1. Uveďte 4 komponenty PKI (Public Key Infrastructure)

1. Registračná autorita (RA)
2. Certifikačná autorita (CA)
3. Validačná autorita (VA)
4. Digitálny certifikát

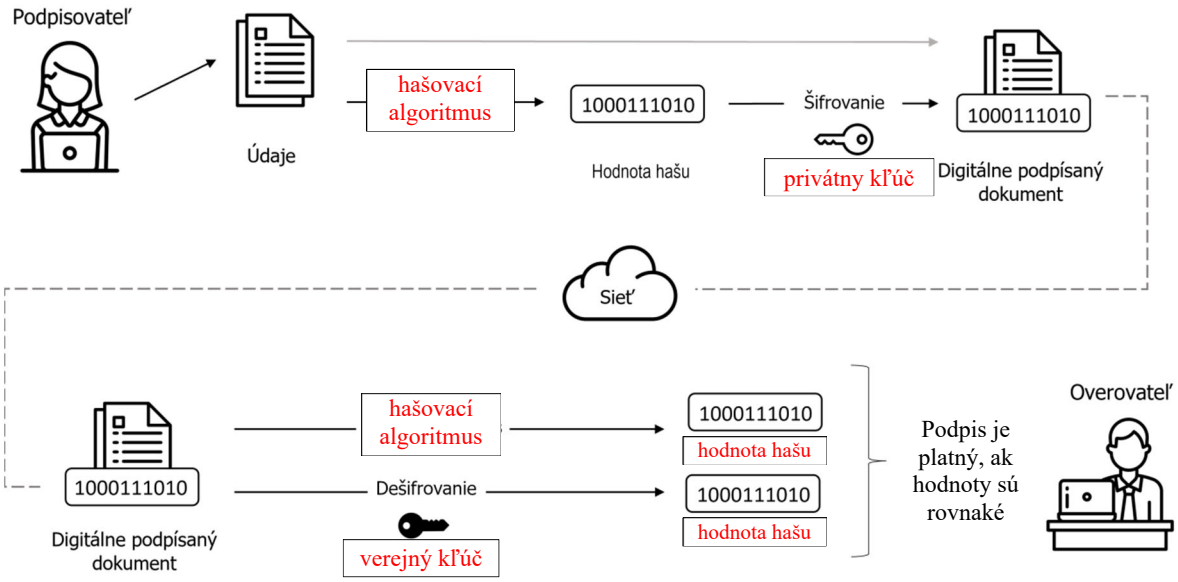
---

2. Opravte text tak, aby nasledujúce tvrdenia boli pravdivé

Proces, aby dve strany mohli bezpečne komunikovať pomocou asymetrického šifrovania, je nasledovný: Obidve strany si vymenia (verejné kľúče / ~~tajné kľúče~~). Osoba 1 zašifruje správu, ktorú chce odoslať pomocou (verejného kľúča / ~~privátneho kľúča~~) osoby 2 a pošle ju osobe 2. Osoba 2 dešifruje správu pomocou jej (~~verejného kľúča~~ / privátneho kľúča).

---

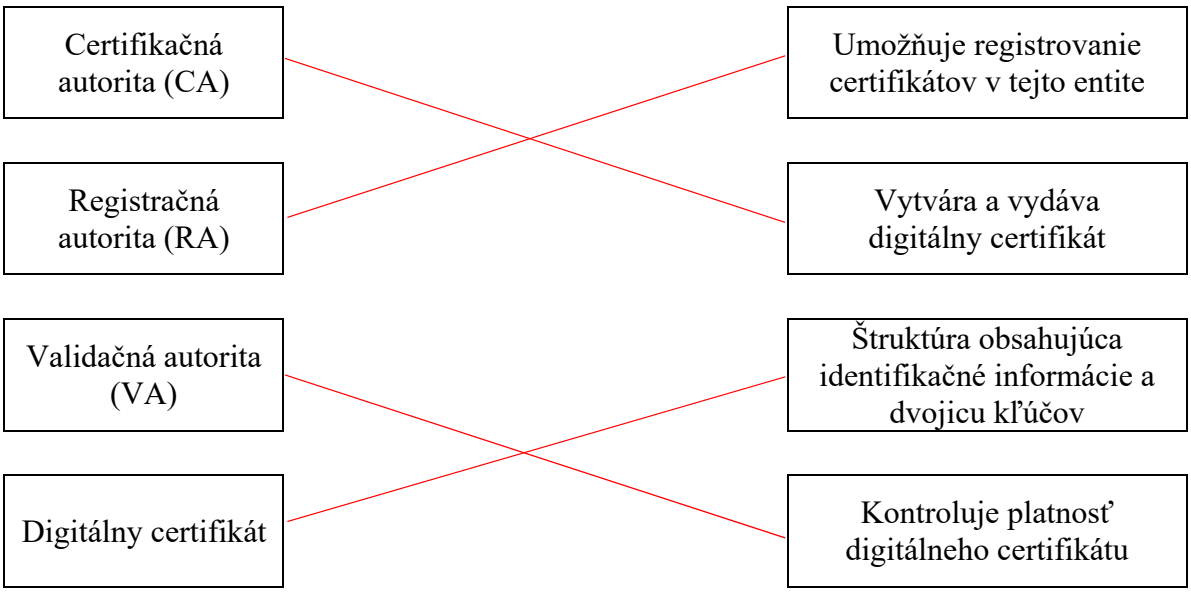
3. Vyberte správne názvy zo zoznamu a napíšte ich do obrázka, aby ste opísali proces digitálneho podpisovania a overenia digitálneho podpisu



Možnosti: hašovací algoritmus, privátny kľúč, verejný kľúč, hodnota hašu

Erasmus+
Tento projekt bol financovaný s podporou Európskej Komisie.
Táto publikácia (dokument) reprezentuje výlučne názor autora a Komisia nezodpovedá za akékoľvek použitie informácií obsiahnutých v tejto publikácii (dokumente).

4. Priraďte výrazy z ľavého stĺpca k príslušným popisom vpravo



---

5. Životný cyklus digitálneho certifikátu možno popísať nasledovne:

1. Zápis certifikátu
2. Vydanie certifikátu
3. Overenie certifikátu
4. Zrušenie certifikátu
5. Obnovenie certifikátu

Erasmus+
Tento projekt bol financovaný s podporou Európskej Komisie.
Táto publikácia (dokument) reprezentuje výlučne názor autora a Komisia nezodpovedá za akékoľvek použitie informácií obsiahnutých v tejto publikácii (dokumente).