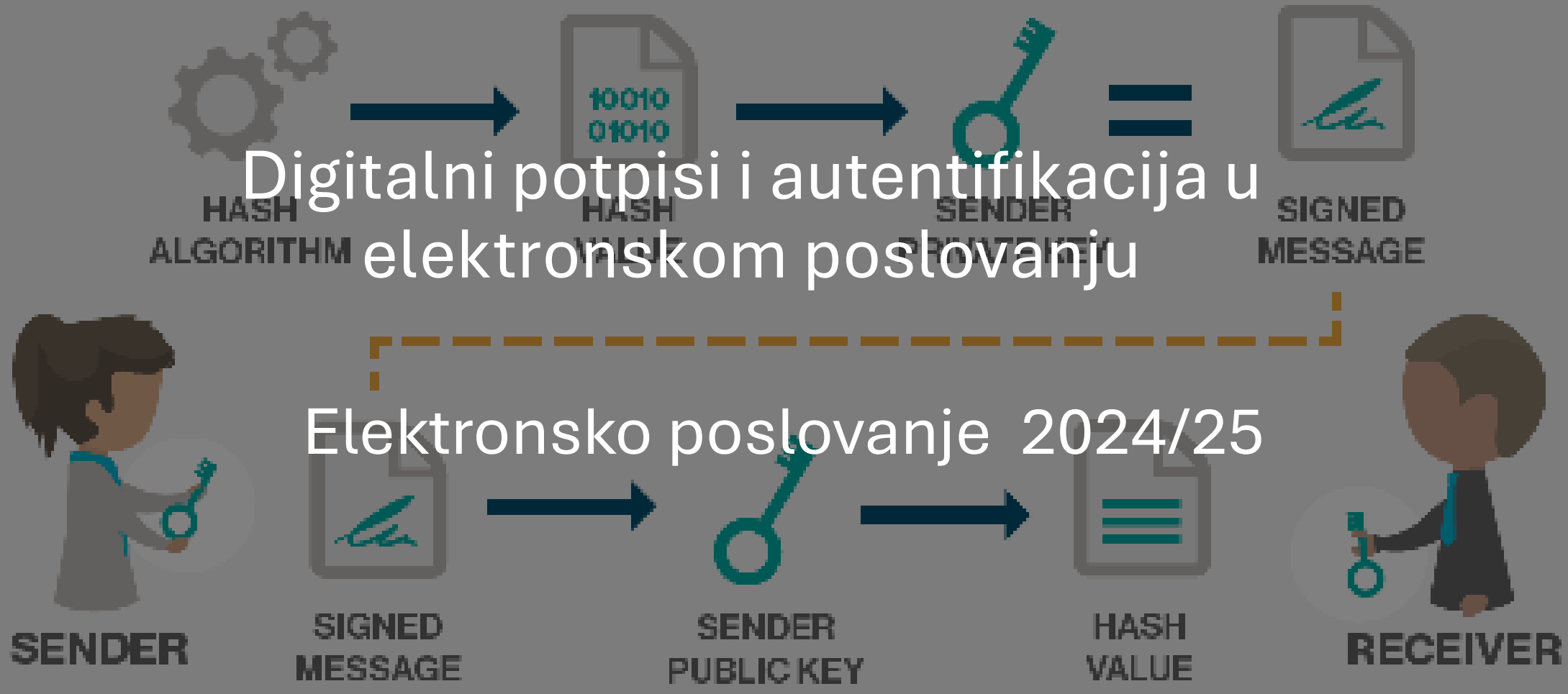
# Digitalni potpisi i autentifikacija u elektronskom poslovanju

Elektronsko poslovanje 2024/25



## Uvod

- Elektronsko poslovanje omogućava brzo, efikasno i globalno povezivanje, ali sa sobom nosi i izazove u vezi sa bezbednošću i verodostojnošću komunikacije.
- **Digitalni potpisi** i **autentifikacija** predstavljaju osnovne stubove poverenja u digitalnom svetu.

