



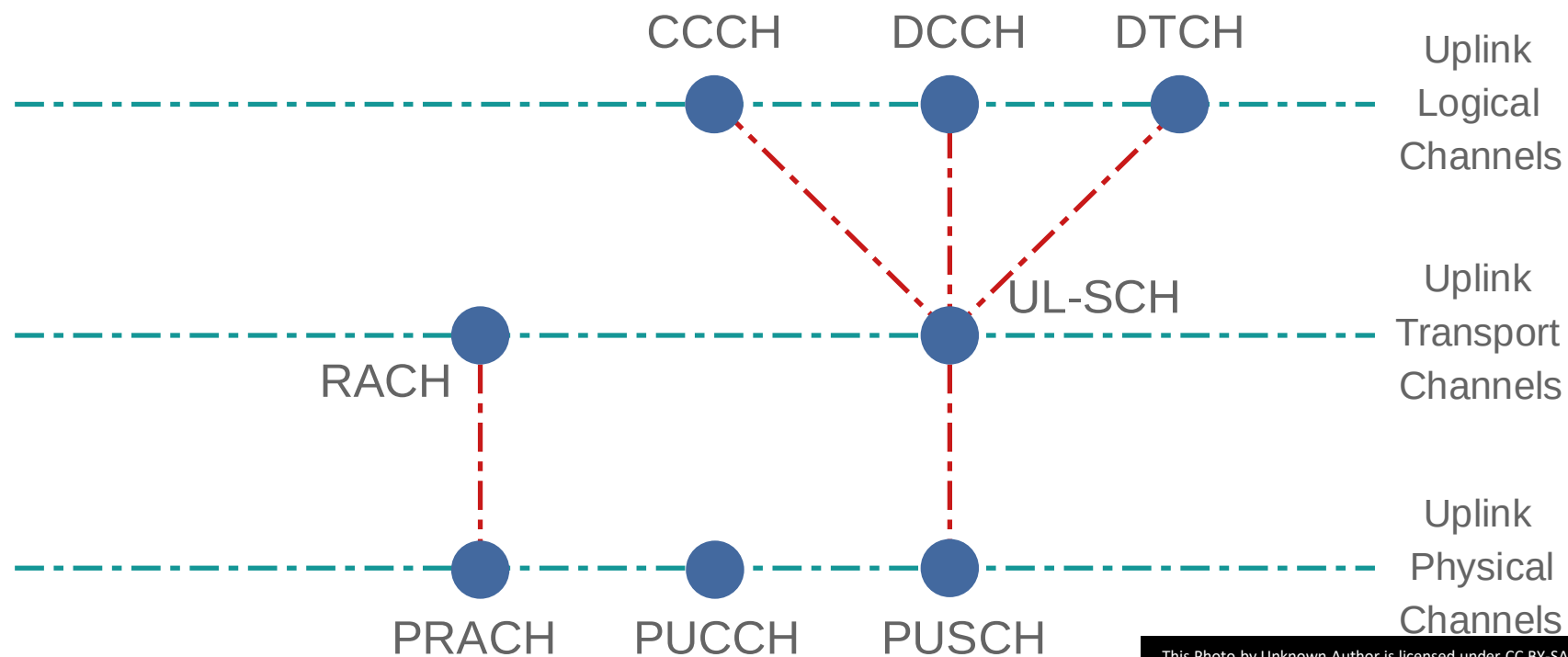
Elektronsko bankarstvo

- Elektronsko bankarstvo koristi digitalne tehnologije za obavljanje bankarskih usluga putem interneta, aplikacija i bankomata.
- Elektronsko poslovanje omogućava brže, efikasnije i globalno dostupno poslovanje uz smanjenje troškova i poboljšanje korisničkog iskustva.

