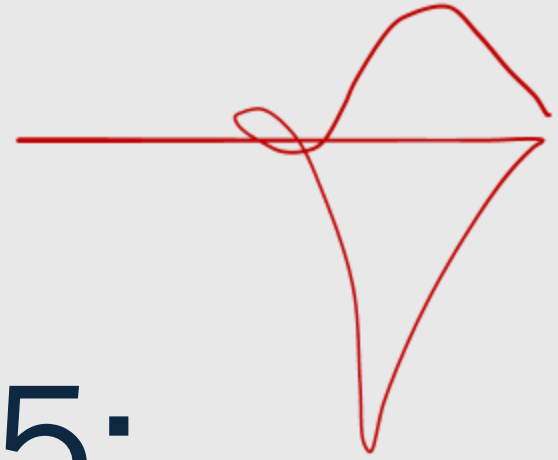


docker exec –it <container-name> /bin/bash

COMP435: *SECURITY CONCEPTS!*

Lecture 25: PKI, Certificates

tinyurl.com/comp435-fa25

Quiz Topics

- Cookies
  - *What are they/what are they for, who sets them, what do they look like (in a GET request)*
- Same Origin Policy
- Cross-Site Request Forgery (CSRF):
  - *What is it conceptually, how does it work technically, defenses*
- Cross Site Scripting (XSS):
  - *What is it conceptually, how does it work technically, defenses, differences from CSRF*
- SQL Injection Attacks:
  - *the dangers/harms of a successful attack, defenses, how the query is constructed by a web server. Understanding the keywords we've gone over in class*
- Certificate chains
  - *Whatever we get through today!*

PUBLIC KEY INFRASTRUCTURE & CERTIFICATES

Motivation:
HTTP over TLS (a.k.a. HTTPS)

Public Key Infrastructure (PKI)

Def’n: set of technologies and protocols for managing public-private key pairs and their use

Public Key Infrastructure (PKI)

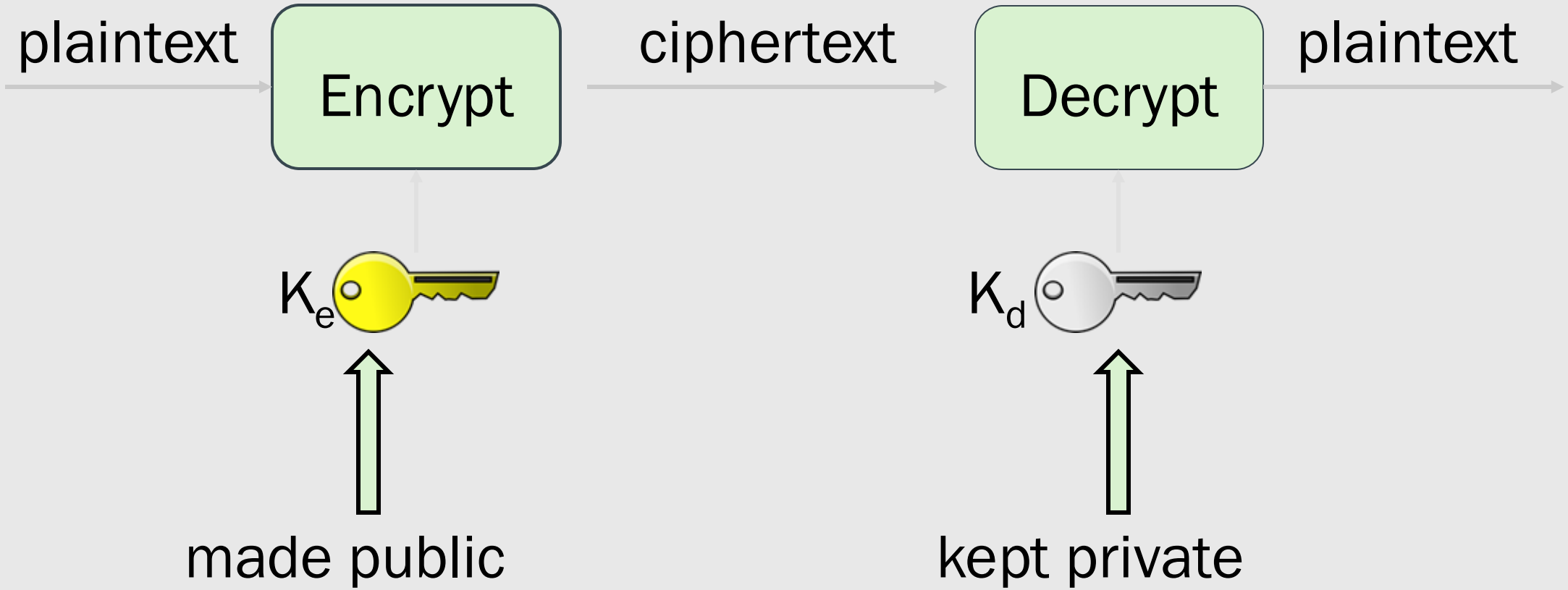
- Data structures: certificates
- Algorithms: key generation, installation, key use
- Architectures: certificate authorities (CA), CA directories
- Protocols: approving, acquiring, updating, and revoking certificates

PKI Use Cases

- HTTP over TLS (HTTPS)
- Encrypted email
- SSH
- IPsec
- DNSSEC

Public Key Encryption (Review)

Public Key Encryption

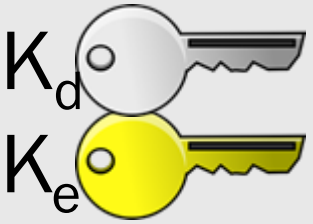


msg

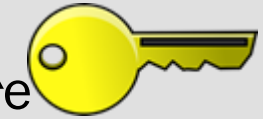
Dear Bob,
The secret word is cookie.
Sincerely,
Alice

Alice

Bob



Hello, World.
This is my public key.

