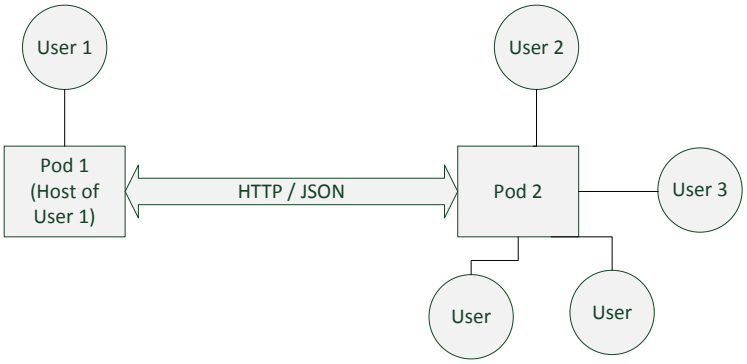
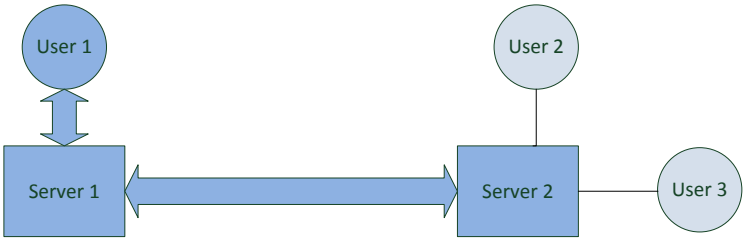
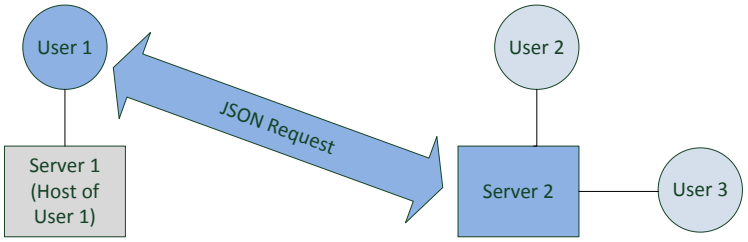

User 1
User 2
Pod 1
(Host of
User 1)
HTTP / JSON
Pod 2
User 3
User
User


User 1
User 2
Server 1
Server 2
User 3


User 1
JSON Request
User 2
Server 1
(Host of
User 1)
Server 2
User 3

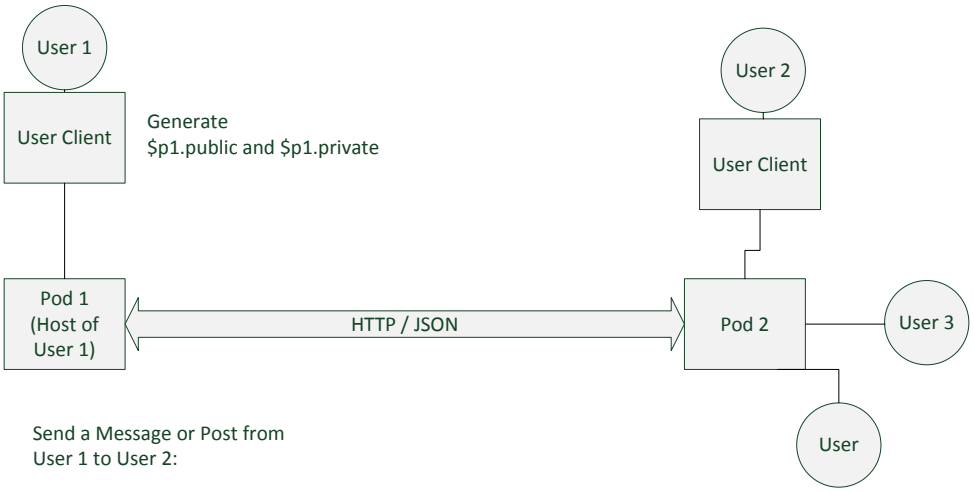
ENCRYPTION CONCEPT II

(Provider can not see user data)

$p = *Entered Password*
$p1 := md5($salt1.$p)
$p2 := md5($salt2.$p)

$p1 is stored local
$p2 is password for host pod

Problems:
- No password recovery from server
- Passwort change would require to transfer ALL data from server to client and recrpyt it.
- Client side app required
- How do we know messages are really from user1, the server could be evil?



Send a Message or Post from User 1 to User 2:

Use Public key of User 2 and private Key of User 1

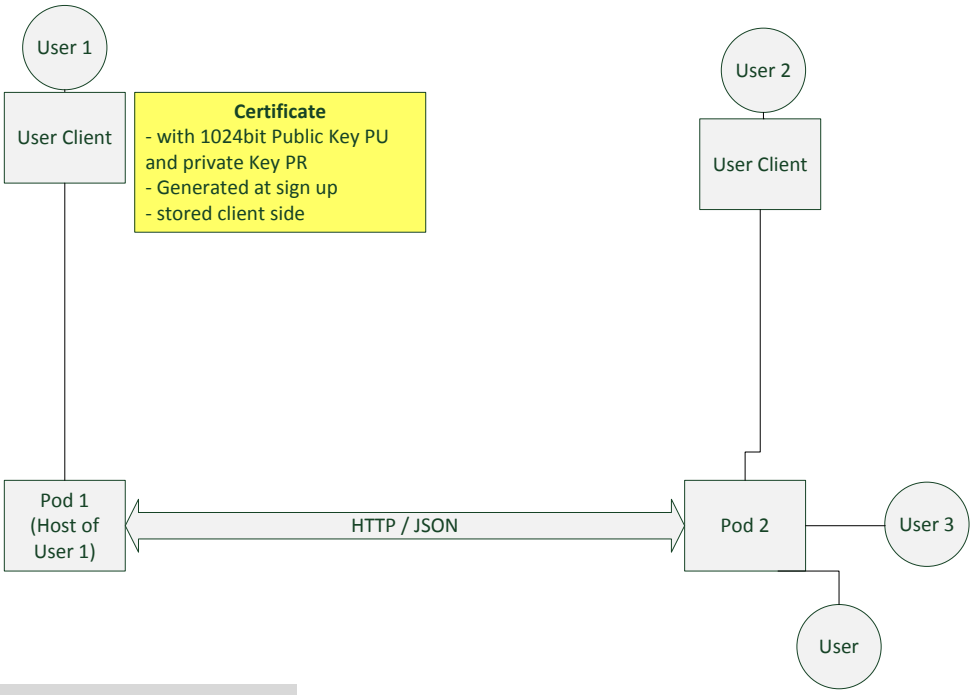
CHARME ENCRYPTION CONCEPT

PGP/ RSA as Certificate

- Certificate is encrypted with first part of password

- Second part of password is

Problems:
- No certificate recovery or change
- Client side app required



Send a Message or Post from User 1 to User 2:

Use Public key of User 2 to encrypt message

Send post to an audience

- Get all public keys of audience
- Generate random key and encrypt message with that key
- encrypt random key with each public key

-> Hybrid cryptosystem