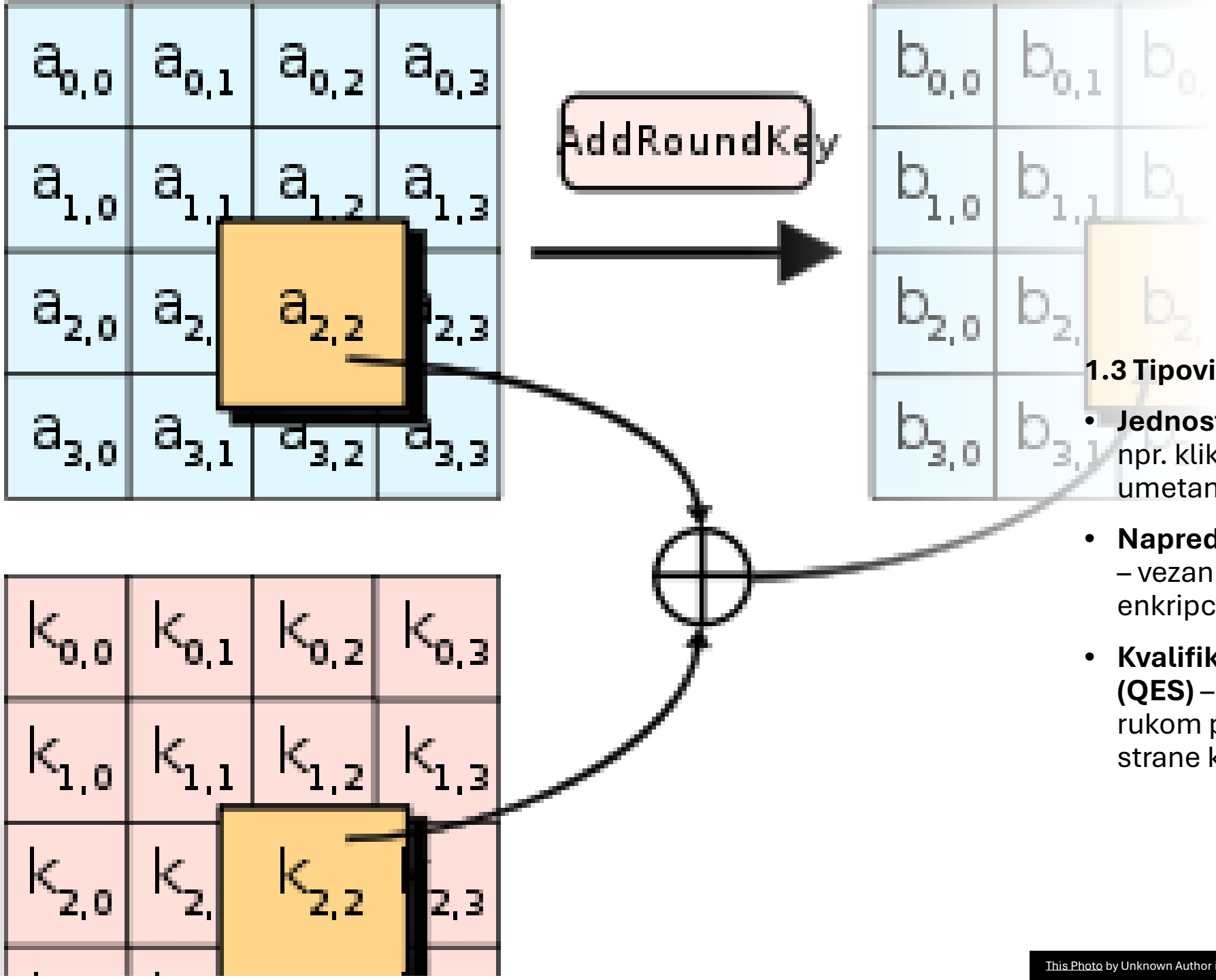
### 1.1 Kriptografska osnova

Digitalni potpis koristi **kriptografiju sa javnim ključem** (Public Key Infrastructure - PKI):

- **Privatni ključ -** koristi ga potpisnik za kreiranje potpisa.
- **Javni ključ -** koristi ga primalac za verifikaciju potpisa.

### 1.2 Hash funkcija

- Pri potpisivanju se sadržaj dokumenta prolazi kroz **hash funkciju** (npr. SHA-256), koja generiše jedinstveni otisak dokumenta. Taj otisak se šifrira privatnim ključem i prilaže dokumentu kao digitalni potpis.