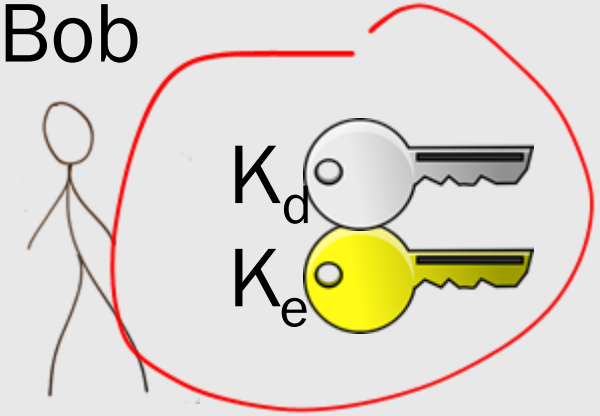
K_e 

msg

Dear Bob,
The secret word is cookie.
Sincerely,
Alice

Alice

Bob



$c = Enc_{Ke}(msg)$

c

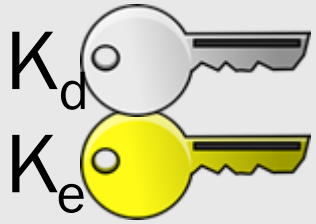
$msg = Dec_{Kd}(c)$

msg

Dear Bob,
The secret word is cookie.
Sincerely,
Alice

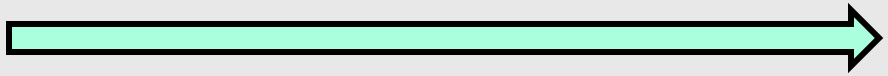
Alice

Bob



$c = Enc_{Ke}(msg)$

c



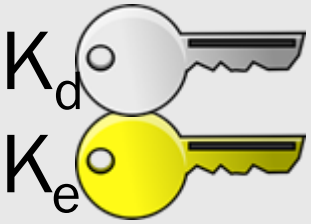
$msg = Dec_{Kd}(c)$

msg

Dear Bob,
The secret word is cookie.
Sincerely,
Alice

Alice

Not Bob



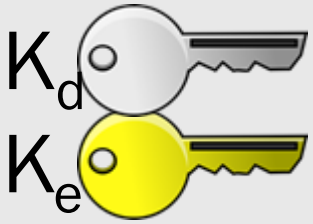
Hello, World. I am Bob. This is my public key.

msg

Dear Bob,
The secret word is cookie.
Sincerely,
Alice

Alice

Not Bob



Hello, World. I am Bob. This is my public key.

