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

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

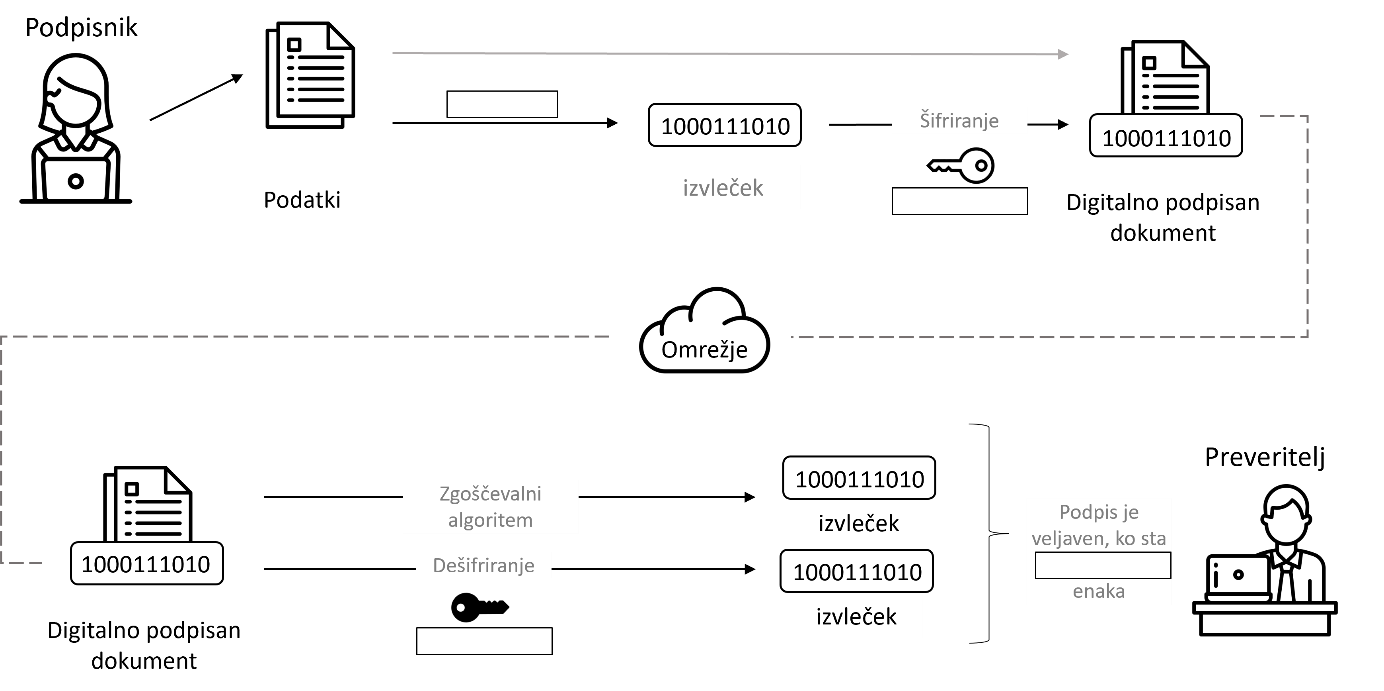
3. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Besedilo popravite tako, da bodo naslednje trditve resnične

Če dve strani varno komunicirata z asimetričnim šifriranjem, je postopek naslednji: Strani si izmenjata . Oseba 1 šifrira sporočilo, ki ga želi poslati, z uporabo osebe 2 in ji ga pošlje. Oseba 2 dešifrira sporočilo s svojim .

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



Izbira: zgoščevalni, zasebni ključ, javni ključ, izvleček

1. 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 |

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

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

5. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_