**Directory/Folder Structure(Client Side)**  
**Note: All names specified are folder name unless there’s an existence of file extension**.  
  
 Application Data  
 -> User  
 -> ID of User  
 -> Authentication\_Data  
 -> Login  
 -> LoginPK.txt  
 -> LoginSK.txt  
 -> Recovery\_Data  
 -> RecoveryPK.txt  
 -> RecoverySK.txt  
 -> SignedCombinedCipheredRandomData.txt  
 -> StreamCipherKey.txt  
 -> Server\_Directory\_Data  
 -> Directory\_ID  
 -> rootPK.txt  
 -> rootSK.txt  
 -> Encrypted\_Files  
 ->File\_ID  
 ->ED25519SK  
 ->SK(Count).txt  
 ->ED25519PK  
 ->PK(Count).txt  
 ->Key  
 ->Key(Count).txt  
 ->FileName.txt  
 ->FileContent(Count).txt  
  
**Cryptographic keys storage format**  
Note: All files that has either one of these **“PK”/”SK”/”Key”** along with **“txt”** file extension are responsible for storing cryptographic keys in **Bytes Array** format with specific good reason(s).  
  
  
**Note to client on storing cryptographic keys:**Please take good care of all cryptographic keys that resides under the directory of **“Server\_Directory\_Data”**. As server/service provider does not hold any of the cryptographic keys that are not visible to public, **server/service provider won’t be responsible for any keys lost on client side**.  
  
**Note to client on storing cryptographic keys(online):**   
If client decided to store cryptographic keys through available online file storage, please make sure that the online file storage has **“no access(Zero access/knowledge encryption or DKMS[Decentralized Key Management System])”**, if client decided to choose one that does not have the above properties though it guarantees ease of use or convenience(For example Google Drive), warning has been given, server/service provider won’t be responsible for any damage lost happened to client.  
  
The best recommended way to store these sensitive keys are the applications that really have “no access(Zero access/knowledge encryption or DKMS[Decentralized Key Management System])” properties, some commonly known applications are “Signal,WhatsApp,Matrix,Session,Threema”.  
  
**Miscellaneous important note to client:**  
**Client must not delete or not backup FileName.txt as it stores the original file name and the file extension in byte array format, losing FileName.txt will result in failure of decryption of fetched endpoint encrypted server files.**