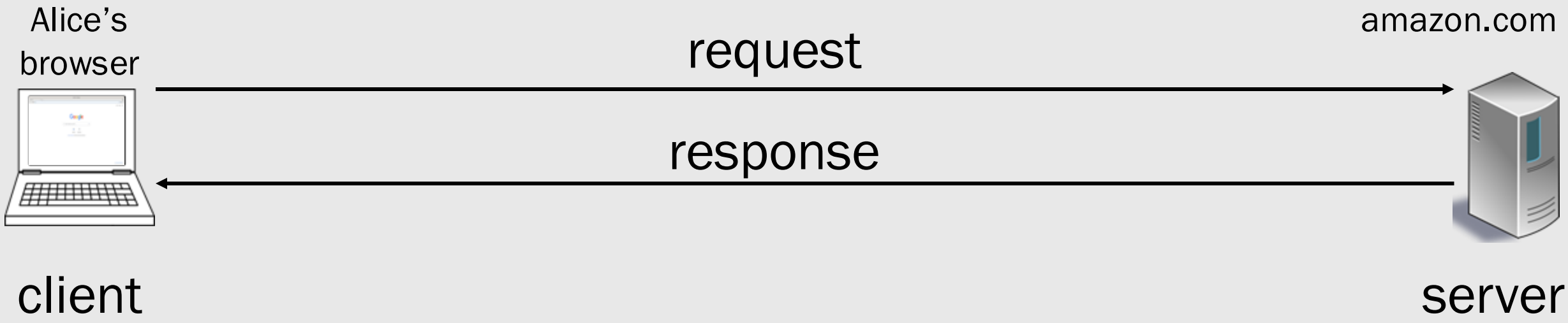
K_e 

PKI enables programmatically tying an entity to its public key

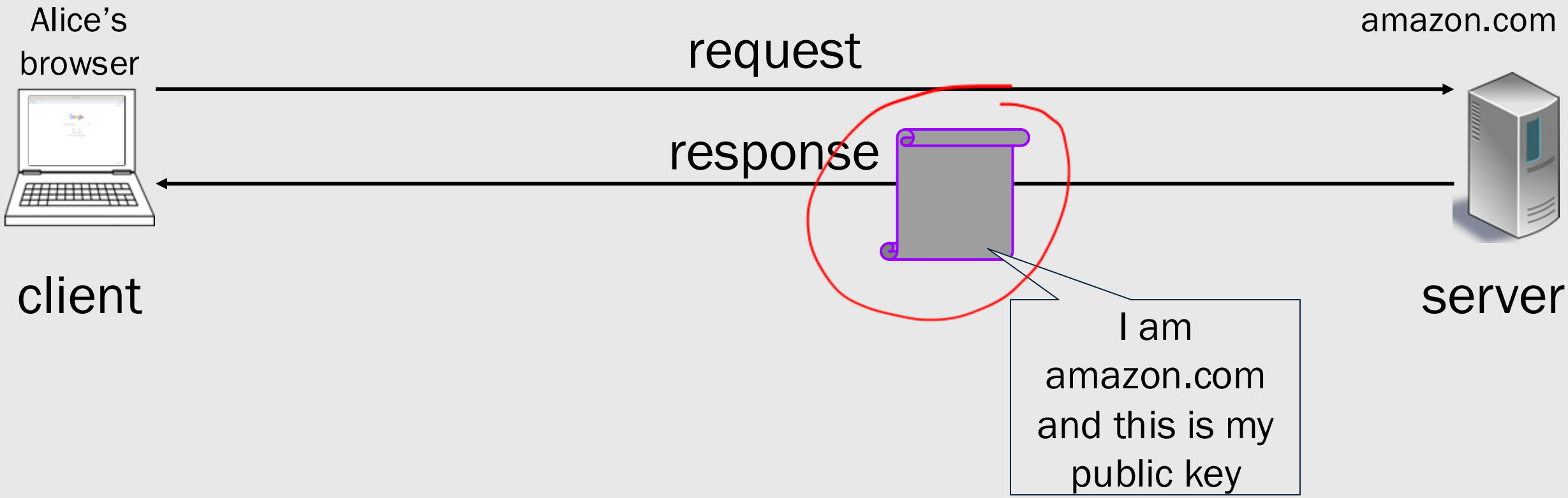
Public Key Infrastructure (PKI)

- **Data structures: certificates**
- Algorithms: key generation, installation, key use
- Architectures: certificate authorities (CA), CA directories
- Protocols: approving, acquiring, updating, and revoking certificates

HTTP over TLS (HTTPS)



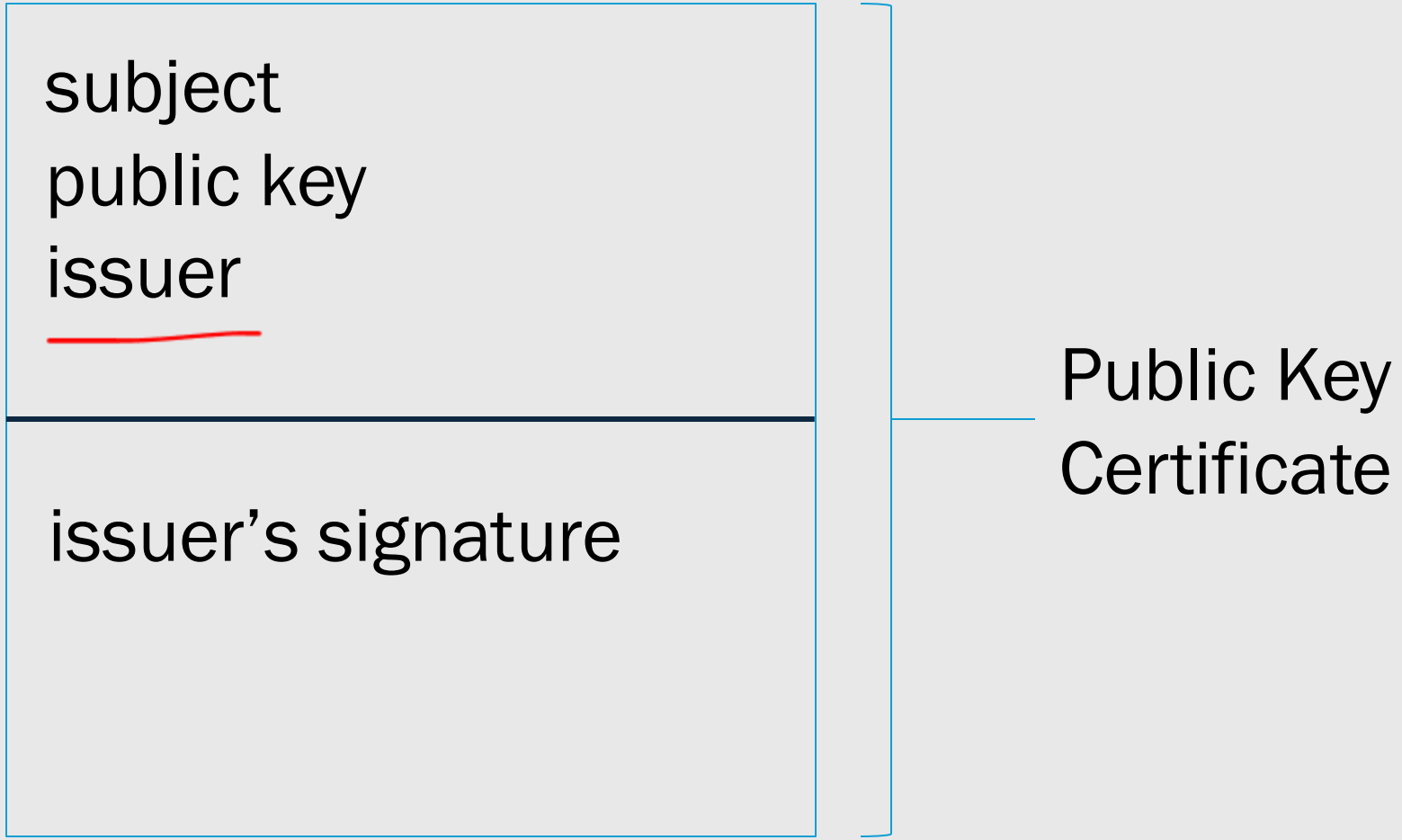
HTTP over TLS (HTTPS)

