

# UPRAVLJANJE IDENTITETOM I PRISTUPOM

---

Predmet: Bezbednost Web aplikacija

Predavač: dr Dušan Stefanović

Upravljanje identitetom i pristupom uključuje:

### **Administracija korisničkih naloga**

Prava koja su dodeljena za upravljanje korisnicima

### **Autentifikacija korisnika**

Provera identiteta

### **Autorizacija pristupa**

Šta je dozvoljeno da uradimo

### **Revizija (Audit)**

Provera da li su prethodne tri stvari urađene korektno

## IDENTIFIKACIJA KORISNIČKIH GRUPA

Identifikacija korisničkih grupa je proces klasifikacije korisnika na osnovu zajedničkih karakteristika kako bi se olakšalo upravljanje pravima pristupa i resursima u informacionim sistemima.

Korisničke grupe se obično formiraju na osnovu:

### **Funkcionalne uloge:**

Korisnici koji obavljaju slične poslove ili zadatke mogu biti grupisani u istu korisničku grupu.

### **Odeljenja:**

Korisnici koji pripadaju istom odeljenju ili sektoru organizacije mogu biti grupisani zajedno

### **Nivo pristupa:**

Korisnici koji zahtevaju isti nivo pristupa određenim resursima mogu biti grupisani zajedno

### **Projekti:**

Korisnici koji rade na istom projektu ili zadatku mogu biti grupisani u posebnu korisničku grupu.

