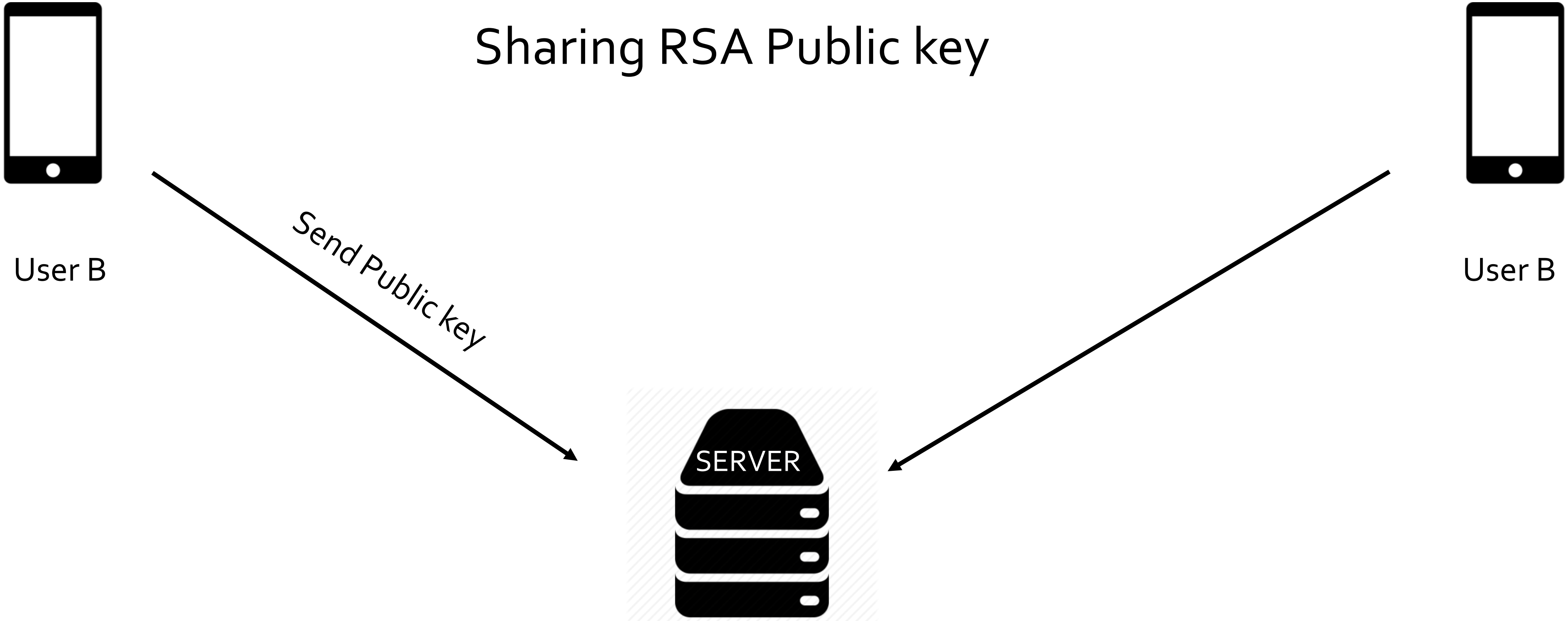
ANDROID JABBER

End to end encryption

Sharing RSA Public key



User B

Send Public key

User B

SERVER

User A - Public RSA Key
User B - Public RSA Key

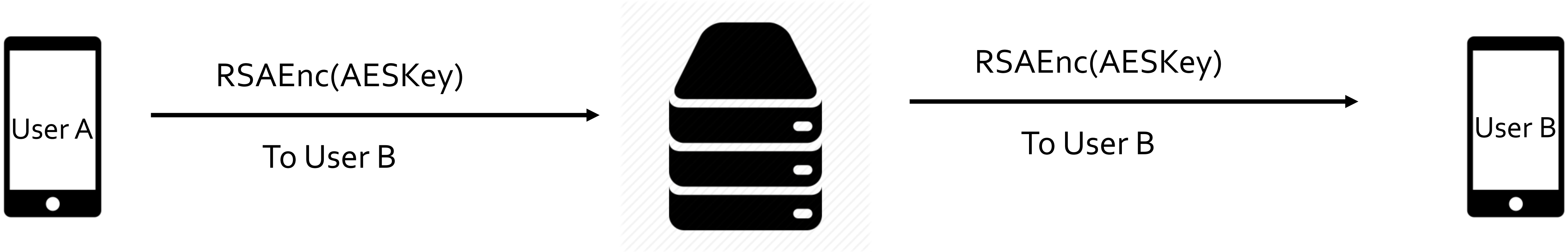
Sharing AES key

User A

- Generate AES key and save a copy
- Encrypt AES Key using User B public key
- Send it through server

User B

- Decrypt AES key using private RSA key
- Save AES key for that session



User A

RSAEnc(AESKey)

To User B

RSAEnc(AESKey)

To User B

User B

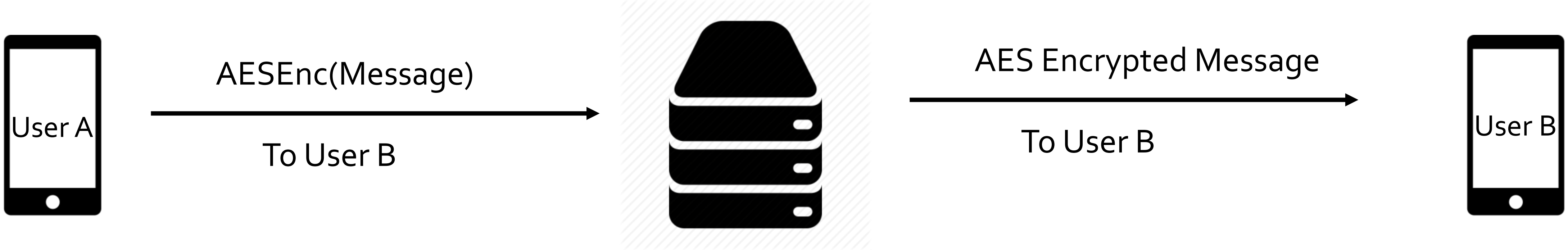
Encryption

User A

- Encrypt message using AES