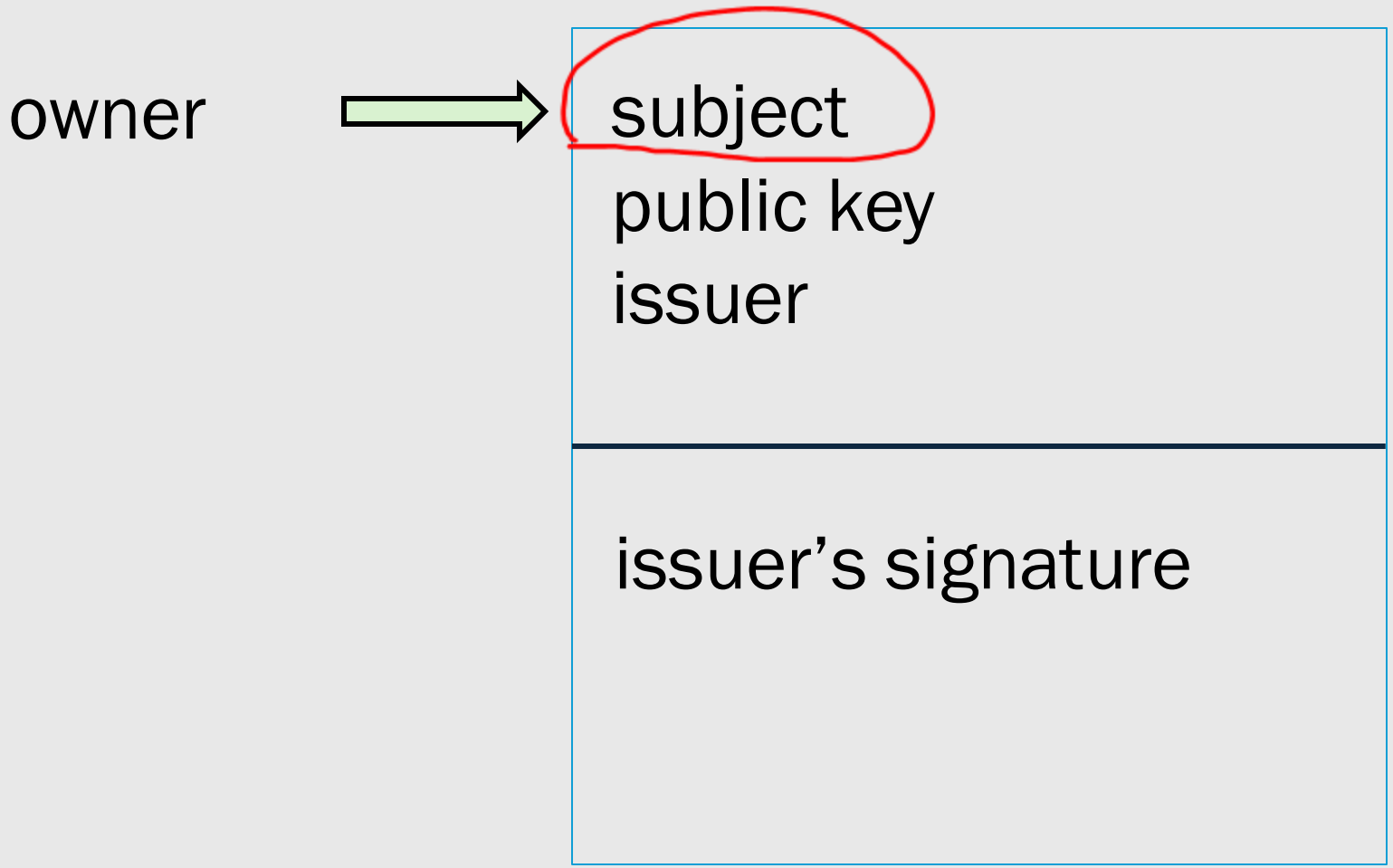


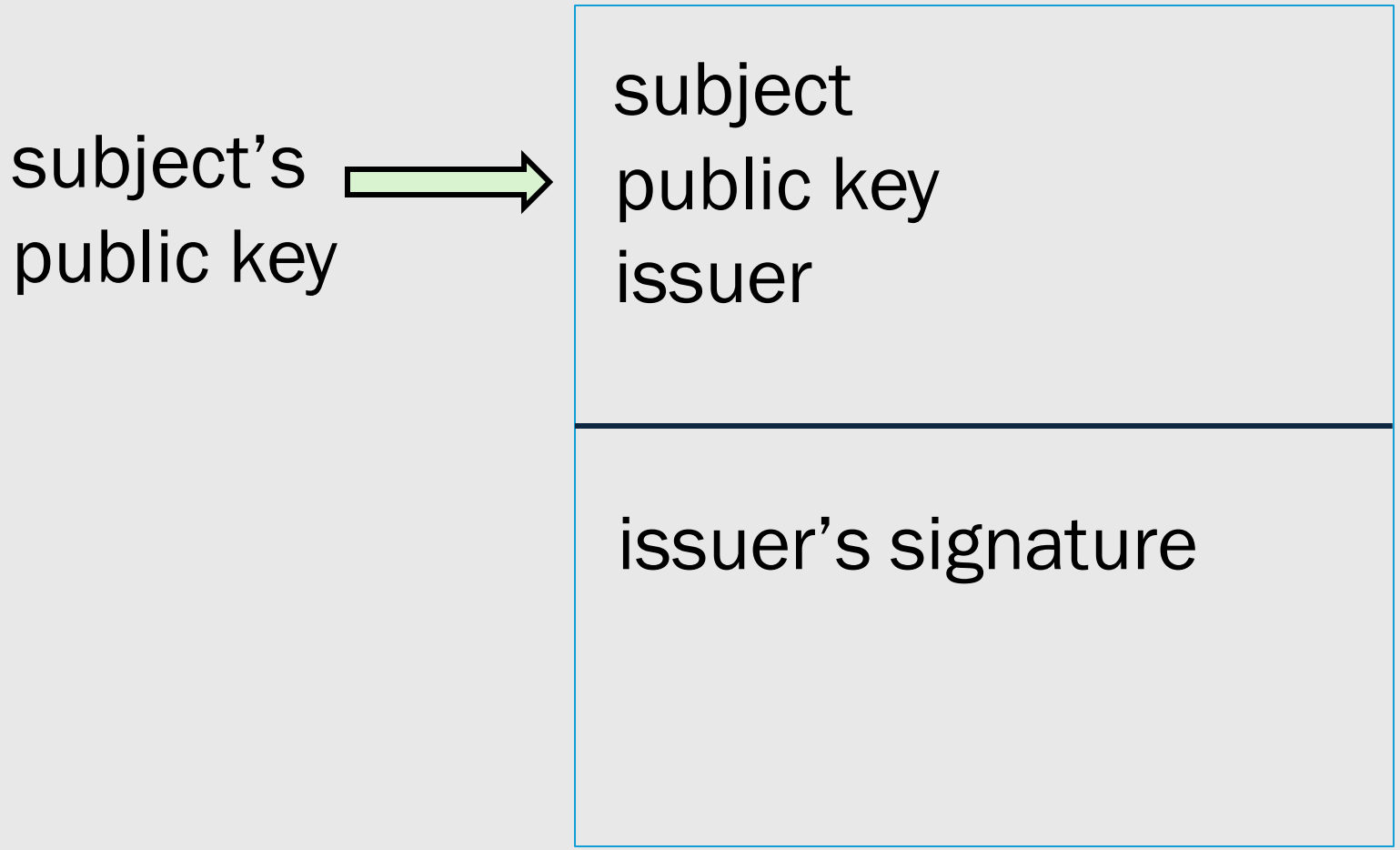
Certificate

Def’n: associates a public key with the owner

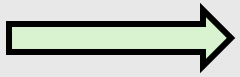
Certificate: data structure that binds public key to subject


subject
public key
issuer
issuer's signature
Public Key
Certificate


owner
subject
public key
issuer
issuer's signature


subject's
public key
subject
public key
issuer
issuer's signature

certification authority (CA)

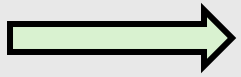


subject
public key
issuer

issuer's signature

CA is a trusted 3rd party

CA's signature



subject
public key
issuer

$\mathtt{Sign}_{Ks}(h(<subject, public\ key, issuer\ldots>))$

The issuer's signature attests to the contents of the top fields

All the fields are hashed using cryptographically secure hash fn

The hash value of the cert is signed by the issuer (CA) using the CA's private key

- subject (country, organization, common name)
- public key (algorithm, key)
- issuer (country, organization, common name)
- version (e.g., X.509v3)
- serial number
- validity period (not-before date, not-after date)
- signature algorithm

issuer's signature

X.509v3 Certificate

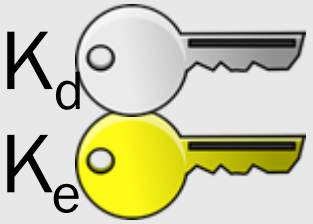
Validating Certificates

msg

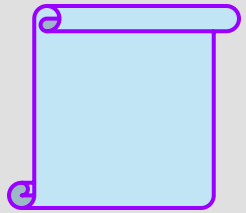
Dear Bob,
The secret word is cookie.
Sincerely,
Alice

Alice

Bob



Hello, Alice. I am Bob. This is my public key certificate.



