

A large, stylized logo of the University of Bern, featuring a thick, curved line in shades of pink and orange that forms a shape reminiscent of a stylized 'B' or a mountain peak.

**ALGEBRA
BERNAYS**
SVEUČILIŠTE



POSLOVNI INFORMACIJSKI SUSTAVI (PIS)

Digitalni certifikati i
E-potpis

Tomislav Bronzin, mag. ing. el.



Digitalni certifikati

Digitalni certifikat

- Elektronički dokument koji dokazuje identitet osobe, organizacije ili uređaja na internetu
- Omogućava sigurnu razmjenu podataka korištenjem enkripcije
- Vrsta kriptografske vjerodajnice koja dokazuje identitet osobe, organizacije ili uređaja u digitalnom svijetu
- Omogućava sigurnu razmjenu podataka korištenjem enkripcije

Digitalni certifikat (2)

- Riječ je o računalnom zapisu koji sadrži:
 - Podatke o vlasniku
 - Njegovom javnom ključu
 - Podatke o izdavatelju digitalnog certifikata (pružatelju kvalificiranih usluga povjerenja)
 - Razdoblju valjanosti

Vrste digitalnih certifikata

- Razlikuju se prema namjeni, stupnju sigurnosti i identitetu korisnika, a **najčešće vrste su:**

RB	Vrsta certifikata	Namjena	Pravna valjanost
1	SSL/TLS certifikati	Sigurna komunikacija web stranica	Ne
2	Korisnički certifikati	Identifikacija korisnika; e-usluge	Djelomična
3	Kvalificirani certifikati	Pravni digitalni potpis	Da
4	Certifikati za elektronički potpis	Digitalno potpisivanje dokumenata	Ovisno
5	Certifikati za enkripciju	Šifriranje poruka i datoteka	Ne
6	Certifikati za potpisivanje koda	Potpisivanje softvera i koda	Ne
7	Certifikati za uređaje (IoT)	Sigurna komunikacija uređaja	Ne
8	Certifikati poslužitelja i klijenata	Autentikacija poslužitelja i klijenata	Djelomična

Vrste digitalnih certifikata (2)

1. SSL/TLS certifikati

- Koriste se za osiguranje **sigurne komunikacije** između korisničkog preglednika i web-poslužitelja.
- **Podvrste prema razini validacije:**
 - **DV (Domain Validation)** – potvrđuje samo vlasništvo nad domenom
 - **OV (Organization Validation)** – potvrđuje identitet organizacije
 - **EV (Extended Validation)** – najviša razina provjere, zelena traka u pregledniku

Vrste digitalnih certifikata (3)

2. Korisnički (osobni) certifikati

- Namijenjeni za identifikaciju pojedinaca, najčešće korišteni za:
- Prijavu u e-usluge (e-Građani, e-Porezna, eIDAS)
- Elektroničko potpisivanje dokumenata
- Sigurno slanje e-mailova (S/MIME)

• 3. Kvalificirani digitalni certifikati

- Izdaju ih kvalificirana tijela (npr. Fina, AKD) i koriste se za:
- Potpisivanje dokumenata s pravnim učinkom
- Elektroničko identificiranje prema eIDAS uredbi
- *Jednaki su vlastoručnom potpisu u pravnom smislu (u EU)*

Vrste digitalnih certifikata (4)

4. Certifikati za elektronički potpis

- Koriste se za **digitalno potpisivanje dokumenata**, mogu biti:
 - **Kvalificirani** (pravno obvezujući)
 - **Nekvalificirani** (za internu uporabu)

• 5. Certifikati za šifriranje (enkripciju)

- Omogućuju **šifriranje i dešifriranje** poruka i datoteka. Koriste se u:
 - Sigurnom e-mailu (S/MIME)
 - Internim komunikacijskim sustavima

Vrste digitalnih certifikata (5)

- **6. Certifikati za potpisivanje koda (Code Signing)**
 - Omogućuju **digitalno potpisivanje softvera ili skripti**, čime se jamči da kod nije izmijenjen nakon izdavanja.
- **7. Certifikati za uređaje (Device/IoT certifikati)**
 - Koriste se za identifikaciju i sigurnu komunikaciju između uređaja u IoT okruženjima, industriji ili mrežnoj opremi.
- **8. Certifikati poslužitelja i klijenata (Server/Client Certificates)**
 - **Server certifikati** – potvrđuju identitet poslužitelja (npr. web server)
 - **Client certifikati** – potvrđuju identitet korisnika/klijenta u mrežnim aplikacijama

Izdavanje (kvalificiranih) dig. certifikata

- Certifikate izdaju ovlaštene organizacije koje se nazivaju **certifikacijska tijela** (engl. Certificate Authority – CA), npr.:
 - AKD, FINA, GlobalSign, DigiCert, RapidSSL, Sectigo, Thawte
- Postupak uključuje:
 - Podnošenje zahtjeva CA-u (online ili osobno)
 - Identifikaciju (osobno, putem sustava e-Građani, ili dokumentima)
 - Preuzimanje i instalaciju certifikata
- Digitalni certifikati najčešće vrijede jednu do pet godina