# IDENTIFIKACIJA KORISNIČKIH GRUPA

Prvi korak je podela korisnika u korisničke grupe

## ZAPOSLENI



Administracija    Proizvodnja    Prodaja

## SNABDEVAČI



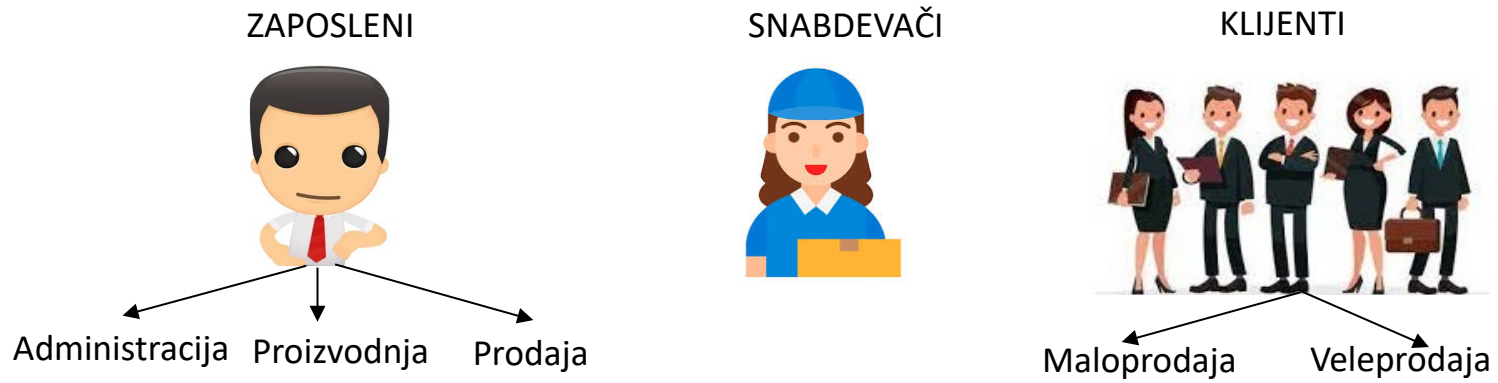
## KLIJENTI



Maloprodaja    Veleprodaja

# DEFINISANJE PRAVA PRISTUPA

Drugi korak je dodela prava grupama za korišćenje servisa

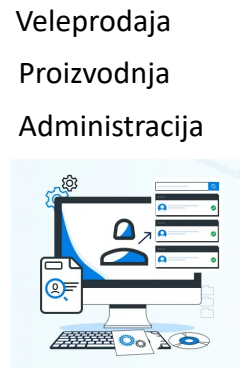


**GRUPE**

**SERVISI**



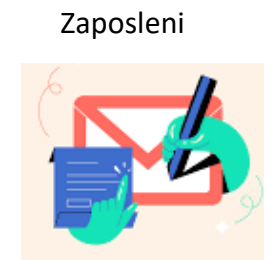
SISTEM ZA HR



CRM SISTEM



SISTEM ZA FINANSIJE



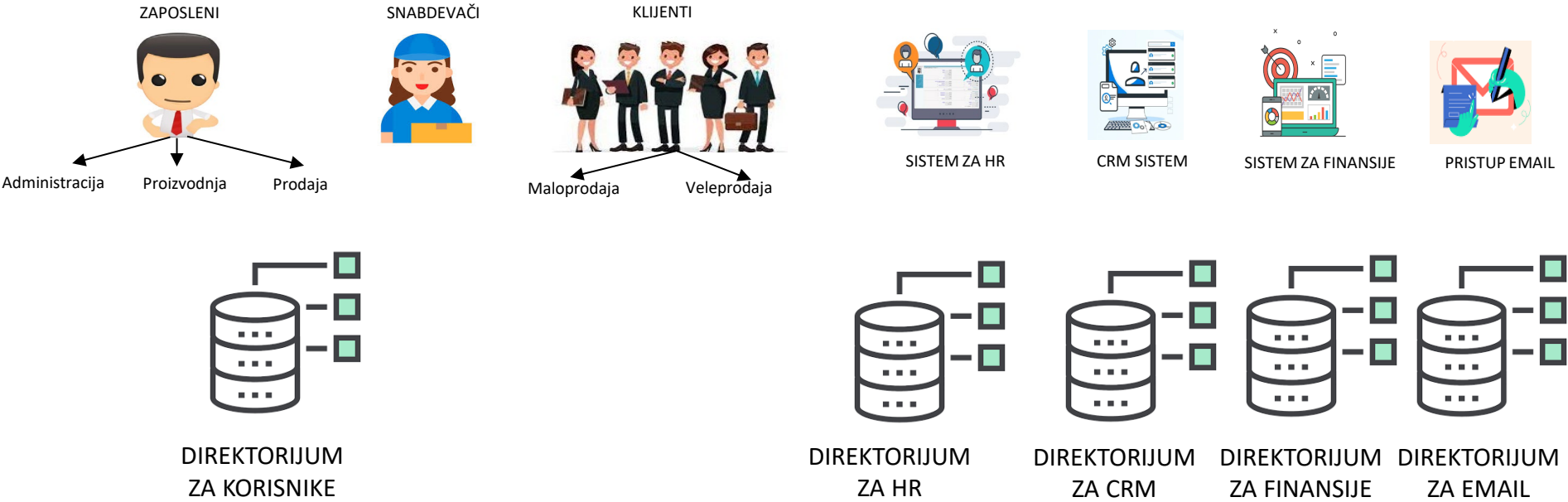
PRISTUP EMAIL

# IAM (Identity Access Management) ARHITEKTURA

Identitet predstavlja bilo koju informaciju o korisniku

Informacije o korisniku se čuvaju u direktorijumu tj. baze podataka poznate kao LDAP direktorijumi.

Svaki servis ima svoj odvojen direktorijum u kome servis čuva podatke



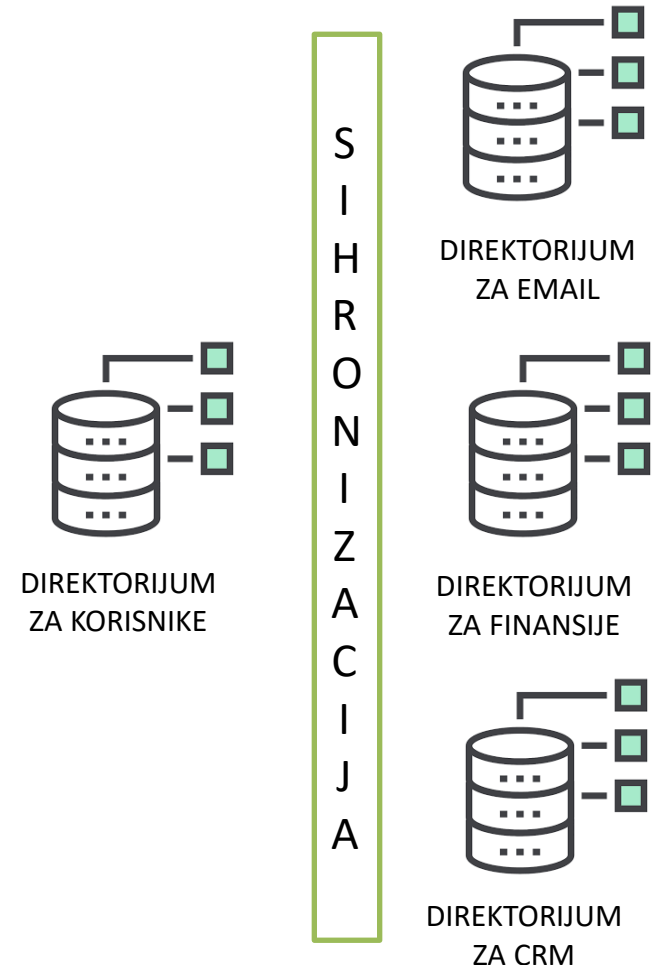
# IAM (Identity Access Management) ARHITEKTURA

Idelano bi bilo da postoji jedinstven direktorijum za čuvanje svih podataka ali zbog specifičnosti sistema i strukture podataka koja se čuva to nije u potpunosti izvodljivo

**Prvi korak u IAM arhitekturi** je da se pronade mesto za čuvanje podataka o korisnicima i njihova sinhronizacija sa podacima iz drugih direktorijuma.

Sihronizacija se može ostvariti na jedan od dva načina

1. Virtuelni direktorijum
2. Meta podaci



# IAM (Identity Access Management) ARHITEKTURA

Virtuelni direktorijum je prvi način da se podaci iz različitih direktorijuma sinhronizuju.

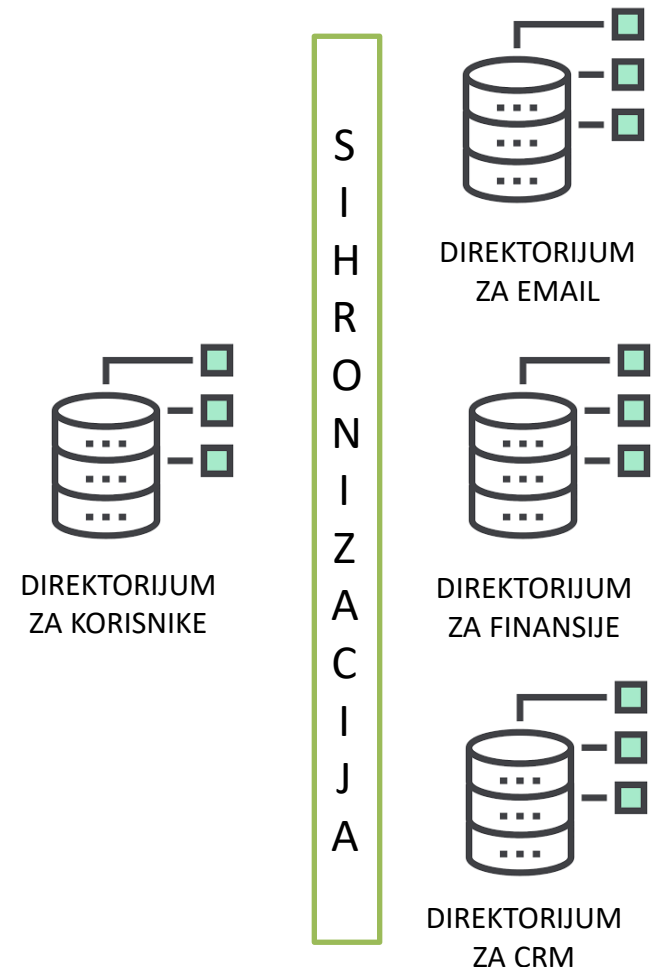
**Virtuelni direktorijum** koji se nalazi u direktorijumu za korisnike je **indeks** koji ima ulogu **pokazivača** tj. sadrži informacije gde se koji podaci iz drugih direktorijuma nalaze.

**Meta direktorijum** je drugi način da se podaci iz različitih direktorijuma sinhronizuju

Meta direktorijum je direktorijum koji sadrži informacije o drugim direktorijumima ili datotekama.

Meta direktorijum ne sadrži sve podatke već čuva metapodatke ili informacije o strukturi i organizaciji drugih direktorijuma ili resursa.