## 1.3 Tipovi digitalnih potpisa

- **Jednostavan elektronski potpis** – npr. klik na dugme "Prihvatam" ili umetanje slike rukopisa.
- **Napredni elektronski potpis (AES)** – vezan je za potpisnika, koristi enkripciju i otkriva izmene.
- **Kvalifikovani elektronski potpis (QES)** – ima istu pravnu snagu kao rukom potpisan dokument; izdat od strane kvalifikovanog tela (CA).

# Autentifikacija – identitet u digitalnom svetu

**Autentifikacija** je proces koji omogućava sistemu da proveri identitet korisnika. Bez pravilne autentifikacije, digitalna komunikacija bi bila ranjiva na krađu identiteta, pristup poverljivim podacima i druge bezbednosne incidente.

# Kategorije autentifikacije

**Nešto što korisnik zna** – lozinka, PIN.

**Nešto što korisnik ima** – pametni telefon, token, USB uređaj.

**Nešto što korisnik jeste** – biometrijski podaci: otisak prsta, skeniranje oka, prepoznavanje lica.

## Metode

**Jednostepena autentifikacija (1FA)** – samo korisničko ime i lozinka.

**Dvofaktorska autentifikacija (2FA)** – dodatni kod koji se šalje na telefon ili generiše aplikacijom.

**Višefaktorska autentifikacija (MFA)** – više faktora zajedno, često u korporativnim sistemima.

# 2.3 Sertifikati i pametne kartice

- U ozbiljnim sistemima koristi se digitalni sertifikat na **smart kartici** (npr. ID kartica državne uprave, poslovne ID kartice) koji automatski identifikuje korisnika pri logovanju i potpisivanju dokumenata.

# 3. Primena u elektronskom poslovanju

## Elektronsko fakturisanje

U Srbiji je uveden sistem **e-Faktura**, koji omogućava:

- digitalno izdavanje, prijem i potpisivanje faktura,
- automatsku obradu i arhiviranje,
- potpunu integraciju sa poreskim sistemom (npr. Poreska uprava vidi sve fakture u realnom vremenu).

- **Bankarstvo**
- Autentifikacija korisnika putem tokena, mobilnih aplikacija, sertifikata.
- Digitalno potpisivanje naloga, zahteva za kredit, izveštaja.
- Automatizovana bezbednosna verifikacija.



## E-uprava

- Građani mogu podneti poreske prijave, izvaditi izvode iz matičnih knjiga ili registrovati vozilo – sve bez odlaska u institucije.
- Primer: **eUprava.gov.rs** koristi kvalifikovani elektronski potpis i 2FA.

**Interna komunikacija i dokumentacija**

- U velikim kompanijama – digitalno potpisivanje internih ugovora, pravilnika, izveštaja i naloga.
- Štedi vreme, smanjuje troškove, omogućava sledljivost.

# 4. Pravni okvir i standardi

**Evropska unija – eIDAS regulativa**

Regulativa (EU) br. 910/2014 o elektronskoj identifikaciji i uslugama od poverenja:

Priznaje pravnu važnost digitalnog potpisa.

Omogućava međusobno priznavanje potpisa između država članica.

Podržava interoperabilnost sistema.

