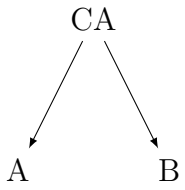
Verwendung einer Zertifizierungsinstanz

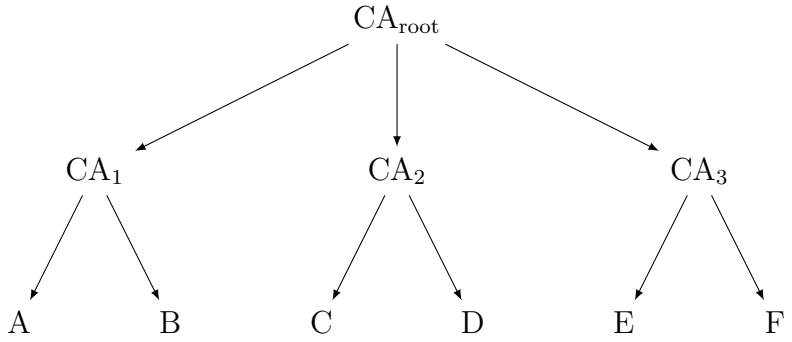


- es gibt nur eine Zertifizierungsinstanz CA, die Zertifikate für alle Teilnehmer ausstellt (Ausstellen von Zertifikaten symbolisiert durch Pfeile)
- alle Teilnehmer (A, B) kennen den Testschlüssel $k_{t,CA}$ der CA
- Vereinfachte Annahme bzgl. Aufbau des Zertifikats:
  (ausstellende CA, Teilnehmer, Testschlüssel des Teilnehmers), Signatur
  z.B. Zertifikat für Teilnehmer A: (CA, A, $k_{t,A}$), $\text{sign}_{k_{s,CA}}$(CA, A, $k_{t,A}$);
  im Folgenden abgekürzt mit cert(CA, $\text{k}_{t,A}$)
- A will Testschlüssel von B überprüfen: A erhält Zertifikat von B und kann mit dem Testschlüssel der CA ($k_{t,CA}$) überprüfen

Verwendung verschiedener Zertifizierungsinstanzen

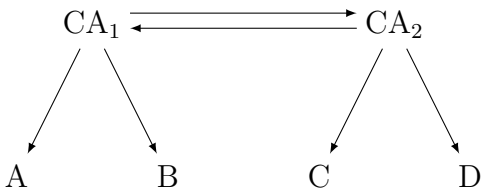
(Beispiele für Möglichkeiten, vereinfacht dargestellt)

Strikte Hierarchie:



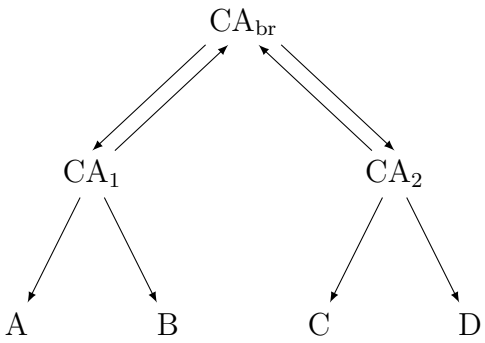
- es gibt eine Wurzelinstanz (CA_{root})
- jede CA stellt Zertifikate für die Instanzen in der nächsten Ebene aus
- jeder Teilnehmer kennt den Testschlüssel der Wurzelinstanz $k_{t,CA_{root}}$

Cross-Zertifizierung:



- die Zertifizierungsinstanzen stellen sich gegenseitig Zertifikate aus:
  CA_1 stellt Zertifikat für CA_2 aus: cert(CA_1, k_{t,CA_2})
  CA_2 stellt Zertifikat für CA_1 aus: cert(CA_2, k_{t,CA_1})
- jeder Teilnehmer kennt den Testschlüssel „seiner“ CA

Bridge-CA:



- die Bridge-CA führt mit möglichst vielen CAs Cross-Zertifizierungen durch
- jeder Teilnehmer muss jeweils nur den Testschlüssel „seiner“ CA kennen