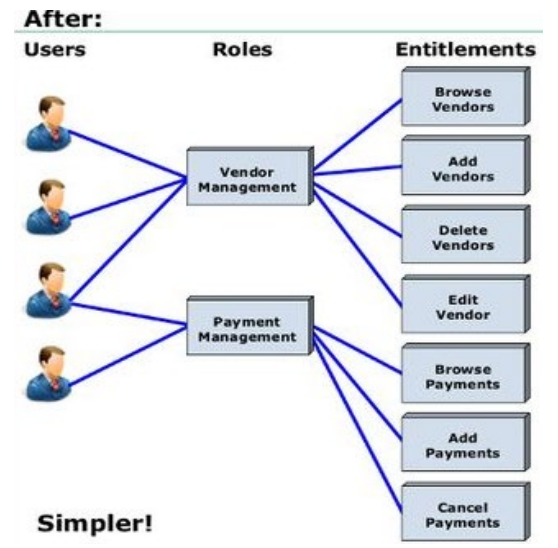
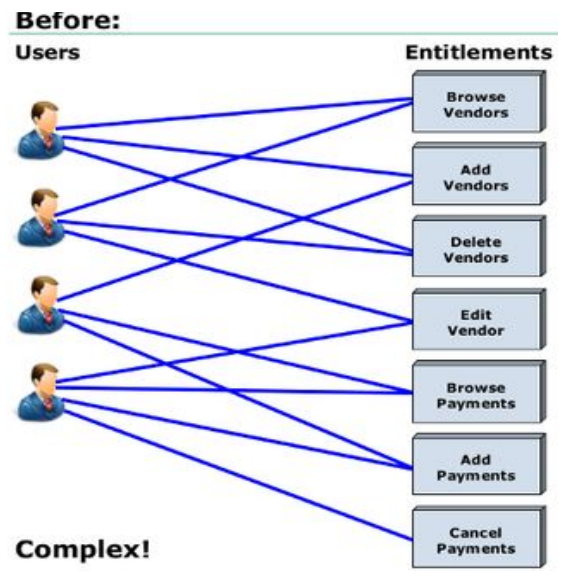
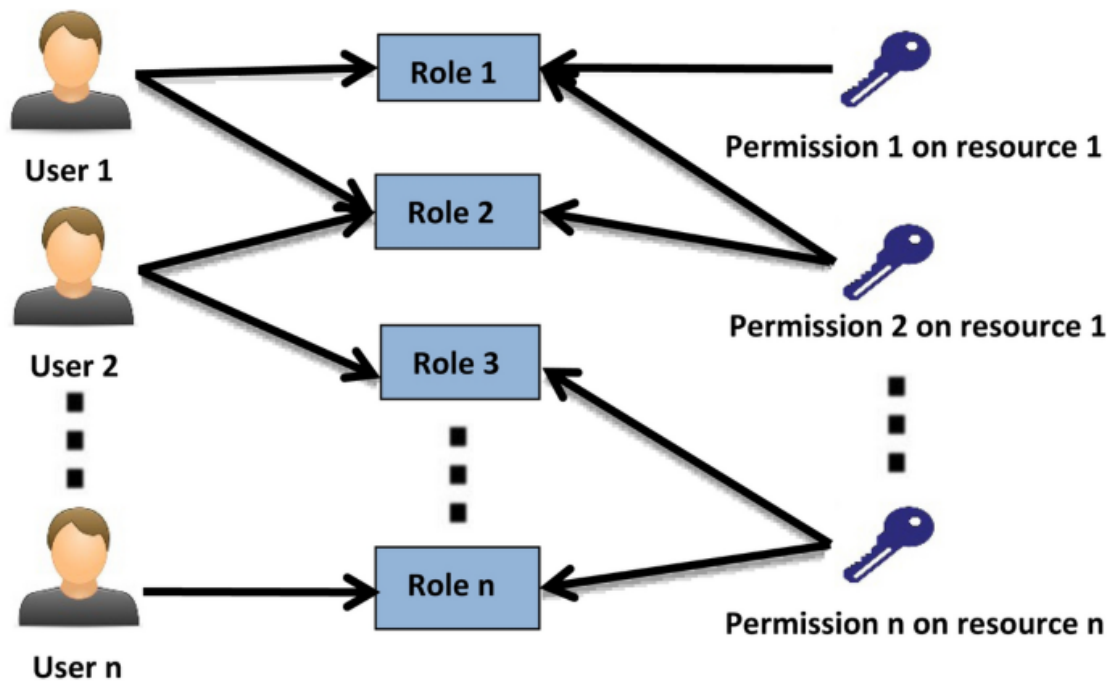
Sadrži više podataka u odnosu na virtuelni direktorijum.



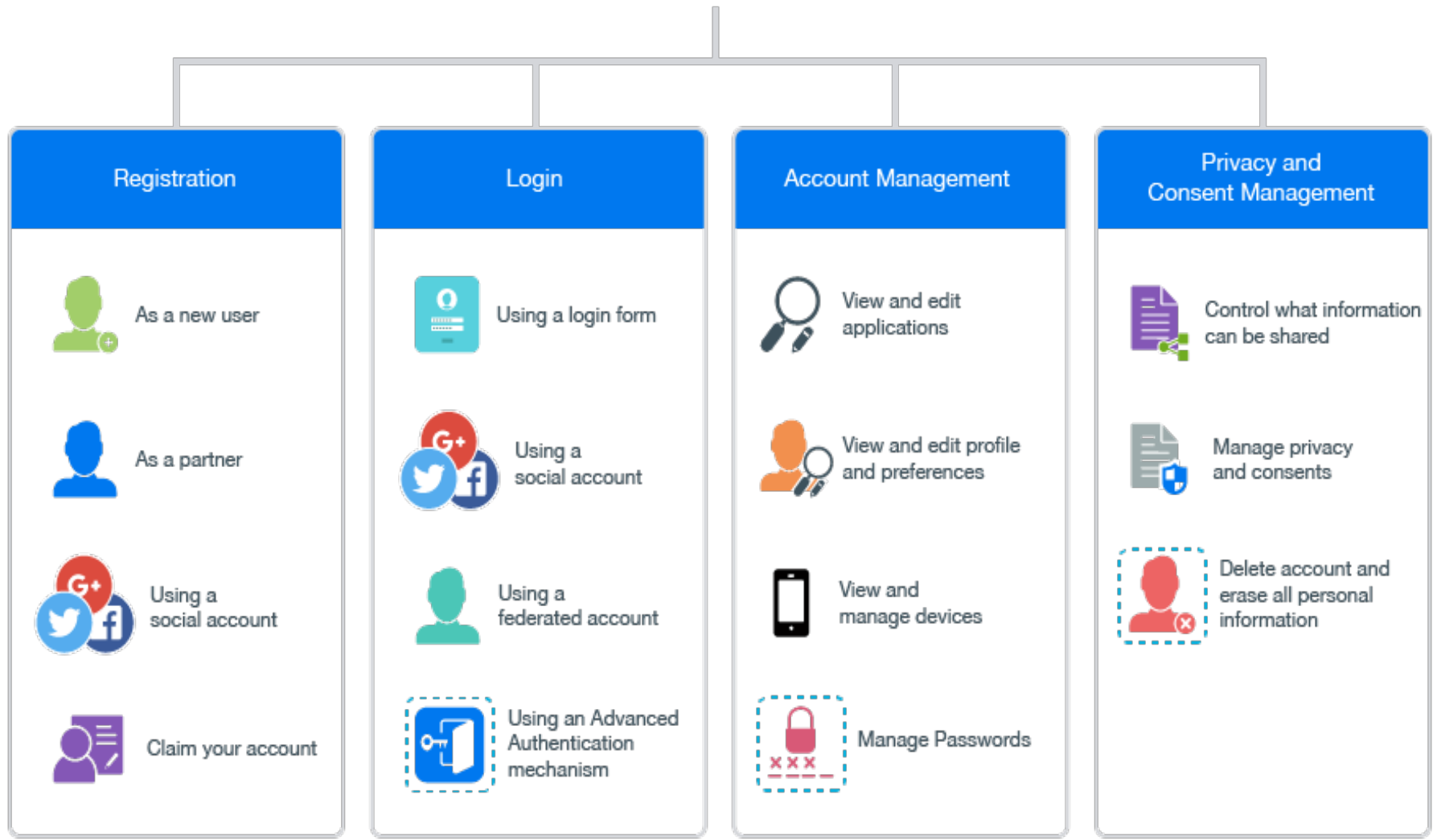
# ADMINISTRIRANJE (Identity Management)