**Srbija**

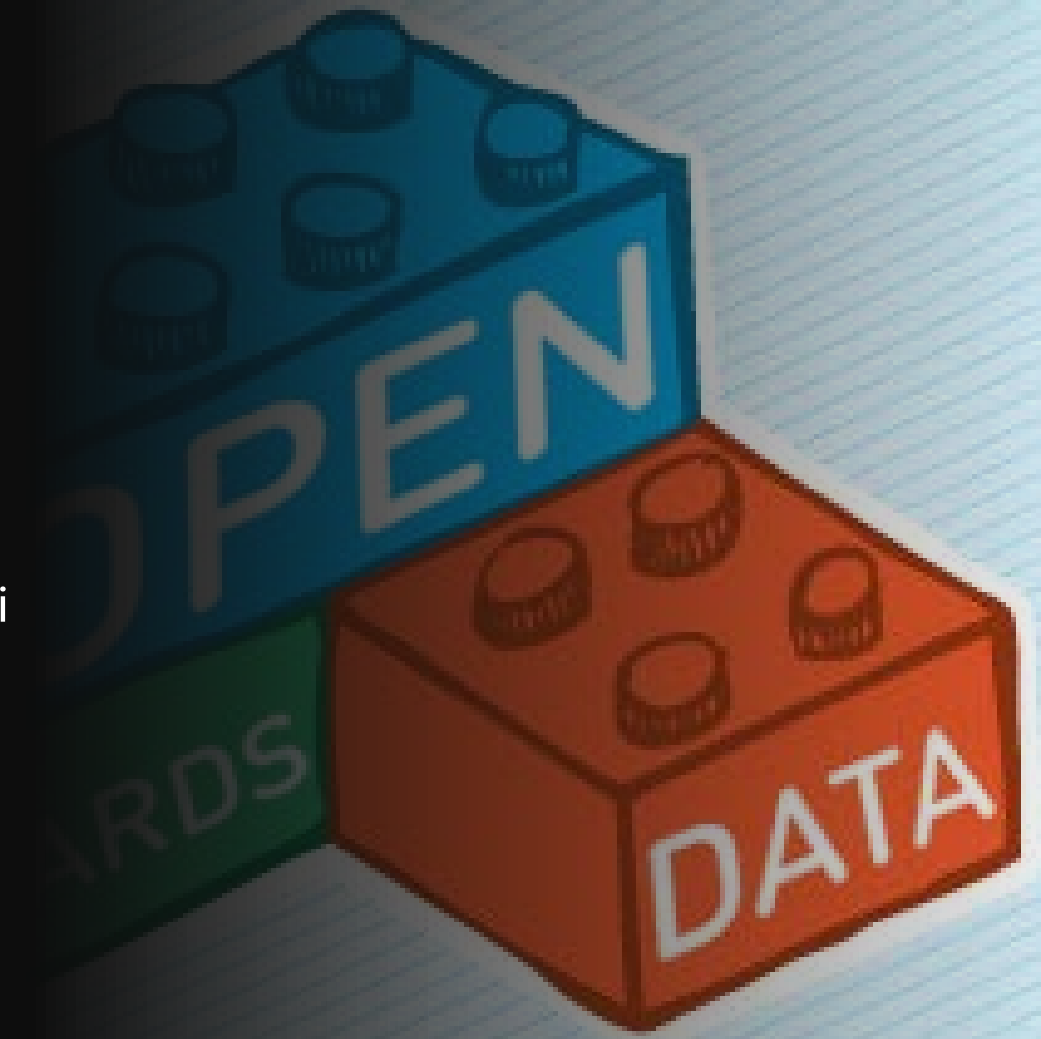
**Zakon o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja** (Službeni glasnik RS, br. 94/17).

Reguliše uslove za kvalifikovane davaoce usluga od poverenja (npr. Pošta Srbije, Halcom).

Priznaje kvalifikovani elektronski potpis kao pravno validan.

## 4.3 Tehnički standardi

- **X.509** – format digitalnog sertifikata.
- **SHA-2, RSA, ECC** – algoritmi za hash i šifrovanje.
- **ETSI EN 319** – standardi za usluge od poverenja.

