X.500, X.509, LDAP

Co to jest X.500?

„X.500 jest zbiorem standardów opisujących usługi katalogowe”.

Czym w takim razie są usługi katalogowe?

- Jest to obiektowa **baza danych**, która może zawierać użytkowników, dane dla aplikacji, zasoby, konfiguracje, adresy, urządzenia sieciowe i inne dane. Baza ma strukturę hierarchicznego drzewa.

Czym w takim razie różni się od standardowej bazy danych?

- Usługa katalogowa kontroluje dostęp do zasobów.

- Zapewnia odporność na błędy.

- DN (Distinguished Name) - czyli nazwa wyróżniająca każdy obiekt.

- Struktura hierarchiczna

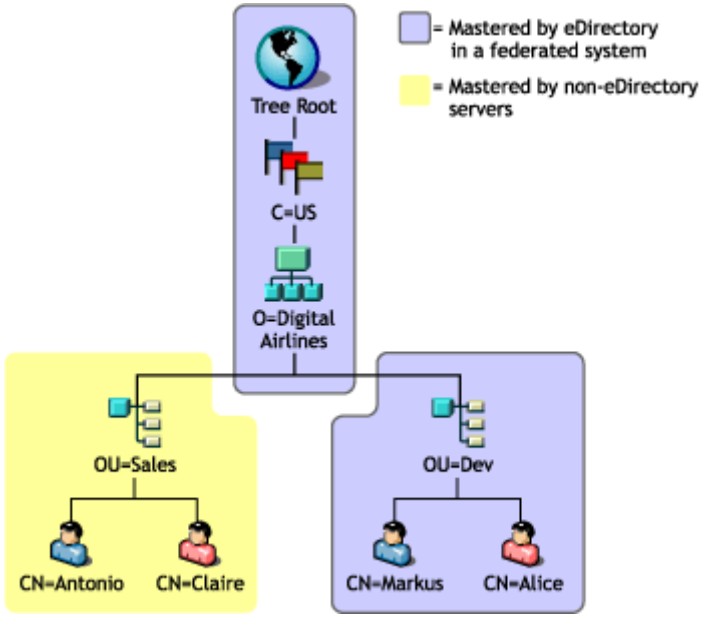
- Reprezentacja w postaci drzewa

- Optymalizujemy odczyt, nie przejmując się zapisem

- Klasy posiadają schematy opisujące atrybuty obiektu w instancji klasy

- Atrybuty, schematy i obiekty są ustandaryzowane

Przykładowa struktura katalogowa:



Przykładowa struktura katalogowa.

Gdzie się tego używa?

- SSL!

Klucze SSL opisuje standard X.509 będący pochodną usług katalogowych X.500.

