Encryption

Public keys and SSL

Valer 13.12.23

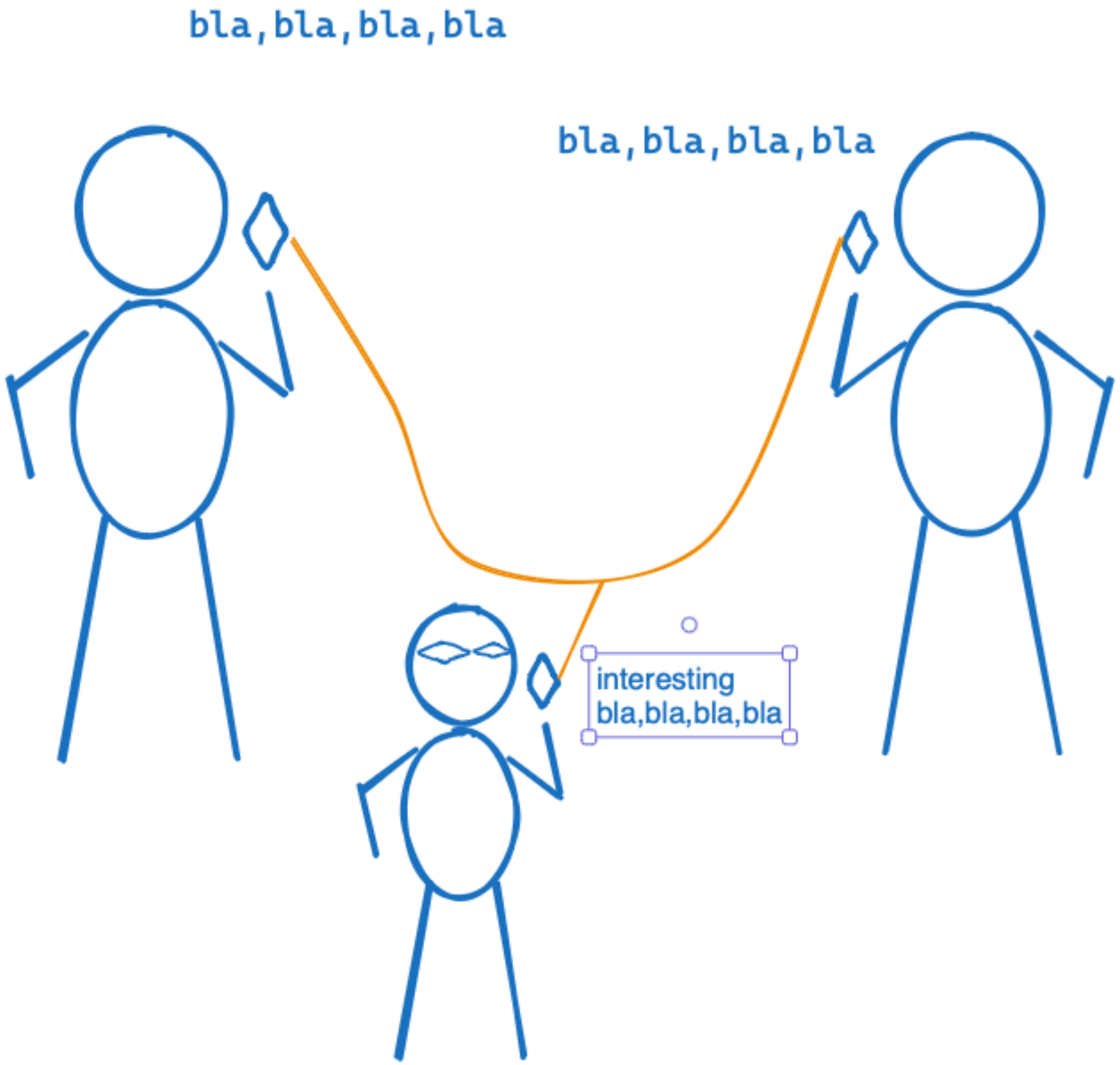
What SSL?

