

Sadržaj:

| | |
|---|-------|
| Uvod..... | 3 |
| 1. Implementacija digitalnog potpisa..... | 3 |
| 1.1. Kriptografija javnog ključa..... | 3 |
| 1.2. Računanje hash sume..... | 3 |
| 2.1. Principi rada digitalnog potpisa..... | 4-5 |
| 2.2. Uloga povjerljive stranke..... | 5 |
| 3. Tehnike digitalnog potpisa..... | 5-6 |
| 4.1. Korištenje RSA..... | 6 |
| 4.2. Korištenje DSA..... | 6 |
| 5. Pregled digitalnog potpisa u potpisanom dokumentu..... | 6-7 |
| 5.1. Pregled digitalnog potpisa: Excel, PowerPoint, Word..... | 7 |
| 5.2. Pregled digitalnog potpisa u potpisanoj poruci e-pošte..... | 8-9 |
| 5.3. Pregled digitalnog potpisa za potpisanu makronaredbu..... | 9 |
| 6. Vjerodostojnost digitalnog potpisa..... | 10-11 |
| 6.1. Problemi vezani za digitalni potpis..... | 11 |
| 6.2. Rješavanje problema digitalnog potpisa..... | 12 |
| 7. Prednosti i nedostaci digitalnog potpisa..... | 12 |
| 8. Digitalni potpis i zakonske regulative..... | 13 |
| 8.1. Norme sigurnosti..... | 13 |
| 9. Prvi digitalni potpis u Republici Srpskoj..... | 14 |
| 10. Zakon o elektronskom poslovanju i elektronskom potpisu u BiH..... | 14-15 |
| Zaključak..... | 16 |
| Literatura..... | 17 |

Uvod:

Opšte prihvaćeni način ovjeravanja dokumenata je ručni potpis i on vuče korjene od samih početaka ljudske pismenosti.

Potpisi se danas nalaze na različitim dokumentima, ugovorima, čekovima, pismima i oni potvrđuju vjerodostojnost tih dokumenata. Prema postojećim zakonima potpisom se smatra ne samo vlastoručni potpis, već i bilo koji drugi znak na dokumentu načinjen s ciljem ovjeravanja dokumenta.

Razvojem i širenjem kompjutera i kompjuterskih mreža postalo je jasno da je potreban sasvim novi način ovjeravanja dokumenata. Različiti znakovi ili tekstualne oznake u datotekama ili elektronskoj pošti ili kopije ručnor potpisa bile su neprimjerene i nepouzdanе zbog mogućnosti krivotvorenja.

Temelji za pouzdanu provjeru porijekla informacija, digitalni potpis, stvoreni su 1976. godine pronalaskom kriptografije javnog ključa (Diffie-Hellman), koja se naziva i asimetričnom kriptografijom.

Digitalni potpis predstavlja prvi stepen u identifikaciji stranaka koje razmjenjuju poruke. On se koristi za provjeru autentičnosti (provjera autentičnosti: postupak koji se provjerava jesu li ljudi i proizvodi ono što tvrde da jesu) digitalnih informacija.

Digitalni potpis pruža sljedeća osiguranja:

Autentičnost – digitalni potpis potvrđuje da je potpisnik onaj za kojeg se izdaje.

Integritet – digitalni potpis potvrđuje da sadržaj nije mijenjan ili iskvaren otkako je digitalno potpisan.

**----- OSTATAK TEKSTA NIJE PRIKAZAN. CEO RAD MOŽETE
PREUZETI NA SAJTU. -----**

www.maturskiradovi.net

MOŽETE NAS KONTAKTIRATI NA E-MAIL: maturskiradovi.net@gmail.com