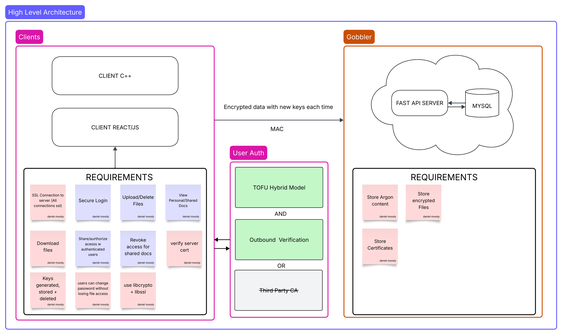
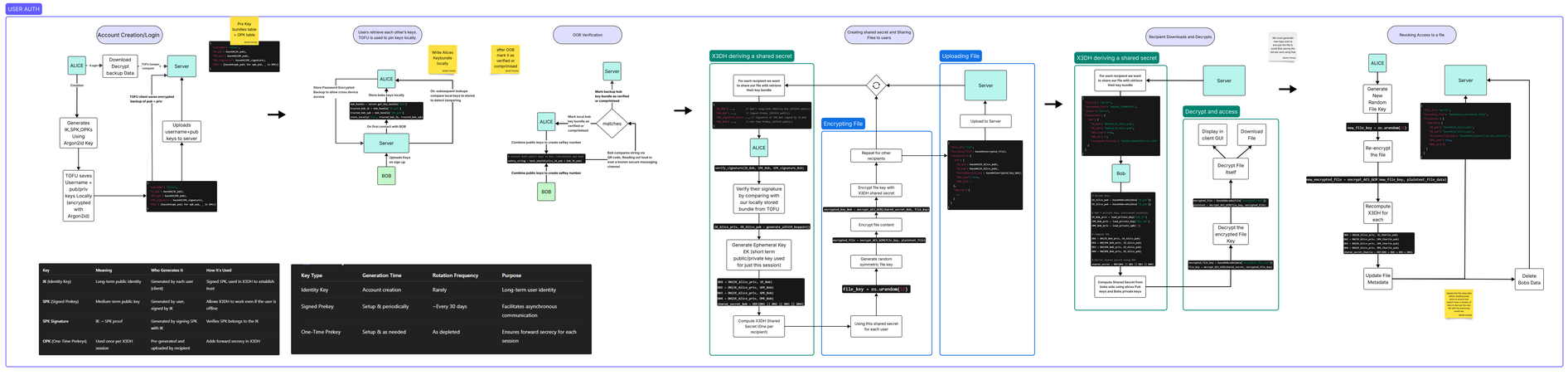


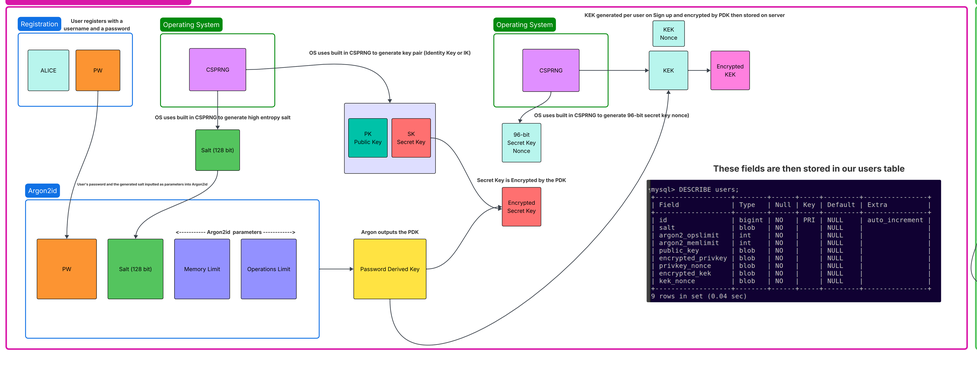


Key	Meaning	Who Generates It	How It's Used
IK (Identity Key)	Long-term public identity	Generated by each user (client)	Signed SPK, used in X3DH to establish trust
SPK (Signed Prekey)	Medium-term public key	Generated by user, signed by IK	Allows X3DH to work even if the user is offline
SPK Signature	IK → SPK proof	Generated by signing SPK with IK	Verifies SPK belongs to the IK
OPK (One-Time Prekeys)	Used once per X3DH session	Pre-generated and uploaded by recipient	Adds forward secrecy in X3DH

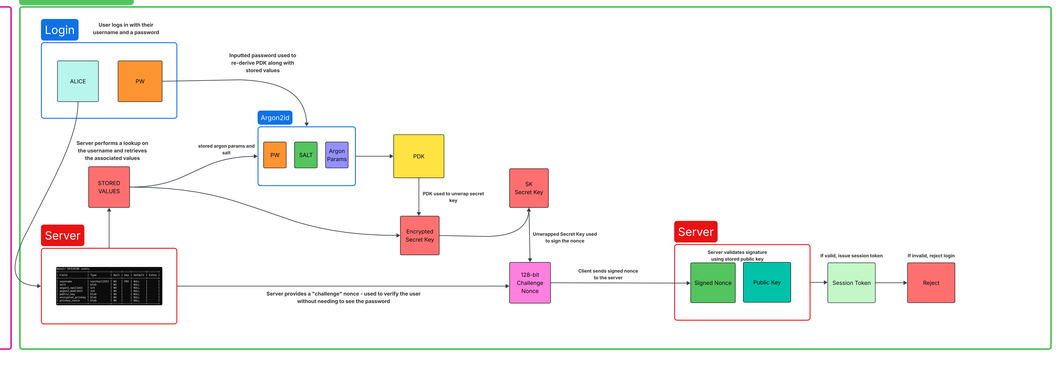
Key Type	Generation Time	Rotation Frequency	Purpose
Identity Key	Account creation	Rarely	Long-term user identity
Signed Prekey	Setup & periodically	~Every 30 days	Facilitates asynchronous communication
One-Time Prekey	Setup & as needed	As depleted	Ensures forward secrecy for each session

REGISTRATION + LOGIN SEQUENCE

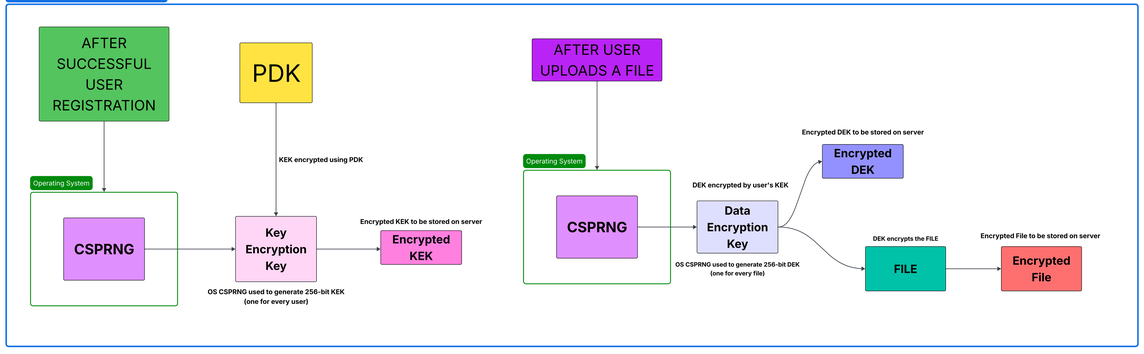
USER REGISTRATION



USER LOGIN



FILE ENCRYPTION



KEY HIERARCHY