- A protocol to ensure the link between server and client is secure and the content hidden from a third party. Message on WhatsApp for i.e. are encrypted point-to-point

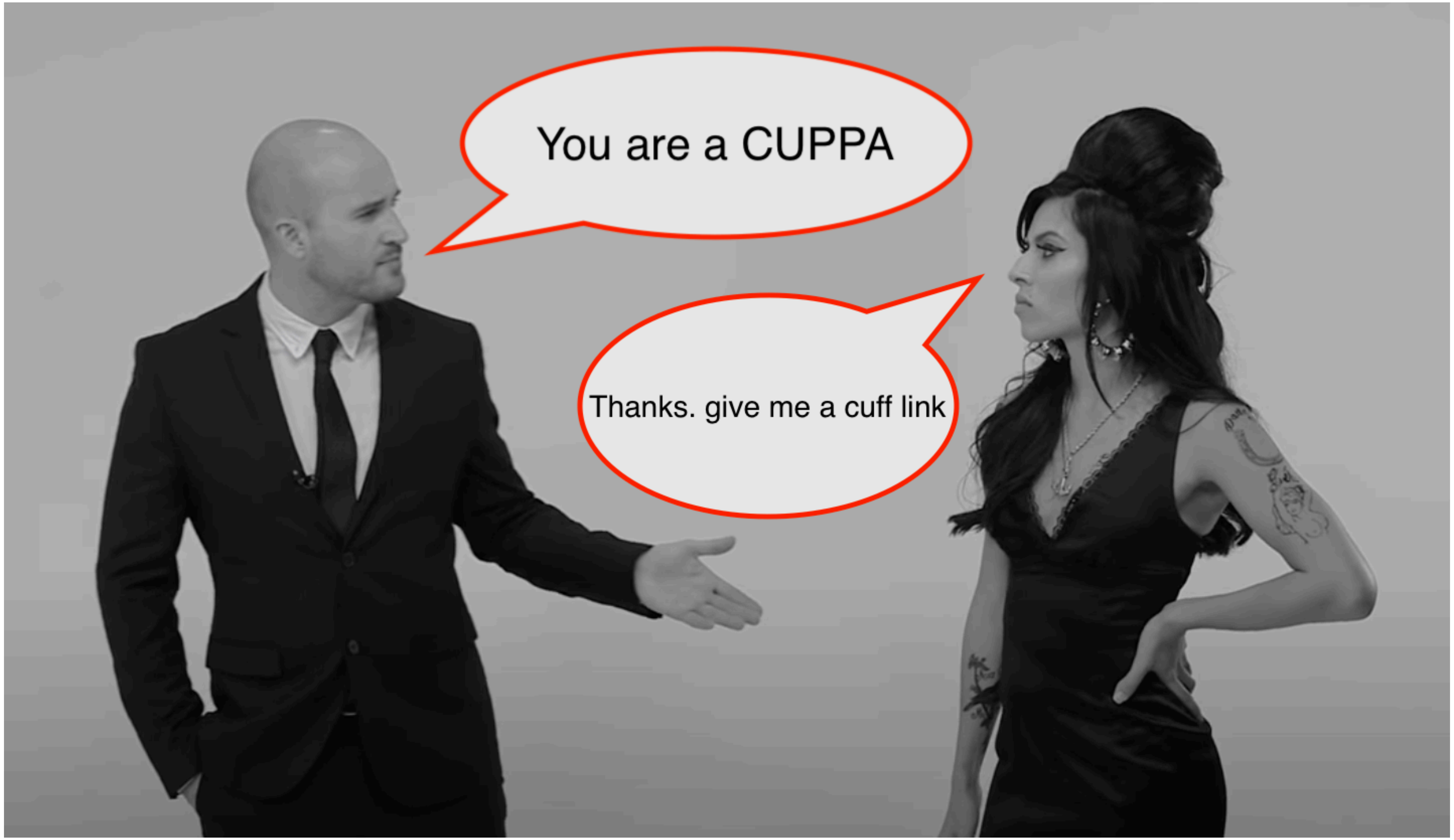
The problem to solve when sending and receiving message:

- Imaging you need to pay a contractor or book a room in advance over the phone. Would you communicate your card details knowing anyone with malicious intentions can tap in your phone or internet and steal your money?

- Back on time there was no way to hide the message.
- The conversation between 2 persons talking over the phone could have been easily intercepted.

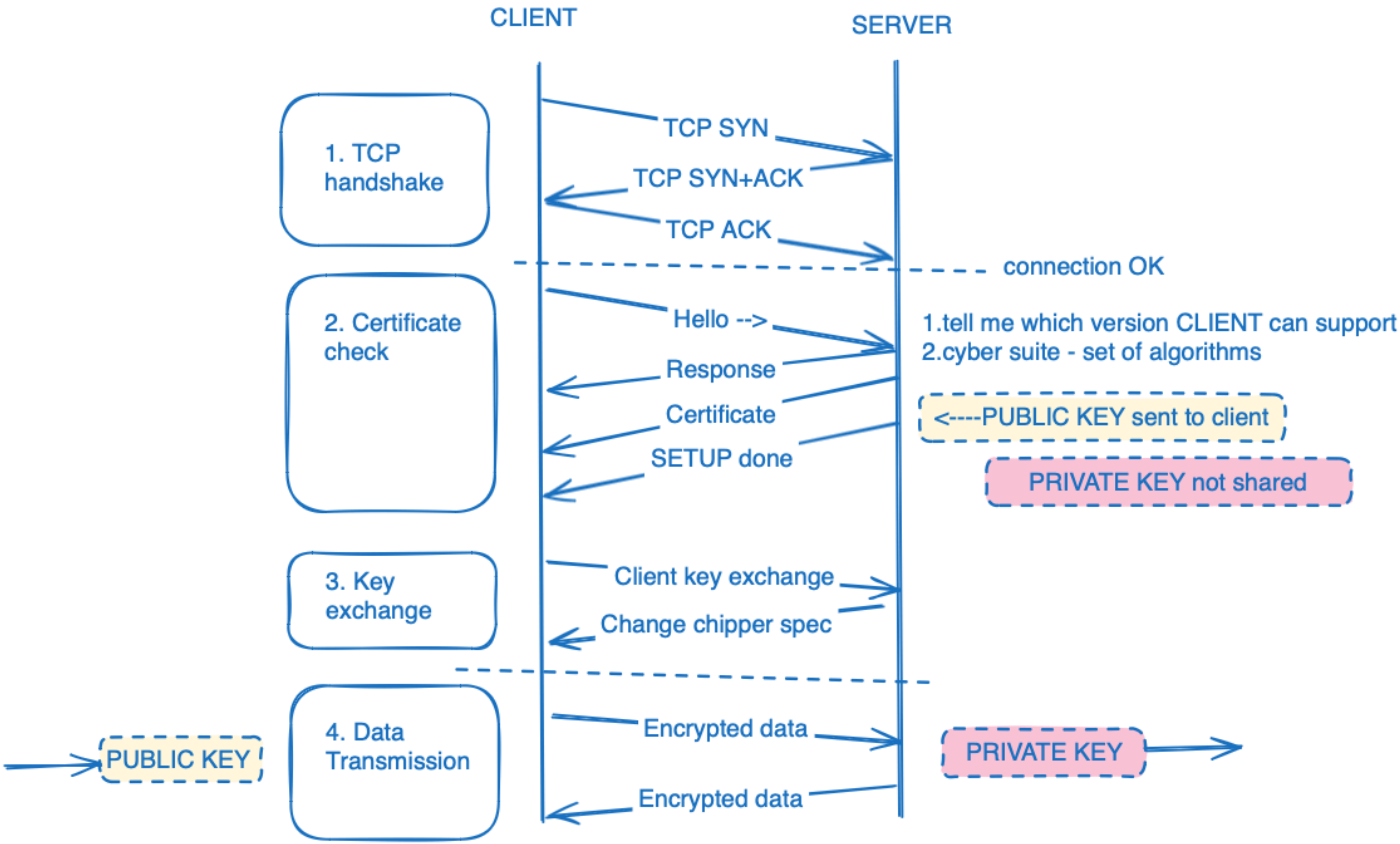


Solution: use a code



Whattt??

- Good but unless you want learn a slang and agree in advance….
- Solution for internet come with SSL.
- Encryption works as a mask which alter the real value of the real message. Think about a mask in photoshop where a bitmap layer is injected to overlap an image to alter the original colours.
- SSL use an asymmetric + Symmetric cryptography
- TLS improved the SSL security
- HTTPS is an extension of the HTTP protocol



CLIENT

SERVER

1. TCP handshake

TCP SYN

TCP SYN+ACK

TCP ACK

connection OK

2. Certificate check

Hello -->

1.tell me which version CLIENT can support
2.cyber suite - set of algorithms

Response

Certificate

<----PUBLIC KEY sent to client

SETUP done

PRIVATE KEY not shared

3. Key exchange

Client key exchange

Change chipper spec

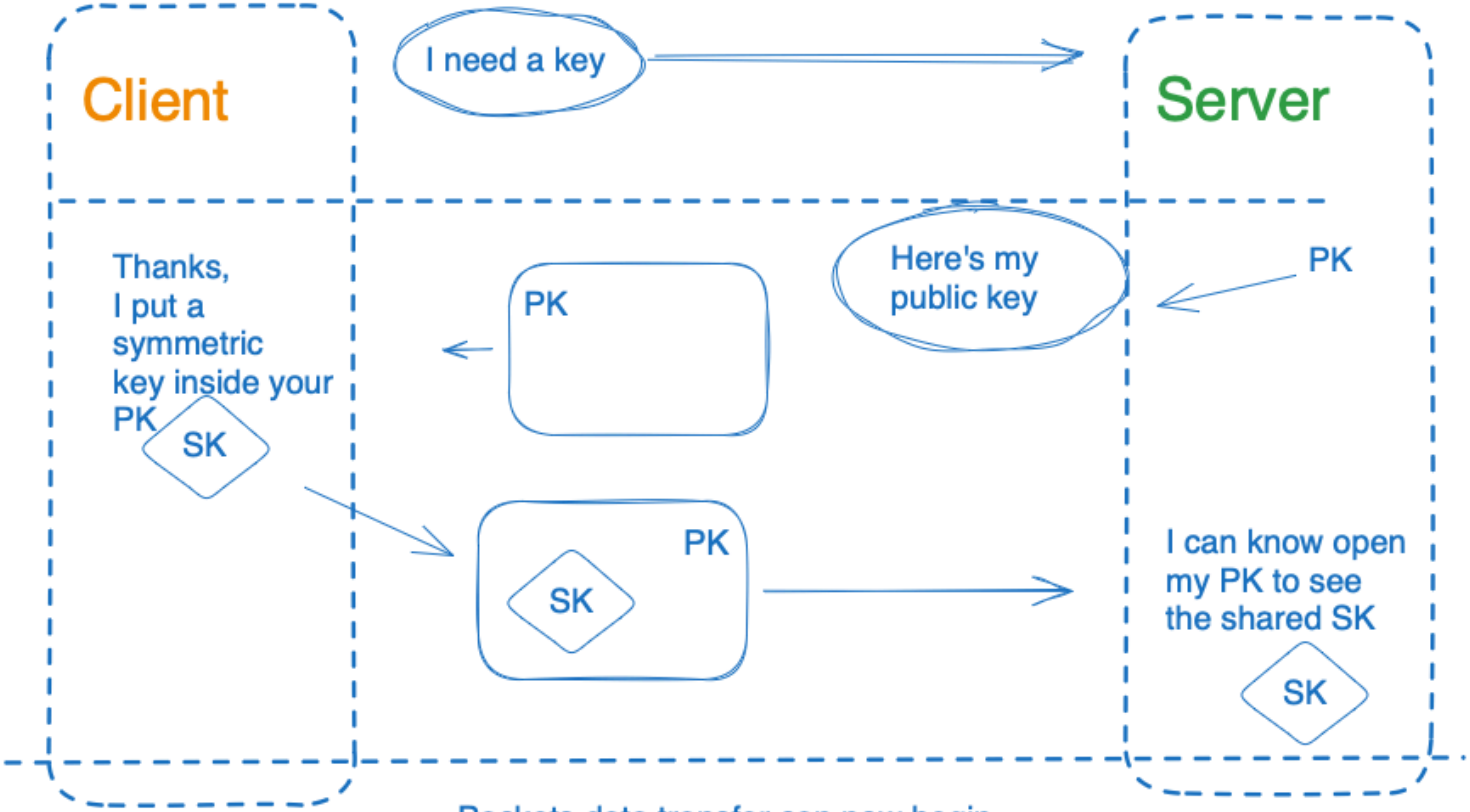
4. Data Transmission