Uključuje kreiranje, brisanje i ažuriranje naloga, promena nivoa privilegija...

Cilj je da prethodno definisane grupe mapiramo u role tj. u IT role .



# ADMINISTRIRANJE



## AUTENTIFIKACIJA

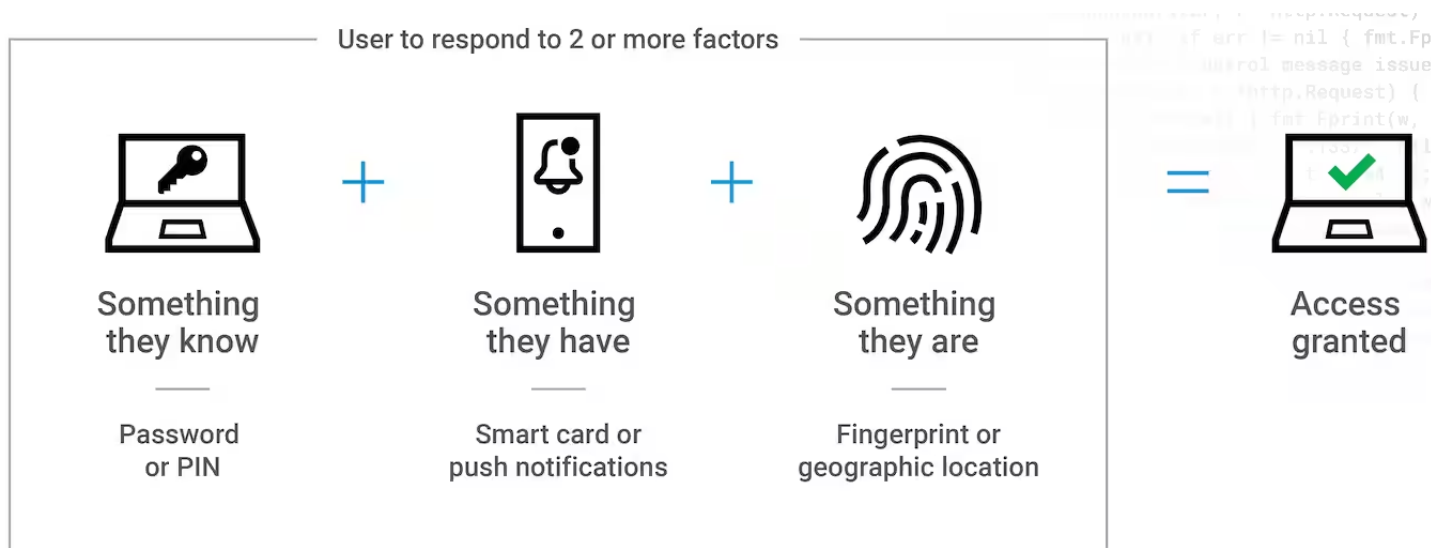
Procesom identifikacije utvrđuje se da li je neka osoba, zaista ona osoba za koju se predstavlja.

