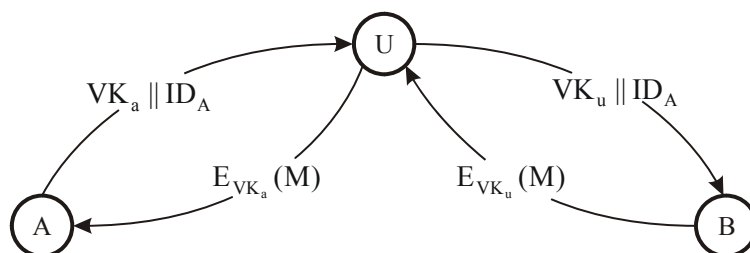
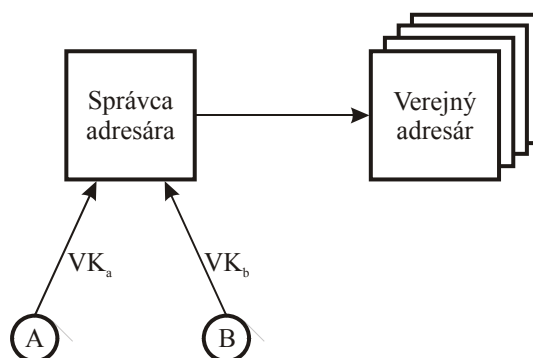


