1. Uveďte 4 komponenty infrastruktury veřejného klíče PKI.

1. registrační autorita (RA)
2. certifikační autorita (CA)
3. validační autorita (VA)
4. (digitální) certifikát

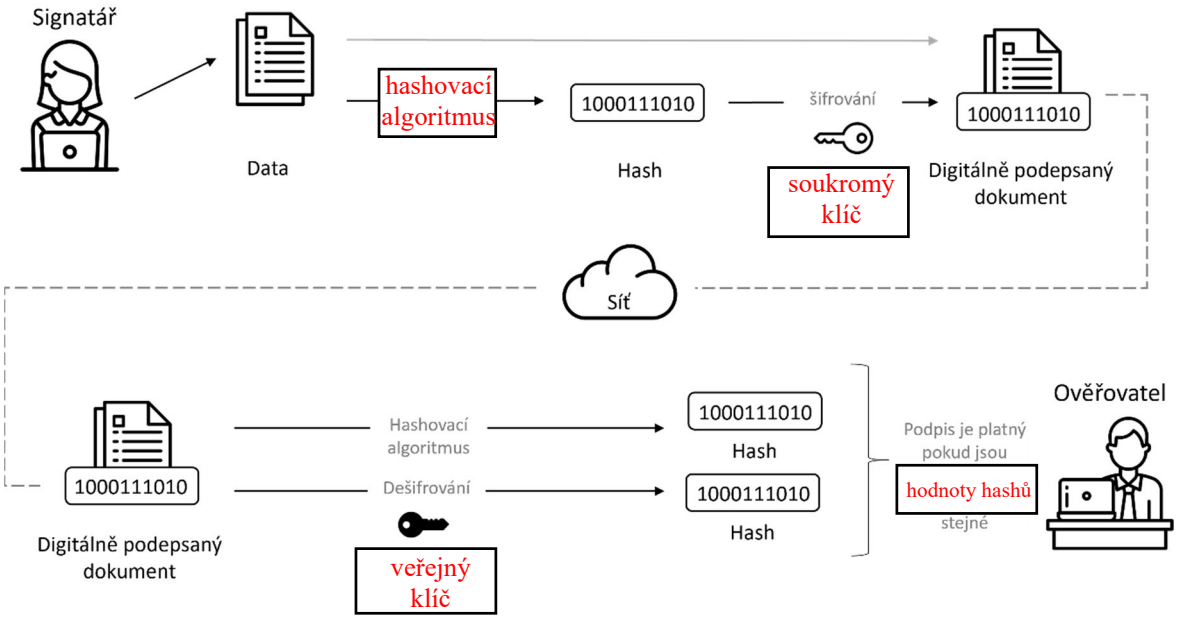
---

2. Opravte následující text tak, aby jednotlivá tvrzení byla pravdivá.

Aby mohly obě strany bezpečně komunikovat prostřednictvím asymetrického šifrování, musí tento proces probíhat následujícím způsobem: Obě strany si navzájem vymění (veřejné klíče / ~~tajné klíče~~). *Osoba 1* zašifruje správu, kterou chce odeslat pomocí (veřejného klíče / ~~soukromého klíče~~) *osoby 2* a následně ji odešle *osobě 2*. *Osoba 2* dešifruje přijatou zprávu pomocí svého (~~veřejného klíče~~ / soukromého klíče).

---

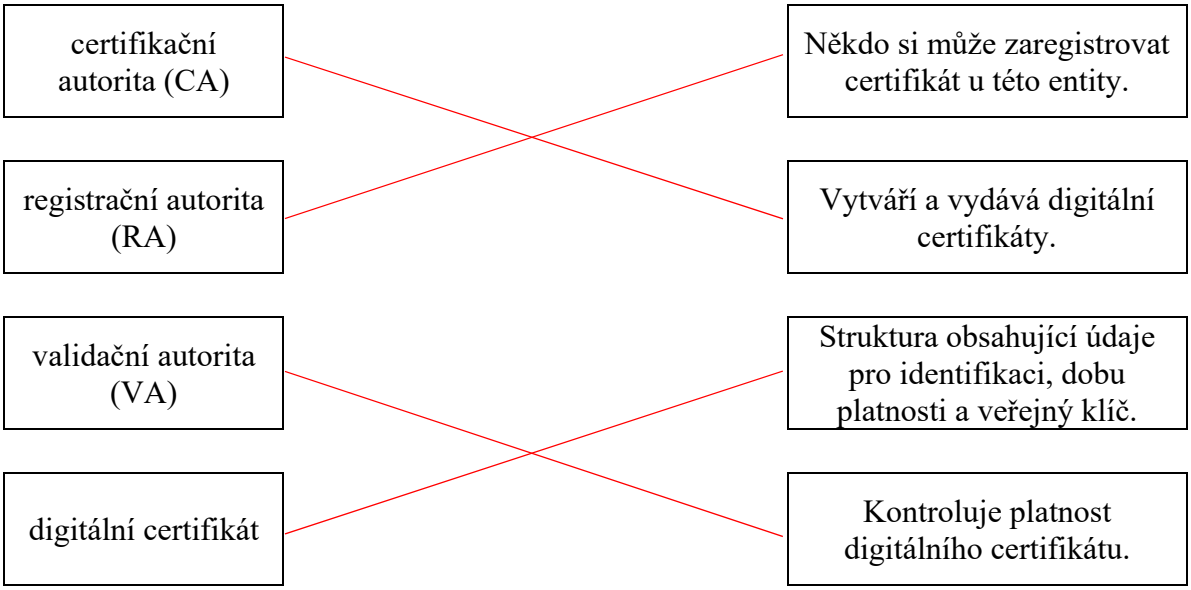
3. Vyberte správné možnosti (termíny) ze seznamu níže a zapište je do obrázku tak, aby vzniklo správné schéma tvorby a ověření digitálního podpisu.



Možnosti: veřejný klíč, hodnoty hashů, hashovací algoritmus, soukromý klíč

Erasmus+
Tento projekt byl realizován za finanční podpory Evropské unie.
Za obsah publikací (sdělení) odpovídá výlučně autor. Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.

4. Přiřaďte termíny z levého sloupce k odpovídajícímu popisu v pravém sloupci.



---

5. Kterými fázemi lze popsat životní cyklus digitálního certifikátu?

1. registrace certifikátu
2. vydání certifikátu
3. ověření certifikátu
4. zrušení certifikátu
5. obnova certifikátu

Erasmus+
Tento projekt byl realizován za finanční podpory Evropské unie.
Za obsah publikací (sdělení) odpovídá výlučně autor. Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.