

# WINDOWS SERVER ADVANCED

AD PIJLERS

# ACTIVE DIRECTORY

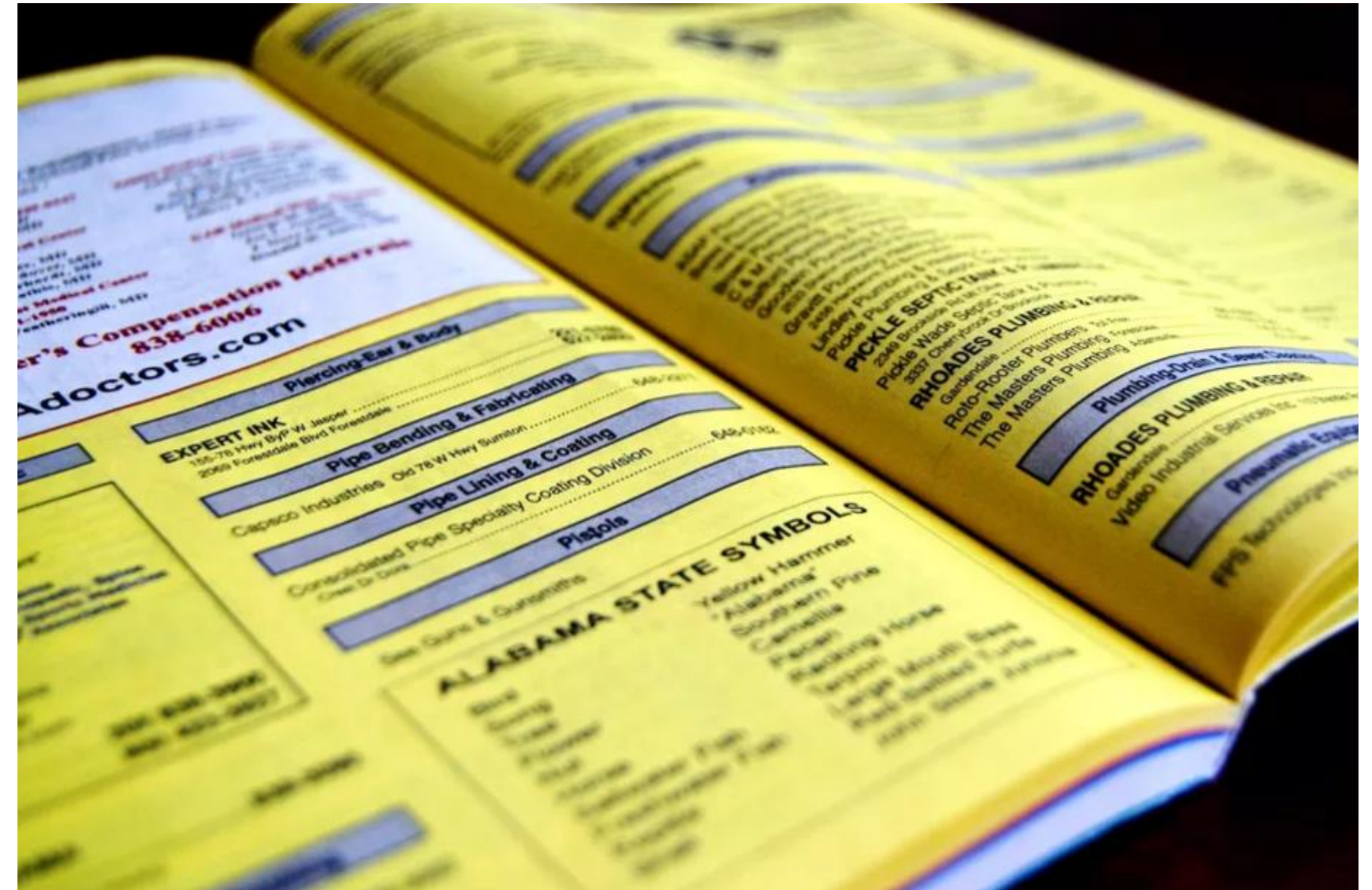
# Active Directory Server Rollen

---

- Active Directory **Domain Services (AD DS)**
  - Binnen deze module verwijst AD hiernaar
- Active Directory **Federation Services**
  - Authenticatie buiten je interne omgeving
- Active Directory **Certificate Services**
  - Opzetten PKI -> authenticeren van users, computers, ...
- Active Directory **Lightweight Directory Services**
  - Kleine broertje/zusje van AD DS
- Active Directory **Rights Management Services**
  - Rechtencontrole op documenten

# Wat is Active Directory

- Directory Service
  - Gebaseerd op X.500 standaard
    - Gegroeid vanuit ervaring telecombedrijven
    - <https://en.wikipedia.org/wiki/X.500>
  - NT Directory Service, nu Active Directory Domain Services (ADDS)
- Een centrale plaats waar je al je gebruikers, computers en andere objecten bewaart en beheert alsook het gedrag van je Windows infrastructuur regelt.
- Access Control Lists
  - Elk object binnen AD heeft een ACL dat de toegang tot dit object regelt!



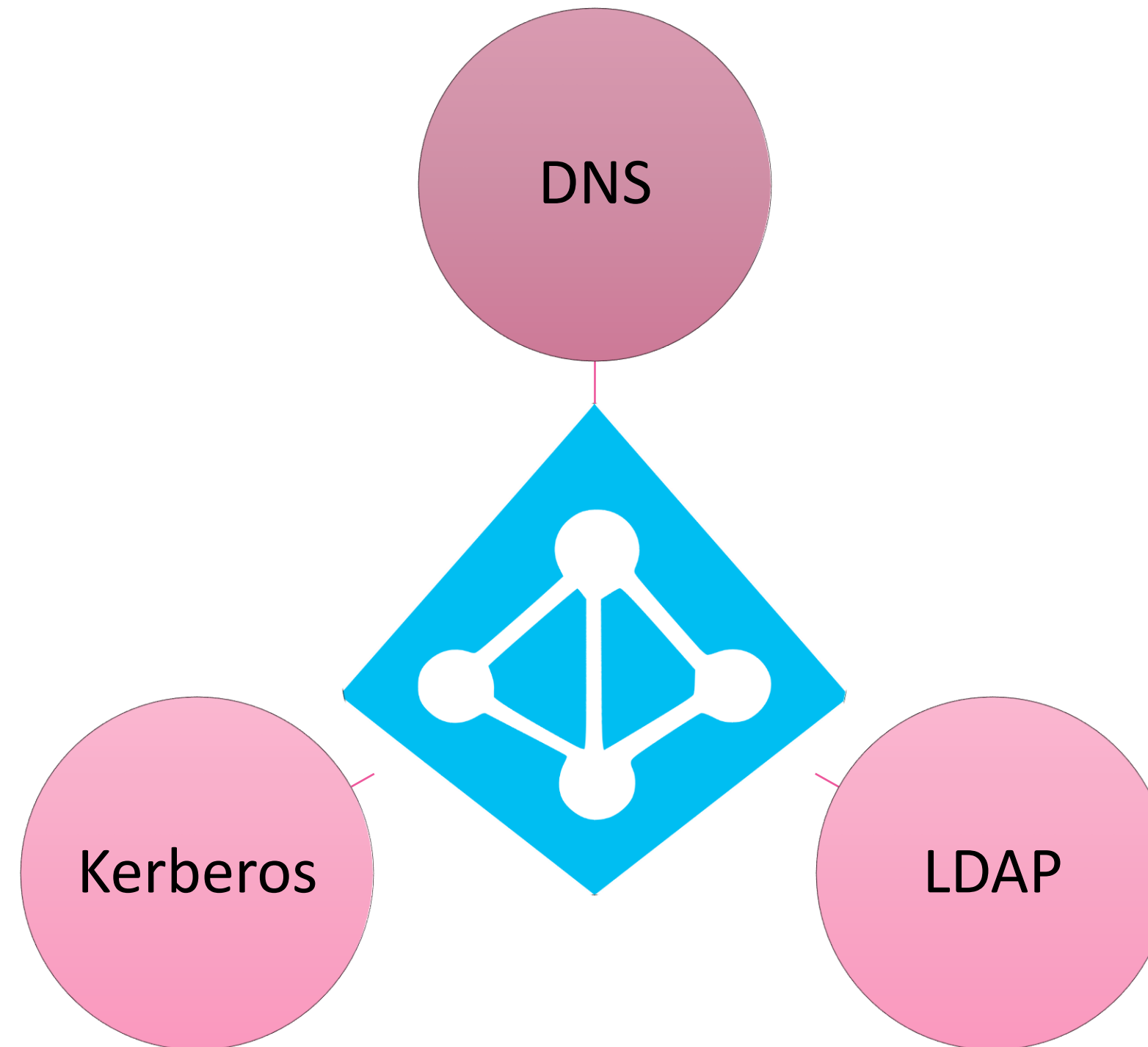
# Waarom gebruiken we AD?