PUBLIC KEY

Encrypted data

PRIVATE KEY

Encrypted data



I need a key

Here's my public key

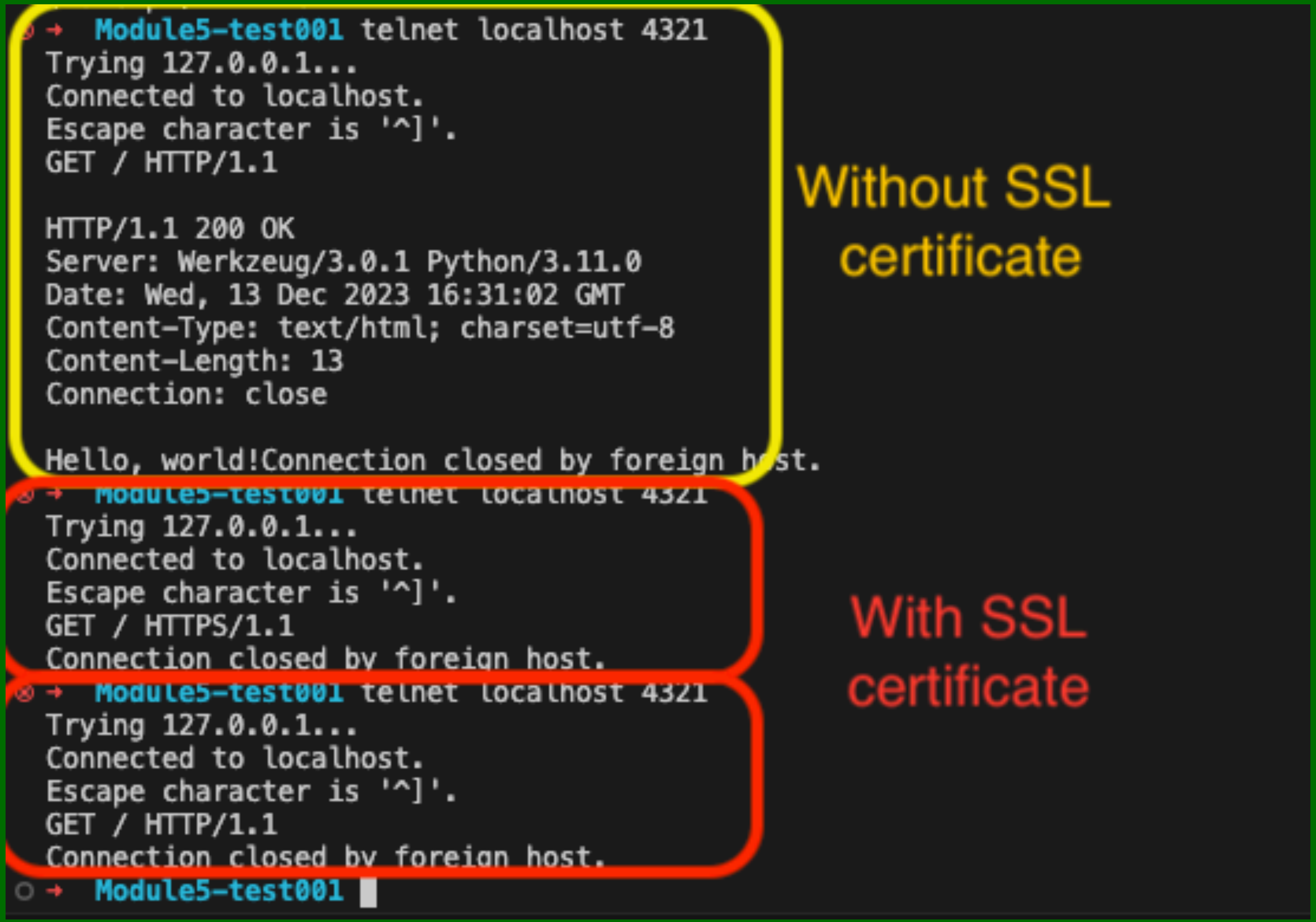
Thanks, I put a symmetric key inside your PK

I can know open my PK to see the shared SK

Packets data transfer can now begin

Running the server on localhost

- It seems TELNET is not granted access when running _flask + SSL_
- Not sure at this stage?!?