Uvod u elektronsko bankarstvo

Ključni elektronski kanali

- Internet
- Mobilne aplikacije
- Bankomati



Funkcije e-bankarstva

- Provera stanja

- Prenos novca

- Plaćanje računa

- Upravljanje karticama

- Kreditni zahtevi

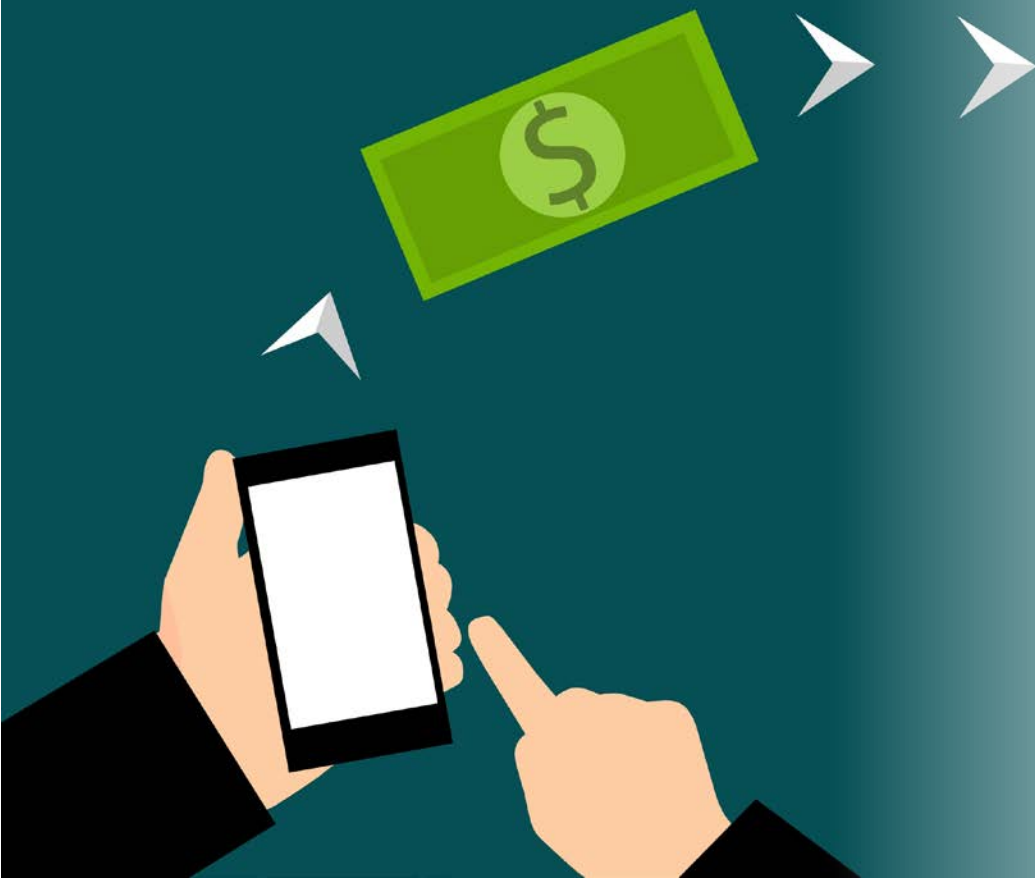
Provera stanja na računu

- Provera stanja je usluga elektronskog bankarstva koja korisniku omogućava da u svakom trenutku vidi trenutno raspoloživo stanje na svom bankovnom računu putem interneta, mobilne aplikacije ili bankomata.
- Proverom stanja korisnik može pratiti prilive i odlive sa računa i kontrolisati lične finansije u realnom vremenu.



This Photo by Unknown Author is licensed under [CC BY-SA](#)

Prenos novca



- Omogućava brze transfere između računa, uključujući nacionalne i međunarodne uplate
- SEPA
- SWIFT

SEPA (Single Euro Payments Area) i SWIFT (Society for Worldwide Interbank Financial Telecommunication)

su međunarodni platni sistemi koji omogućavaju sigurne i brze transfere novca između banaka, ali se koriste za različite vrste transakcija

1. SEPA

1. SEPA je evropski platni sistem koji omogućava jednostavne i brze transfere unutar eurozone. Koristi se za prenos novca u evrima između zemalja članica EU, kao i nekoliko drugih zemalja.
2. Omogućava jednaku jednostavnost plaćanja kao domaći transferi unutar jedne zemlje.