U suštini, to su uvek dva vezana procesa koji se nazivaju Identification and Authentication (I&A).

## AUTENTIFIKACIJA

Sistemi ili metodi identifikacije zasnovani su na sledećim faktorima:

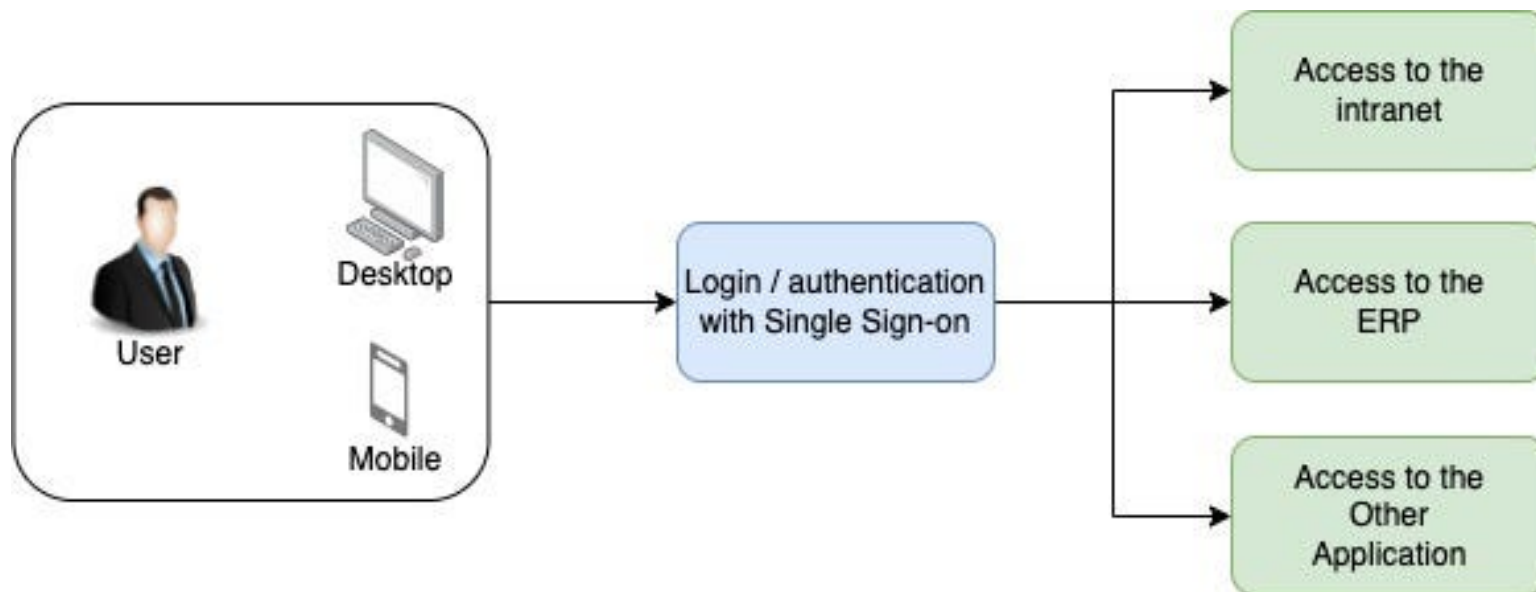
1. Na nečemu što **korisnik zna**, kao što su lozinka ili PIN
2. Na nečemu što **korisnik poseduje**, poput smart kartice ili nekog identifikacijskog uređaja npr. telefona
3. Na nečemu što **fizički određuje korisnika**, kao što su otisak prsta ili izgled lica, oka, boja glasa, DNK skeneri i td.



## SINGLE SIGN ON (SSO) AUTENTIFIKACIJA

Single Sign-On (SSO), ili jednokratna prijava, je tehnika autentifikacije koja omogućava korisnicima da pristupe različitim aplikacijama ili uslugama koristeći samo jedan set podataka za autentifikaciju, kao što su korisničko ime i lozinka.

Cilj SSO-a je da korisnik ima jednu "master" autentifikaciju koja omogućava pristup svim aplikacijama ili uslugama koje podržavaju ovu tehnologiju.



# SINGLE SIGN ON (SSO) ARHITEKTURA

## Provajder identiteta (IdP):

To je sistem koji autentifikuje korisnika i potvrđuje njegov identitet.

IdP obično čuva korisničke podatke i pruža autentifikacijske usluge za različite aplikacije.

