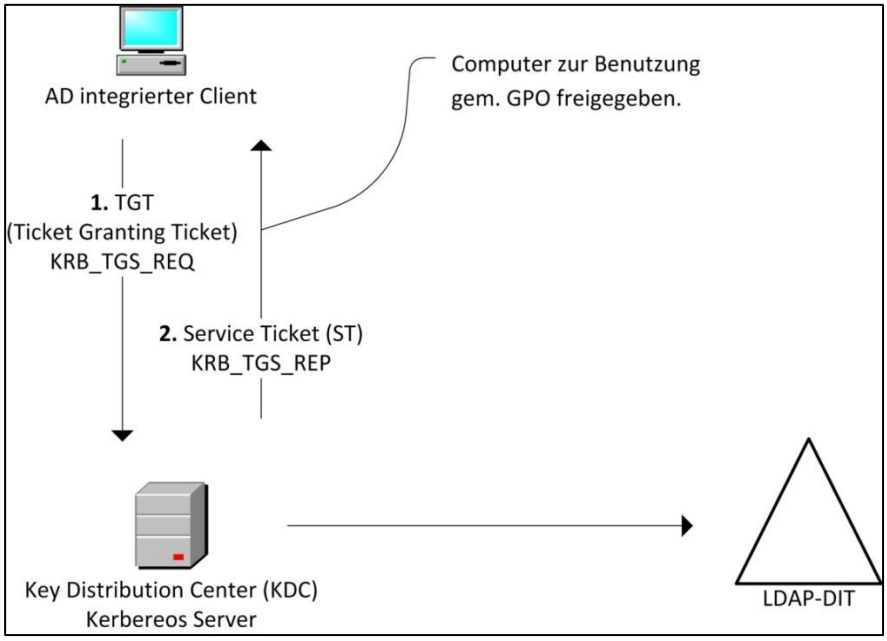


Abbildung 32: Vorgang zum Erwerb eines Service Tickets für den Zugriff auf den lokalen Computer (Schema 1)

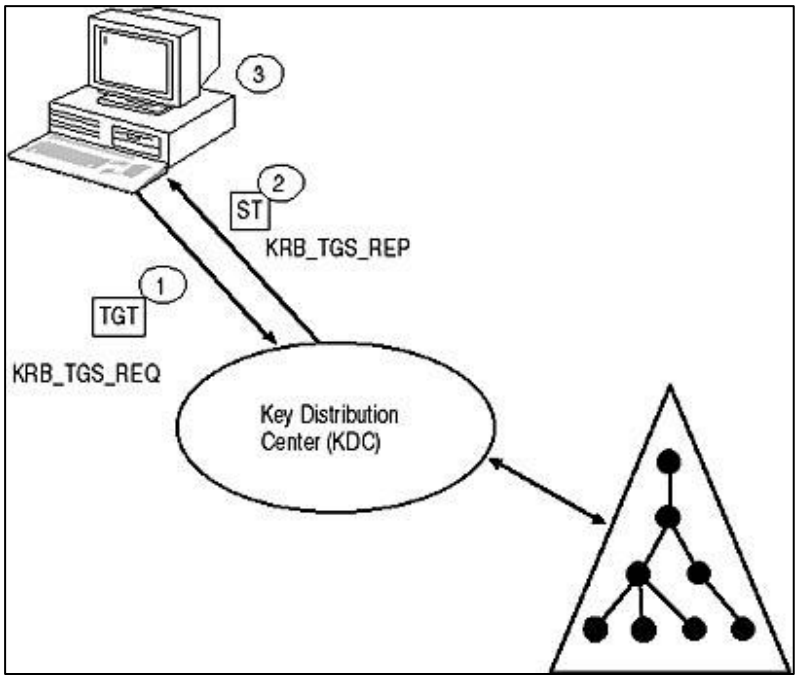


Abbildung 33: Vorgang zum Erwerb eines Service Tickets für den Zugriff auf den lokalen Computer (Schema 2)

Der Vorgang läuft in folgenden Schritten ab:

1. Der Betriebssystem sendet unter der Benutzerkennung des angemeldeten Benutzers ein Ticket Granting Service Anforderung (KRB_TGS_REQ – Nachricht) an den KDC um ein Service Ticket zu erhalten, das es dem an der Domäne angemeldeten Benutzer erlaubt, Ressourcen auf seinem eigenen Client-computer zu verwenden. Diese Nachricht enthält ein Authentifizierungs-merkmal des Benutzers und sein TGT.
2. Der KDC überprüft das Authentifizierungsmerkmal des Benutzers und sein TGT. Wenn beides gültig ist, erstellt der Ticket Granting Service des KDC ein Service Ticket für den Client Computer und sendet dies in einer KRB_TGS_REP) an den Client Computer.
3. Auf dem Client Computer wird das Service Ticket der lokalen Sicherheits Autorität (local Security Autority) präsentiert, die dann ein Access Token für den Benutzer erstellt. Ab diesem Zeitpunkt können lokale Prozesse, die unter der Benutzerkennung des angemeldeten Benutzers laufen, auf die Ressourcen gemäss ACL zugreifen.