2. SWIFT

1. SWIFT je globalni sistem koji omogućava međunarodne banke da međusobno razmenjuju platne informacije. Koristi se za slanje i primanje međunarodnih uplata u različitim valutama.
2. SWIFT kodovi identifikuju banke koje učestvuju u transferima.

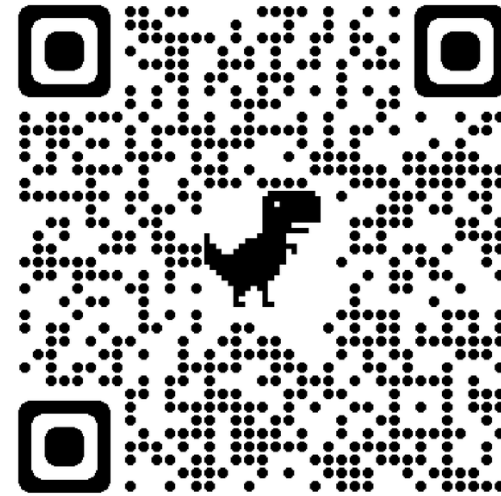
Oba sistema omogućavaju sigurne i efikasne međunarodne uplate, ali SEPA je specifičan za eurozonu, dok SWIFT pokriva globalne transfere u različitim valutama.



Pláćanje računa

Plaćanje putem QR koda,

- Plaćanje putem QR koda omogućava korisnicima da brzo i sigurno izvrše transakcije skeniranjem koda sa mobilnog uređaja, dok skeniranje uplatnica omogućava automatsko popunjavanje podataka za plaćanje, a podešavanje automatskih plaćanja omogućava redovne transakcije na unapred određeni datum, što sve doprinosi većoj efikasnosti i praktičnosti u upravljanju finansijama.



This Photo by Unknown Author is licensed under [CC BY-SA](#)

IPS (Instant Payments System)



- **IPS (Instant Payments System)** je sistem za instant plaćanja koji omogućava momentalne transfere novca između različitih banaka u realnom vremenu, 24/7, bez obzira na praznike ili vikende. Koristi se za brzo i sigurno plaćanje između računa unutar iste zemlje, omogućavajući korisnicima da odmah šalju i primaju novac, što je korisno za online kupovine, plaćanje usluga ili hitne transfere.



