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

1. _____
2. _____
3. _____
4. _____

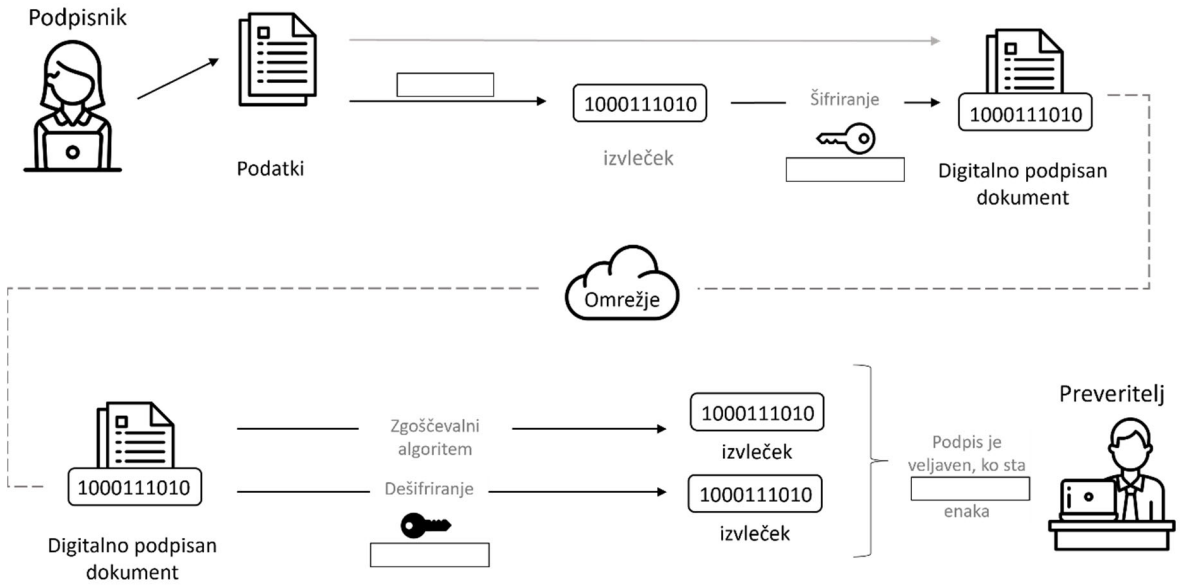
---

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.

overitelj (CA)	Nekdo se pri tem subjektu prijavi za dig. potrdilo.
registracijski organ (RA)	Ustvari in izda dig. potrdilo
organ za potrjevanje (VA)	Struktura, ki vsebuje identifikacijske podatke in par ključev
digitalno potrdilo	Preverjanje veljavnosti digitalnega potrdila

---

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

1. _____
2. _____
3. _____
4. _____
5. _____

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.