Privatni i javni ključ

- Digitalni certifikat sadrži **privatni i javni ključ**
- Privatni ključ
 - Tajna
 - Koristi za digitalno potpisivanje i dešifriranje
 - Mora biti strogo zaštićen, jer omogućuje potvrdu identiteta vlasnika
- Javni ključ
 - Služi za provjeru identiteta nekog korisnika
 - Služi za šifriranje koje se može dešifrirati samo privatnim ključem koji je u paru s javnim ključem

Kreiranje i funkcioniranje digitalnog certifikata (1)

- Digitalni certifikat radi na temelju infrastrukture javnog ključa (PKI), koja omogućuje sigurnu komunikaciju putem interneta pomoću asimetrične enkripcije.
- Kreiranje i upotrebe uključuje sljedeće korake:
 1. Stvaranje para ključeva
 2. Zahtjev za certifikat
 3. Provjera valjanosti
 4. Izdavanje potvrda
 5. Distribucija certifikata
 6. Sigurno poslovanje
 7. Lanac povjerenja

Kreiranje i funkcioniranje digitalnog certifikata (2)

1. Stvaranje para ključeva

- Sigurna web stranica stvara par kriptografskih ključeva za novog vlasnika digitalnog certifikata
- Jedan javni i jedan privatni
- Javni ključ uključen je u digitalni certifikat, dok je privatni ključ sigurno pohranjen i dostupan samo vlasniku.

2. Zahtjev za certifikat

- Web stranica šalje zahtjev za potpisivanje certifikata (CSR) tijelu za digitalne certifikate,
- DOP uključuje javni ključ i identifikacijske podatke internetske stranice

Kreiranje i funkcioniranje digitalnog certifikata (3)

3. Provjera valjanosti

- Izdavatelj digitalnog certifikata potvrđuje identitet vlasnika (onoga koji je zatražio izdavanje certifikata) i zahtjev za potpis certifikata

4. Izdavanje potvrda

- Izdavatelj digitalnog certifikata potvrđuje identitet vlasnika (onoga koji je zatražio izdavanje certifikata) i zahtjev za potpis certifikata

5. Distribucija certifikata

- Digitalni certifikat postaje javno dostupan i omogućuje provjeru identiteta vlasnika

Kreiranje i funkcioniranje digitalnog certifikata (4)

6. Sigurno poslovanje

- Nositelj digitalnog certifikata može sigurno potpisivati elektroničke dokumente svojim privatnim ključem
- Valjanost potpisa može se pouzdano provjeriti pomoću javnog ključa i identiteta vlasnika (putem digitalnog certifikata koji povezuje javni ključ s vlasnikom)

7. Lanac povjerenja

- Budući da posjetitelji vjeruju izdavatelju digitalnog certifikata uključenom u njihove preglednike, posljedično vjeruju i certifikatu vlasnika.



Elektronički potpis (E-potpis)

Elektronički potpis

- Sigurnosni mehanizam koji se koristi za potvrđivanje autentičnosti i integriteta elektroničkih dokumenata i poruka.
- U poslovnim informacijskim sustavima koristi se kako bi se osiguralo da:
 - Pošiljatelj dokumenta ili poruke zaista jest onaj za koga se predstavlja
 - Digitalni potpis omogućuje identifikaciju autora dokumenta.
 - Dokument nije mijenjan nakon što je potpisan
 - Svaka promjena sadržaja dokumenta nakon potpisivanja poništava valjanost potpisa.
 - Omogućuje pravnu valjanost elektroničkih dokumenata, slično kao vlastoručni potpis na papirnatom dokumentu

Što je još elektronički potpis?

- Digitalna alternativa rukopisnom potpisu
- Skup podataka u elektroničkom obliku koji se dodaju ili logički povezuju s drugim podacima u elektroničkom obliku i koje potpisnik upotrebljava za potpisivanje
- Prema uredbi eIDAS, ona omogućuje provjeru identiteta potpisnika i služi kao digitalna verzija vlastoručnog potpisa
- Elektroničkim potpisom označavamo pristanak, odobrenje ili potvrdu sadržaja digitalnog dokumenta ili transakcije
- E-potpis pruža udoban i učinkovit način potpisivanja dokumenata

eIDAS klasifikacija za e-potpis

- Prema eIDAS uredbi razlikujemo 3 vrste:
 - Elektronički potpis (ES):
 - Najčešći tip jednostavan je za korištenje i ne zahtijeva provjeru identiteta
 - Napredni elektronički potpis (AES):
 - Kreiran na temelju podataka za generiranje elektroničkog potpisa koji potpisnik može koristiti isključivo pod svojom kontrolom, omogućuje identifikaciju potpisnika i otkriva sve naknadne promjene u podacima
 - Kvalificirani elektronički potpis (QES)
 - Nadograđena verzija AES-a, temeljena na kvalificiranom digitalnom certifikatu kvalificiranog pružatelja usluga povjerenja i posebnom sigurnom uređaju za potpisivanje, nudi istu pravnu valjanost kao i vlastoručni potpis na papiru.