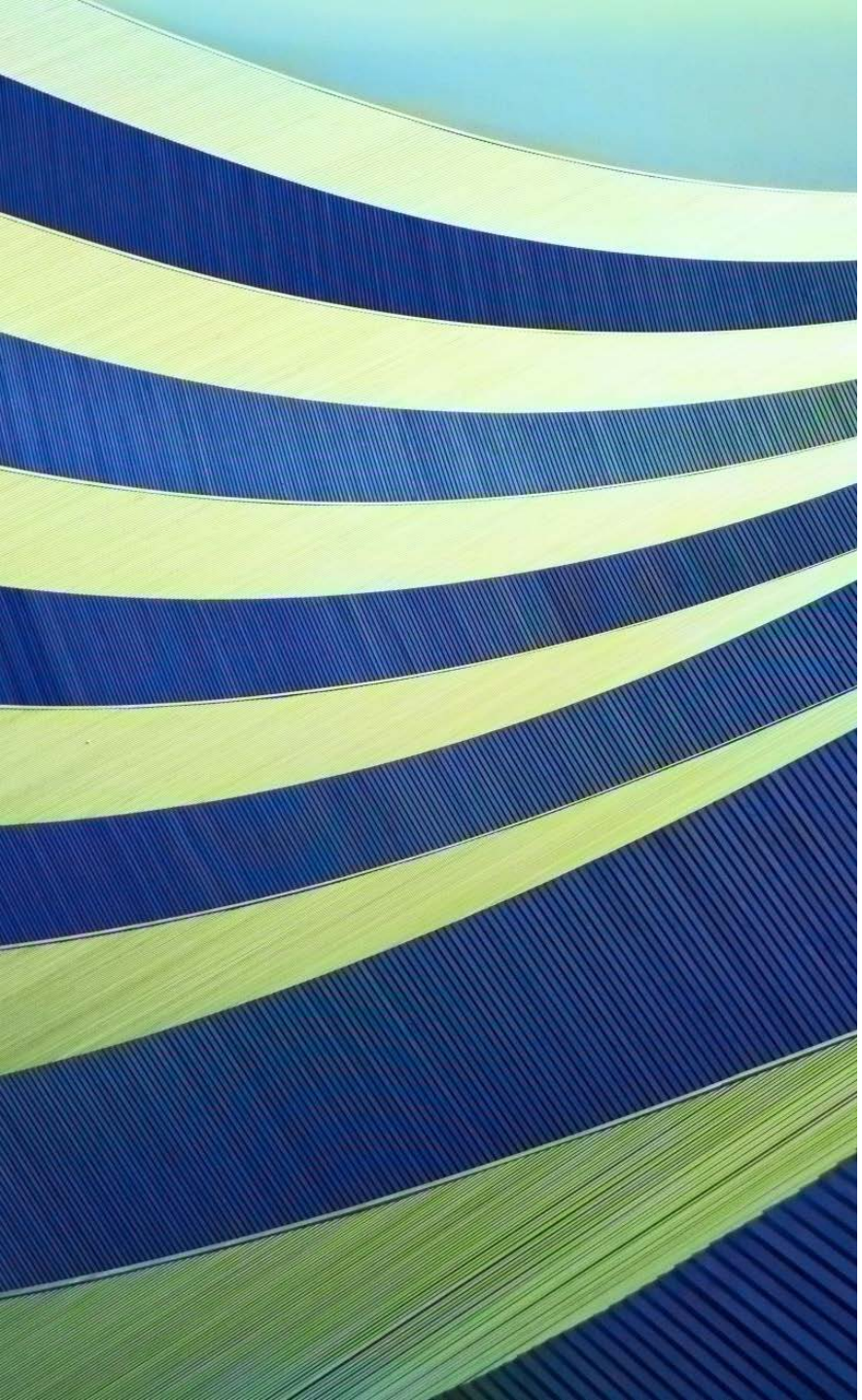


# Prednosti implementacije digitalnih potpisa i autentifikacije

| Prednost | Opis |
| --- | --- |
| Pravna sigurnost | Digitalni potpis ima dokaznu snagu na sudu. |
| Zaštita podataka | Kriptografija sprečava neovlašćenu izmenu i pristup dokumentima. |
| Ušteda vremena i novca | Nema potrebe za štampanjem, slanjem, arhiviranjem u papirnom obliku. |
| Ekološka održivost | Smanjena potrošnja papira i $CO_2$ emisije. |
| Globalna dostupnost | Dokument se može potpisati bilo kada i bilo gde. |
| Interoperabilnost | Dokumenti potpisani u jednoj državi priznaju se i u drugim jurisdikcijama. |

# Izazovi i rizici

- **Kompleksnost implementacije** – potrebna je integracija sa postojećim sistemima.
- **Bezbednosni rizici** – loša zaštita privatnog ključa može dovesti do zloupotreba.
- **Otpornost korisnika** – starije generacije i konzervativna preduzeća teže prihvataju digitalne alate.
- **Troškovi sertifikacije** – dobijanje kvalifikovanog potpisa i održavanje sistema nije besplatno.



# Trendovi i budućnost

**Biometrijski potpisi** – integracija sa AI i biometrijom za dodatnu sigurnost.

**Blockchain tehnologija** – omogućava decentralizovanu proveru identiteta i potpisa.

**Digitalni identiteti (eID)** – koncept „jednog identiteta za sve servise“, koji se koristi u Estoniji i nordijskim zemljama.

**Mobilni potpisi** – korišćenje mobilnih aplikacija za brzo potpisivanje dokumenata.