Team10 - Moritz Rupp, Viktor Brandl

1.5 Kontrollfrage

Bearbeitet von Moritz Rupp und Victor Brandl

Frage 2.1

> Welche Aufgabe erfüllt eine CA?

Eine **CA** bzw. Certification Authority ist eine *"trusted third party"*, welche die Identitäten aller Beteiligten bestätigt und ihnen mittels Zertifikaten Schlüssel zuweist.

Frage 2.2

> Was ist der Unterschied zwischen den Dateien root.cer und root.key und wofür werden sie jeweils verwendet? Wie sind sie aus Sicherheitsgesichtspunkten zu behandeln?

root.cer beinhaltet das Public-Key Zertifikat für die CA. root.key beinhaltet den dazu passenden Private-Key. Beides dient zur Authentifikation der CA.

Private Keys sollten nicht geteilt und nach Möglichkeit mit einer Passphrase geschützt werden. Die ".cer" Datei muss hingegen geteilt werden, damit andere die Identität bestätigen können.

Frage 2.3

> Was verbirgt sich im Praktikum hinter Dateien mit dem Namen *.csr. Wofür werden sie verwendet?

Hierbei handelt es sich um die Anfragen an die CA, ein Schlüsselpaar zu erstellen. Es beinhaltet alle Daten welche die **CA** zum Ausstellen eines Zertifikats benötigt. Darunter Ínformationen zur Website und dem Inhaber (z.B. Common Name, Domain Name, Ort etc.). Den Public Key und Informationen zu diesem wzB. Länge und Art.

Frage 2.4

> Warum beklagt sich der Firefox Browser beim Aufruf der neuen Website über https? Welche Möglichkeiten gibt es, diese Meldung zu beseitigen und welche Sicherheitsauswirkungen haben diese jeweils?

Firefox kann die Identität des Servers nicht bestätigen, da kein gültiges Zertifikat für die CA vorliegt. Das Zertifikat der **CA** kann in Firefox importiert werden, oder man kann eine Unverschlüsselte Verbindung eingehen. Dabei nimmte man in Kauf, dass Daten manipuliert oder abgehört werden können.