GAP | Governance Accountability Project
Projekat upravne odgovornosti

PRILOG 2

Procedura podnošenja zahtjeva i odobrenja digitalnog potpisa

USAID FROM THE AMERICAN PEOPLE
SWEDEN
Kingdom of the Netherlands

PRILOG 2

Procedura podnošenja zahtjeva i odobrenja digitalnog potpisa

PRILOG 2

Procedura podnošenja zahtjeva i odobrenja digitalnog potpisa

Elektronski potpis (DS) predstavlja skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa drugim podacima u elektronskom obliku i koji služe za identifikaciju potpisnika i autentičnost potpisanog elektronskog dokumenta. Poput svojeručnog potpisa u standardnom poslovanju (papirni dokumenti), elektronski potpis se koristi u elektronskom poslovanju (elektronskim dokumentima).

Elektronski potpis predstavlja tehnologiju čijom se primjenom u sistemima elektronskog poslovanja omogućava provjera autentičnosti potpisnika, date poruke ili dokumenta. Dodatna osobina elektronskog potpisa je da štiti integritet elektronski potpisane poruke. Postoje tri osnovne vrste elektronskih potpisa: biometrijski potpis, digitalni potpis i skenirani ručni potpis (koji nema pravnu snagu).

Vremenski pečat (TS) predstavlja sistem koji dodatno osigurava digitalni dokument jer ga označava tačnim vremenom (trenutkom) digitalnog potpisivanja, čime se omogućava provjera validnosti digitalnog potpisa i nakon opoziva certifikata koji je korišten za potpisivanje.

Digitalne certifikate korisnicima izdaju posebno akreditovana pravna lica (državne ustanove ili privatne kompanije), na osnovu posebnih odobrenja državnih organa, (npr. Ministarstva za promet i komunikacije BiH, Ministarstva za civilne poslove BiH, Agencije za akreditacije ili drugih sličnih institucija i ustanova) kojima je zakonom prenesena ova nadležnost. Ova pravna lica nazivaju se 'certifikacioni autoriteti' (CA) i zaduženi su za izdavanje javnih i tajnih ključeva, te razmjenu javnih ključeva.

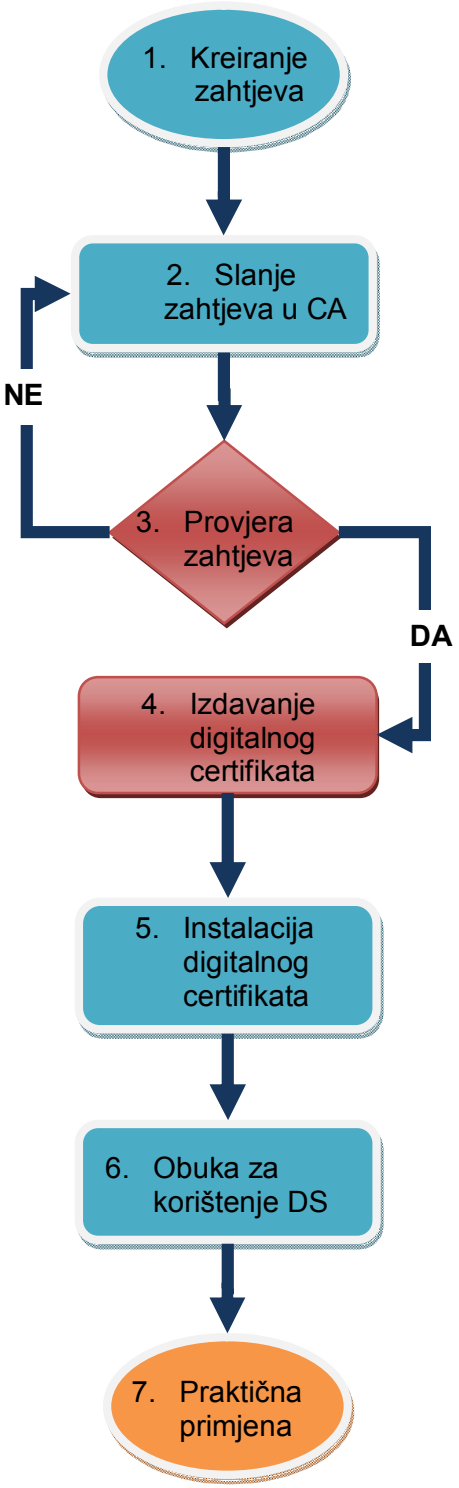
U Bosni i Hercegovini još uvijek nije usvojena standard izdavanja certifikata za izdavanje digitalnih potpisa, a zbog složenosti državne organizacije, najvjerovatnije će se primijeniti princip „*Bridging of Trust*“ koji spaja najbolje osobine hijerarhijskog modela PKI izdavanja certifikata sa „*Pareto pristupom*“ koji autonomno uvode pojedini poslovni sistemi (najčešće banke). Nadležno tijelo za definisanje politike u ovoj oblasti je Ministarstvo za promet i komunikacije Bosne i Hercegovine.

Bez obzira na budući model certificiranja digitalnih potpisnika u Bosni i Hercegovini, svakako je neophodno da svaki poslovni sistem kreira interni pravilnik o načinu

apliciranja zahtjeva za izdavanje certifikata za digitalni potpis u kojem bi se definisali sljedeći koraci:

1. Definisanje broja certifikata i imena korisnika - digitalnih potpisnika.
2. Slanje zahtjeva u CA (u klasičnom papirnom mediju ili digitalno, zavisno od tehnologije); U slučaju potrebe, u svakom momentu je moguće izvršiti promjene digitalnih potpisnika (produženje važnosti certifikata, izdavanje novih ili povlačenje postojećih certifikata).
3. Nakon provjere ispravnosti zahtjeva, CA:
   - izdaje i dostavlja korisniku certifikat(e) za digitalni potpis
   - korisniku izdaje **tajni – privatni ključ**, koji služi za digitalno potpisivanje elektronskih dokumenata; privatni ključ se najčešće koristi u vidu posebne lozinke ili putem posebnih dodataka – uređaja poput pametne (SMART) kartice i čitača ili tokena; (Napomena: pametne kartice i tokeni trenutno predstavljaju najpouzdanije sredstvo zaštite elektronskog potpisa);
   - registruje korisnika elektronskog potpisa u svojoj bazi podataka u vidu **javnog ključa** i distribuira je svim svojim korisnicima, koji na osnovu njega mogu provjeriti pravi identitet osobe koja je potpisala elektronski dokument.
4. Korisnik vrši instalaciju primljenog digitalnog certifikata na svoj(e) računar(e).
5. Korisnik organizuje obuku svih uposlenika koji će se služiti elektronskim potpisom.

DIJAGRAM TOKA PODNOŠENJA ZAHTJEVA, ODOBRENJA I PRIMJENE ELEKTRONSKOG POTPISA



1. **Korisnik** (na osnovu internog Pravilnika): definisanje broja certifikata i imena korisnika

2. **Korisnik**:
Slanje (digitalnog ili papirnatog) zahtjeva u CA (eventualna dorada, u slučaju neispunjenja zahtjeva)

3. **CA**: provjera ispravnosti zahtjeva

4. **CA**: Izdavanje i dostava certifikata za digitalni potpis

5. **Korisnik**:
Instalacija certifikata

6. **Korisnik**: