**IMENIŠKE STRUKTURE IN LDAP**

1. **Standard X509 definira certifikate, ki jih Peter in Janez uporabljata v prejšnjem vprašanju. Standard predvideva v certifikatu vrsto polj in med njimi so tudi (z imeni v angleščini) polja:**

Issuer, Subject, Subject Public Key Info, ki vključuje (pod) polji Public Key Algorithm, Subject Public Key ter še polje Subject Unique Identifier

1. **Kaj je shranjenega v posameznem polju in ali so vsa našteta polja obvezna?**

* **Issuer** – Kdo je izdal certifikat
* **Subject** – Komu pripada certifikat
* **Public Key Algorithm** – Algoritem po katerem poteka avtenticeranje z tem ključem
* **Subject Public Key** – Javen ključ osebe kateri pripada certifikat
* **Subject Unique Identifier** – Glede na to, da je lahko več osebkov z npr. enakim imenom itd. certifikatu iz tega razloga dodamo se identifier, ki unikatno pove kdo točno je ta oseba

1. **Beseda certifikat pomeni potrdilo. Kdo in kaj potrjuje z X509 potrdilom? Kako vemo, da je vsebina potrdila verodostojna?**

* Z certifikatom njegov lastnik potrjuje, da se na drugem koncu prav zares nahaja on in ne nekdo drug.
* O verodostojnosti potrdila moramo vprašati certifikatno agencijo. **MORAMO JI ZAUPATI**

1. **Katere načine varne komunikacije ponuja protokol LDAP?**

* Avtorizacijo z certifikati in varnost podatkov prek storitve TLS (SSL).
* Ter močne varnostne storitve SASL-a za avtentikacijo in varnost podatkov

**PODATKI ZA DELOVANJE OMREŽJA**

1. **Eden od prilastkov DNS protokola je TXT. Kako je prilastek TXT povezan s podatki o elektronski pošti?**

* TXT zapis je namenjen administratorjem, da vstavijo poljuben tekst zapis DNS na primer komentarje in zapiske npr. **DomainKeys Idnetified Mail** za preverjanje legitimnih e-mail virov iz domene

1. **Peter je včasih prav čuden možakar. Tokrat si je vbil v glavo, da ne bo nadgradil svojega LDAP strežnika, da bi uporabljal protokol LDAPv3 namesto LDAPv2. Napišite tri primere, ko ga njegova trdoglavost ne bo prizadela. Utemeljite svoj odgovor.**

* Še vedno bo lahko normalno komuniciral
* Še vedno bo protokol enako upošteval metashemo shranjenih podatkov
* Še vedno bo lahko uporabljal vse različne operacije nad podatke
* **Tako rekoč ohranil bo vse funkcionalnosti ki jih ponuja LDAPv3 razen varnost, saj LDAPv2 ne ponuja NOBENE VARNOSTI!!**

1. **Po krajšem pogovoru, smo ugotovili, zakaj nima namena nadgraditi svojega strežnika – njegovo kodo je napisal sam. No, končno se je le dal prepričati, da ga bo nadgradil. Pri nadgradnji se mu je zataknilo pri izvedbi ukaza bind, medtem ko je vse ostale spremembe uspešno implementiral. Komentirajte omenjeno pomankljivost. Jo lahko kako drugače nadomesti? Utemeljite odgovor.**

* Sedaj bo imel problem z avtentikacijo ampak bo lahko vseeno dostopal do sistema kot anonymous (do nekaterih delov)
* Lahko zažene ukaz **start TLS** prek katerega se bo avtenticiral na transportni plasti

**Podatki za delovanje omrežja**

1. **Ko govorimo o LDAP, kaj je pravzaprav to: kos programske opreme, opis podatkov, ki jih odjemalec lahko pridobi, protokol ali nekaj tretjega? Utemeljite odgovor.**

* Je protokol za komunikacijo, ku upošteva metashemo podatkov zato ker definira kako se dostopa do določenih podatkov, ukaze, varnost ipd.

1. **Na predavanjih smo omenili, da obstajata dve inačici LDAP: v2 in v3. Zapišite in opišite vsaj dve podrobnosti, v katerih se razlikujeta.**

* V LDAPv3 je dodana avtorizacija z certifikati in varnost podatkov prek storitve TLS (SSL)
* V LDAPv3 se uporablja kodiranje UTF-8
* V LDAPv3 definira močne varnostne storitve SASL-a za avtentikacijo in varnost podatkov

1. **Med odjemalcem in strežnikom se pri LDAP vzpostavi seja. Med drugim sta ukaza, ki jih seja pozna, bind in unbind. Ali v seji oba ukaza vedno nastopata? Utemeljite odgovor – morda najbolje z opisom primera.**

* Pri LDAPv2 se vedno uporabita. Pri LDAPv3 pa ni nujno.
* Lahko do določenih podatkov dostopamo kot anonymous ponavadi z omejenimi pravicami.. Ali pa se avtenticiramo z ukazom start TLS na transportni plasti