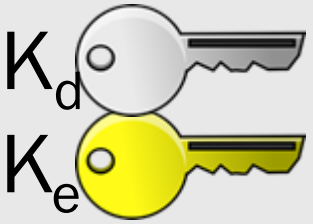
msg

Dear Bob,
The secret word is cookie.
Sincerely,
Alice

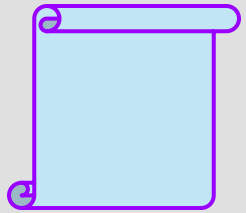
Alice

relying party

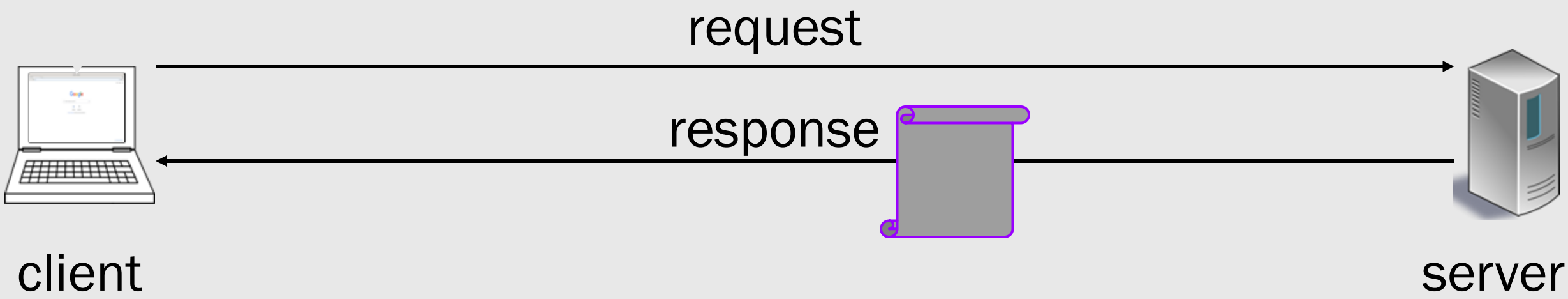
Bob



Hello, Alice. I am Bob. This is my public key certificate.



relying party



Certificate Validation

- Check validity period on certificate
- Check revocation status of certificate
- Verify signature using CA's public key
- Check subject matches current use

Certificate Chains

Certificate Chain

Def’n: a chain of certificates that allows for establishing trust in one public key from another public key

subject: www.amazon.com
public key: RSA, 2048, 65537, 99:5C:32:A5:F8:BD:7E:...
issuer: DigiCert Global CA G2
<signature>

---

subject: DigiCert Global CA G2
public key: RSA, 2048, 65537, D3:48:7C:BE:F3:05:86:5D:...
issuer: DigiCert Global Root G2
<signature>

---

subject: DigiCert Global Root G2
public key: RSA, 2048, 65537, BB:37:CD:34:DC:7B:6B:...
issuer: DigiCert Global Root G2
<signature>

subject: www.amazon.com
public key: RSA, 2048, 65537, 99:5C:32:A5:F8:BD:7E:...
issuer: DigiCert Global CA G2
<signature>

---

subject: DigiCert Global CA G2
public key: RSA, 2048, 65537, D3:48:7C:BE:F3:05:86:5D:...
issuer: DigiCert Global Root G2
<signature>

---

subject: DigiCert Global Root G2
public key: RSA, 2048, 65537, BB:37:CD:34:DC:7B:6B:...
issuer: DigiCert Global Root G2
<signature>

subject: www.amazon.com
public key: RSA, 2048, 65537, 99:5C:32:A5:F8:BD:7E:...
issuer: DigiCert Global CA G2
<signature>

---

subject: DigiCert Global CA G2
public key: RSA, 2048, 65537, D3:48:7C:BE:F3:05:86:5D:...
issuer: DigiCert Global Root G2
<signature>

---

subject: DigiCert Global Root G2
public key: RSA, 2048, 65537, BB:37:CD:34:DC:7B:6B:...
issuer: DigiCert Global Root G2
<signature>

subject: www.amazon.com
public key: RSA, 2048, 65537, 99:5C:32:A5:F8:BD:7E:...
issuer: DigiCert Global CA G2
<signature>

subject: DigiCert Global CA G2
public key: RSA, 2048, 65537, D3:48:7C:BE:F3:05:86:5D:...
issuer: DigiCert Global Root G2
<signature>

subject: DigiCert Global Root G2
public key: RSA, 2048, 65537, BB:37:CD:34:DC:7B:6B:...
issuer: DigiCert Global Root G2
<signature>

subject: www.amazon.com
public key: RSA, 2048, 65537, 99:5C:32:A5:F8:BD:7E:...
issuer: DigiCert Global CA G2
<signature>