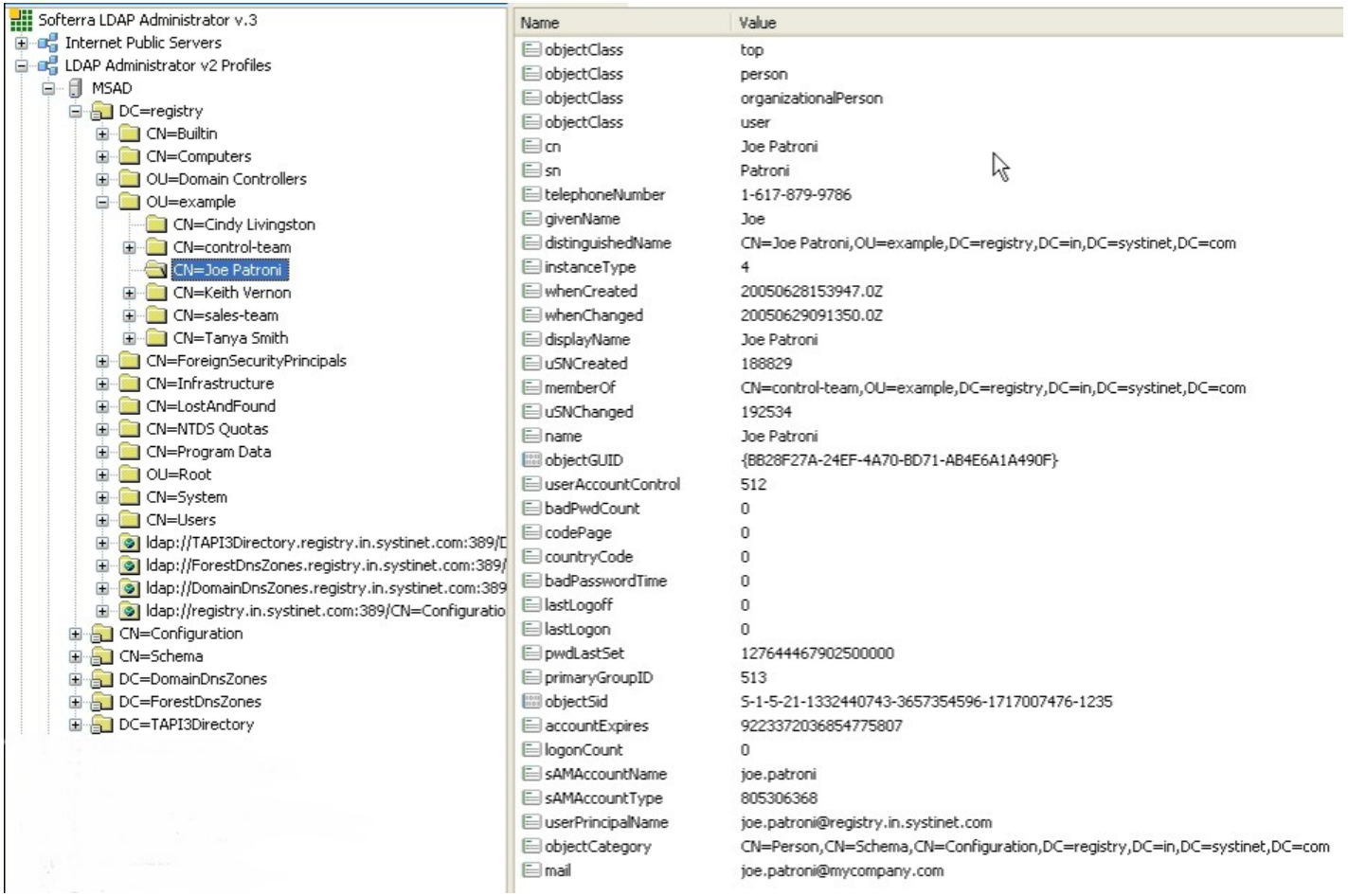
```
SHA1 Fingerprint=E3:59:EE:C9:58:F5:46:11:07:AF:63:AE:D0:12:62:B0:D9:CA:5B:B0
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 6 (0x6)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=PL, ST=Dolnoslaskie, L=Wroclaw, O=czakey networks, OU=Home,
CN=czakey networks SSL/emailAddress=czakey@czakey.net
        Validity
            Not Before: Aug 11 07:36:02 2009 GMT
            Not After : Aug  9 07:36:02 2019 GMT
        Subject: C=PL, ST=Dolnoslaskie, O=czakey networks, OU=Home,
CN=router.czakey.net/emailAddress=czakey@czakey.net
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
[...]
```

- Centralizacja informacji

LDAP - Lightweight Directory Access Protocol czyli protokół „lajtowego” dostępu do katalogu.