---

- Centraal beheer
- **A**uthenticatie
  - Accounts
  - Paswoorden
- **A**utorisatie
  - Rechtenbeheer (ACL's)
  - Instellingen van servers
  - Instellingen van clients
  - Group Policies
- **A**ccounting
  - Logging
  - Auditing

# Pijlers

---

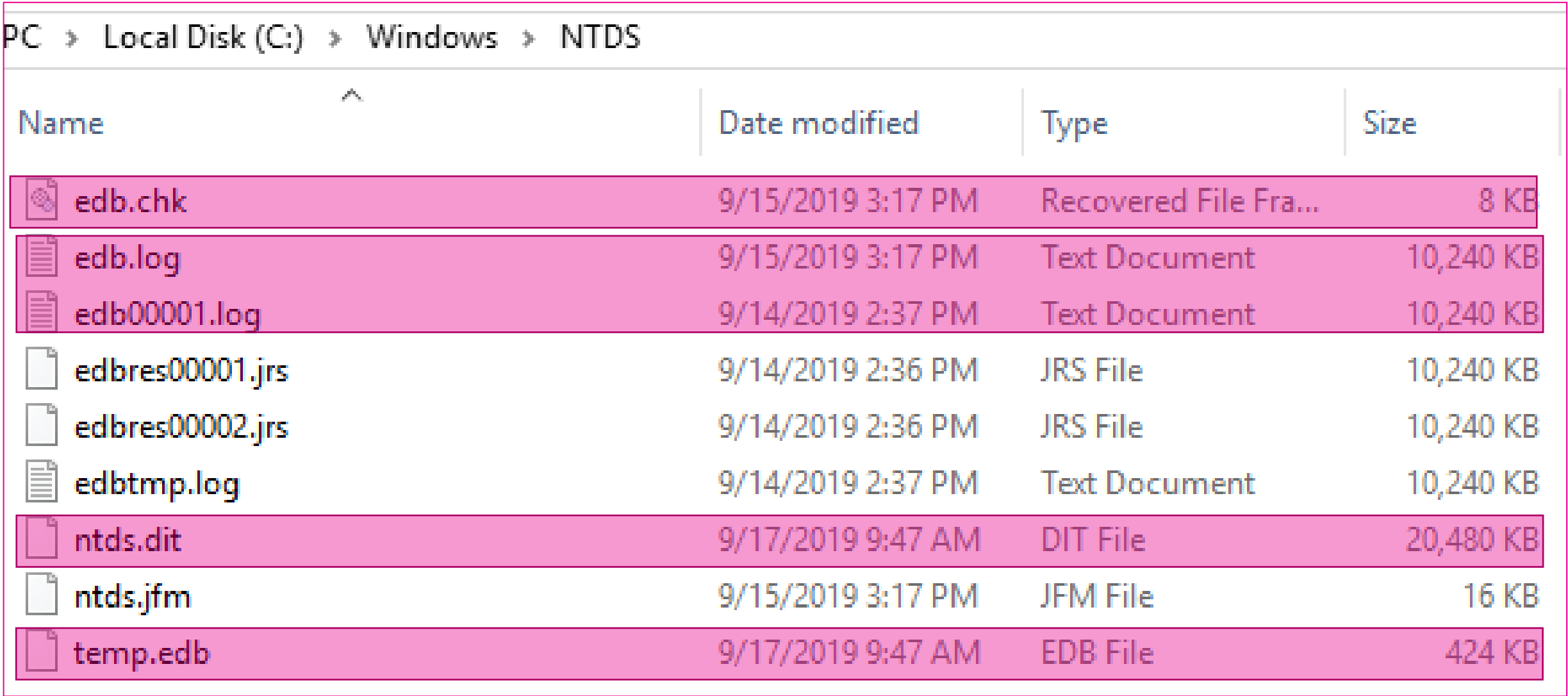


# Welke poorten gebruikt Active Directory

Service Name	UDP	TCP
DNS	53	53
LDAP	(389)	389
LDAP SSL	-	636
Global Catalog LDAP	-	3268
Global Catalog LDAP SSL	-	3269
Kerberos	88	88
Kerberos (kpassword)	464	464
SMB over TCP/IP	(445)	445
NetBIOS Name Service	137	-
NetBIOS Datagram Service	138	-
NetBIOS Session Service	-	139
RPC Endpoint Mapper (EPM)	135	135
RPC Dynamic Ports (DCERPC)	-	49152-65535 (“ephemeral ports”)

# AD DATABASE - FYSIEK

- NTDS.DIT
  - Eigenlijke AD DB
- EDBxxx.LOG
  - Logfiles. Deze bevatten de AD transacties vooraleer ze naar de DB worden weggeschreven
  - Elke logfile <= 10 MB
- EDB.CHK
  - Bijhouden van data transactie *committed* in DB
- TEMP.EDB
  - Data bijhouden tijdens AD onderhoud en grote AD data transacties

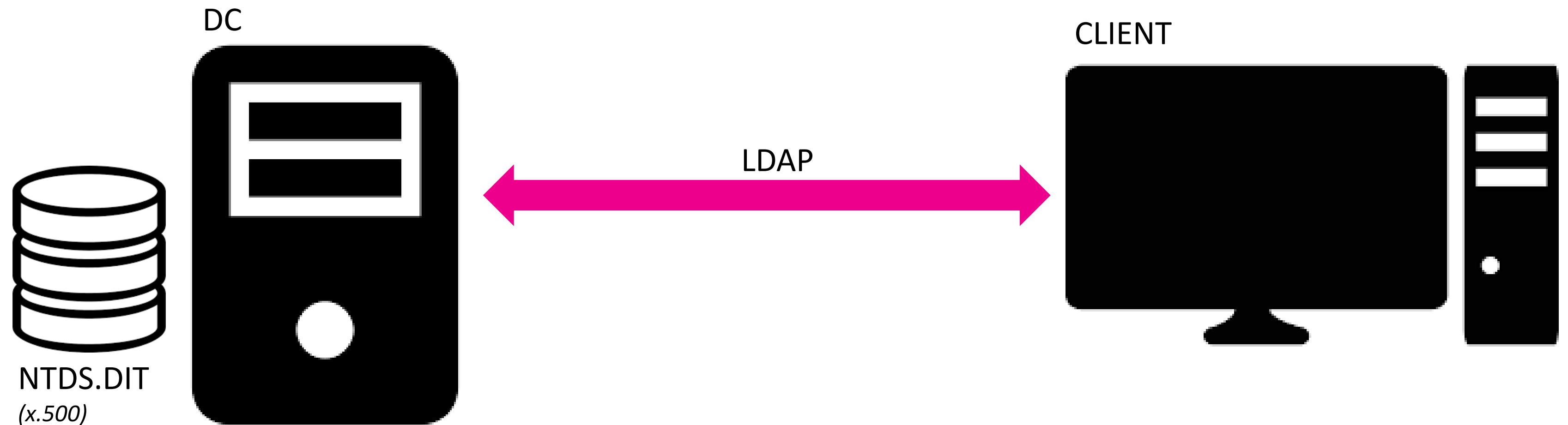


PC > Local Disk (C:) > Windows > NTDS				
Name		Date modified	Type	Size
edb.chk		9/15/2019 3:17 PM	Recovered File Fra...	8 KB
edb.log		9/15/2019 3:17 PM	Text Document	10,240 KB
edb00001.log		9/14/2019 2:37 PM	Text Document	10,240 KB
edbres00001.jrs		9/14/2019 2:36 PM	JRS File	10,240 KB
edbres00002.jrs		9/14/2019 2:36 PM	JRS File	10,240 KB
edbtmp.log		9/14/2019 2:37 PM	Text Document	10,240 KB
ntds.dit		9/17/2019 9:47 AM	DIT File	20,480 KB
ntds.jfm		9/15/2019 3:17 PM	JFM File	16 KB
temp.edb		9/17/2019 9:47 AM	EDB File	424 KB



LDAP

# Lightweight Directory Access Protocol: NUT?

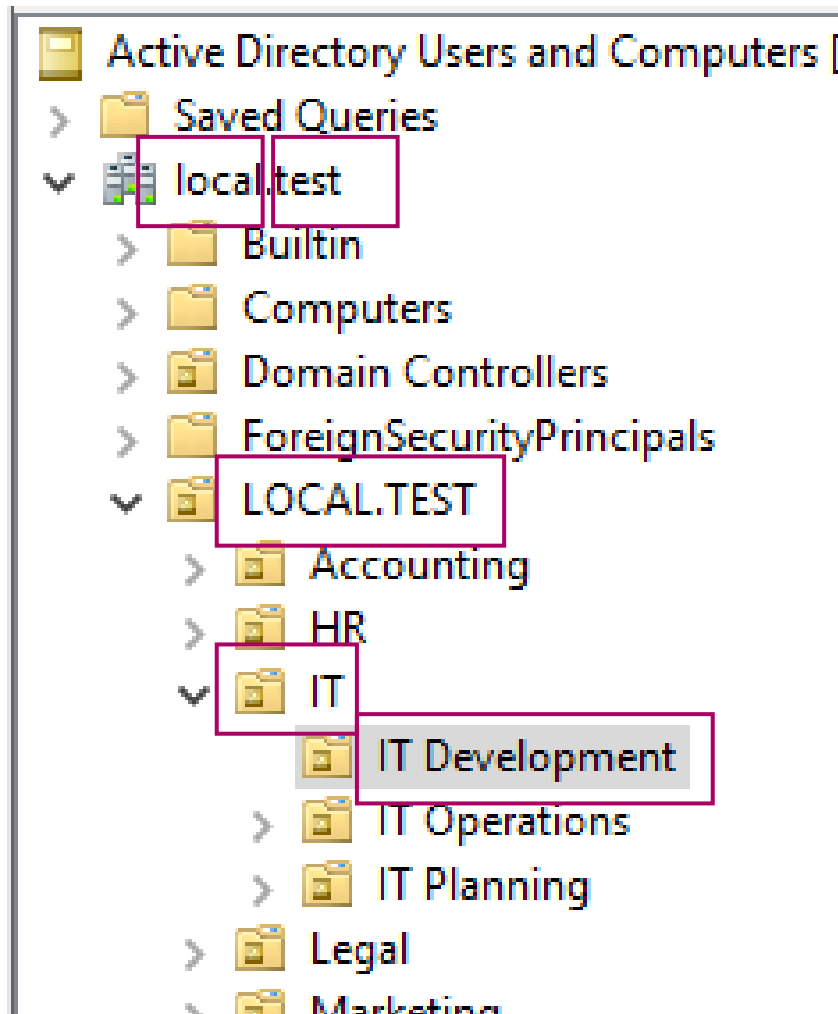


# LDAP Distinguished Name (1/3)

---

- Elk object in AD heeft een unieke identifier
  - GUID – 128-bit nummer
    - Statistisch onwaarschijnlijk om een zelfde nummer te bekomen vooraleer het jaar 3400!
  - Niet eenvoudig om te onthouden
    - => ander eenvoudiger systeem nodig -> Distinguished Name (DN)
- Hiërarchische paden binnen AD heten DN's
  - Mogelijk om object uniek te identificeren volgens LDAP standaard.
    - Vergelijkbaar met een directory structuur
      - Bijvoorbeeld: C:\Windows\NTDS\NTDS.DIT
    - Van rechts naar links lezen om vanaf de root (wortel) te lezen
  - DN bestaat uit verschillende RDN's
    - Relative Distinguished Name
    - Unieke referentie van een object binnen z'n parent container