- Send the encrypted message

User B

- Decrypt message using AES
- Display Message



User A

AESEnc(Message)

To User B

AES Encrypted Message

To User B

User B

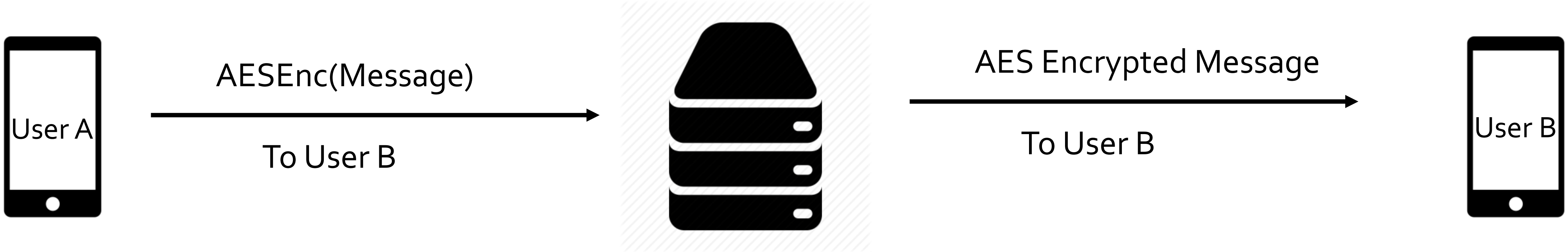
Authentication/Validation

User A

- Get hash value of message using SHA-256
- AES encrypt hash value
- Send it with the encrypted message

User B

- Decrypt message using AES
- Hash1 = Get hash value of message using SHA-256
- Hash2 = Decrypt hash(encrypted) received from server
- If(Hash1 == Hash2)   VALIDATED



User A

AESEnc(Message)

To User B

AES Encrypted Message

To User B

User B

DEMONSTRATION

THANK YOU