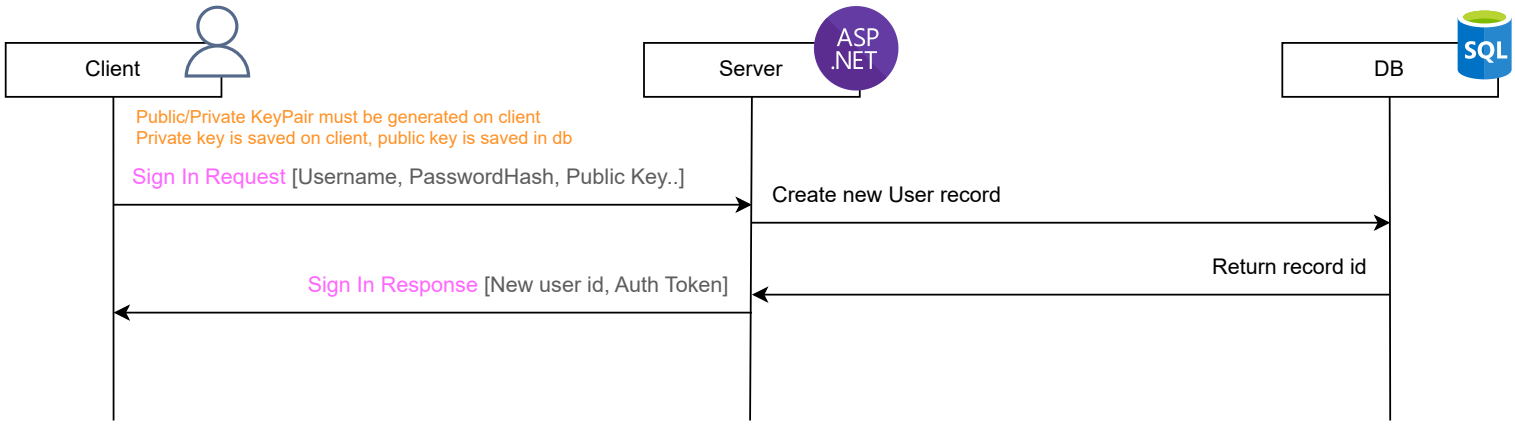
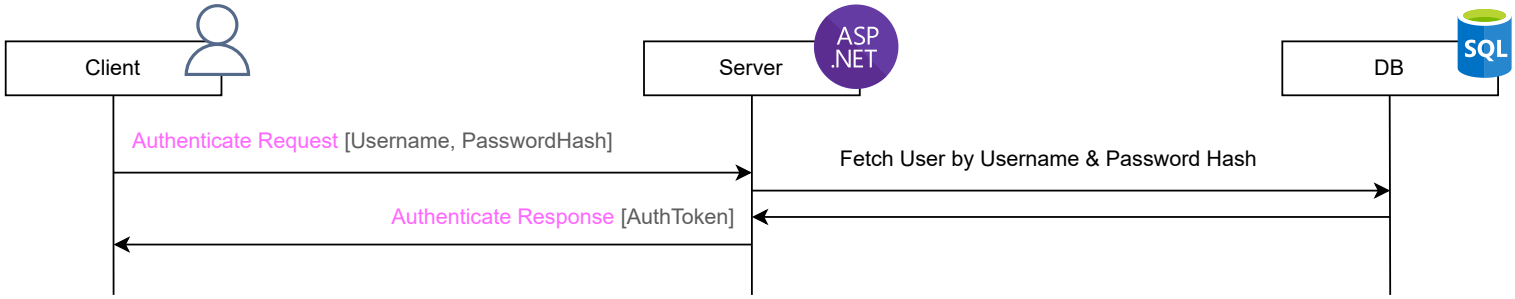
Zero Knowledge Architecture

