1. Naštejte 4 komponente infrastrukture javnih ključev (PKI).

1. Registracijski organ (RA)
2. Overitelj (CA)
3. Organ za potrjevanje (VA)
4. (digitalno) potrdilo

---

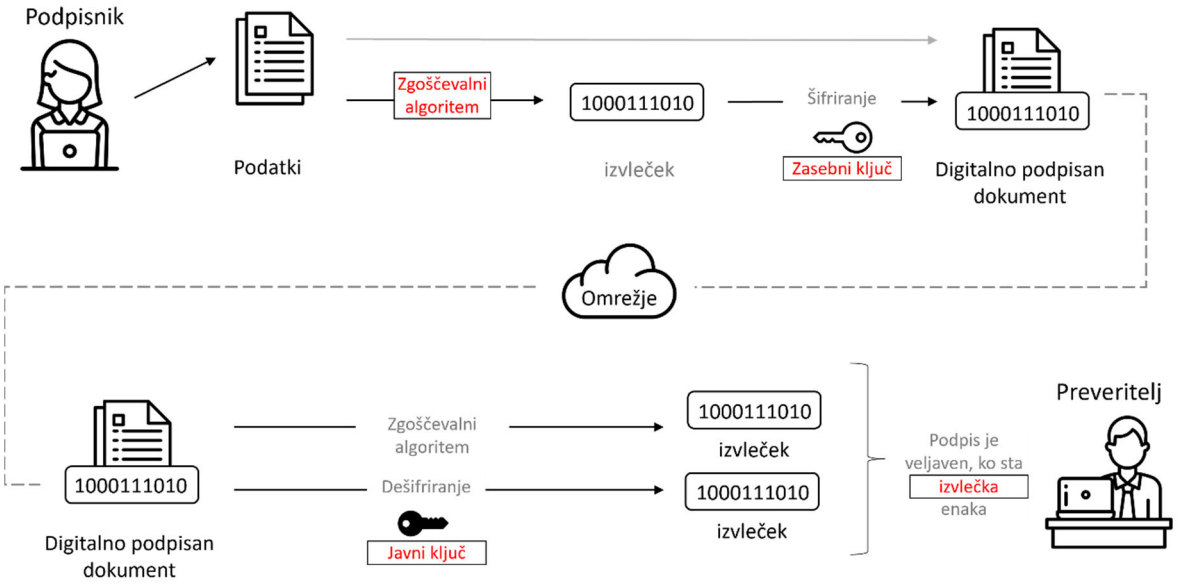
2. Besedilo popravite tako, da bodo naslednje trditve resnične

Če dve strani varno komunicirata z asimetričnim šifriranjem, je postopek naslednji:

Strani si izmenjata (javna ključa / ~~zasebna ključa~~). Oseba 1 šifrira sporočilo, ki ga želi poslati, z uporabo (javni ključ / ~~zasebno ključ~~) osebe 2 in ji ga pošlje. Oseba 2 dešifrira sporočilo s svojim (javnim ključem / ~~zasebnim ključem~~).

---

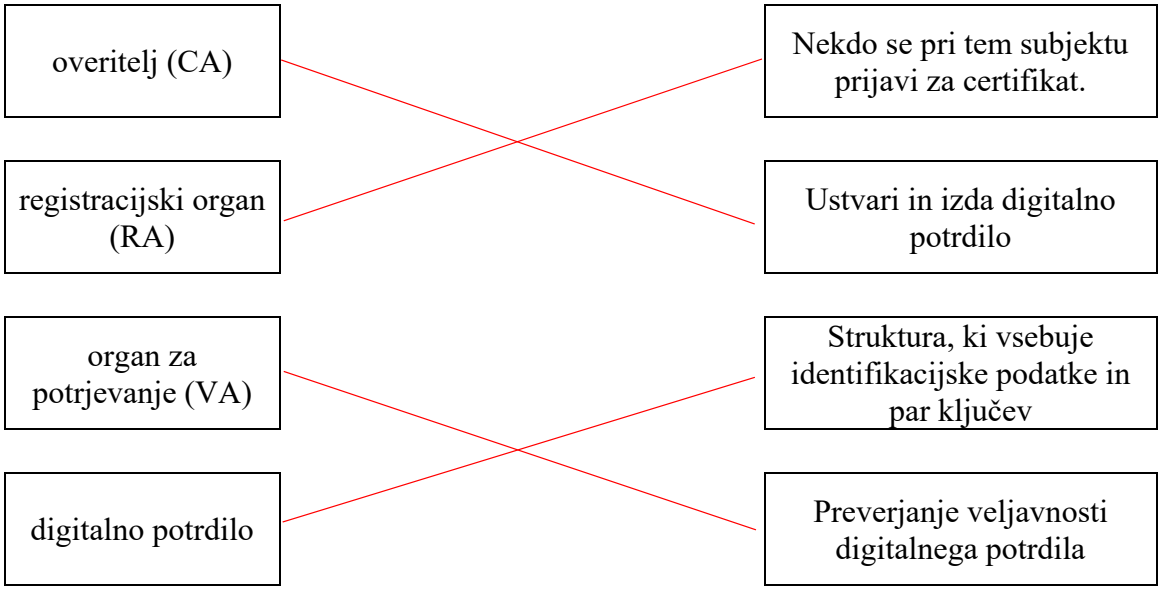
3. Izberite pravilne oznake s seznama in jih zapišite v sliko, da opišete proces digitalnega podpisovanja.



Izbira: zgoščevalni, zasebni ključ, javni ključ, izvleček

Erasmus+
Izvedba tega projekta je financirana s strani Evropske komisije.
Vsebina publikacije (komunikacije) je izključno odgovornost avtorja in v nobenem primeru ne predstavlja stališč Evropske komisije.

4. Izrazom iz levega stolpca pripišite ustrezne opise v desnem stolpcu.



---

5. Življenjski cikel digitalnega potrdila lahko razložimo na naslednji način:

1. Zaprosilo za dig. potrdilo
2. Izdaja dig. potrdila
3. Potrjevanje dig. potrdila
4. Preklic dig. potrdila
5. Podaljšanje dig. potrdila

Erasmus+
Izvedba tega projekta je financirana s strani Evropske komisije.
Vsebina publikacije (komunikacije) je izključno odgovornost avtorja in v nobenem primeru ne predstavlja stališč Evropske komisije.