# LDAP Distinguished Name (2/3)



Boomstructuur

=

**Directory Information Tree**

Name	Type
Rand Al Thor	User

**Distinguished Name =**

**CN=Rand Al Thor,OU=IT Development,OU=IT,OU=LOCAL.TEST,DC=local,DC=test**

**Relative Distinguished Name =**

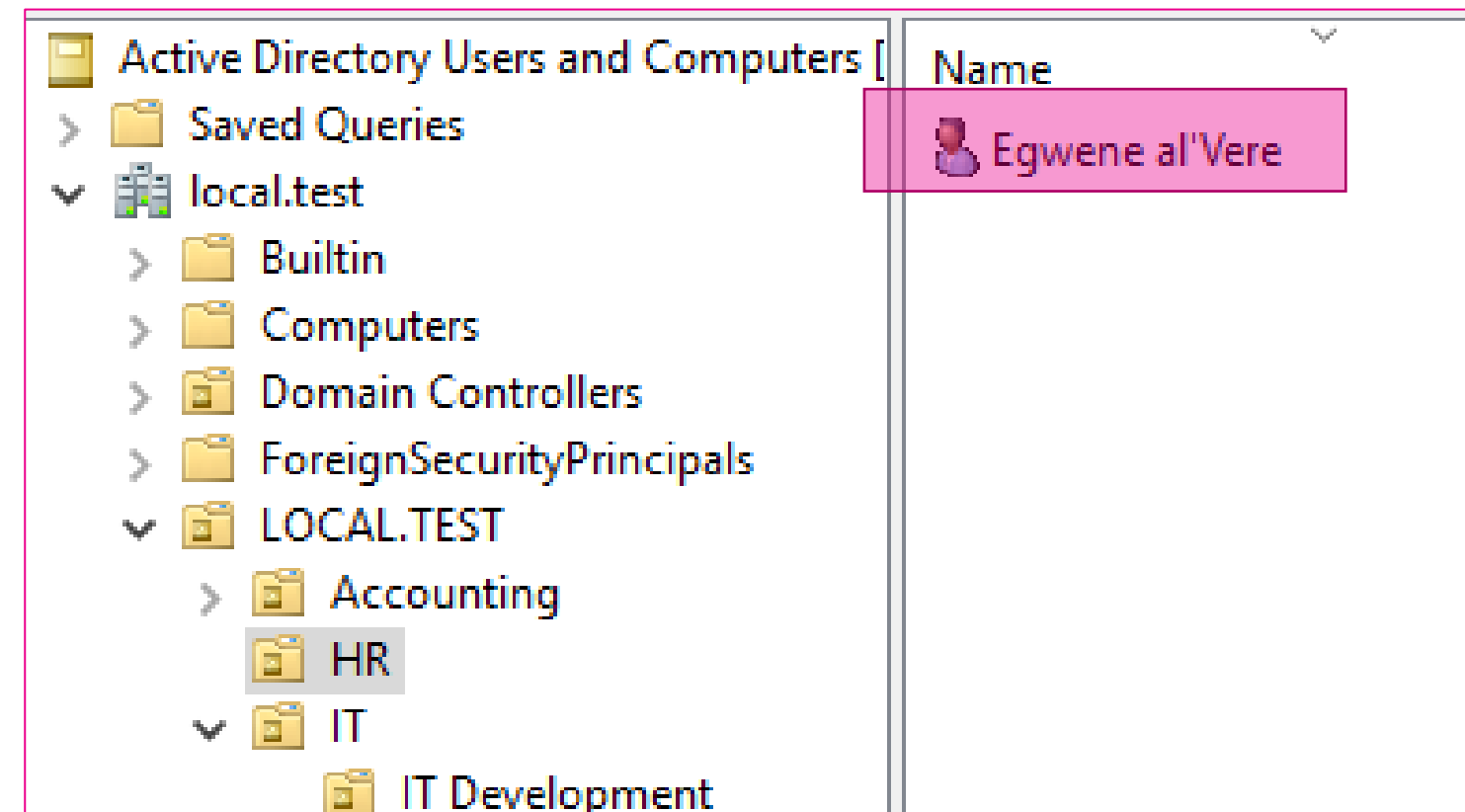
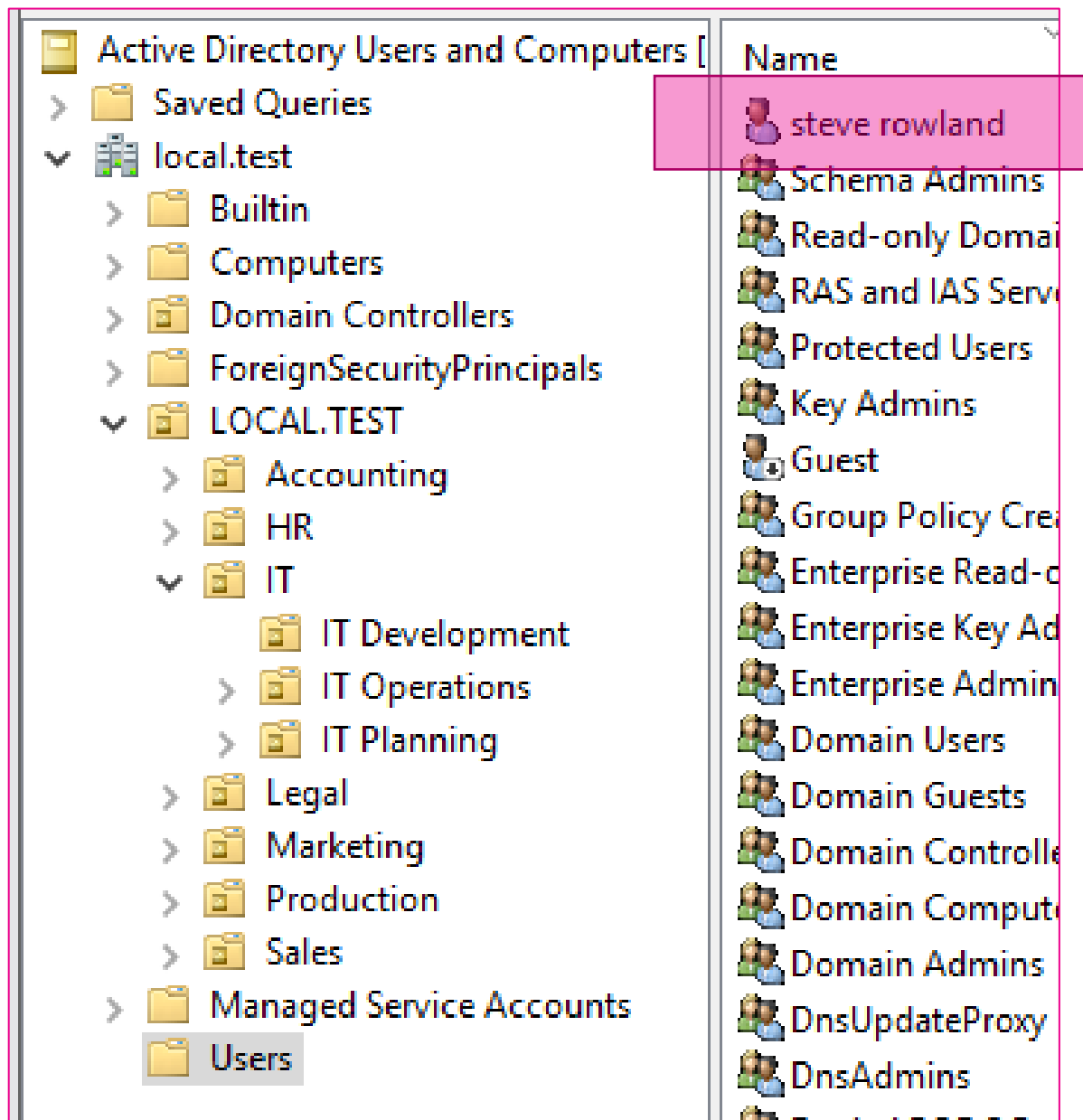
**CN=Rand Al Thor**

Elk type object krijgt een lettercode:

- DC = Domain Component
- OU = Organizational Unit
- CN = Common Name
  - Default naam indien geen specificatie
  - = groepen, users, printers, ...

# LDAP Distinguished Name (3/3) - TOEPASSING

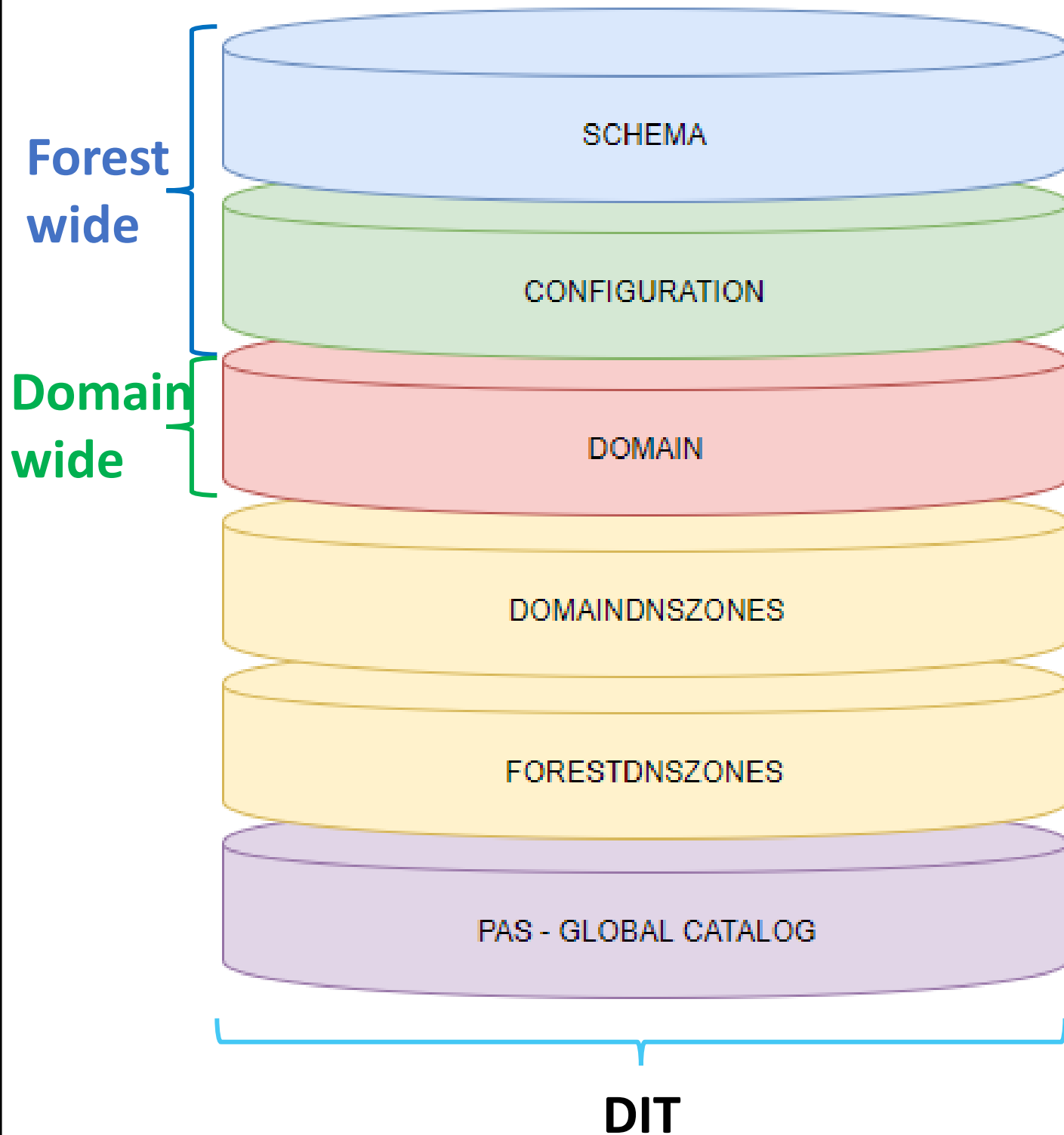
- Geef telkens de DN van volgende 2 objecten:



