Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 621.39
DOI: https://doi.org/10.24867/13BE25Vuletas

PROVERA IDENTITETA KORISNIKA KORIŠĆENJEM QR KODA

USERS AUTHENTICATION USING QR CODE

David Vuletaš, *Fakultet tehničkih nauka, Novi Sad*

Oblast – SOFTVERSKO INŽENJERSTVO I INFORMACIONE TEHNOLOGIJE

Kratak sadržaj – *U radu je opisan sistem za dvostruku verifikaciju identiteta korisnika skeniranjem QR koda, arhitektura aplikacije, komunikacija, model komponenti.*

Ključne reči: *QR kod, bezbednost, 2FA, Dvostruka verifikacija identiteta, C4 model*

Abstract – *The paper describes a system for two factor verification of user identity by scanning a QR code, application architecture, communication, component model..*

Keywords: *QR code, security, 2FA, Two factor verification of identity, C4 model*

1. UVOD

Dvostruka verifikacija identiteta korisnika rešava neke od problema u očuvanju bezbednosti naloga dodavanjem dodatnog sloja bezbednosti. To zahteva izvršavanje još jednog dodatnog koraka od strane korisnika neposredno pre pristupanja resursu [1].

Koncept verifikacije identiteta korisnika u ovom radu ogleda se kroz dva faktora. Prvi faktor predstavlja uobičajeni postupak unošenja korisničkog imena i lozinke putem forme u okviru aplikacije. Kao dodatni odnosno drugi faktor predstavlja skeniranje QR (Quick Response) koda putem mobilne aplikacije uz pomoć koje se potvrđuje identitet korisnika [1].

U ovom radu će biti predstavljen sistem za generisanje QR koda kao i očitavanje pomenutog koda u cilju uspešnog omogućavanja koncepta dvostruke verifikacije identiteta korisnika, prikaz arhitekture sistema, odnosno od čega se sastoji ovaj sistem. S obzirom da je bezbednost veoma bitna kod ovakvih sistema, biće prikazano na koji način se generiše bezbedan QR kod i kako je jedino moguće pročitati vrednost tog koda.

2. TEORIJSKE OSNOVE

Za razumevanje rada potrebno je poznavanje pojmova kao što su QR kod, i dvostruka verifikacija korisničkog identiteta (2FA).

2.1. QR kod

Kao i kod razvoja mnogih tehnologija, QR kodovi su stvoreni iz nužde. QR kodovi su zapravo počeli kao bar kodovi sa svojom namenom u supermarketima.

Pre nego što su postojali bar kodovi, blagajnici su morali ručno da unose pojedinačne predmete, s obzirom da je to uzimalo dosta vremena poslodavci su shvatili da im je potreban način da sve prate [2].

QR kodovi predstavljaju dvodimenzionalne (matrice) kodove koji su razvijeni na način da u njih mogu da se jednostavno smeste informacije kao što su web adrese ili lokacije na mapi koji mobilni uređaj može brzo i jednostavno da skenira. Struktura QR koda je prikazana na slici u nastavku (Slika 2.1).

Slika 2.1. *Struktura QR koda* [3]

2.1.1. Generisanje QR koda

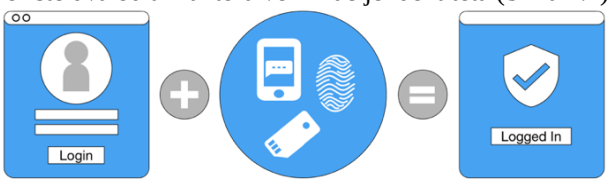
Proces kreiranje QR koda se svodi na 7 značajnih koraka: Analiza podataka, kodiranje podataka, kodiranje ispravke greške, strukturiranje završne poruke, smeštanje modula u matricu, maskiranje podataka i dodavanje informacija o formatu i verziji [4] .

2.2. Dvostruka verifikacija korisničkog identiteta (2FA)

Dvostruka verifikacija korisničkog identiteta vezuje se za moderne tehnologije, takođe se naziva i više faktorska verifikacija korisničkog identiteta. Tradicionalni postupak verifikacije korisničkog identiteta pruža samo jedan faktor, obično nešto što korisnik može veoma lako da zapamti, lični brojevi (PIN) i lozinke su tipični primeri ove vrste verifikacije [5].

Načini upotrebe dvostruke verifikacije identiteta korisnika koji se često koriste su putem SMS poruke, mobilne aplikacije, upotrebe USB uređaja za dodatnu potvrdu identiteta korisnika.

