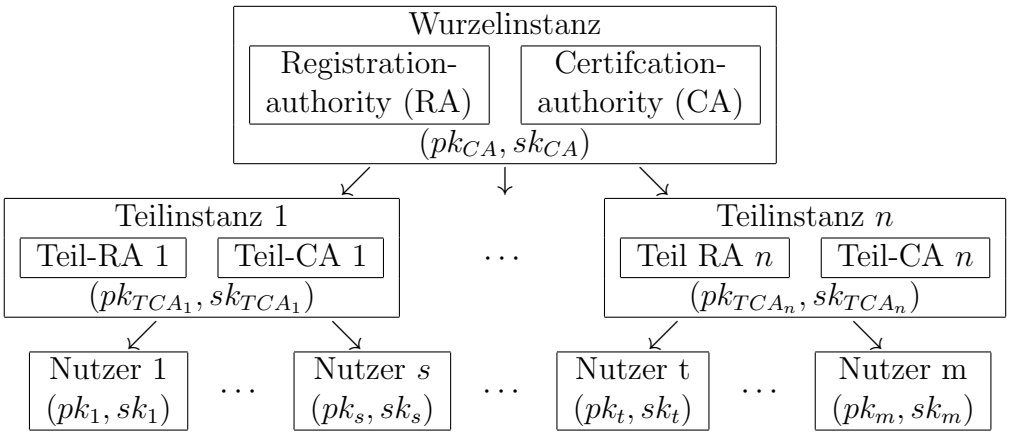
5. Übungsblatt

SS 2015
Rechnersicherheit
Ausgegeben am 13.05.2015
Abgabe 21.05.2015

Marian Margraf
Inst. für Informatik
Freie Universität Berlin

Aufgabe 1 (Public Key Infrastructure)



Erklären Sie den Ablauf von Signaturerstellung und -Verifikation in einer, wie oben dargestellten, mehrstufigen PKI. Geben Sie dazu an, welche Elemente der Signierende und der Verifizierende benötigt und welche Elemente versendet werden.

(*a*) Signierender und Verifizierender sind Mitglied einer selben Teilinstanz.

(*b*) Signierender und Verifizierender sind Mitglied verschiedener Teilinstanzen der selben Wurzelinstanz.

(*c*) Signierender und Verifizierender sind Mitglied verschiedener Wurzelinstanzen.
(Stichworte: Bridge-CA, Cross-Certification)

Aufgabe 2. (qualifizierte elektronische Signatur)

Was ist eine qualifizierte elektronische Signatur?
Wie sieht die PKI hierfür aus? Beschreiben Sie die verantwortlichen Institutionen für alle Komponenten dieser PKI.

Aufgabe 3. (OpenPGP Protocol)

Wie realisiert man mit dem OpenPGP Protocol die drei in der Vorlesung vorgestellten Vertrauensmodelle. Skizzieren Sie die möglichen Szenarien für den Schlüsselaustausch. Erläutern Sie für alle drei Modelle, wer Schlüssel signiert.