---

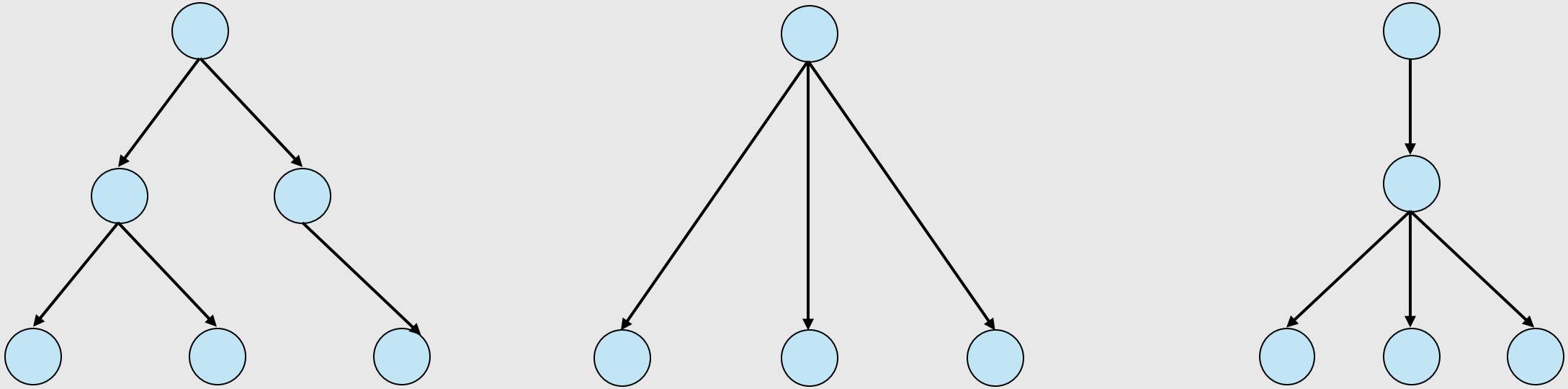
subject: DigiCert Global CA G2
public key: RSA, 2048, 65537, D3:48:7C:BE:F3:05:86:5D:...
issuer: DigiCert Global Root G2
<signature>

trust anchor

subject: DigiCert Global Root G2
public key: RSA, 2048, 65537, BB:37:CD:34:DC:7B:6B:...
issuer: DigiCert Global Root G2
<signature>