Dvostruka verifikacija korisničkog identiteta predstavlja veći izazov za korisnika zbog toga što je potrebno da se koriste dva od tri faktora verifikacije identiteta (Slika 2.2).



Slika 2.2. *Pristup servisu korišćenjem višestruke verifikacije identiteta korisnika [5]*

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Goran Sladić, vanr. prof.

2.2.1. Google-ova implementacija dvostruke verifikacije identiteta

U cilju očuvanja bezbednosti naloga korisnika, Google podržava više opcija za dvostruku verifikaciju identiteta. Jedna opcija predstavljena je korišćenjem mobilne aplikacije Google Authenticator, dok se druga opcija ogleda u korišćenju servisa notifikacija Google-a [6].

2.2.2. Microsoft-ova implementacija dvostruke verifikacije identiteta

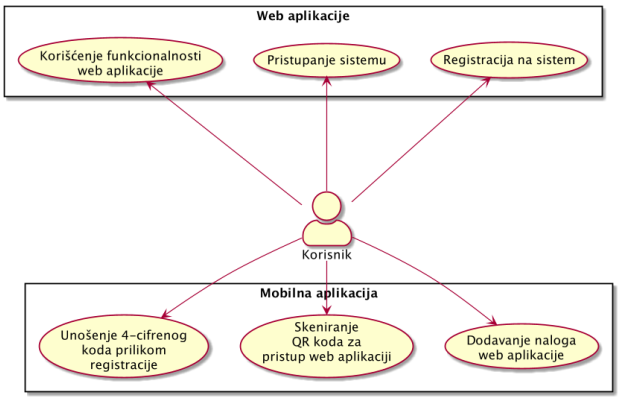
Microsoft omogućava svojim korisnicima pristup resursima na siguran način. Microsoft Authenticator se često koristi u većim kompanijama gde je potrebno postići dodatni nivo bezbednosti postavljanjem dvostruke verifikacije identiteta [7].

2.2.3. Okta Verify aplikacija

Kompanija Okta je razvila platformu za skladištenje aplikacija na jedan nalog, gde se jednostavno prilikom pristupanja sistemu korisniku omogućuje da pristupi bilo kojoj aplikaciji sa kojom je integracija izvršena. Okta Verify je aplikacija koja je podržana za iOS kao i za Android platformu [8].

3. MODEL SISTEMA

Broj funkcionalnosti koje korisnik može da izvrši korišćenjem ovog sistema nije velik, zbog toga što je glavni fokus sistema na bezbednom generisanju QR koda, kao i očitavanju. Dijagram korišćenja prikazan je u nastavku (Slika 3.1).

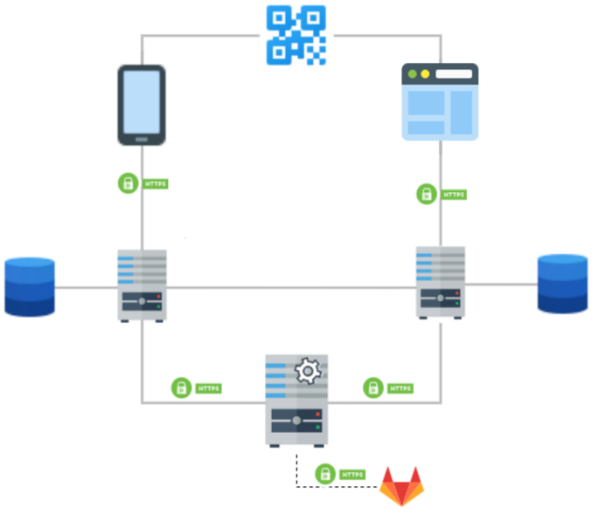


Slika 3.1. *Dijagram korišćenja sistema*

3.1. Arhitektura sistema

Glavne komponente koje čine ovakav sistem su: web aplikacija, mobilna aplikacija, konfiguracioni server kao i baze podataka. Pomenute komponente su prikazane na slici u nastavku (Slika 3.2).

