Evidence Poin 55

Digisign membuat KMS (Key Management System) sendiri dengan menggunakan library yang disediakan oleh HSM NCipher. Dengan menggunakan library itu maka pasangan kunci pemilik akan digenerate pada HSM dan plainkey dari private key tidak dapat diexport atau keluar dari HSM.

6 nCipherKM JCA/JCE CSP

The nCipherKM JCA/JCE CSP (Cryptographic Service Provider) allows Java applications and services to access the secure cryptographic operations and key management provided by nCipher hardware. This provider is used with the standard JCE (Java Cryptographic Extension) programming interface.

To use the nCipherKM JCA/JCE CSP, you must install:

- the nShield Java package which includes the nShield Java jars and Keysafe.

Hasil dari generate pasangan kunci pada hsm adalah file key blob. Key blob dapat disimpan di external storage, karena key blob ini merupakan format keystore terenkripsi yang dikeluarkan oleh HSM dan hanya dapat dibaca dengan menggunakan HSM dengan kunci master yang aman.

Key blob

A key blob is a key object with its ACL and application data encrypted by a module key, a logical token, or a recovery key. Key blobs are used for the long-term storage of keys. Blobs are cryptographically secure; they can be stored on the host computer's hard disk and are only readable by units that have access to the same module key.

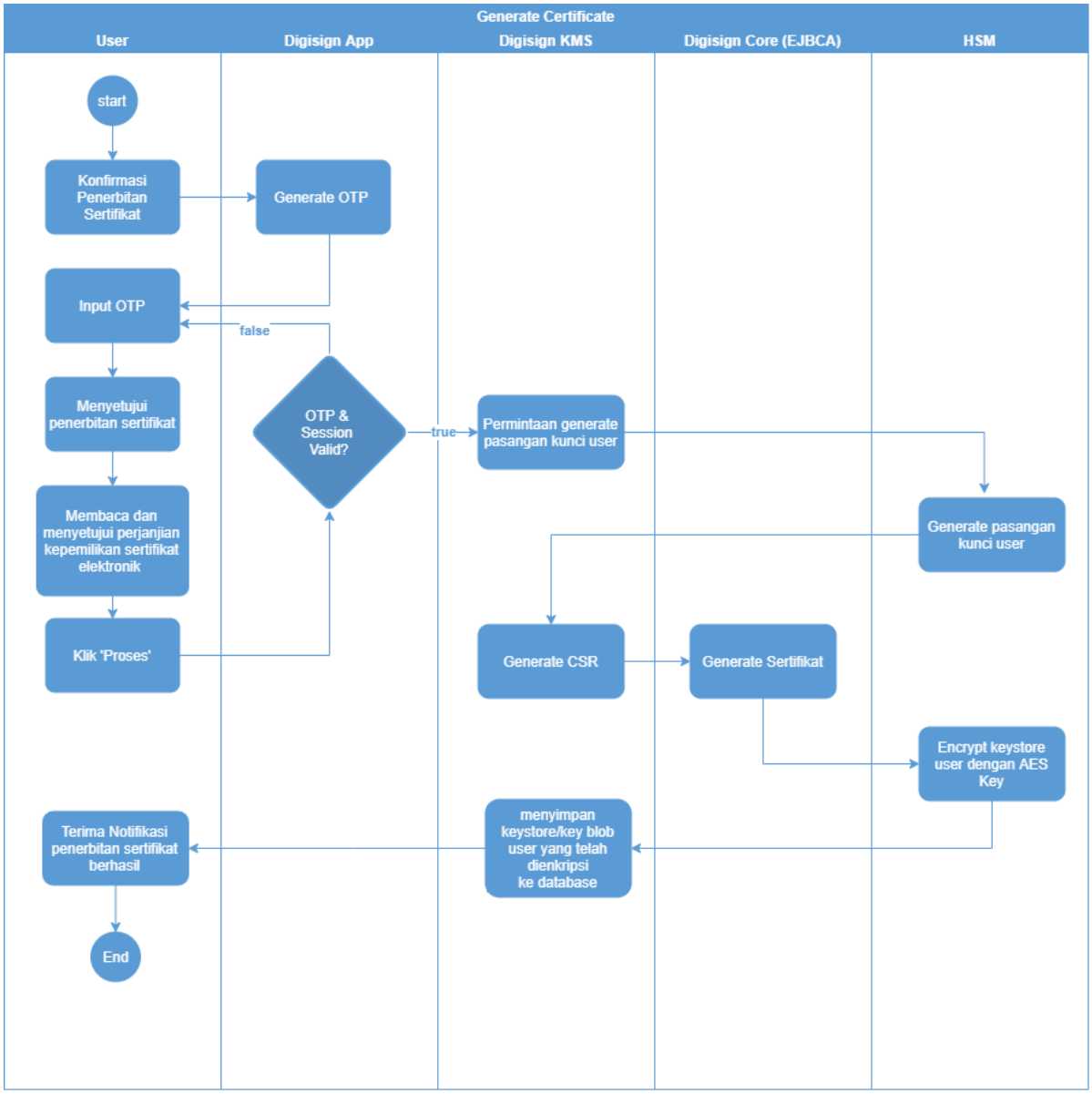
Segala jenis aktivitas enkripsi menggunakan private key user tersebut hanya dapat dilakukan di dalam HSM.

Berikut cuplikan kode java yang kami pakai untuk mengenerate pasangan kunci pemilik menggunakan Crypto provider yang disediakan oleh HSM yaitu 'nCipherKM' dan type keystore 'nCipher.sworld' .

```
String keystoretype = "nCipher.sworld";
String cryptoprovider = "nCipherKM";

KeyPairGenerator keyGen;
try {
    // Generate an RSA Key pair with HSM Lib
    keyGen = KeyPairGenerator.getInstance(algorithm: "RSA",cryptoprovider);
    keyGen.initialize(keysize: 2048, new SecureRandom());
    KeyStore keyStore = KeyStore.getInstance(keystoretype, cryptoprovider);
    KeyPair keyPair = keyGen.generateKeyPair();
```

Flow Chart untuk penerbitan sertifikat



Flowchart Penandatangan Dokumen