CN=steve rowland,CN=Users,DC=local,DC=test

CN=Egwene al'Vere,OU=HR,OU=LOCAL.TEST,DC=local,DC=test

# AD PARTITIONS / NAMING CONTEXTS / DIT



- **DIT**: Directory Information Tree
- **Schema**: het forest-wide schema van de database. De *blauwdruk* van hoe de AD objecten eruitzien.
  - objectSchema
  - attributeSchema
- **Configuration**: bevat data omtrent de configuratie van de forest of forest-brede applicaties
  - Sites, subnets, DC's, LDAP policies, ...
- **Domain**: eigenlijke domeinobjecten
  - User Accounts, Computer Accounts, groups, Ous, printers, ...
- **Application [optioneel]**: eventuele applicatiedata die in de database wordt opgeslaan. Bijvoorbeeld AD-integrated DNS
  - DomainDnsZones
  - ForestDnsZones
- **PAS – Global Catalog**: DC's die GC zijn bevatten een aparte partitie hiervoor. PAS = Partial Attribute Set = GC

# AD PARTITIONS / NAMING CONTEXTS / DIT

---

- Voordelen werken met partities
  - Zonder partities zou alle data moeten gerepliceerd worden tussen DC's. Nu enkel bepaalde data (NC).
    - = vlottere replicatie
  - Bepaalde data is nodig op alle DC's van een domein, niet daarbuiten.

# KERBEROS



# Kerberos

---

- Protocol uitgevonden aan MIT (Massachusetts Institute of Technology)
  - Hoe veilig communiceren over een onveilig netwerk met (soms) onbeveiligde partners?
  - Werkt met tickets. Paspoort om identiteit te bewijzen en dienst te bekomen
- Versie 5 in 1993 – momenteel release 1.21.3 (26/06/2024)
  - Open standaard ([RFC4120](#))
- Mythologie: 3-koppige bewaker van de Styx-rivier, zodat de doden niet konden ontsnappen
- 3 koppen:
  - client, server en vertrouwde 3<sup>e</sup> partij of KDC

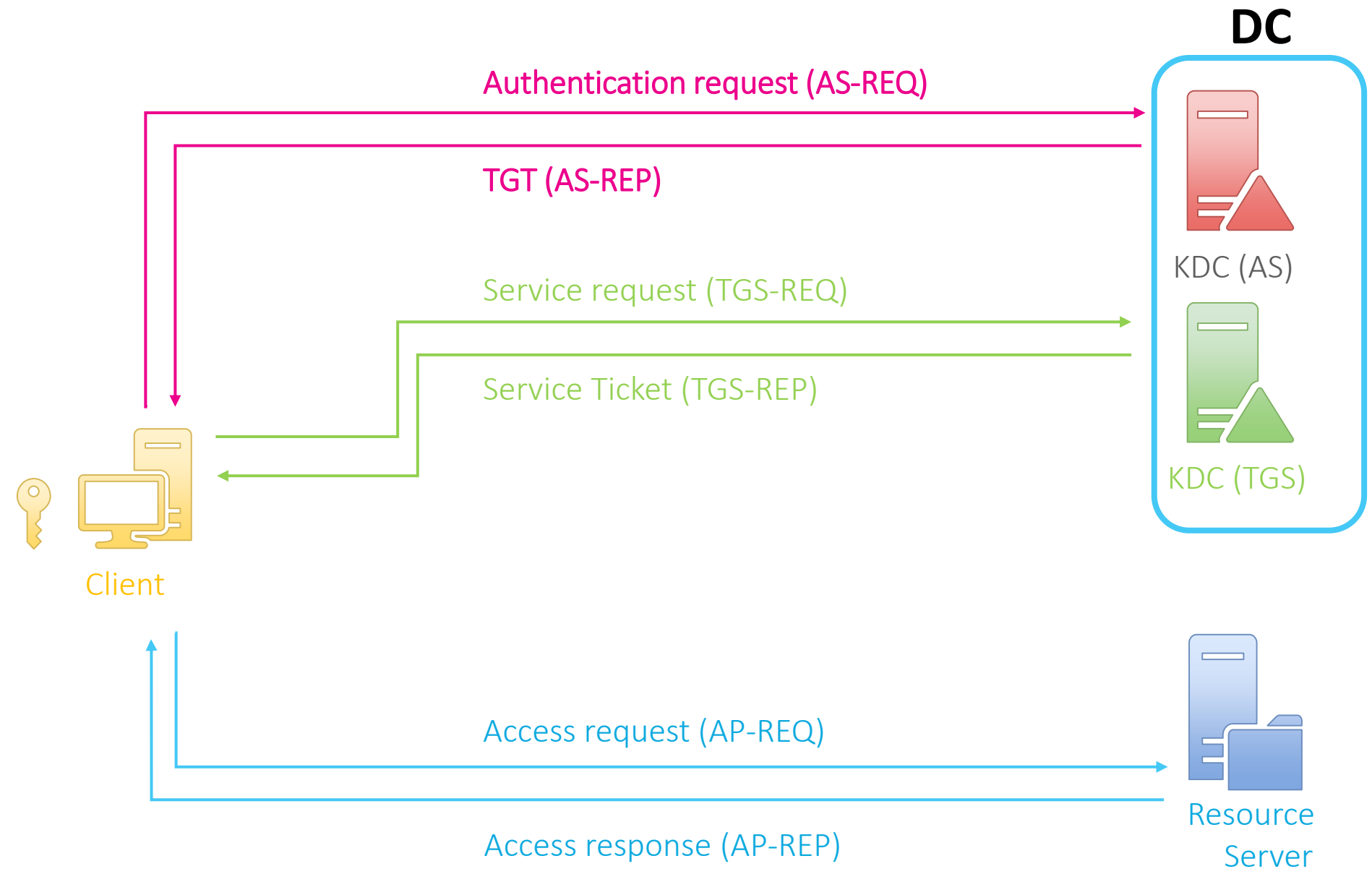
# Onderdelen

---

- KDC (*Key Distribution Center*)
  - AS (*Authentication Service*)
  - TGS (*Ticket Granting Service*)
- SP (*Security Principal*)
  - Een entiteit herkend door het beveiligingssysteem
    - User, group, computer, ...
- TGT (*Ticket Granting Ticket*)
  - Een ticket, beperkt in tijd, met informatie om bepaalde services (diensten) te bekomen via de TGS. Enkel leesbaar door KDC en uitgegeven door de AS. Bevat het User Access Token waar o.a. instaat in welke groepen de user zit.
- Session Key
  - Tijdelijke sleutel om toekomstige communicatie met een DC te beveiligen => geen user ww meer nodig!