Upravljanje karticama

Mogućnost

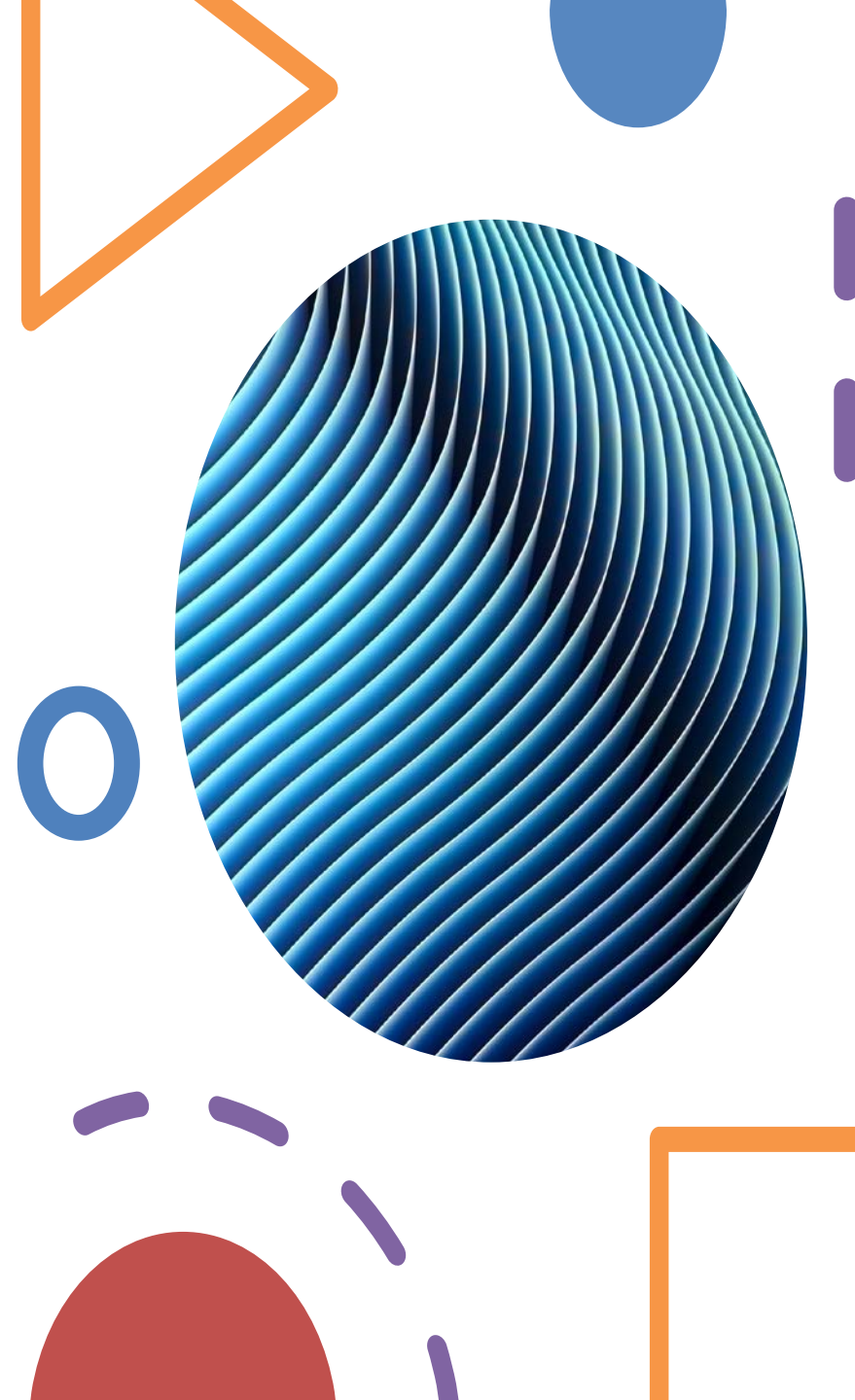