Upotreba elektroničkog potpisa

- Koristi se u poslovnim informacijskim sustavima za:
 - Potpisivanje elektroničkih faktura i ugovora
 - Ovjeravanje elektroničkih dokumenata unutar ERP, DMS i dr.
 - Sigurno komuniciranje između poslovnih partnera
 - Autentifikaciju korisnika prilikom pristupa osjetljivim poslovnim podacima ili sustavima
- Upotreba elektroničkog potpisa:
 - Povećava sigurnost
 - Smanjuje potrebu za fizičkim dokumentima
 - Ubrzava poslovne procese

Kako elektronički potpis funkcionira u praksi?

- Postupak uključuje sljedeće jednostavne korake:
 1. Stvaranje dokumenta
 2. Priprema dokumenta za potpis
 3. Provjera autentičnosti
 4. Potpis
 5. Zaključivanje postupka potpisivanja
- 1. Lokacije elektroničkog potpisa (Hrvatska):
 1. Na osobnoj iskaznici – čipu na kartici
 2. Certilia – mobilna osobna iskaznica i potpis u cloud-u
 3. FINA potpisi

Elektronički pečat

- Digitalni ekvivalent tradicionalnog pečata tvrtke
- Prvenstveno ga koriste pravne osobe kako bi se osiguralo podrijetlo i cjelovitost elektroničkih dokumenata
- Ključne karakteristike:
 - Izdaje se pravnim osobama
 - Osigurava integritet dokumenta
 - Automatizirano - može se automatski primijeniti na velike količine dokumenata bez ljudske intervencije
 - Pravno priznavanje: eIDAS EU-a: elektronički pečati imaju definiran pravni status, čime se osigurava njihovo prihvaćanje u svim državama članicama.

Primjeri upotrebe e-potpisa

- Elektronički potpisi mogu se koristiti za potpisivanje:
 - Police osiguranja
 - Ugovori o bankovnom kreditu
 - Logistička dokumentacija, pošiljke, narudžbe
 - Zdravstveni kartoni
 - Ugovori o najmu
 - Kadrovska dokumentacija
 - Projektna izvješća, tehnička dokumentacija
 - Ugovori o povjerljivosti, zapisnici o primopredaji i mnogi drugi

Zaključak

- Digitalni certifikati i elektronički potpisi
 - Imaju ključnu ulogu u osiguravanju sigurnosti, integriteta i autentičnosti internetske komunikacije i transakcija
- Digitalni certifikati
 - Omogućavaju uspostavu povjerenja u izvor i sadržaj web stranica, te šifriranje podataka koji se prenose putem interneta, čime se osigurava sigurnost identiteta i veze
- Elektronički potpisi
 - Od jednostavnih do kvalificiranih, pružaju učinkovit i pravno usklađen način potpisivanja dokumenata i izvršavanja digitalnih transakcija

Pitanja



Okvirna pitanja na provjerama znanja

- Što je to digitalni certifikat?
- Što sadrži u svom zapisu?
- Objasnite korištenje digitalnih certifikata.
- Nabrojite najčešće vrste digitalnih certifikata
 - Objasnite namjenu i pravnu valjanost pojedine vrste digitalnih certifikata
 - Objasnite SSL/TLS certifikate, čemu služe
 - Navedite podvrste SSL/TLS certifikata prema razini validacije
 - Objasnite namjenu korisničkih (osobnih) digitalnih certifikata
 - Objasnite namjenu kvalificiranih digitalnih certifikata
 - Objasnite namjenu digitalnih certifikata za šifriranje
- Objasnite izdavanje (kvalificiranih) digitalnih certifikata, tko ih izdaje, koji je postupak za izdavanje i koliko vrijede.
- Objasnite privatni i javni ključ

Okvirna pitanja na provjerama znanja

- Objasnite kako se kreira i funkcionira digitalni certifikat i koje korake uključuje postupak?
- Objasnite što je to elektronički potpis
- Navedite gdje se u poslovnim informacijskim sustavima koristi elektronički potpis
- Objasnite eIDAS klasifikacija za e-potpis
- Objasnite upotrebu elektroničkog potpisa
- Objasnite kako elektronički potpis funkcionira u praksi
- Što je to elektronički pečat?
- Nevedite primjere upotrebe e-potpisa



**ALGEBRA
BERNAYS**
SVEUČILIŠTE