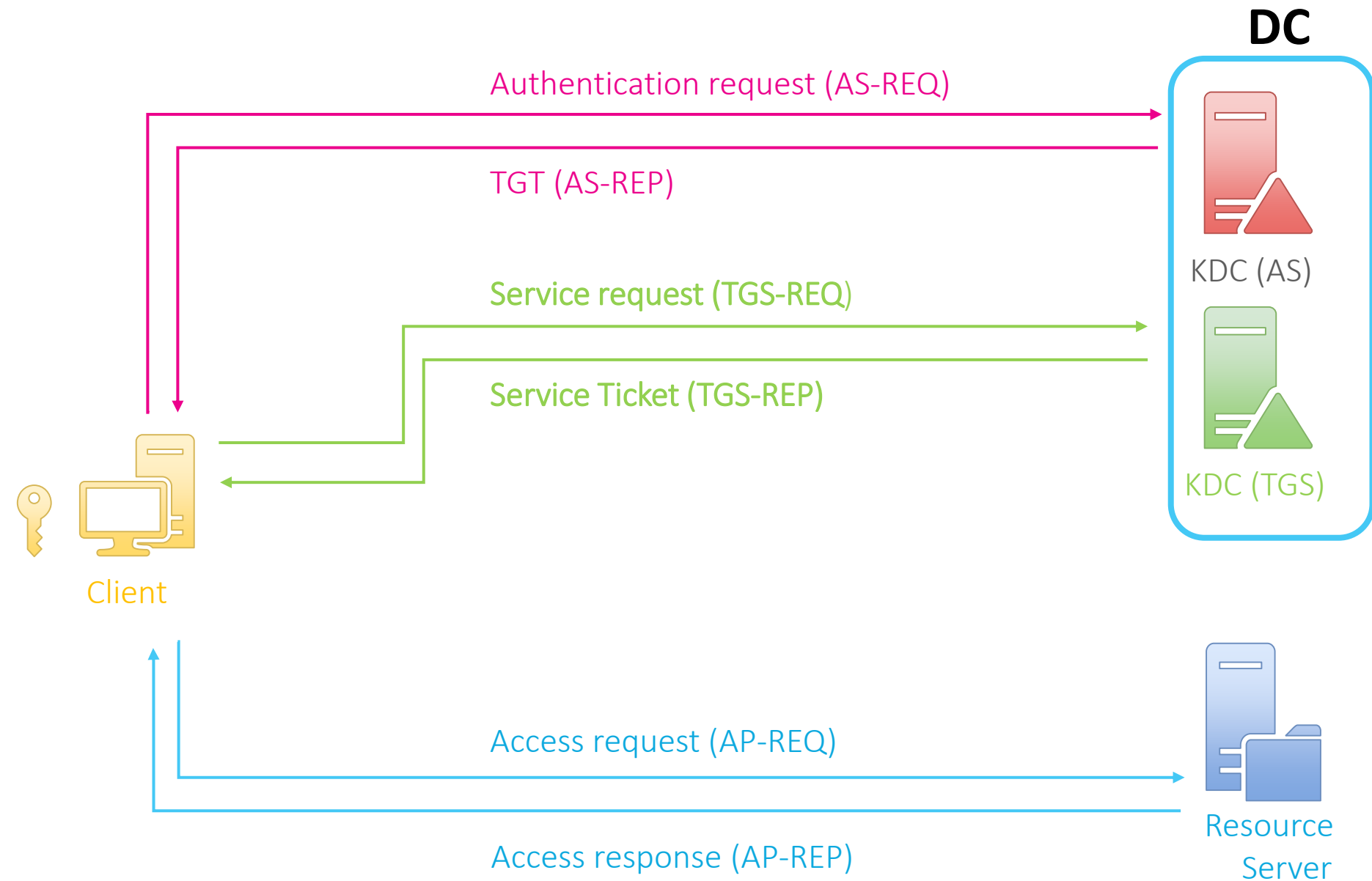
# Kerberos Proces (1/3)

- **AS-REQ** bevat o.a.
  - Username
  - Client Tijd
    - Geëncrypteerd met hash van gebruikerswachtwoord
    - AS decrypteert met z'n eigen hash uit AD
    - Tijd binnen 5 minuten tolerantie?
- **AS-REP** bevat o.a.
  - Session key
  - TGT (Ticket Granting Ticket)



# Kerberos Proces (2/3)

- **TGS-REQ** bevat o.a.
  - Service Principal Name (SPN)
    - Unieke identificatie van de service dat de user wil raadplegen
  - TGT
    - Om aan te tonen dat de user reeds geauthenticeerd is
- **TGS-REP** bevat o.a.
  - Service Ticket
    - Dit zal de client presenteren aan de service om toegang te krijgen.
    - Niet leesbaar door client -> geëncrypteerd
    - Beperkt bruikbaar in de tijd



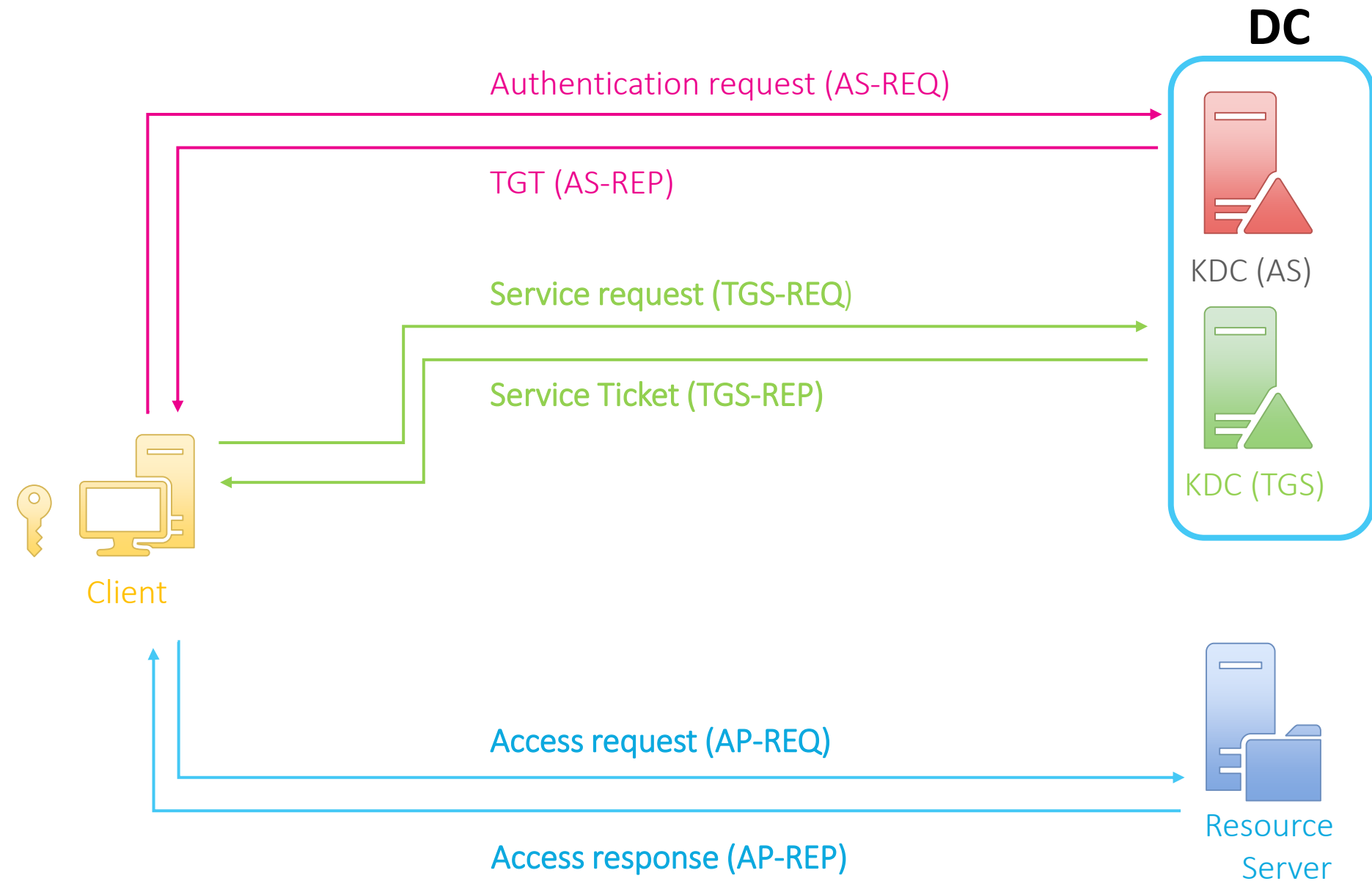
# Kerberos Proces (3/3)