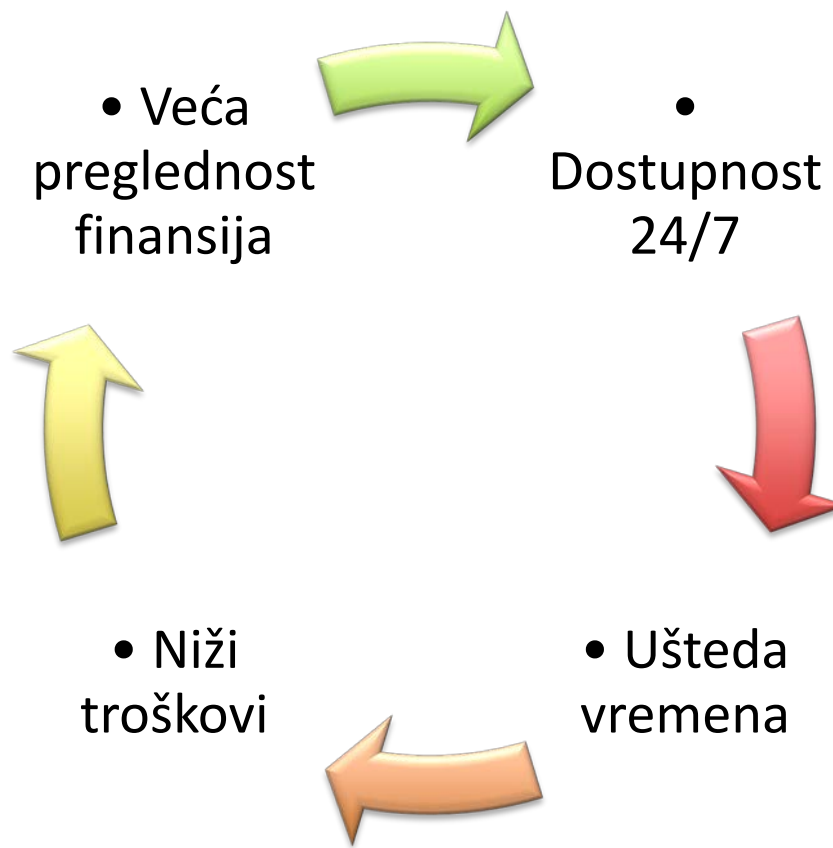
- blokiranja,
- aktivacije,
- podešavanja limita
- nadzora troškova.