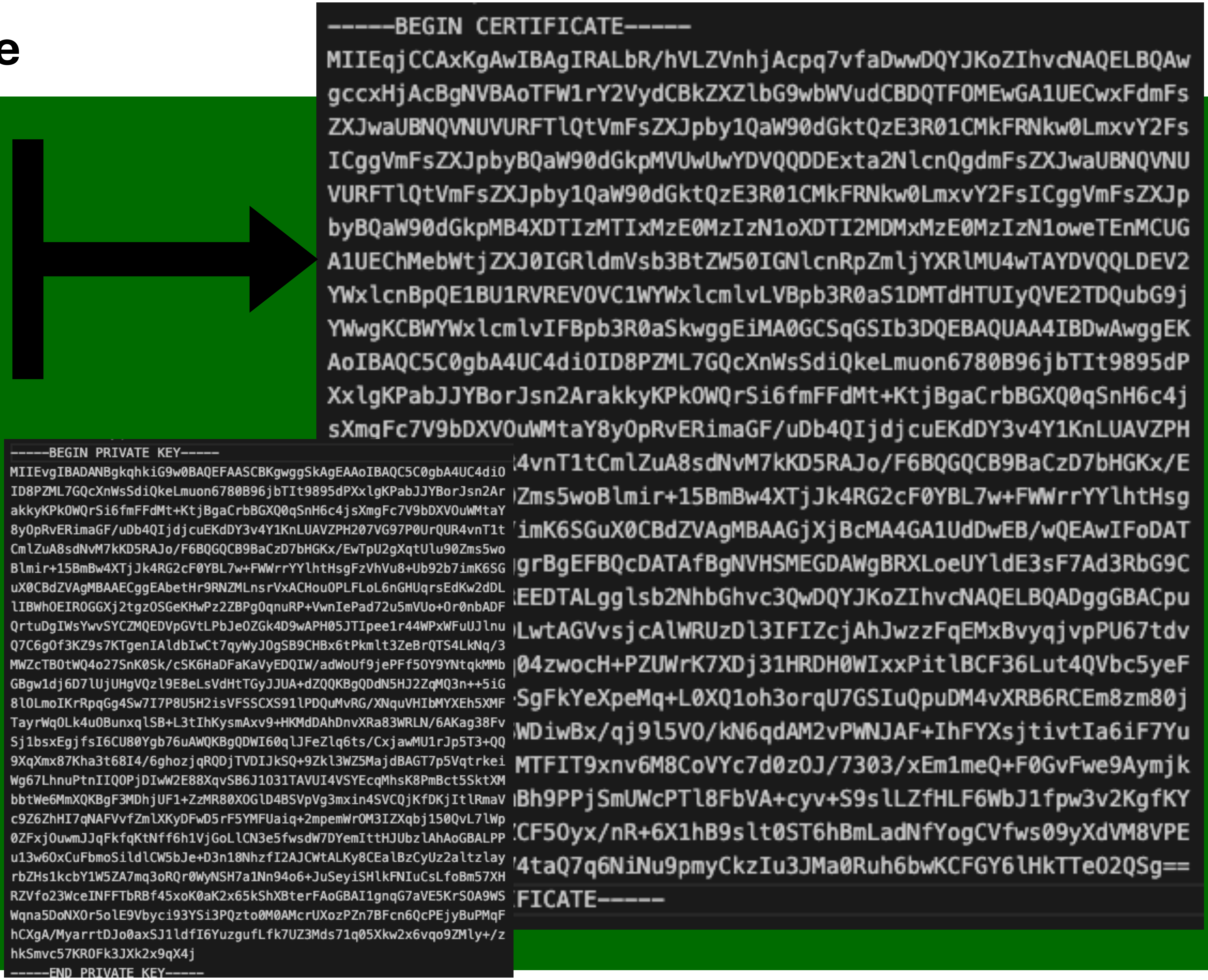
```
→  Module5-test001 telnet localhost 4321
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
GET / HTTP/1.1

HTTP/1.1 200 OK
Server: Werkzeug/3.0.1 Python/3.11.0
Date: Wed, 13 Dec 2023 16:31:02 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 13
Connection: close

Hello, world!Connection closed by foreign host.
⊗ →  Module5-test001 telnet localhost 4321
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
GET / HTTPS/1.1
Connection closed by foreign host.
⊗ →  Module5-test001 telnet localhost 4321
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
GET / HTTP/1.1
Connection closed by foreign host.
○ →  Module5-test001
```

