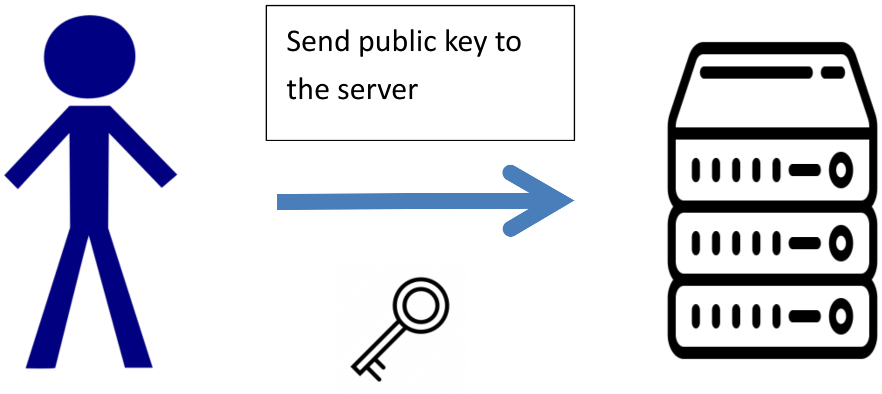
What is FIDO?

To understand FIDO, you must first understand public key cryptography's digital signature algorithm.

FIDO uses a mechanism which is not publicly known. This mechanism was called public key authentication.

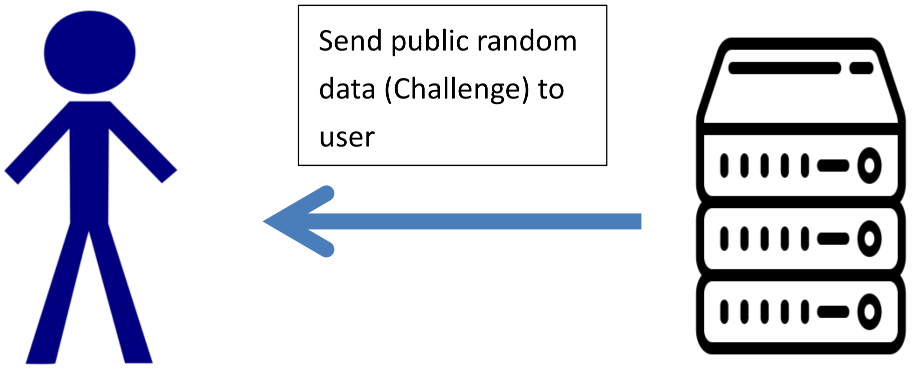
Assuming you are Bob, you have a key pair which consists of public and private key.

You send your public key to the server during registration or signing up.



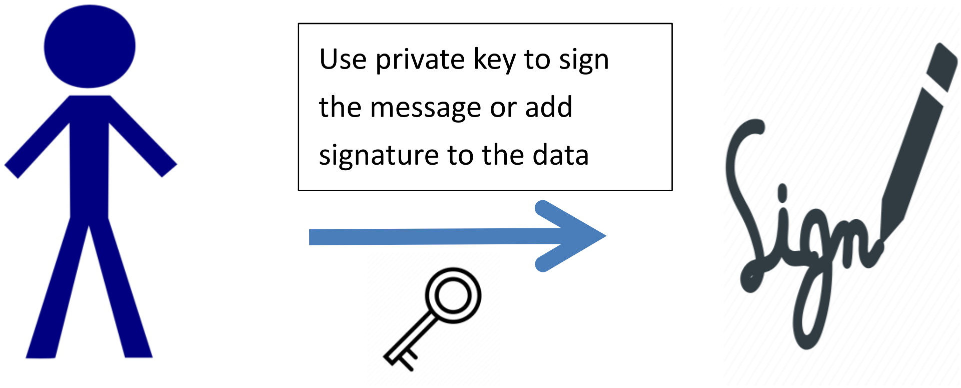
Send public key to the server

If you want to login into the server, you request the server to generate and send you a random public data which in technical terms was called "challenge".



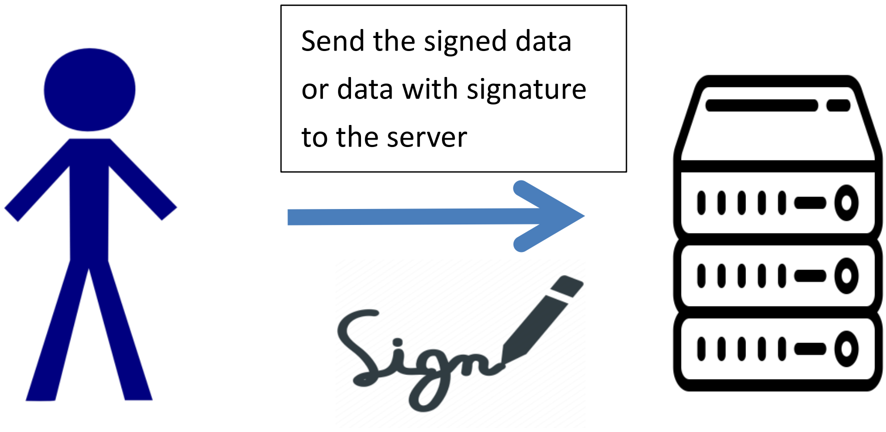
Send public random data (Challenge) to user

Once you get the data, you use your private key to encrypt or sign the data. You can assume it as using private key to generate a unique and tamper-proof version of real life signature.



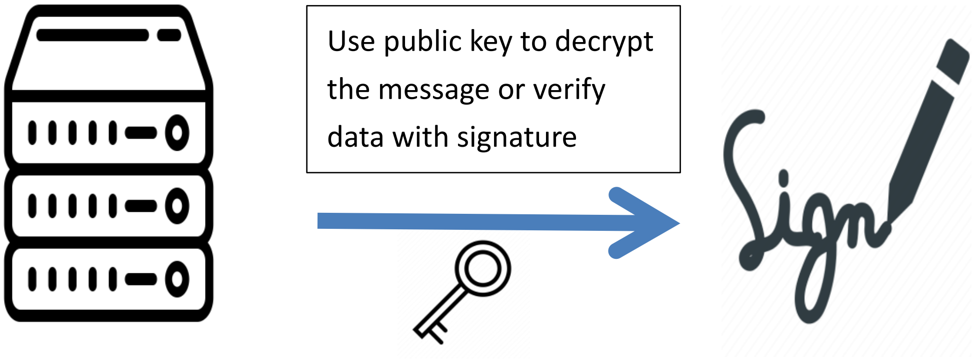
Use private key to sign the message or add signature to the data

Once you applied the signature to the data or sign the data or encrypt the data by using private key. You send back the signed data to the server.



Send the signed data or data with signature to the server

Once you have done that, the server will take the signature and verify/decrypt it using public key that you have sent during registration/sign up process.



Use public key to decrypt the message or verify data with signature

The server will then send either success or failed message to the user. Success indicates the user has now logged into the system and vice versa.

Pros (Advantage)

1. This process involves no user secret such as password or passphrase on server side. It also means that there's no password/passphrase to leak. Leaking the public key is not in criminal's interest as they can't get private key through public key.

2. This process if done correctly, user does not need to rely on problematic passwords to login anymore as this mechanism guarantees the same security for all users.

3. Users can change the public key that was stored on the server if they have bind identity/credentials such as email/phone number.

Cons (Disadvantage)

1. This mechanism was relatively new and introducing it will deliver user experience issues towards the user.

2. Binding identity such as email/phone number does pose a problem which the user may be vulnerable to social engineering or any other applicable attacks.