Zahtevi za kredite

Kroz elektronsko bankarstvo, korisnici mogu jednostavno podneti zahtev za kredit putem online platforme, što uključuje unos ličnih podataka, iznos kredita i tražene uslove. Uz to, sve potrebne dokumente, poput potvrda o zaposlenju, prihodu ili kreditnoj istoriji, korisnici mogu učitati direktno na platformu ili aplikaciju banke.



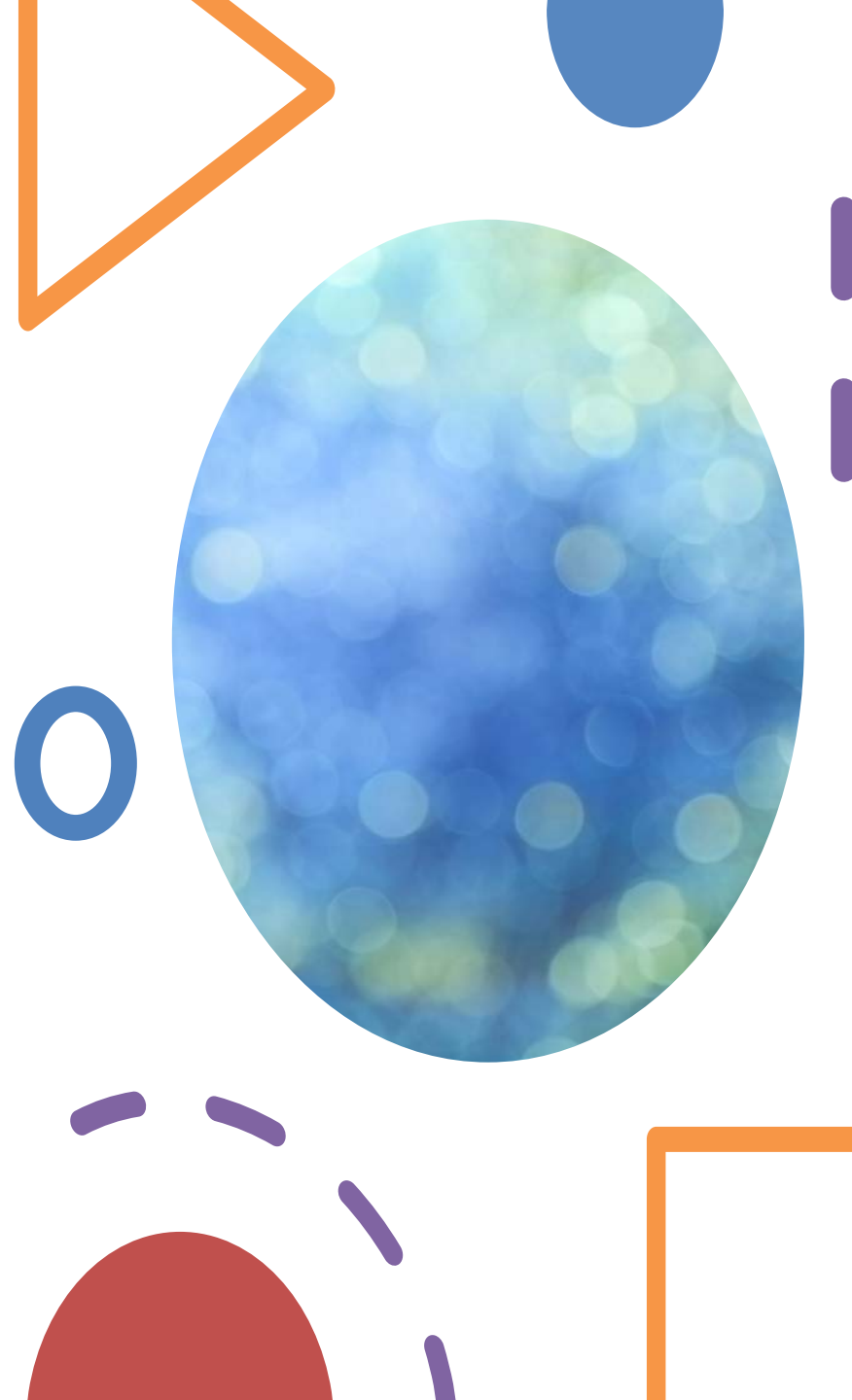
Prednosti e-bankarstva



Nakon što banka pregleda i obradi zahtev, korisnik može potpisati ugovor elektronski, koristeći digitalni potpis ili autentifikaciju putem SMS koda ili biometrijskih podataka (npr. otisak prsta).



Ovaj proces omogućava bržu i sigurniju obradu kredita, bez potrebe za fizičkom prisutnošću klijenta u banci, čime se ubrzava postupak i smanjuje administrativni rad.



Rizici e-bankarstva

- Mogućnost hakerskih napada

- Phishing i krađa identiteta

- Tehnički problemi

Bezbednosne tehnologije

- Enkripcija podataka
- Tokeni
- Biometrijska autentifikacija

Pametne kartice

Kartice sa čipom (poznate i kao **EMV kartice**) koriste čip za zaštitu podataka i obavljanje sigurnih transakcija.

1. **Sigurnost** – Čip kartice generiše dinamičke podatke tokom svake transakcije, što čini teško presrećivanje ili falsifikovanje podataka, u poređenju sa tradicionalnim magnetnim trakama.
2. **Autentifikaciju korisnika** – Prilikom plaćanja, čip se koristi za autentifikaciju korisnika, čineći transakciju sigurnijom, dok dodatne metode, poput PIN-a ili biometrijske autentifikacije, mogu dodatno osigurati identifikaciju.
3. **Globalna prihvaćenost** – EMV kartice su široko prihvaćene u trgovinama, bankama, bankomatima i online platnim sistemima, omogućavajući korisnicima bezbedno obavljanje transakcija širom sveta



This Photo by Unknown Author is licensed under [CC BY-SA-NC](#)