Without SSL certificate

With SSL certificate

SSL certificate

- Server public’s key
- Server info
- Dig signature

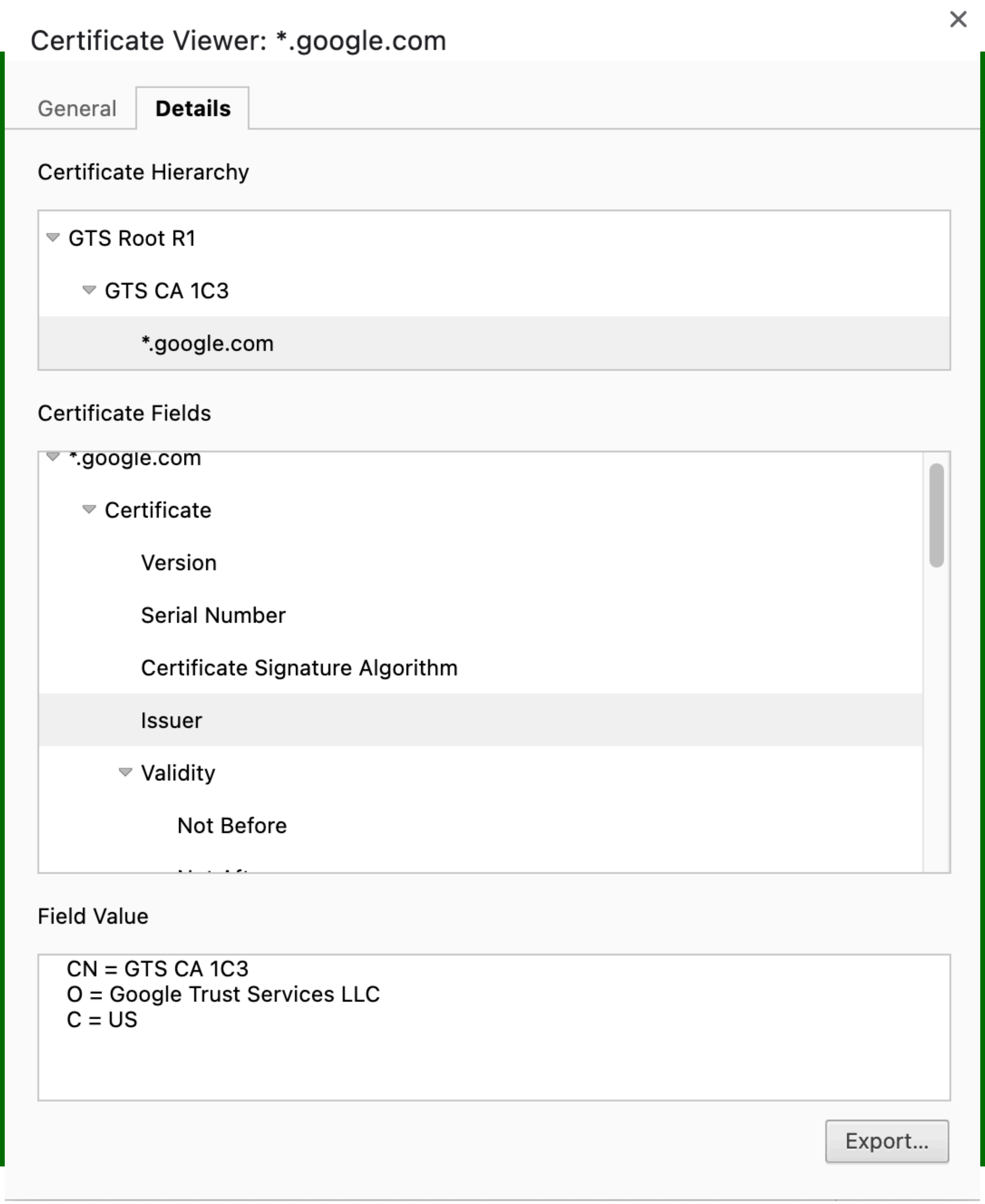


```
------BEGIN CERTIFICATE------
MIIEqjCCAxKgAwIBAgIRALbR/hVLZVnhjAcpq7vfaDwwDQYJKoZIhvcNAQELBQAw
gccxHjAcBgNVBAoTFW1rY2VydCBkZXZlbG9wbWVudCBDQTFOMEwGA1UECwxFdmFs
ZXJwaUBNQVNUVURFTlQtVmFsZXJpby1QaW90dGktQzE3R01CMkFRNkw0LmxvY2Fs
ICggVmFsZXJpbyBQaW90dGkpMVUwUwYDVQQDDExta2NlcnQgdmFsZXJwaUBNQVNU
VURFTlQtVmFsZXJpby1QaW90dGktQzE3R01CMkFRNkw0LmxvY2FsICggVmFsZXJp
byBQaW90dGkpMB4XDTIzMTIxMzE0MzIzN1oXDTI2MDMxMzE0MzIzN1oweTEnMCUG
A1UEChMebWtjZXJ0IGRldmVsb3BtZW50IGNlcnRpZmljYXRlMU4wTAYDVQQLDEV2
YWxlcnBpQE1BU1RVREVOVC1WYWxlcmlvLVBpb3R0aS1DMTdHTUIyQVE2TDQubG9j
YWwgKCBWYWxlcmlvIFBpb3R0aSkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQC5C0gbA4UC4diOID8PZML7GQcXnWsSdiQkeLmuon6780B96jbTIt9895dP
XxlgKPabJJYBorJsn2ArakkyKPkOWQrSi6fmFFdMt+KtjBgaCrbBGXQ0qSnH6c4j
sXmgFc7V9bDXVOuWMtaY8yOpRvERimaGF/uDb4QIjdjcuEKdDY3v4Y1KnLUAVZPH
4vnT1tCmlZuA8sdNvM7kKD5RAJo/F6BQGQCB9BaCzD7bHGKx/E
Zms5woBlmir+15BmBw4XTjJk4RG2cF0YBL7w+FWWrrYYlhtHsg
imK6SGuX0CBdZVAgMBAAGjXjBcMA4GA1UdDwEB/wQEAwIFoDAT
grBgEFBQcDATAfBgNVHSMEGDAWgBRXLoeUYldE3sF7Ad3RbG9C
EEDTALgglsb2NhbGhvc3QwDQYJKoZIhvcNAQELBQADggGBACpu
LwtAGVvsjcAlWRUzDl3IFIZcjAhJwzzFqEMxBvyqjvpPU67tdv
04zwocH+PZUWrK7XDj31HRDH0WIxxPitlBCF36Lut4QVbc5yeF
SgFkYeXpeMq+L0XQ1oh3orqU7GSIuQpuDM4vXRB6RCEm8zm80j
WDiwBx/qj9l5VO/kN6qdAM2vPWNJAF+IhFYXsjtivtIa6iF7Yu
MTFIT9xnv6M8CoVYc7d0zOJ/7303/xEm1meQ+F0GvFwe9Aymjk
Bh9PPjSmUWcPTl8FbVA+cyv+S9slLZfHLF6WbJ1fpw3v2KgfKY
CF5Oyx/nR+6X1hB9slt0ST6hBmLadNfYogCVfws09yXdVM8VPE
4taQ7q6NiNu9pmyCkzIu3JMa0Ruh6bwKCFGY6lHkTTeO2QSg==
FICATE------
```

