Technische Hochschule Rosenheim
Fakultät für Informatik
Prof. Dr. Reiner Hüttl

IT-Security

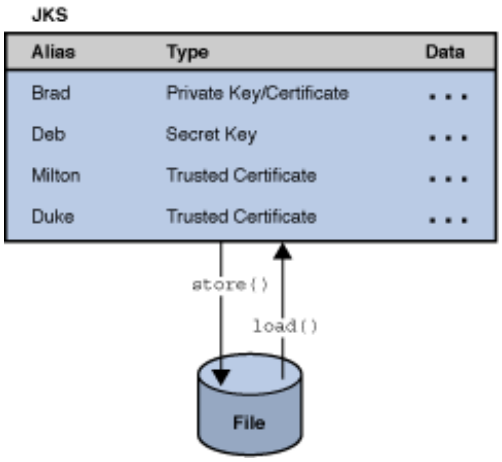
Übung 3

In dieser Übung ändern wir unser Programm zur Verschlüsselung einer Datei aus Übung 2.

Aufgabe 1: Abspeicherung des Schlüssels in einem KeyStore

Diesmal wird der Schlüssel nicht als Byte-Array in einer Datei gespeichert, sondern in einem **KeyStore** nach dem Standard PCKS#12.

Sehen sie sich dazu die Klasse **java.Security.KeyStore** an.



Ändern sie die Methoden **saveKey( )** und **readKey( )**. Schützen sie den KeyStore und den Schlüssel mit unterschiedlichen Passwörtern. Schreiben sie den KeyStore in eine Datei und lesen sie in wieder aus dieser Datei.

Hinweis:

- Verwenden sie als KeyStore-Type "JCEKS"
- Starten sie den Testtreiber nachdem sie saveKey() und readKey() implementiert haben

Aufgabe 2: Änderung des Verschlüsselungsmodus von ECB auf GCM

Bei der Änderung des Verschlüsselungsmodus auf **Galois Counter Mode** müssen sie einen **Initialisierungsvektor** der Länge 12 Byte und **Authentication Data** von 128 bit als zusätzliche Eingabe für die Ver- und Entschlüsselung erzeugen.

Hinweis:

- Die Methoden generateKey(), writeToFile(), readFromFileBase64() können sie von der letzten Übung übernehmen.
- Die Methoden saveKey(), readKey(), encrypt(), decrypt() müssen sie neu schreiben.
- Sehen sie sich die Klasse **javax.crypto.spec.GCMParameterSpec** an

Aufgabe 3: Passen sie ihren Testtreiber an und testen die Änderungen