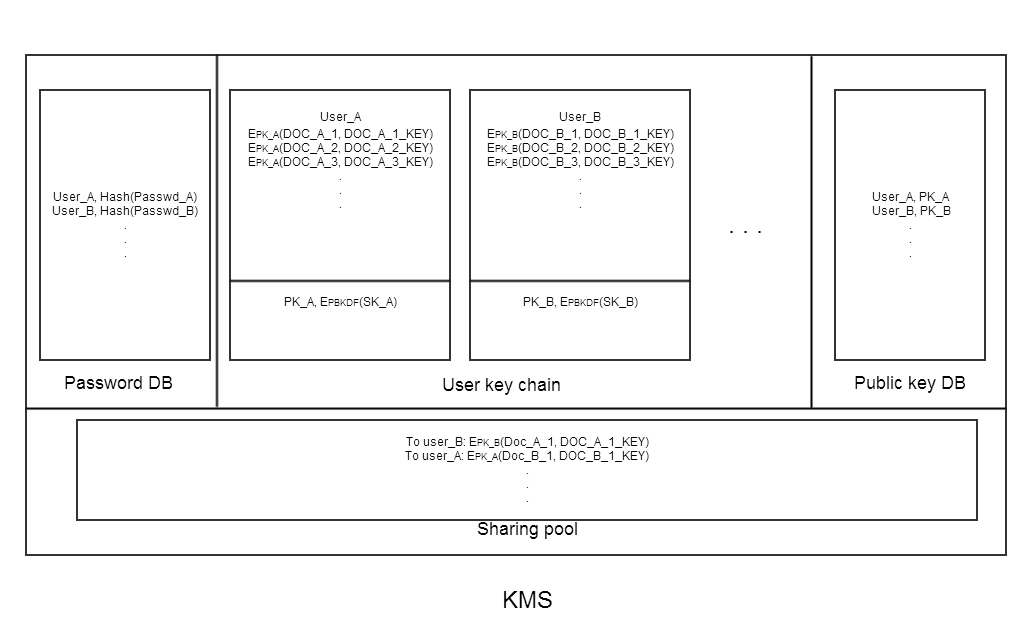
****

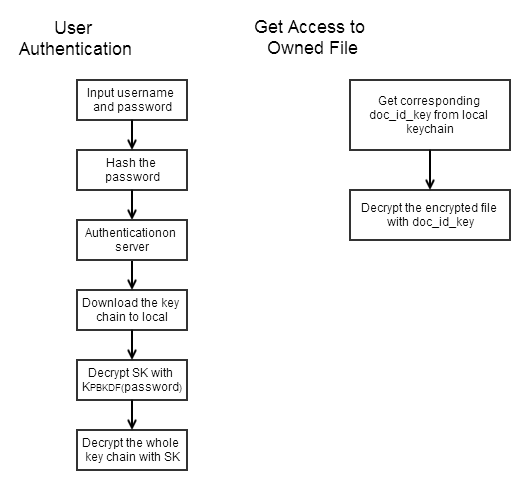
**Password DB stores user’s authentication information. Password is stored as hash code but not plaintext.**

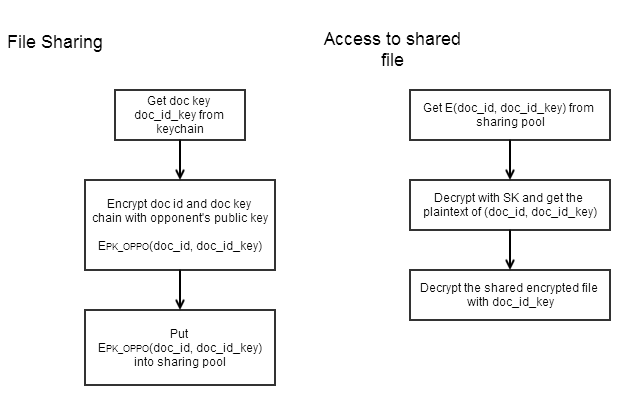
**User key chain includes encrypted pairs of (doc\_id, doc\_key). They are encrypted with user’s public key. The pair of PK and SK is also stored in this block but the SK is encrypted with a key derived from user’s password.**

**Public key database stores the public key of all the users. When sharing file with other user in the system, public key could be fetched from this database and applied in encrypting the pair (doc\_id, doc\_key).**

**Sharing pool includes the encrypted pairs of (doc\_id, doc\_key). The shared file recipient get such pairs from sharing pool and decrypt it locally with owned SK.**

**Some main procedures’ design which indicate the essence of this system are proposed as follows:**

****

****