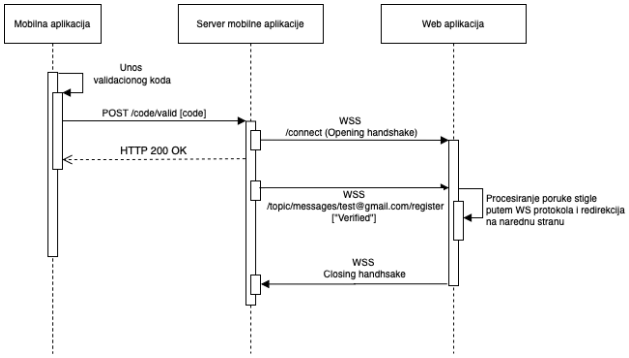
Korisnik web aplikaciju koristi za obavljanje funkcionalnosti koje pripadaju sklopu oblasti za koje je ona namenjena. Da bi korisnik uspeo uspešno da pristupi web aplikaciji potrebno da je potvrdi identitet putem mobilne aplikacije. Korisnik pomoću aplikacije skenira QR kod i na taj način verifikuje svoj identitet. Postojanje konfiguracionog servera ogleda se u smeštanju ključeva koji se koriste za kodiranje podataka prilikom kreiranja QR koda, takođe kao što je potrebno postojanje ključeva za kodiranje tako je i potrebno imati i ključeve za dekodiranje podataka koji se nalaze u QR kodu.



Slika 3.2 *Komponente sistema*

Baza podataka je zadužena za čuvanje podataka web aplikacije i mobilne aplikacije. Podaci koji se najčešće čuvaju su vezani za informacije o QR kodovima i korisnicima.

Prilikom uspostavljanja komunikacije između komponenti sistema koriste se dva načina uspostavljanja komunikacije. Komunikacija između klijenta i servera web aplikacija kao i mobilne aplikacije ostvaruje se putem HTTP protokola odnosno njegovo korišćenje je uspostavljeno putem RESTful servisa. Komunikacija između mobilne aplikacije i web aplikacije se ostvaruje korišćenjem Web socket-a protokola. Na slici u nastavku je prikazan primer komunikacije između mobilne i web aplikacije korišćenjem Web socket protokola.



Slika 3.3. *Komunikacija putem Web socket protokola*

4. IMPLEMENTACIJA

Da bi na bezbedan način sistem funkcionisao potrebno je ispravno izvršiti generisanje QR koda. Jedan od izazova prilikom izrade aplikacije bio je izabrati najbezbedniji način za generisanja QR koda. Potrebno je bilo odabrati da li će se kod generisati na strani web aplikacije odnosno na klijentskom delu korišćenjem biblioteka za generisanje slika koji će momentalno generisati korisniku QR kod ili je to bolje uraditi na strani web servera pa na neki način dostaviti to na klijentsku aplikaciju koja će samo prikazati podatke u vidu QR koda.

Otvoreni tekst QR koda u sistemu za verifikaciju identiteta predstavljen je strukturom JSON objekta sa poljima koja su prikazana u nastavku (slika 4.1)

```
{
    "email": "master@gmail.com",
    "generatedTime": "01-11-2020 20:30",
    "validTimeUntil": "01-11-2020 20:35"
}
```


Slika 4.1. *QR kod otvorenog teksta*

4.1.1. Šifrovanje podataka

Za šifrovanje podataka iz otvorenog teksta korišćen je AES algoritam. AES algoritam predstavlja bezbedni algoritam simetričnog šifrovanja, odnosno to znači da pripada grupi algoritama gde se sa istim ključem može izvršiti šifrovanje i dešifrovanje te je veoma bitan način na koji se vrši dostavljanje ključeva ovim stranama [9]

Kod implementiran u programskom jeziku Java prikazan je u nastavku (Listing 4.1).

```
public static String encryptData(String data) {
    try {
        IvParameterSpec iv = new IvParameterSpec(
                secretInitialFromProperties.
                getBytes(StandardCharsets.UTF_8));
        SecretKeySpec skeySpec = new SecretKeySpec(
                secretKeyFromProperties.
                getBytes(StandardCharsets.UTF_8), "AES");

        Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5PADDING");
        cipher.init(Cipher.ENCRYPT_MODE, skeySpec, iv);
        byte[] encrypted = cipher.doFinal(data.getBytes());
        return Base64.getEncoder().encodeToString(encrypted);
    } catch (Exception e) {
        log.error("Error while encrypting: " + e.toString());
    }
    return null;
}
```

Listing 4.1. *Šifrovanje korišćenjem AES algoritma*

4.1.2. Kreiranje sadržaja QR koda

Nakon što su podaci šifrovani i više se ne nalaze u obliku otvorenog teksta, na kraj niza podataka se dodaje tekst otvorenog oblika koji daje informaciju kojoj aplikaciji je namenjen QR kod tako da bi aplikacija znala da čita isključivo kodove koji su namenjeni njoj.

