## Datastore

| Key | Value | Key Derivation |
|---|---|---|
| saltUUID | random salt | saltHash = Hash(username + 'salt')<br>saltUUID = fromBytes(saltHash[:16]) |
| userUUID | {symmetrically encrypted user, mac} | sourceKey = Argon2Key(password, salt, 16)<br>userUUIDKey = HashKDF(sourceKey, username)<br>userUUID = fromBytes(userUUIDKey[:16]) |
| filePointerUUID | {symmetrically encrypted filePointer, mac} | filePointerUUID = uuid.New() |
| fileBlobUUID | {symmetrically encrypted fileBlob, mac} | fileBlobUUID = uuid.New() |
| invitationUUID | {symmetrically encrypted invitation, mac} | invitationUUID = uuid.New() |

## Symmetric Encryption Key Derivation

| Authenticate/ Encrypted Item | Key Derivation |
|---|---|
| User | sourceKey = Argon2Key(password, salt, 16)<br>encKey = HashKDF(sourceKey, username + "enc key")<br>macKey = HashKDF(sourceKey, username + "mac key") |
| FilePointer | sourceKey = Argon2Key(filePointerUUID.String(), salt, 16)<br>encKey = HashKDF(sourceKey, "enc key")<br>macKey = HashKDF(sourceKey, "mac key") |
| FileBlob | sourceKey = Argon2Key(fileBlobUUID.String(), salt, 16)<br>encKey = HashKDF(sourceKey, "enc key")<br>macKey = HashKDF(sourceKey, "mac key") |
| Invitation | sourceKey = Argon2Key(invitationUUID.String(), salt, 16)<br>encKey = HashKDF(sourceKey, "enc key")<br>macKey = HashKDF(sourceKey, "mac key") |