- **AP-REQ**

- Client presenteert Service Ticket aan service
- Service gebruikt deze info om gebruiker te authenticeren

- **AP-REP**

- Optionele bevestiging van de authenticatie



# Bronnen

---

- Professor Messer - Kerberos  
<https://www.youtube.com/watch?v=VpBCJ8vS7T0>
- Kerberos uitgelegd a.d.h.v. figuren  
<https://danlebrero.com/2017/03/26/Kerberos-explained-in-pictures/>

DNS

# Fully Qualified Domain Name (FQDN)

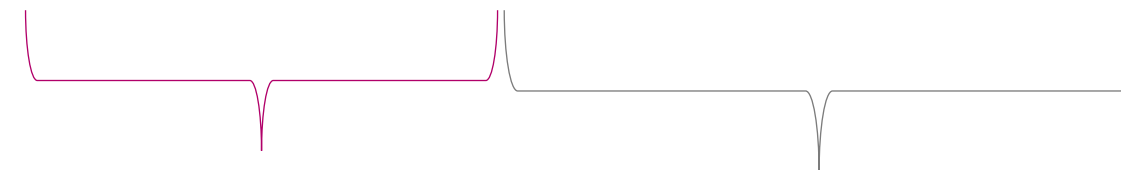
---

www

mail

ftp

student.howest.be.