Generisanje QR koda se vrši korišćenjem Google-ove biblioteke ZXing [10] implementirane u Javi koja je namenjena za obradu slika u jednoj ili dve dimenzije za rad sa kodovima. Implementacija generisanja koda prikazana je u nastavku (Listing 4.2)

```
public String generateQRCode(String email) {
    QRCode valueOfQRCode = QRCode.builder()
        .email(email).build();
    valueOfQRCode.generateNewTime();
    String data =  EncryptionAlgorithm
        .encryptData(valueOfQRCode.asString());
    data += ";applicationName: finance";
    BitMatrix matrix = null;
    ByteArrayOutputStream outputStream =
        new ByteArrayOutputStream();
    try {
        matrix = qrCodeWriter.encode(data,
         BarcodeFormat.QR_CODE, 350, 350);
        MatrixToImageWriter
                .writeToStream(matrix,
                        "PNG", outputStream);
    } catch (WriterException e) {
        log.error("Error while
                generating QR code
                {}", e.getMessage());
    }
    String base64bytes = Base64.getEncoder()
        .encodeToString(
                outputStream.toByteArray());
    return "" + base64bytes;
}
```

Listing 4.2. *Generisanje QR koda*

4.1.3. Prikazivanje QR koda

Nakon što web server izvrši generisanje QR koda i dostavi ga web aplikaciji, potrebno je da aplikacija prikaže korisniku QR kod kako bi on mogao da ga očita, i time nastavi korišćenje sistema.

QR kod je ograničen vremenom, odnosno čitanje i verifikacija koda moguća je isključivo u određenom vremenskom opsegu koji se definiše prilikom generisanja kao jedan od parametara.

Zbog prethodno navedenog ograničenja, korisniku je potrebno na neki način predstaviti informaciju o vremenskom opsegu u kome može da izvrši očitavanje koda.

Ukoliko korisnik ne izvrši skeniranje u vremenu određenom za to, odnosno ako tajmer prikaže da je vreme za skeniranje QR koda isteklo, korisniku će biti prikazan taster za ponovno generisanje QR koda. Nakon što korisnik klikne na dugme za ponovno generisanje QR koda, web aplikacija će pozvati server da generiše kod koji se sada sastoji od istih podataka dok će jedino vreme važenja i generisanja biti drugačije.

4.1.4. Očitavanje i prikaz informacija QR koda

Generisani QR kod koji je prikazan korisniku putem web aplikacije u web pretraživaču sadrži informacije na osnovu kojih korisnik može da potvrdi svoj identitet. Da bi korisnik potvrdio svoj identitet potrebno je da poseduje mobilnu aplikaciju koja poseduje logiku za očitavanje podataka i verifikaciju identiteta korisnika.

S obzirom da su podaci iz QR koda zaštićeni šifrovanjem podataka, ukoliko bilo koji korisnik pokuša da očita kod korišćenjem raznih aplikacija za skeniranje kodova, dobiće podatke ali mu oni ništa neće značiti zbog toga što su zaštićeni i predstavljaju tekst koji nema nikakvo značenje, odnosno neće znati kojem korisniku su namenjeni kao i druge informacije koje kod sadrži.

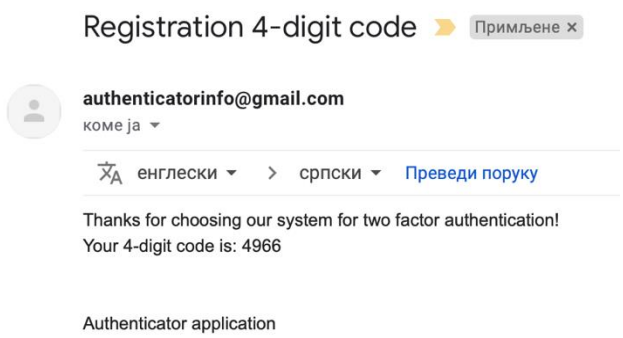
4.1.5. Komuniciranje mobilne i web aplikacije nakon uspešnog skeniranja koda

Nakon što korisnik putem mobilne aplikacije uspešno izvrši očitavanje QR koda, potrebno je obavestiti korisnika u web aplikaciji da je njegov QR kod uspešno očitan i da može nastaviti korišćenje web aplikacije.

S obzirom da mobilna aplikacije nema direktnu vezu sa web aplikacijom putem HTTP-a, komunikacija se ostvaruje korišćenjem WS (WebSocket) protokola. Komunikacija korišćenjem web socket-a ostvarena je između servera mobilne aplikacije i korisničkog dela web aplikacije.