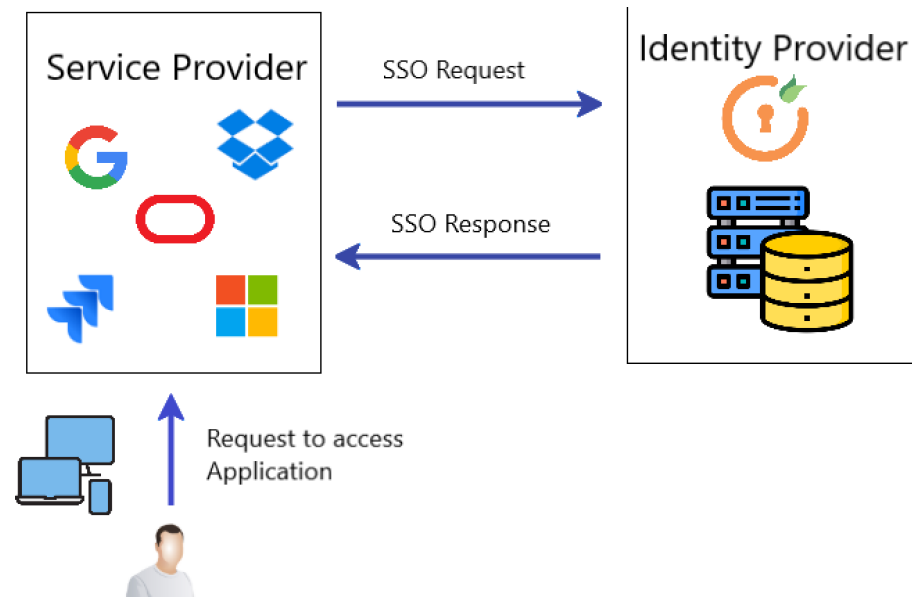
## Provajder usluge (SP):

To je aplikacija ili usluga kojoj korisnik želi pristupiti nakon autentifikacije.

SP prepoznaje i prihvata autentifikacijske podatke koje je korisnik dobio od IdP-a.

## Protokoli za razmenu informacija o autentifikaciji (SAML, OpenID Connect, OAuth, Kerberos):

Koriste se za razmenu informacija o autentifikaciji, autorizaciji i attribute korisnika između provajdera identiteta i provajdera usluge u okviru Single Sign-On (SSO) infrastrukture.



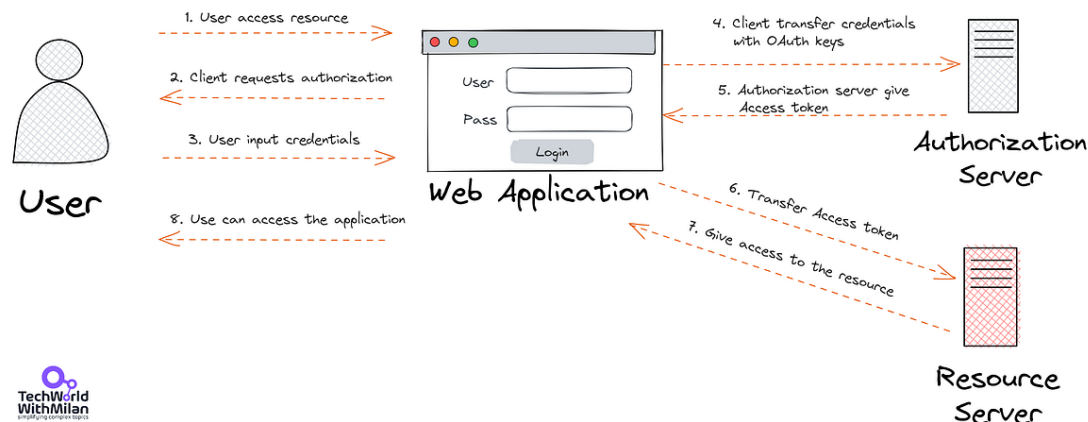
# OAuth 2.0

OAuth 2.0 je otvoren protokol za autorizaciju koji omogućava aplikacijama da dobiju ograničen pristup resursima u ime korisnika bez potrebe da dele svoje korisničko ime i lozinku.

OAuth 2.0 omogućava korisnicima da dele ograničene resurse (kao što su podaci o profilu ili slike) sa trećim stranama (aplikacijama) uz njihov pristanak.

OAuth 2.0 je široko korišćen u raznim aplikacijama i servisima širom interneta, uključujući društvene mreže, cloud servise, mobilne aplikacije i mnoge druge.

Omogućava korisnicima kontrolisano deljenje svojih podataka sa trećim stranama, uz visok nivo sigurnosti i privatnosti.