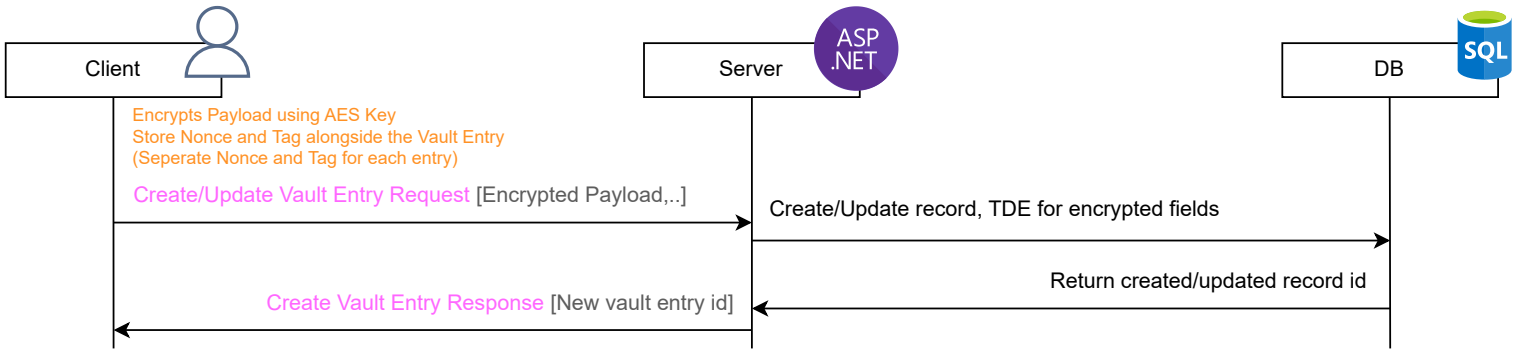
User Flow



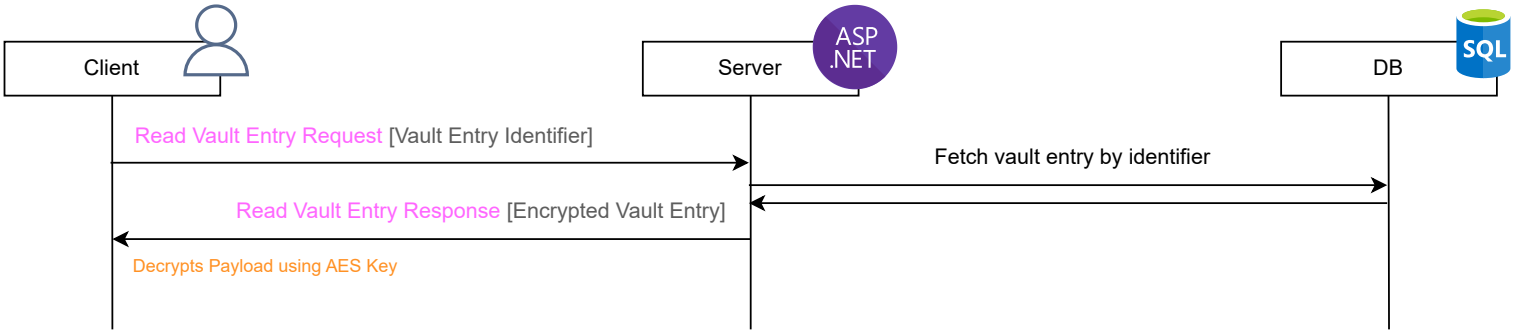
Authentication Flow



VaultEntry Create/Update Flow

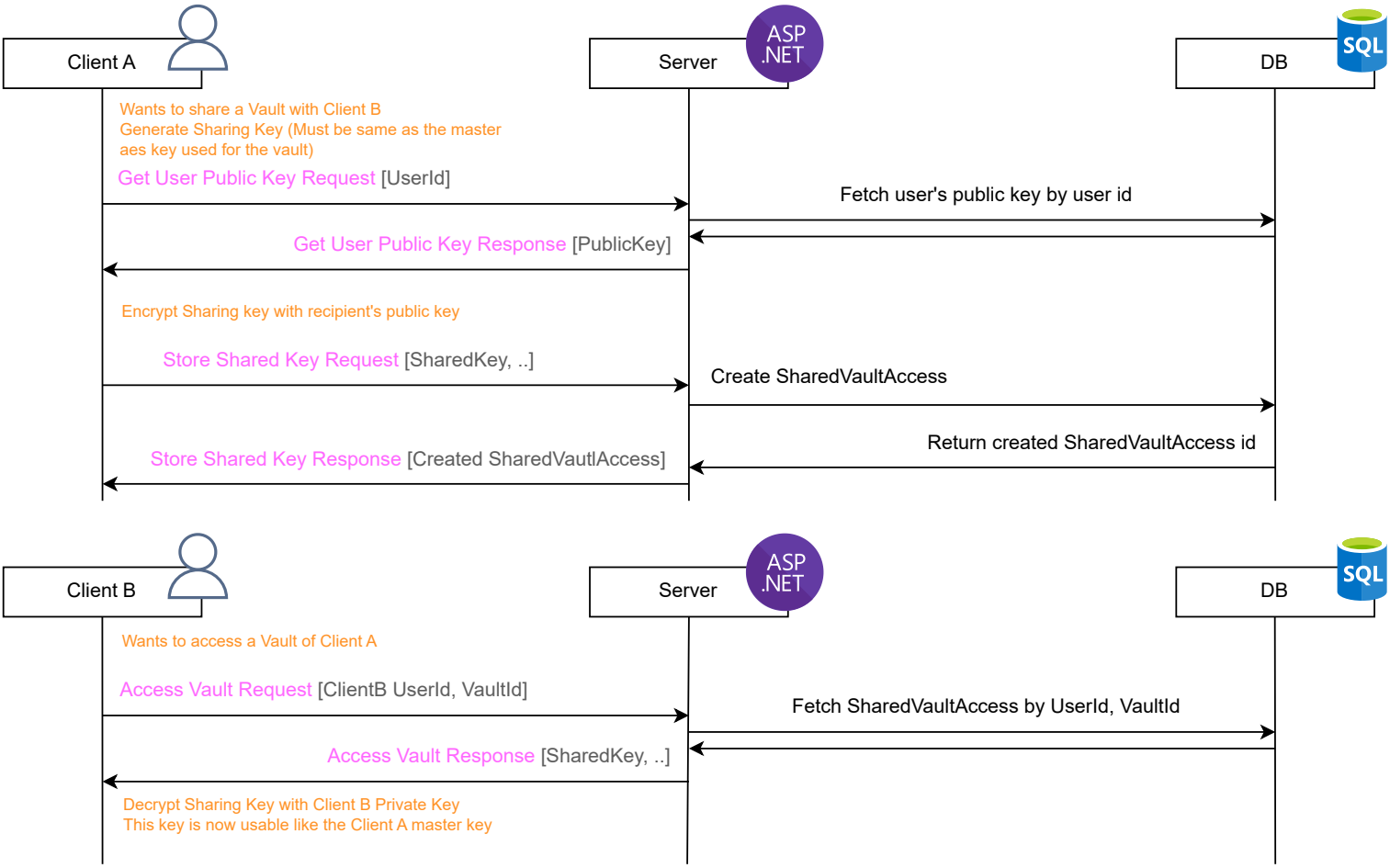


VaultEntry Read Flow



As seen, all sensitive data is ONLY encrypted/decrypted by the client. This means the server has no cryptographic information of the vault entries besides the used initialization vector and authentication tag (Zero knowledge Architecture)
Several other requests like creating/updating/deleting a Vault, User Management through an Admin etc. are not additionally encrypted

Shared Access Key Flow



For sharing a vault, a seperate SharedVaultAccess table is requried. There the Client A's aes key is encrypted with an rsa public key, so the zero knowledge architecture approach is still given and valid