# Autentifikacija s dvostrukim faktorom

**Almaši, Ivan**

**Master's thesis / Diplomski rad**

**2015**

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **Josip Juraj Strossmayer University of Osijek, Faculty of Electrical Engineering / Sveučilište Josipa Jurja Strossmayera u Osijeku, Elektrotehnički fakultet**

*Permanent link / Trajna poveznica:* https://urn.nsk.hr/urn:nbn:hr:200:469654

*Rights / Prava:* In copyright / Zaštićeno autorskim pravom.

*Download date / Datum preuzimanja:* **2025-03-21**

*Repository / Repozitorij:*

Faculty of Electrical Engineering, Computer Science and Information Technology Osijek

**SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU**
**ELEKTROTEHNIČKI FAKULTET**

**Sveučilišni studij**

# AUTENTIFIKACIJA S DVOSTRUKIM FAKTOROM

**Diplomski rad**

**Ivan Almaši**

**Osijek, 2015.**

# Sadržaj

1. UVOD ..... 1
1.1. Zadatak diplomskog rada ..... 1
2. KORIŠTENE TEHNOLOGIJE ..... 2
2.1. HTML ..... 2
2.2. CSS ..... 2
2.3. JavaScript ..... 3
2.4. PHP ..... 4
2.4.1. Laravel programski okvir ..... 5
2.5. MySQL ..... 6
2.6. Android ..... 6
2.6.1. Java ..... 7
2.6.2. XML ..... 7
2.7. QR kod ..... 8
2.7.1. Kreiranje QR kodova ..... 8
2.7.2. Skeniranje QR kodova ..... 9
3. AUTENTIFIKACIJA S DVOSTRUKIM FAKTOROM ..... 10
3.1. RFC 4226 ..... 10
3.1.1. Zahtjevi algoritma ..... 10
3.1.2. HOTP algoritam ..... 11
3.1.3. Zahtjevi protokola za autentifikaciju ..... 13
3.1.4. Potvrda HOTP vrijednosti ..... 13
3.1.5. Proporcionalnost na poslužitelju ..... 14
3.1.6. Ponovna sinkronizacija brojača ..... 14
3.1.7. Upravljanje dijeljenim tajnama ..... 15
3.2. RFC 6238 ..... 15
3.2.1. Zahtjevi algoritma ..... 15

3.2.2. TOTP algoritam ..... 16
3.2.3. Provjera i veličina vremenskog koraka ..... 16
3.2.4. Ponovna sinkronizacija ..... 18
3.3. Stvaranje jednokratne zaporke po RFC 6238 ..... 18
4. SUSTAV ZA AUTENTIFIKACIJU S DVOSTRUKIM FAKTOROM ..... 20
4.1. Web aplikacija ..... 20
4.1.1. Izgled i kretanje kroz web aplikaciju ..... 20
4.1.2. Funkcionalnost web aplikacije ..... 25
4.1.3. Izrada web aplikacije ..... 28
4.2. Android aplikacija ..... 30
4.2.1. Izgled i kretanje kroz Android aplikaciju ..... 30
4.2.2. Funkcionalnost Android aplikacije ..... 33
4.2.3. Izrada Android aplikacije ..... 34
5. ZAKLJUČAK ..... 36
LITERATURA ..... 37
SAŽETAK ..... 39
ABSTRACT ..... 40
ŽIVOTOPIS ..... 41
PRILOZI (na CD-u) ..... 42

# SAŽETAK

U sklopu ovog diplomskog rada izrađen je sustav za autentifikaciju s dvostrukim faktorom. Sustav se sastoji od web i Android aplikacije, te omogućava korištenje autentifikacije s dvostrukim faktorom prema memorandumima RFC 4226 i RFC 6238. Svaki korisnik nakon registracije na web stranicu može uključiti autentifikaciju s dvostrukim faktorom za bolju zaštitu svog korisničkog računa. Prilikom aktivacije korisniku su prikazane sve upute i link za preuzimanje Android aplikacije, koja stvara jednokratnu zaporku potrebnu za korištenje autentifikacije s dvostrukim faktorom. Kako bi se spriječile neugodnosti korisnika prilikom prijave u svoj korisnički račun, za aktivaciju autentifikacije s dvostrukim faktorom potrebno je upisati ispravnu jednokratnu zaporku, stvorenu pomoću Android aplikacije, za taj korisnički račun.

**Ključne riječi:** autentifikacija s dvostrukim faktorom, web, Android, memorandum, RFC 4226, RFC 6238

## ABSTRACT

System for the two factor authentication was created as a part of this graduation paper. System consists of web and Android application and allows usage of two factor authentication following the RFC 4226 and RFC 6238 memos. After registration on the website, every user can turn on the two factor authentication for the better protection of her or his own user account. All the instructions and download link for the download of the Android application, which creates the one-time password needed for two factor activation, are shown to the user during the activation process. To prevent user inconvenience with logging in to her or his own user account, for the activation of two factor activation, it is required to enter correct one-time password, created with the Android application, for that user account.

**Keywords:** two factor authentication, web, Android, memo, RFC 4226, RFC 6238