1. Uveďte 4 komponenty infrastruktury veřejného klíče PKI.

1. registrační autorita (RA)

2. certifikační autorita (CA)

3. validační autorita (VA)

4. (digitální) certifikát

1. 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 . Osoba 1 zašifruje správu, kterou chce odeslat pomocí osoby 2 a následně ji odešle osobě 2. Osoba 2 dešifruje přijatou zprávu pomocí svého .

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



soukromý klíč

hodnoty hashů

veřejný

klíč

hashovací

algoritmus

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

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

|  |  |  |
| --- | --- | --- |
| certifikační autorita (CA) |  | Někdo si může zaregistrovat certifikát u této entity. |
|  |  |  |
| registrační autorita (RA) |  | Vytváří a vydává digitální certifikáty. |
|  |  |  |
| validační autorita (VA) |  | Struktura obsahující údaje pro identifikaci, dobu platnosti a veřejný klíč. |
|  |  |  |
| digitální certifikát |  | Kontroluje platnost digitálního certifikátu. |

1. Kterými fázemi lze popsat životní cyklus digitálního certifikátu?

1. registrace certifikátu

2. vydání certifikátu

3. ověření certifikátu

4. zrušení certifikátu

5. obnova certifikátu