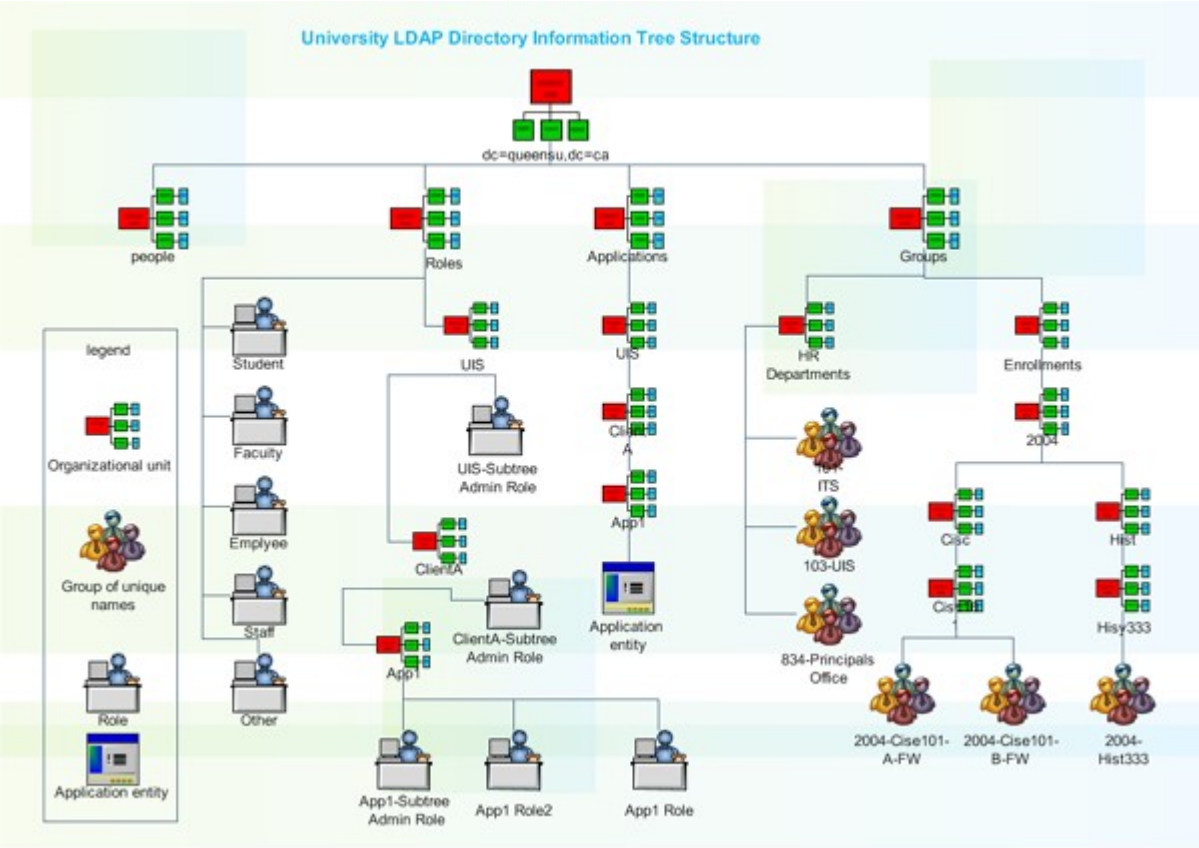
LDAP jako centralna baza użytkowników i haseł
LDAP jako centralna książka telefoniczna
LDAP jako centralna baza konfiguracji
Active Directory

Centralna baza użytkowników:



Użytkownicy w centralnej bazie LDAP.

Struktura mieszana z użytkownikami, aplikacjami, grupami, ...



Użytkownicy, grupy, role, aplikacje

Przykład DN:

```
cn=czakey,ou=Studenci,dc=ii,dc=uni,dc=wroc,dc=pl
```

Hierarchiczna struktura jest czasem problematyczna. Np. powyżej jeśli jest się zarówno studentem jak i pracownikiem UNIQUE ID nie pozwoli istnieć w dwóch OU.

Standardowe atrybuty (w schemacie core):

O (Organization) - organizacja
DC (Domain Component) - część domeny (np. dc=ii,dc=yebood,dc=com)
OU (Organizational Unit) – jednostka organizacyjna
UID (User Identifier) - identyfikator użytkownika
RID (Relative Identifier) - liczbowy identyfikator użytkownika
CN (Common Name) - nazwa uzytkownika, imię
SN (Surname) - nazwisko
C (Country) - państwo

Operacje wykonywane na LDAP-ie:

- bind oraz unbind
- search
- add
- delete
- modify

Ataki na LDAP:

LDAP injection - jak SQL injection tylko "wstrzykujemy" zapytania LDAP.

Przykład:

In a page with a user search form, the following code is responsible to catch input value and generate a LDAP query that will be used in LDAP database.

```
<input type="text" size=20 name="userName">Insert the username</input>
```

The LDAP query is narrowed down for performance and the underlying code for this function might be the following:

```
String ldapSearchQuery = "(cn=" + $userName + ")";
System.out.println(ldapSearchQuery);
```

If the variable $userName is not validated, it could be possible accomplish LDAP injection, as follows:

* If a user puts “*” on box search, the system may return all the usernames on the LDAP base
* If a user puts “jonys) (| (password = *))”, it will generate the code bellow revealing jonys’ password (cn = jonys) (| (password = *))