Private Key

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQC5C0gbA4UC4diO
ID8PZML7GQcXnWsSdiQkeLmuon6780B96jbTIt9895dPXxlgKPabJJYBorJsn2Ar
akkyKPkOWQrSi6fmFFdMt+KtjBgaCrbBGXQ0qSnH6c4jsXmgFc7V9bDXVOuWMtaY
8yOpRvERimaGF/uDb4QIjdjcuEKdDY3v4Y1KnLUAVZPH207VG97P0UrQUR4vnT1t
CmlZuA8sdNvM7kKD5RAJo/F6BQGQCB9BaCzD7bHGKx/EwTpU2gXqtUlu90Zms5wo
Blmir+15BmBw4XTjJk4RG2cF0YBL7w+FWWrrYYlhtHsgFzVhVu8+Ub92b7imK6SG
uX0CBdZVAgMBAAECggEAbetHr9RNZMLnsrVxACHouOPLFLoL6nGHUqrsEdKw2dDL
lIBWhOEIROGGXj2tgzOSGeKHwPz2ZBPgOqnuRP+VwnIePad72u5mVUo+Or0nbADF
QrtuDgIWsYwvSYCZMQEDVpGVtLPbJeOZGk4D9wAPH05JTIpee1r44WPxWFuUJlnu
Q7C6gOf3KZ9s7KTgenIAldbIwCt7qyWyJOgSB9CHBx6tPkmlt3ZeBrQTS4LkNq/3
MWZcTBOtWQ4o27SnK0Sk/cSK6HaDFaKaVyEDQIW/adWoUf9jePFf5OY9YNtqkMMb
GBgw1dj6D7lUjUHgVQzl9E8eLsVdHtTGyJJUA+dZQQKBgQDdN5HJ2ZqMQ3n++5iG
8lOLmoIKrRpqGg4Sw7I7P8U5H2isVFSSCXS91lPDQuMvRG/XNquVHIbMYXEh5XMF
TayrWqOLk4uOBunxqlSB+L3tIhKysmAxv9+HKMdDAhDnvXRa83WRLN/6AKag38Fv
Sj1bsxEgjfsI6CU80Ygb76uAWQKBgQDWI60qlJFeZlq6ts/CxjawMU1rJp5T3+QQ
9XqXmx87Kha3t68I4/6ghozjqRQDjTVDIJkSQ+9Zkl3WZ5MajdBAGT7p5Vqtrkei
Wg67LhnuPtnIIQOPjDIwW2E88XqvSB6J1O31TAVUI4VSYEcqMhsK8PmBct5SktXM
bbtWe6MmXQKBgF3MDhjUF1+ZzMR80XOGlD4BSVpVg3mxin4SVCQjKfDKjItlRmaV
c9Z6ZhHI7qNAFVvfZmlXKyDFwD5rF5YMFUaiq+2mpemWrOM3IZXqbj150QvL7lWp
0ZFxjOuwmJJqFkfqKtNff6h1VjGoLlCN3e5fwsdW7DYemIttHJUbzlAhAoGBALPP
u13w6OxCuFbmoSildlCW5bJe+D3n18NhzfI2AJCWtALKy8CEalBzCyUz2altzlay
rbZHs1kcbY1W5ZA7mq3oRQr0WyNSH7a1Nn94o6+JuSeyiSHlkFNIuCsLfoBm57XH
RZVfo23WceINFFTbRBf45xoK0aK2x65kShXBterFAoGBAI1gnqG7aVE5KrSOA9WS
Wqna5DoNXOr5olE9Vbyci93YSi3PQzto0M0AMcrUXozPZn7BFcn6QcPEjyBuPMqF
hCXgA/MyarrtDJo0axSJ1ldfI6YuzgufLfk7UZ3Mds71q05Xkw2x6vqo9ZMly+/z
hkSmvc57KROFk3JXk2x9qX4j
-----END PRIVATE KEY-----
```

- Check the certificate
- if a website look suspicious



Certificate Viewer: *.google.com

Certificate Hierarchy

- GTS Root R1
  - GTS CA 1C3
    - *.google.com

Certificate Fields

- *.google.com
  - Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - Issuer
    - Validity
      - Not Before

Field Value

```
CN = GTS CA 1C3
O = Google Trust Services LLC
C = US
```

END