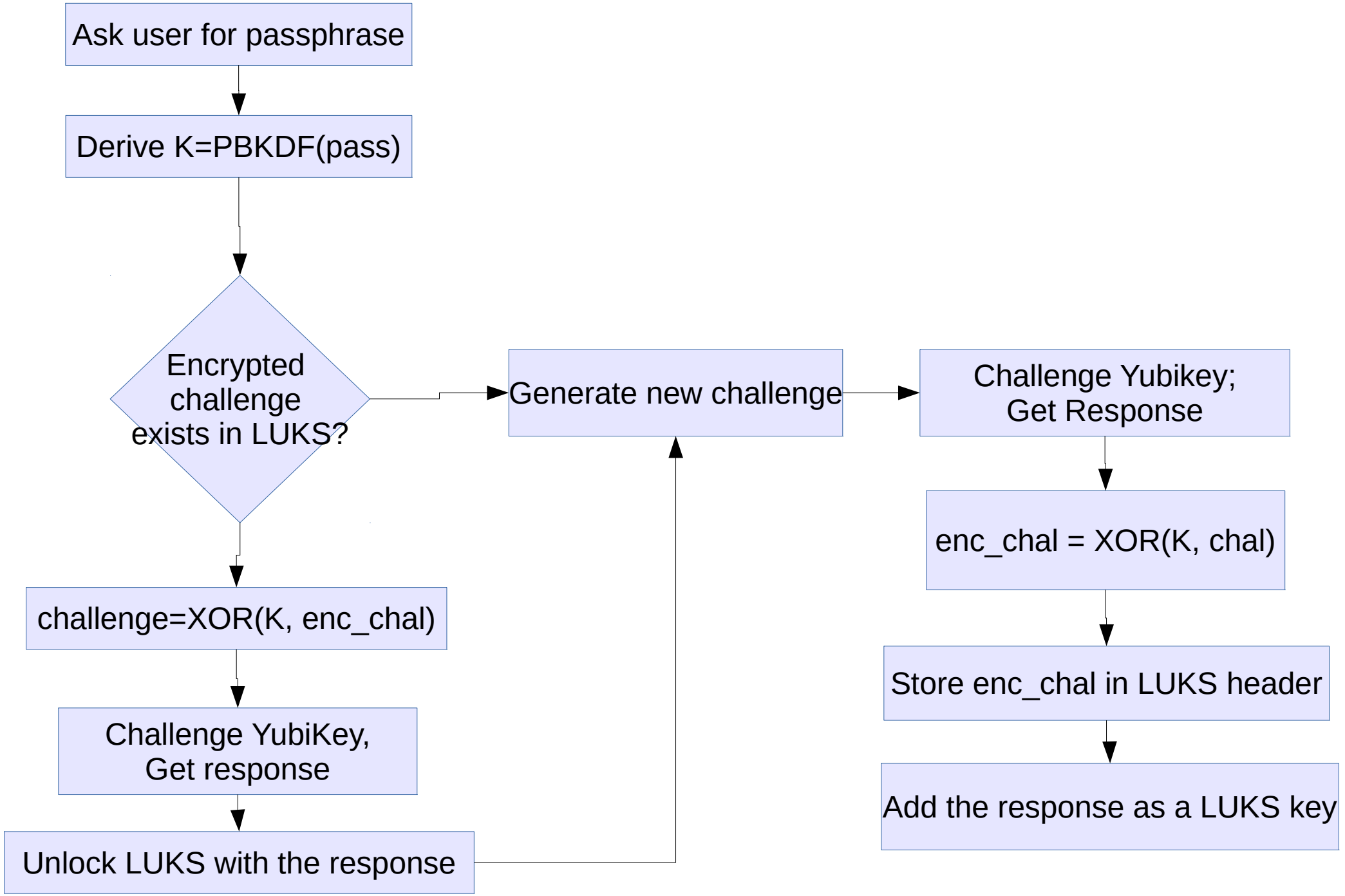
Ask user for passphrase
Derive K=PBKDF(pass)
Encrypted challenge exists in LUKS?
challenge=XOR(K, enc_chal)
Challenge YubiKey, Get response
Unlock LUKS with the response
Generate new challenge
Challenge Yubikey; Get Response
enc_chal = XOR(K, chal)
Store enc_chal in LUKS header
Add the response as a LUKS key