Lightweight Directory Access Protocol je prva implementacija X.500 standarda imeniške strukture. Definiran je v RFC 4510 - 4519 kjer je RFX 4510 imenik in pregled za ostalih 9 RFC-jev. ![[Pasted image 20230112195935.png]]

LDAP je bil razvit po SCRUM razvojni metodi in obstaja v trej verzijah: - LDAP 1.0, ta se ne uporablja več in ne obstaja, je bila teorija - LDAP 2.0 ta je bila dejansko prva delujoča verzija - LDAP 3.0 je ta ki se danes v produkciji uporablja ![[Pasted image 20230112200302.png]]

LDAP je zgolj TCP protokol za komunikacijo podatkov iz baze, ne ukvarja se s tem kako so podatki zgrajeni to je metashemo, le to komunicira navzven. Poznamo različne implementacije takšnega protokola: - OpenLDAP - Active Directory (MicroSoft, popularno orodje), ta dejansko implementira DNS in LDAP skupaj, kot močno orodje.

Varnost lahko prepustimo drugim protokolom https ipd. lahko pa uporabimo preklop na TLS/SSL način komunikacije v samem ldap-u z ukazom *start TLS*. Druga možnost je namestitev strežnika na druga vrata in izvedba celotnega pogovora v SSL komunikaciji: LDAPS, ta je sicer od 2000 deprecated in se uporablja startTLS.

V osnovnem protokolu obstaja ukaz *bind*, ki dopušča avtentikacijo komunikacije in tistega na drugi strani, tako dobi večji dostop do ostalih parametrov komunikacije. Seja je lahko tudi neavtenticirana, vendar z omejenim dostopom. *Unbind* je pa ukaz za zaključek seje.

Za pregledovanje LDAP poda dva ukaza: - *search*, vrne objekt, ki ga iščemo. Rezultat je odvisen od tega ali je uporabnik avtenticiran ali ne. GESLA NIKOLI NE VRNE - *compare* se uporablja za primerjanje vnešene vrednosti in tiste v bazi, tako lahko preverimo če je geslo pravo. Ta ukaz vrača le True ali False.

Za manipulacijo podatko: - *add*, dodamo predmet v bazo - *delete*, brišemo predmet iz baze - *modify*, spremenimo vrednosti prilastkov predmeta

Za dodatno uporavljanje seje: - *abandon*, prekine izvajanje zahteve, ki smo jo poslali (lahko prekinemo iskanje in primerjanje, ter popravke baze) - *extended*, generična možnost poljubnega dodatnega ukaza

Shema združuje različne predmete in prilastke (uporaba vključevalnih ukazov include). Nato pa razredi združujejo prilastke, te so zapisani z zapisom ASN.1, so del hierarhije in dedujejo lastnosti staršov, ter določajo obvezne in neobvezne prilastke.

LDAP pri prenašanju podatkov uporabljajo poseben format imenovan LDIF: ![[Pasted image 20230112203847.png]]