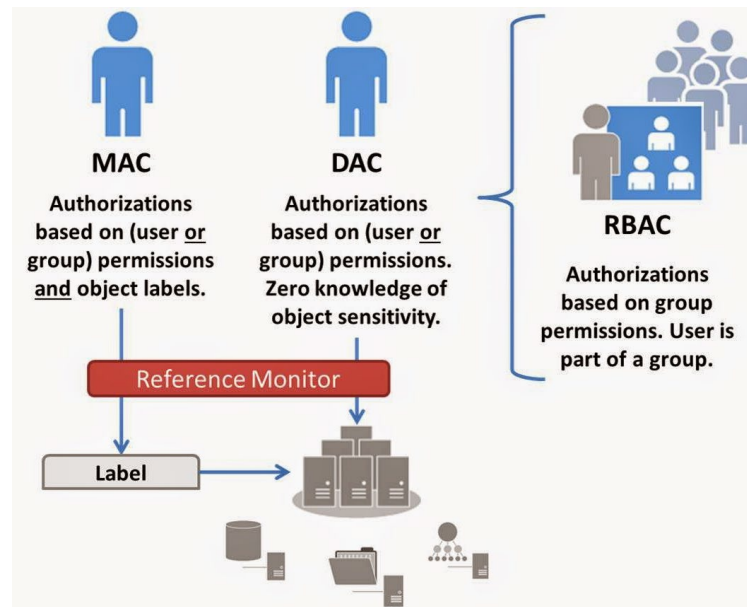


# KONTROLA PRISTUPA (AUTORIZACIJA)

Kontrola pristupa reguliše koji korisnici, aplikacije i uređaji mogu da uređuju, dodaju i brišu resurse.

Kontrola pristupa je jedna od ključnih praksi za zaštitu osetljivih podataka od krađe, zloupotrebe i drugih pretnji.

Postoje dva nivoa kontrole pristupa: fizički i logički.



# KONTROLA PRISTUPA (AUTORIZACIJA)

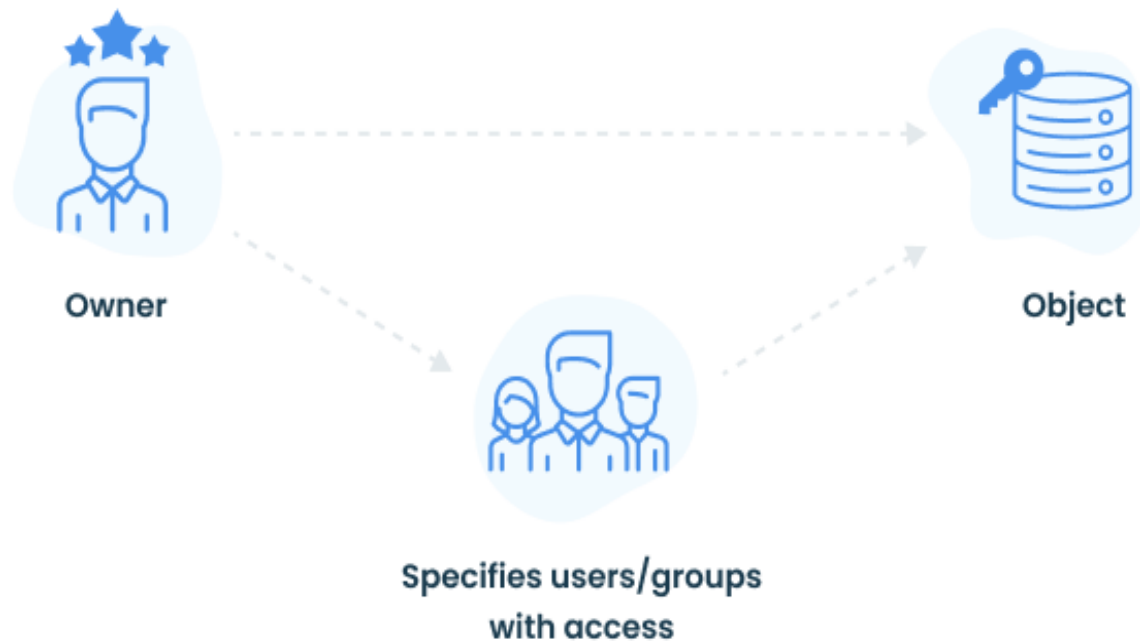
**Mandatory Access Control (MAC)**, obavezna kontrola pristupa predstavlja statički model koji koristi unapred definisani skup prava pristupa ka resursima u nekom računarskom sistemu.

Parametre definiše sistem administrator koji ih dodeljuje nalozima, datotekama ili resursima i koristi labele za definisanje nivoa osjetljivosti.



# KONTROLA PRISTUPA (AUTORIZACIJA)

**Discretionary Access Control (DAC)**, proizvoljna kontrola pristupa predstavlja model prava pristupa koji definiše vlasnik podataka-resursa. U ovom modelu labele nisu obavezne. DAC model omogućava deljenje datoteka između korisnika, odnosno rad sa datotekama koje je neka druga osoba proglasila djeljivim.



# KONTROLA PRISTUPA (AUTORIZACIJA)

**Role-Based Access Control (RBAC)**, kontrola pristupa na osnovu uloga, predstavlja model koji definiše ulogu koju korisnik ima u organizaciji.

Korisnicima se dodjeljuju određene uloge na nivou čitavog sistema, na osnovu kojih oni obavljaju određene funkcije ili dužnosti.

RBAC model uobičajen je za razne uloge administratora na mreži.