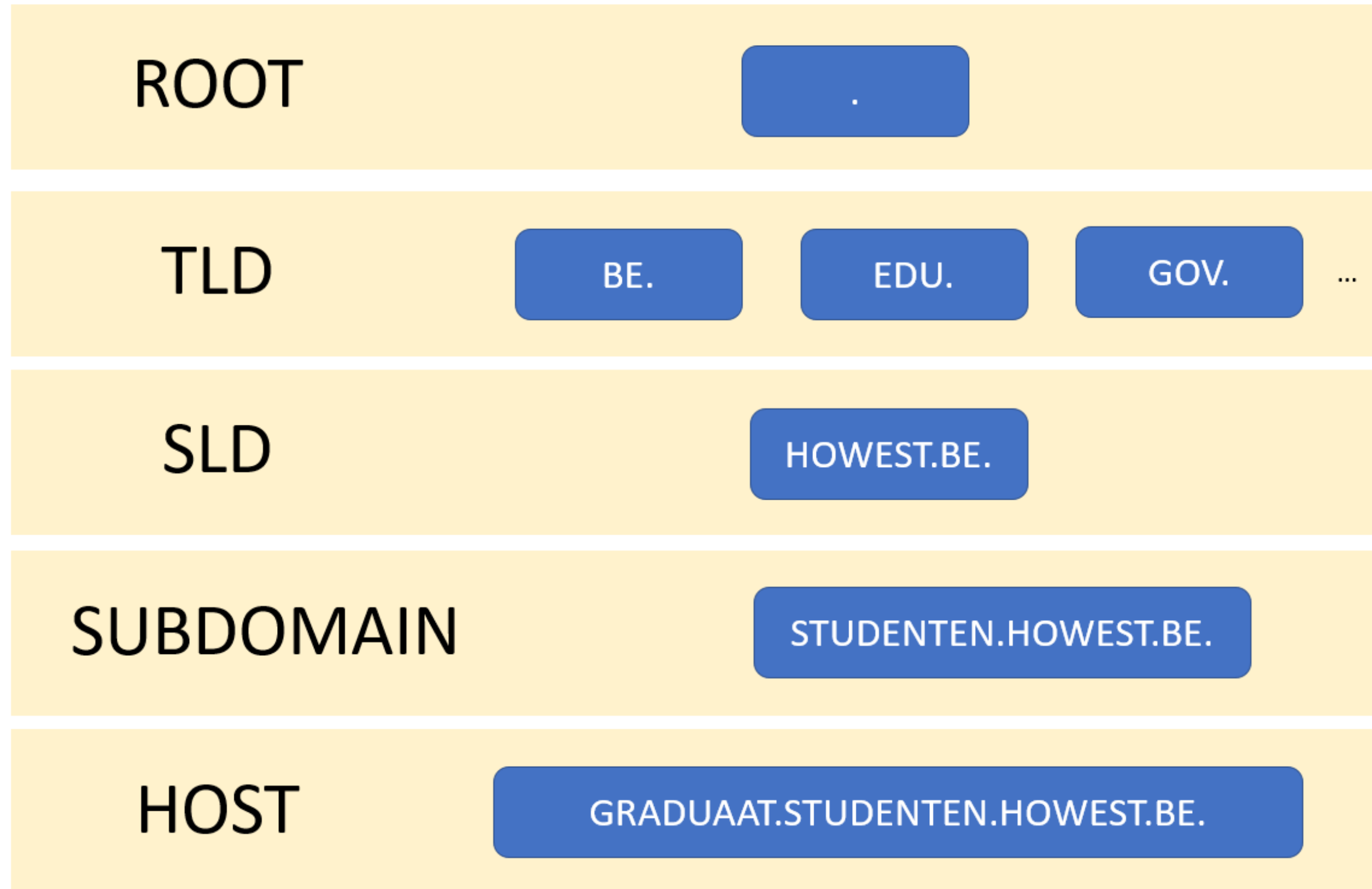


host . domein

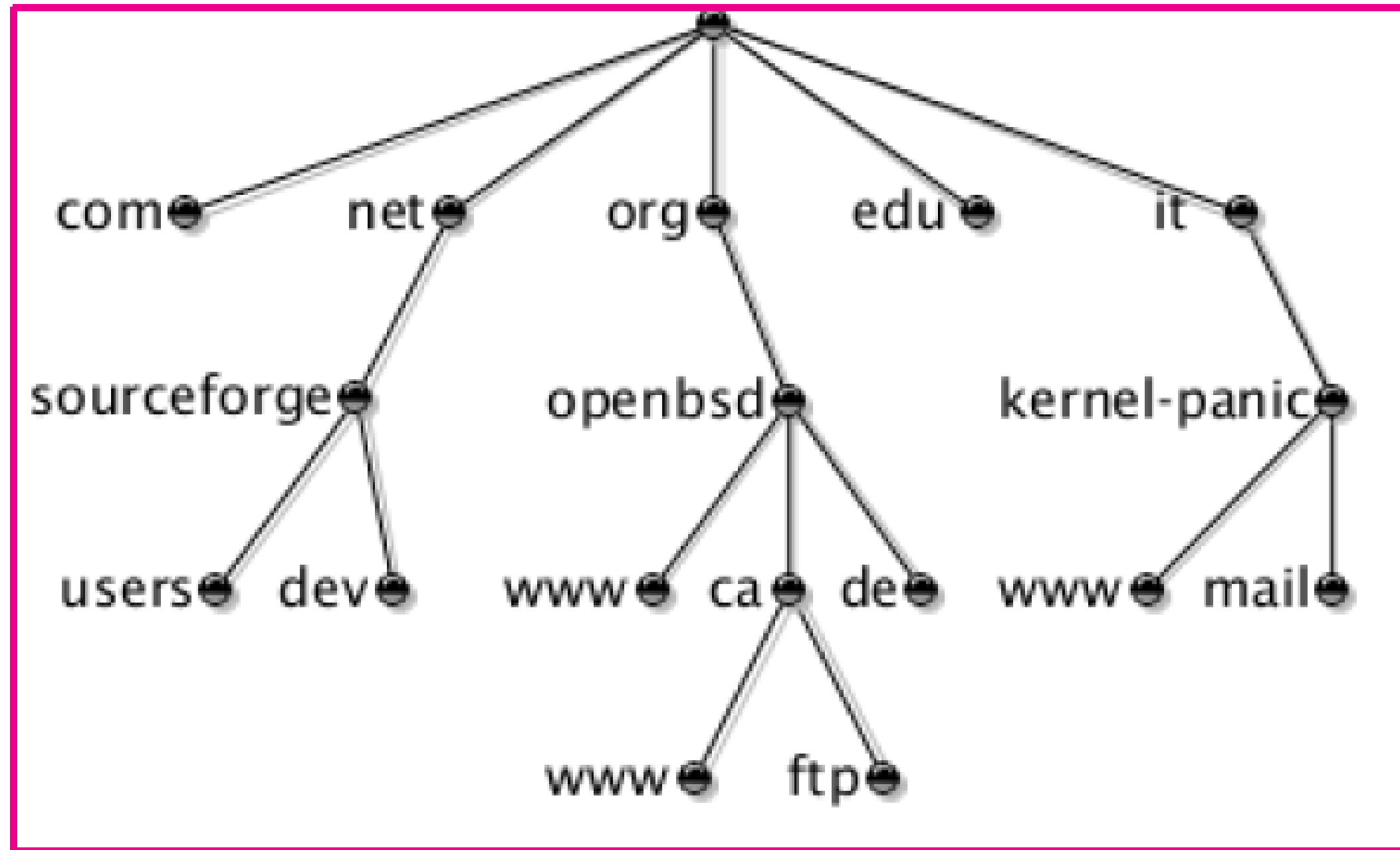


# Hiërarchische opbouw

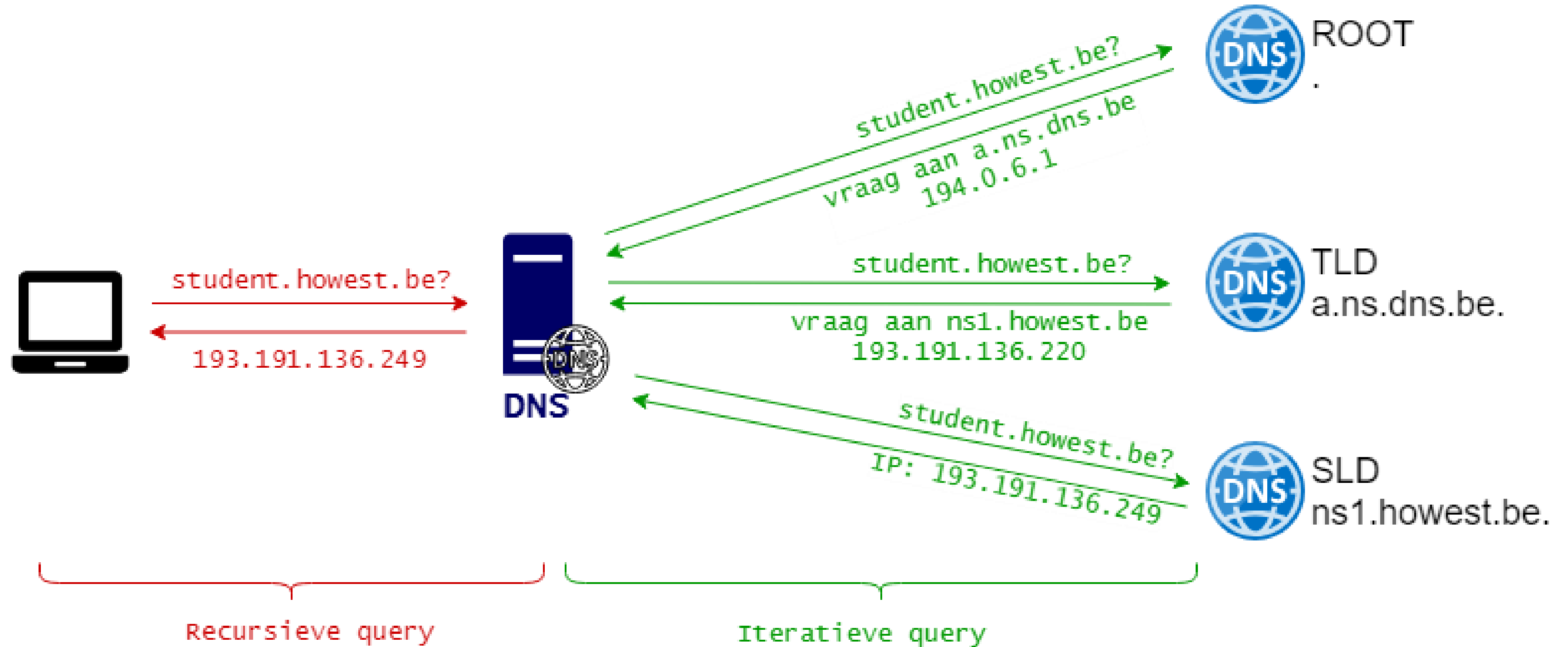
---



# DNS Namespace



# DNS Query – Hoe werkt DNS?



# Forward versus Reverse Lookup Zones

---

- Forward lookup: van domeinnaam naar IP

Zone howest.be.

student    IN        A        193.191.136.249

- Reverse lookup: van IP naar hostname

Zone 136.191.193.in-addr.arpa

249            IN        PTR            student.howest.be.

# Resource Records

- Eenheid van informatie binnen DNS

Recordtype	Functie
SOA	Start of Authority, geeft info over een DNS zone en primaire NS
NS	Name Server, duidt de verantwoordelijke server(s) aan
A of AAAA	Address, het IP van de hostname
CNAME	Canonical Name, een alias voor een hostname
SRV	Service Locator, laten je toe om servers te registreren gebruikt voor specifieke protocollen (services)
MX	Mail Exchange, duidt de mailserver aan voor een domein
PTR	Pointer, gebruikt voor reverse lookups
TXT	Text, gebruikt om extra info op te slaan

# DNS in AD nut?

---

- Vinden van resources
  - Domeincontrollers
  - Global Catalog
  - KDC (Kerberos)
  - Andere servers
- Vinden van clients

# Extra Bronnen

---

- DNS en IP adressen: [link](#)
- DNS en AD: <https://www.youtube.com/watch?v=pmMxT9YKzTE>
- What is DNS?  
<https://www.youtube.com/watch?v=W07dxCREOTc>
- DNS Namespace  
<https://www.youtube.com/watch?v=7fJwSLo65wo>
- DNS zones  
<https://www.youtube.com/watch?v=833Qnc-7-ug>
- DNS records  
<https://www.youtube.com/watch?v=6uEwzkfViSM>
- Nslookup  
<https://www.youtube.com/watch?v=8WIHluQaEbs>