Autentifikacija sa više faktora

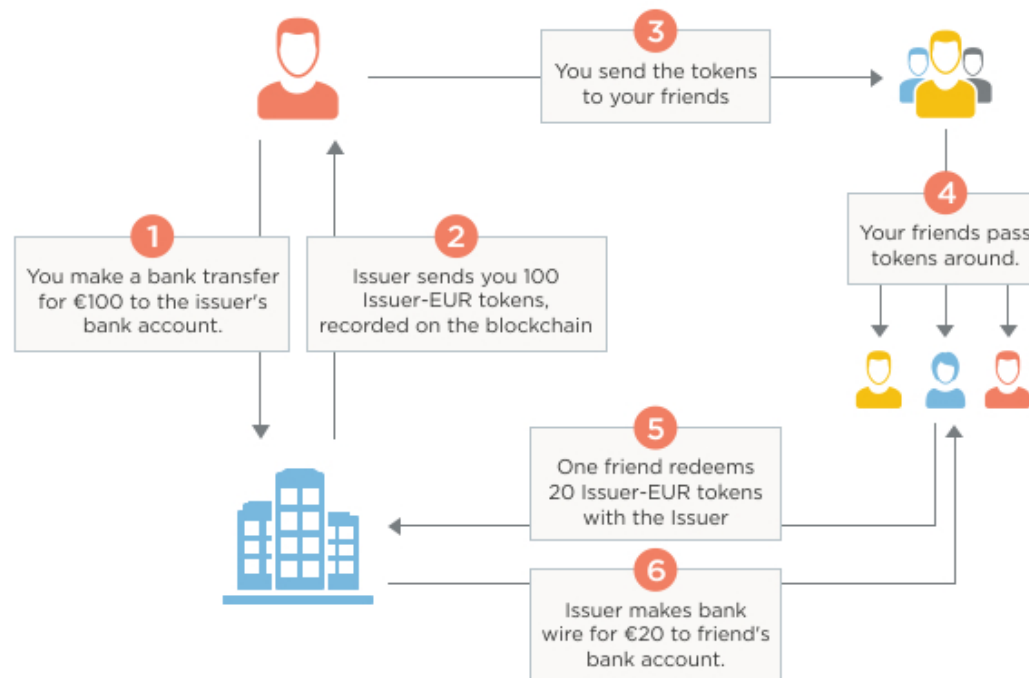
Autentifikacija sa više faktora (MFA) je sigurnosni proces koji zahteva od korisnika da pruži dva ili više oblika autentifikacije pre nego što dobije pristup sistemu ili obavi transakciju. Cilj MFA je da poveća sigurnost, smanjujući rizik od neovlašćenog pristupa.

MFA obično uključuje sledeće faktore:

1. **Nešto što korisnik zna** – Ovo je najčešći faktor, kao što je lozinka ili PIN.
 2. **Nešto što korisnik ima** – To mogu biti uređaji poput mobilnog telefona (koji generišu jednokratne šifre putem aplikacija poput Google Authenticator ili SMS-a) ili fizički tokeni i kartice sa čipom.
 3. **Nešto što korisnik jeste** – Biometrijski podaci poput otiska prsta, prepoznavanja lica ili irisa oka.
- Kombinovanjem ovih faktora, MFA značajno poboljšava sigurnost jer čak i ako neko uspe da ukrade lozinku, neće moći da pristupi sistemu bez drugih faktora, kao što je mobilni telefon ili biometrijska autentifikacija.
 - .

Tokeni i soft tokeni

Uređaji ili aplikacije koje generišu sigurnosne kodove za pristup bankarstvu.





Tokeni

- Token je fizički uređaj (npr. mali uređaj koji generiše jednokratne šifre) koji korisnik nosi sa sobom.
- Uglavnom se koristi za dvofaktorsku autentifikaciju, gde korisnik mora uneti šifru koja se generiše na tokenu zajedno sa svojim korisničkim podacima.
- Tokene koristi većina banaka za potvrdu transakcija ili za prijavu na internet bankarstvo.



Soft tokeni

- Soft tokeni su virtuelni ekvivalenti fizičkih tokena, obično u obliku aplikacije na mobilnim uređajima ili računaru. Ove aplikacije generišu jednokratne šifre ili koriste biometrijsku autentifikaciju za pristup sistemima.
- Soft tokeni su praktičniji jer ne zahtevaju dodatni fizički uređaj, a korisnici mogu lako generisati šifre putem aplikacije (npr. Google Authenticator, banka aplikacije).

E-bankarstvo u Srbiji



Saveti za korisnike

- Ne deliti lozinke

- Koristiti sigurnu mrežu

- Ažurirati aplikacije

- Aktivirati 2FA