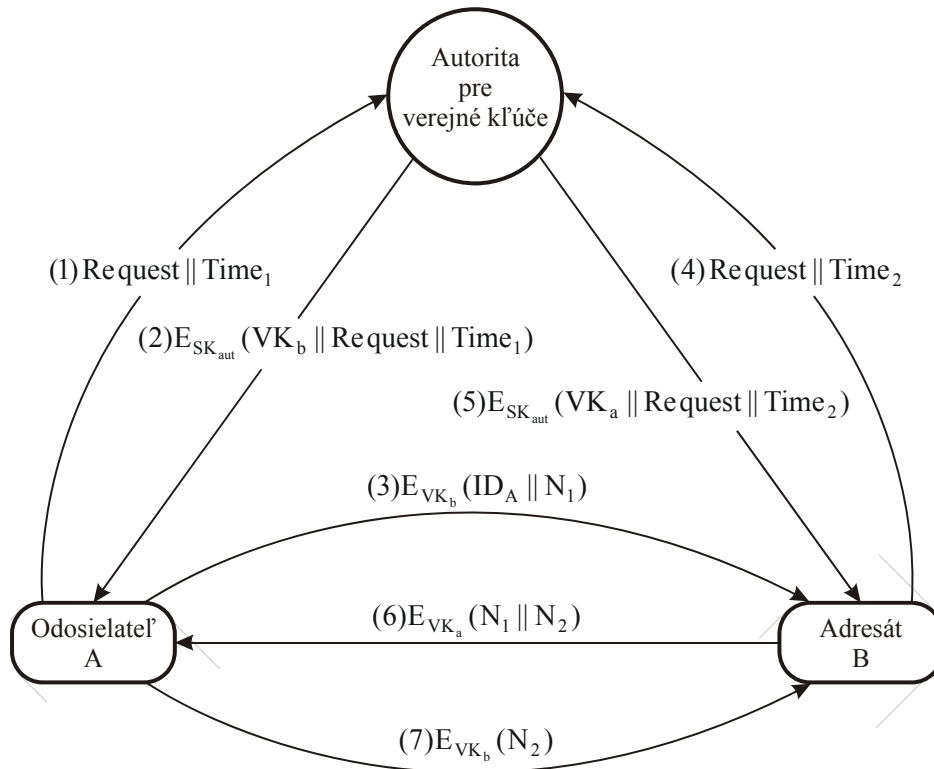
8 MANAŽMENT KLÍČOV



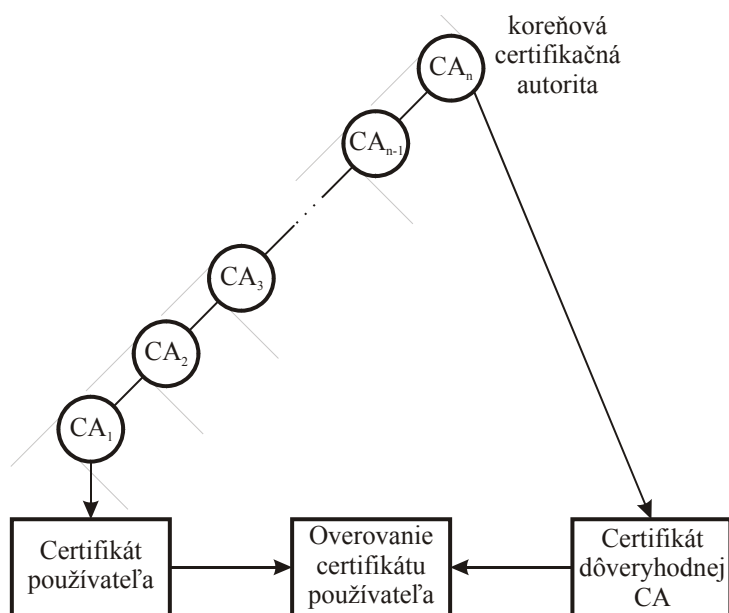
Obr. 8.1 Podvrhnutie verejného kľúča



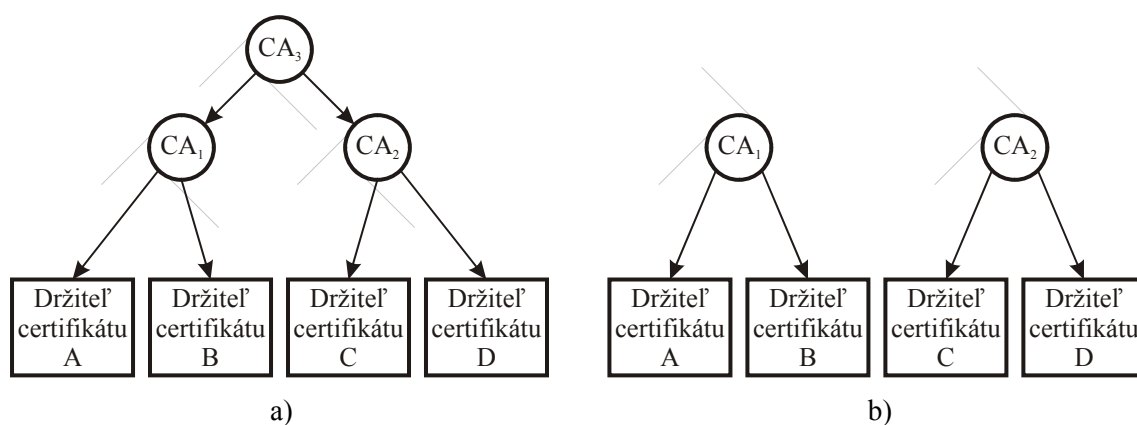
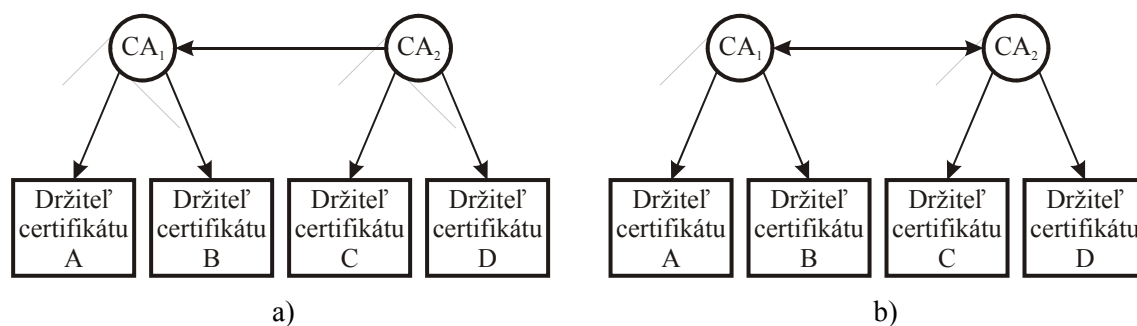
Obr. 8.2 Princíp verejne dostupného adresára



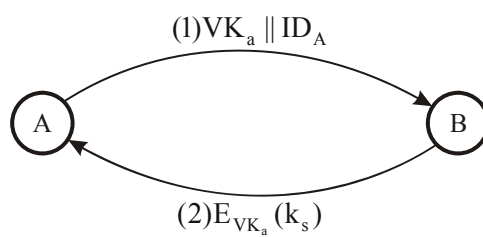
Obr. 8.3 Distribúcia verejných kľúčov pomocou autority pre verejné kľúče



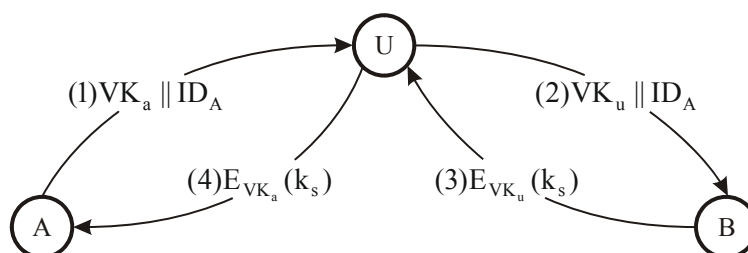
Obr. 8.6 Ret'az certifikátov

Obr. 8.7 a) stromová štruktúra certifikačných autorít CA₁, CA₂, CA₃
b) stromová štruktúra certifikačných autorít CA₁ a CA₂

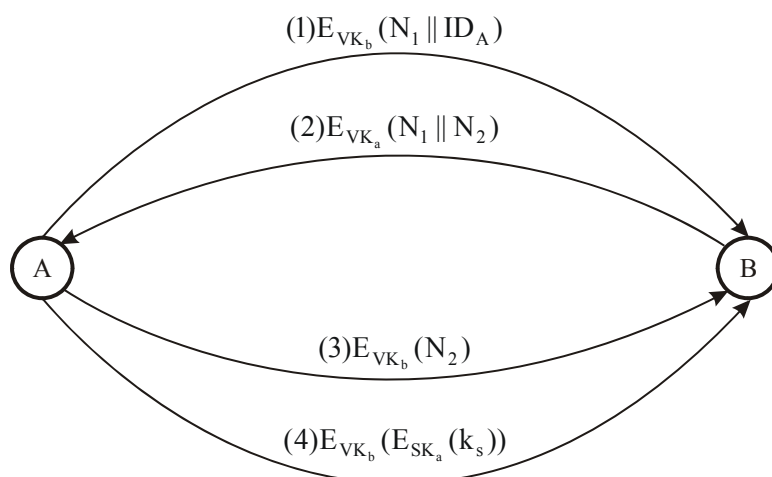
Obr. 8.8 a) jednosmerná certifikácia, b) obojsmerná certifikácia



Obr. 8.9 Jednoduchá distribúcia tajných kľúčov



Obr. 8.10 Získanie tajného kľúča podvrhnutím verejného kľúča



Obr. 8.11 Výmena tajných kľúčov s utajením a autentizáciou