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

1. Registracijski organ (RA)

2. Overitelj (CA)

3. Organ za potrjevanje (VA)

4. (digitalno) potrdilo

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.

Diagram

Description automatically generated with medium confidence

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 certifikat. |
|  |  |  |
| registracijski organ (RA) |  | Ustvari in izda digitalno 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. Zaprosilo za dig. potrdilo

2. Izdaja dig. potrdila

3. Potrjevanje dig. potrdila

4. Preklic dig. potrdila

5. Podaljšanje dig. potrdila