1. Uveďte 4 komponenty PKI (Public Key Infrastructure)

1. Registračná autorita (RA)

2. Certifikačná autorita (CA)

3. Validačná autorita (VA)

4. Digitálny certifikát

1. Opravte text tak, aby nasledujúce tvrdenia boli pravdivé

Proces, aby dve strany mohli bezpečne komunikovať pomocou asymetrického šifrovania, je nasledovný: Obidve strany si vymenia . Osoba 1 zašifruje správu, ktorú chce odoslať pomocou osoby 2 a pošle ju osobe 2. Osoba 2 dešifruje správu pomocou jej .

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



hašovací

algoritmus

privátny kľúč

verejný kľúč

hodnota hašu

hašovací

algoritmus

hodnota hašu

Podpis je platný, ak hodnoty sú rovnaké

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

1. Priraďte výrazy z ľavého stĺpca k príslušným popisom vpravo

|  |  |  |
| --- | --- | --- |
| Certifikačná autorita (CA) |  | Umožňuje registrovanie certifikátov v tejto entite |
|  |  |  |
| Registračná autorita (RA) |  | Vytvára a vydáva  digitálny certifikát |
|  |  |  |
| Validačná autorita (VA) |  | Štruktúra obsahujúca identifikačné informácie a dvojicu kľúčov |
|  |  |  |
| Digitálny certifikát |  | Kontroluje platnosť digitálneho certifikátu |

1. Životný cyklus digitálneho certifikátu možno popísať nasledovne:

1. Zápis certifikátu

2. Vydanie certifikátu

3. Overenie certifikátu

4. Zrušenie certifikátu

5. Obnovenie certifikátu