## **Lockbox Scheme** Passphrase Salt Entered Hashed Passphrase Passphrase SHA256 PBKDF2 Derived Key Salt Derived Initialization Key Vector Encrypted Plain File IVs Random Key Random Key AES256 Plain Encrypted Random Key Random Key AES256