Technische Hochschule Rosenheim

Fakultät für Informatik

Prof. Dr. Reiner Hüttl

IT-Security

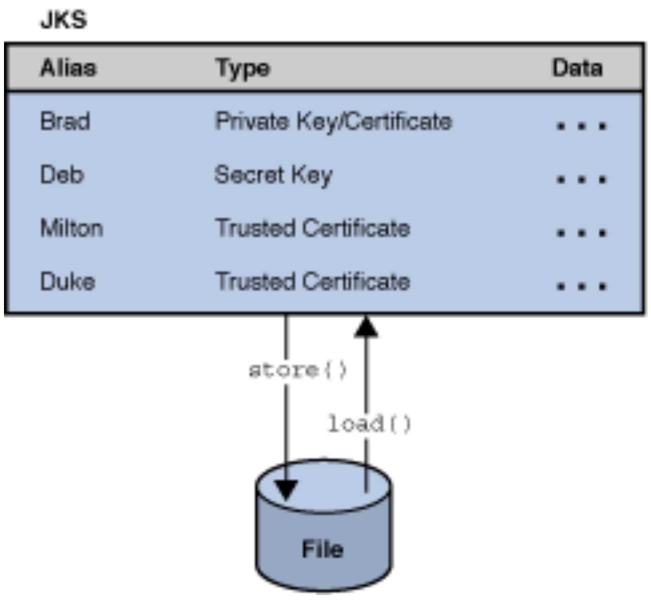
Exercise3

In this exercise we change our program to encrypt a file from exercise 2.

Task 1: Store the key in a KeyStore

This time, the key is not stored as a byte array in a file, but in a **KeyStore** according to the PCKS#12 standard.

See the **java class. Security.KeyStore.**
https://docs.oracle.com/en/java/javase/16/docs/api/java.base/java/security/KeyStore.html



First implement the class **KeyStoreUtils**. Protect the KeyStore and the key with different passwords. Write the KeyStore to a file and read it from this file again.

Hint:

1. Use "PKCS12" as KeyStore type

2. Start the test driver **TestKeyStore** after implementing the methods in the KeyStoreUtils class

Task 2: Change the encryption mode from ECB to AES-GCM

When changing the encryption mode to **Galois Counter Mode**, you must generate an **initialization vector** of length 12 bytes and authentication **data** of 128 bits (16 byte) as additional input for encryption and decryption.
Implement all missing methods in the classes **EncryptAesGcm** and **DecryptAesGcm** and test them with the test driver **TestAesGcmEncryption**.

Hint:

- The methods getRandomNonce(), generateAESKey(), readFromFile(), readFromFileBase64(), writeToFileBase64() can be found in the **CryptoUtils** class
- The methods saveKey(), readKey(), encrypt(), decrypt() must be rewritten.
- Look at the **javax.crypto.spec class. GCMParameterSpec** on

Task 3: Encryption with streams

When encrypting large amounts of data, it makes sense to perform the encryption operation piece by piece. To do this, implement the missing methods in the **StreamEncryption** and **StreamDecryption** classes using Java IO streams and then test them with the TestStreamEncryption test driver .

Hints:

- **FileStreams** can wrap each other
- Look at the **javax.crypto.CipherOutputStream** class

https://docs.oracle.com/en/java/javase/16/docs/api/java.base/javax/crypto/CipherOutputStream.html