6.5 Vorgang zum Erwerb eines Service Tickets für den Netzwerkzugriff

Mit diesem Vorgang wird der Benutzer mit einem Ticket Grantin Ticket ausgerüstet, mit dem er auf Ressourcen im Domänen- oder Gesamtstruktur-weiten Netzwerk gemäss den geltenden ACLs zugreifen kann

Die nachfolgend beschriebenen Schritte sind für den Erwerb eines Service Tickes erforderlich, Der Vorgang läuft für den Benutzer transparent ab. Der genau gleiche Vorgang läuft auch ab, wenn der Benutzer ein Service-Ticket für eine beliebige, andere Ressource im AD anfordert.

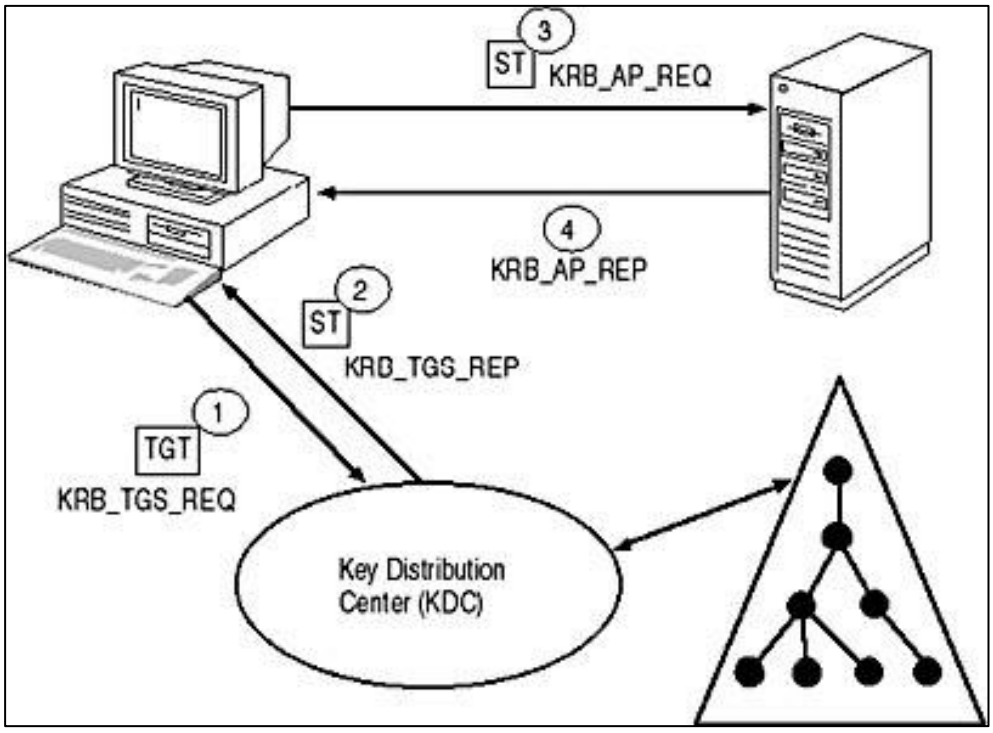


Abbildung 34: Vorgang zum Erwerb eines Service Tickets für den Netzwerkzugriff

1. Unter der Benutzerkennung wird eine Ticket-Granting Service Request (KRB_TGS_REQ - Nachricht) zum KDC um ein Service Ticket für die Benutzung des remote Computers anzufordern. Die KRB_TGS_REQ-Nachricht beinhaltet das TGS und Authentifizierungs-Daten.
2. Der Ticket-Granting Service des KDCs überprüft die Authentifi-zierungs-Daten und das TGT, erstellt ein neues Service Ticket und sendet dieses mit einer Kerberos Ticket-Granting Service Response-Nachricht (KRB_TGS_REP) an den Client-Rechner zurück. Das Service Ticket ist mit dem gemeinsamen Schlüssel des KDCs und dem Anforderungs-Dienst auf dem remote-Computer verschlüsselt.
3. Der Benutzer sendet das Service Ticket und seine Authentifizierungs-Daten an den Ziel-Service auf dem remote Computer. Dies macht er mit einer Kerberos Application Request-Nachricht (KRB_AP_REQ).
4. Der Ziel-Rechner überprüft das Service Ticket mit den Authentifizierungs-Daten, entschlüsselt den mitgelieferten Session Key mit Hilfe des Master Keys, den er zusammen mit dem KDC unterhält. Schliesslich sendet er eine Kerberos Applicaton Response-Nachricht an den Zugriffs-Client zurück.

7 Glossar

Begriff	Bezeichnung
DDNS	Dynamic Domain Name System (ungleich DynDNS)
DIT	Directory Information Tree
DN	Distinguished Name
DynDNS	Dynamic Domain Name System (ungleich DDNS)
PSK	Pre-Shared-Key
RR	Resoure Records

8 Abbildungsverzeichnis

9 Kontakt

Name	Janik von Rotz
E-Mail	contact@janikvonrotz.ch
Website	http://www.janikvonrotz.ch