4.1.6 Generisanje koda za potvrdu identiteta prilikom registracije

Prilikom procesa registracije na sistem posle korisnikovog skeniranja QR koda putem mobilne aplikacije potrebno je da se izvrši još jedan korak koji predstavlja dodatni nivo bezbednosti prilikom registracije, a to je unos jedinstvenog koda koji je prilikom registracije poslat korisniku putem mail-a. (primer mail-a koji stiže korisniku prilikom registracije, Slika 4.2)



Slika 4.2. *Unos koda putem mobilne aplikacije*

5. ZAKLJUČAK

Glavni fokus rada bio je opisati kompletan proces generisanja bezbednog QR koda, počev od podataka koje QR kod sadrži te opisa algoritma za šifrovanje pomenutih podataka, smeštanje šifrovanih podataka u QR, prikazivanja koda korisniku putem web aplikacije kao i međusobno komuniciranje između web aplikacije i mobilne aplikacije nakon uspešnog očitavanja koda. S obzirom da je jedinstvenost QR koda veoma bitna, objašnjeno je čemu služi jedinstveni kod prilikom registracije kao i na koji način se sprečava ponovno očitavanje već generisanog QR koda

Dodatna unapređenja u sistemu za dvostruku verifikaciju identiteta koja se mogu dodati su vezana najviše za distribuciju ključeva između web aplikacija i mobilne aplikacije, a takođe i jedna veoma bitna stvar je da se omogući postavljanje servera mobilne i web aplikacije na neki od Cloud provajdera (Google, Amazon, itd.) da bi se aplikaciji moglo pristupati i van mreža na kojima se nalaze serveri. Nakon što bi se servisi izvršavali na platformama nekih od Cloud provajdera, bilo bi potrebno i omogućiti da se mobilne aplikacije mogu preuzeti preko nekih od poznatih IOS i Android prodavnica kao što su Google Play i App Store.

6. LITERATURA

[1] Brian P. Sutton “The Effects of Technology in Society and Education,, 2013 https://digitalcommons.brockport.edu/cgi/viewcontent.cgi?article=1196&context=ehd_theses (pristupljeno u januaru 2021.)

[2] Ako Muhammad Abdullah, Roza Hikmat Hama Aziz “Evaluating the Use of Quick Response (QR) Code at Sulaimani University Libraries” 2014 https://www.researchgate.net/publication/270879583 (pristupljeno u januaru 2021.)

[3] Zhongpai Gao, Guangtao Zhai and Chunjia Hu “The Invisible QR Code” 2015 https://www.researchgate.net/publication/309350866 (pristupljeno u januaru 2021.)

[4] Shuai Chen, “Evaluation of Two-Dimensional Codes for Digital Information Security in Physical Documents“, https://scholarworks.umass.edu/cgi/viewcontent.cgi?article=1235&context=masters_theses_2 (pristupljeno u januaru 2021.)

[5] Jori Kymäläinen, “IMPLEMENTING TWO-FACTOR AUTHENTICATION”, 2018 https://www.theseus.fi/bitstream/handle/10024/145670/Thesis_Jori_Kymalainen.pdf?sequence=1&isAllowed=y (pristupljeno u januaru 2021.)

[6] Google, American company https://www.britannica.com/topic/Google-Inc (pristupljeno u januaru 2021.)

[7] About Microsoft, https://www.microsoft.com/en-us/about (pristupljeno u januaru 2021.)

[8] Okta Verify, https://help.okta.com/en/prod/Content/Topics/Mobile/okta-verify-overview.htm (pristupljeno u januaru 2021.)

[9] Mahmoud A. eltatar, “Modified Advanced Encryption Standard Algorithm for Reliable Real-Time Communications” Dec/2017 https://library.iugaza.edu.ps/thesis/123123.pdf (pristupljeno u januaru 2021.)

[10] ZXing image processing library, Javadoc https://zxing.github.io/zxing/apidocs/ (pristupljeno u januaru 2021.)

Kratka biografija:

David Vuletaš je rođen 25. oktobra 1995. godine u Zrenjaninu, Republika Srbija. Godine 2014. upisao je Fakultet Tehničkih nauka u Novom Sadu smer Softversko inženjerstvo i informacione tehnologije. 2018. godine diplomirao je na osnovnim studijama na Fakultetu Tehničkih nauka, iste godine potom upisuje Master studije na smeru Softversko inženjerstvo i informacione tehnologije.