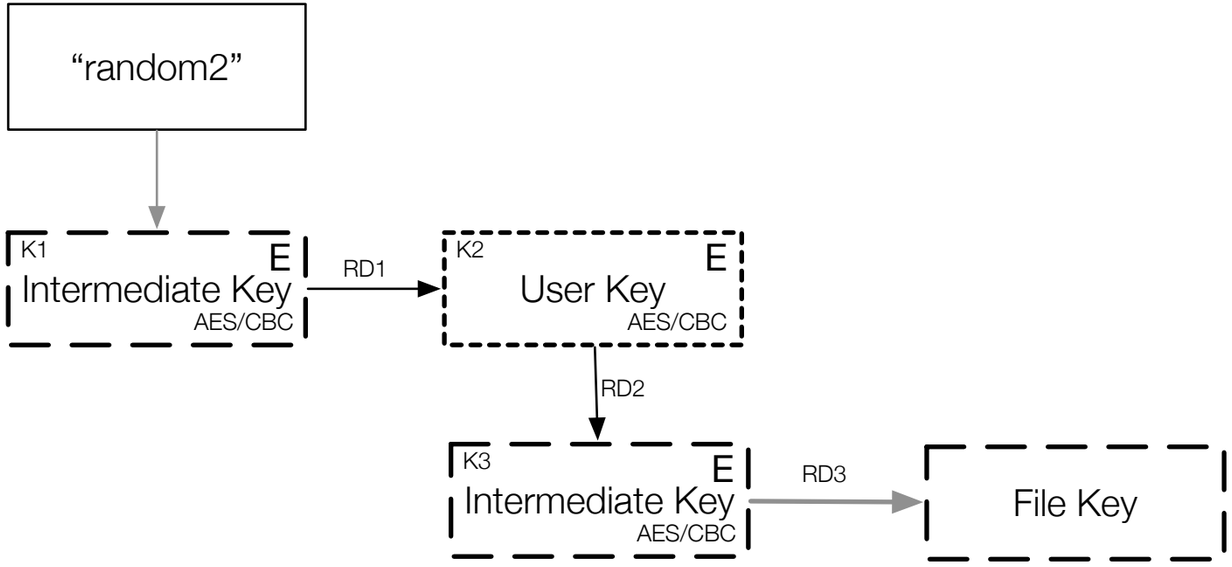

Book file key derivation process:

1º K1 = PBKDF2(sha224(user.username + "fcp" + book.identifier), random2)
2º RD1 = AES/CBC(Random2, K1)
3º K2 = PBKDF2(sha224(user.username + "deti" + random1), random1)
4º RD2 = AES/CBC(RD1, K2)
5º K3 = PBKDF2(sha224(n + “ua” + book.identifier), random2)
6º RD3 = AES/CBC(RD2, K3)

File Key = RD3

Note: The server and the player knows: file_identifier

— — — — — — Available in server and player

- - - - - - - - - - - - - - - Only available in server