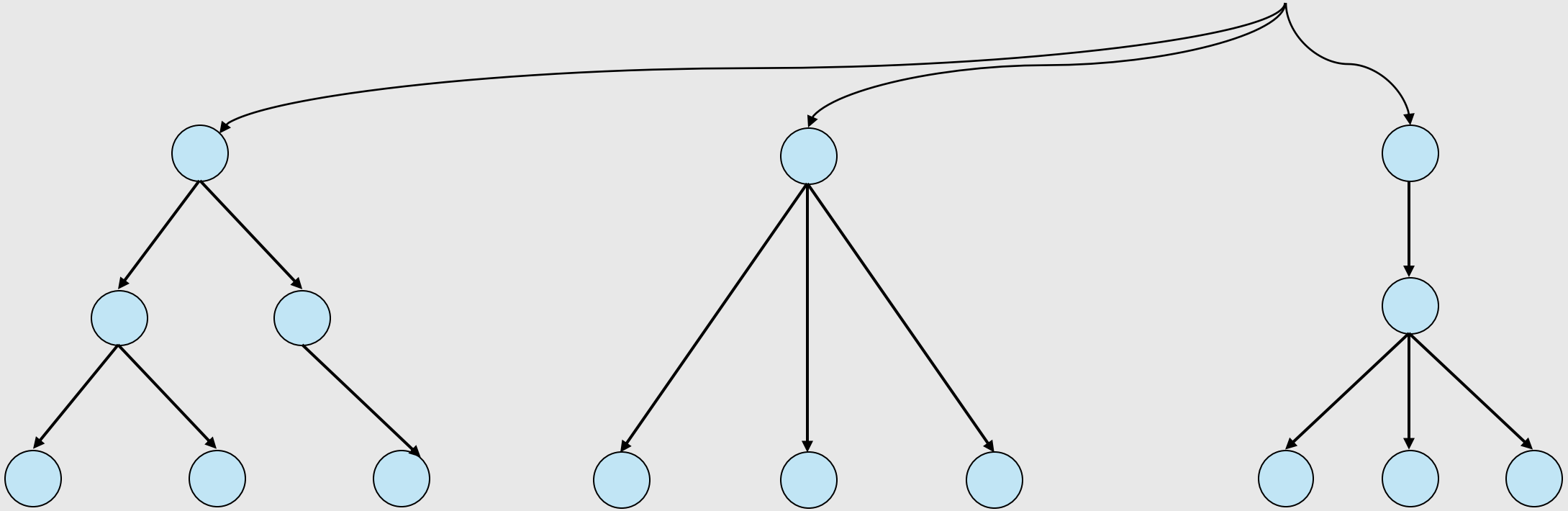
Trust Models

Browser Model: forest of disjoint hierarchical trees

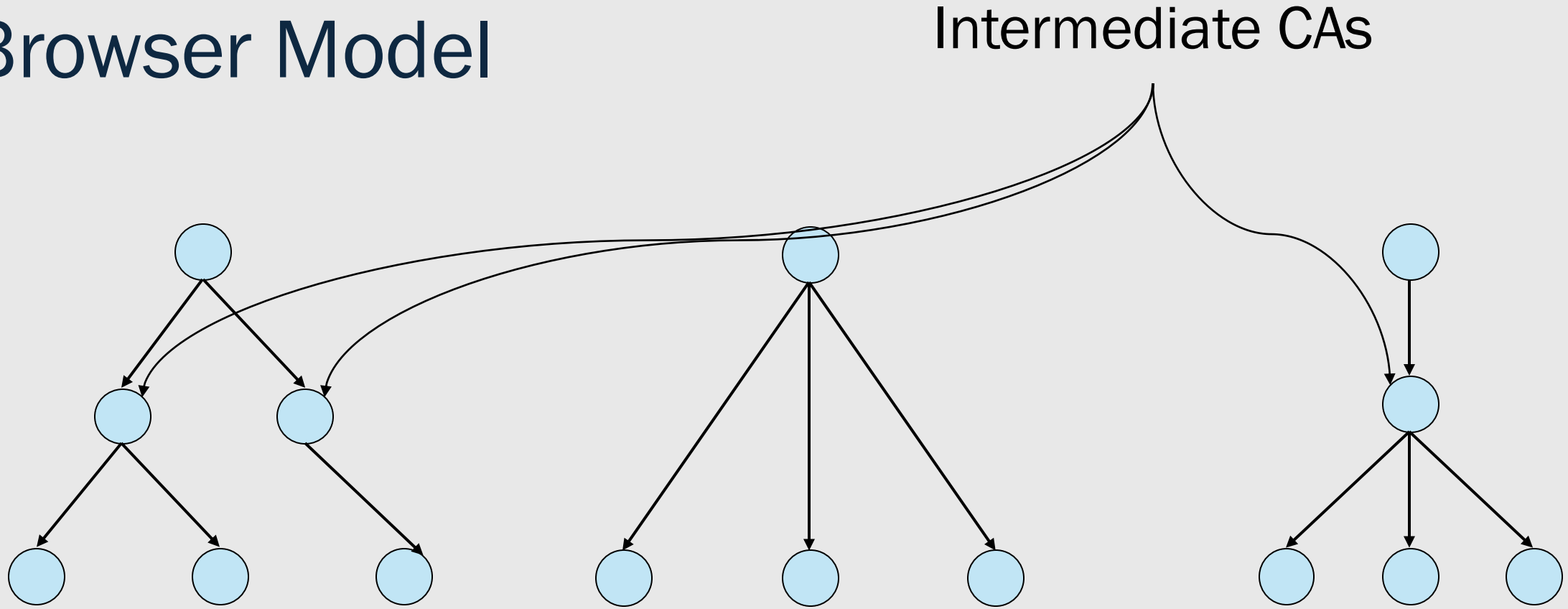


Browser Model

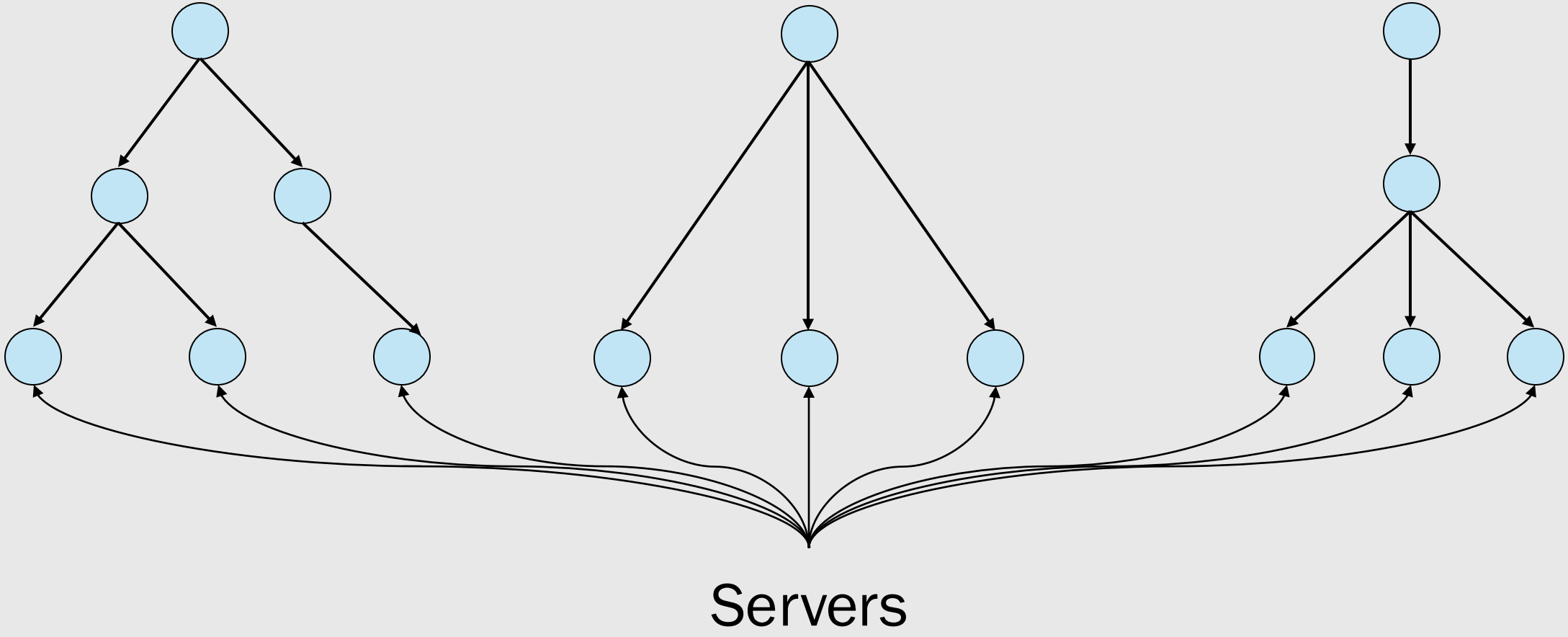
CAs: trust anchors



Browser Model



Browser Model



TLS CERTIFICATES

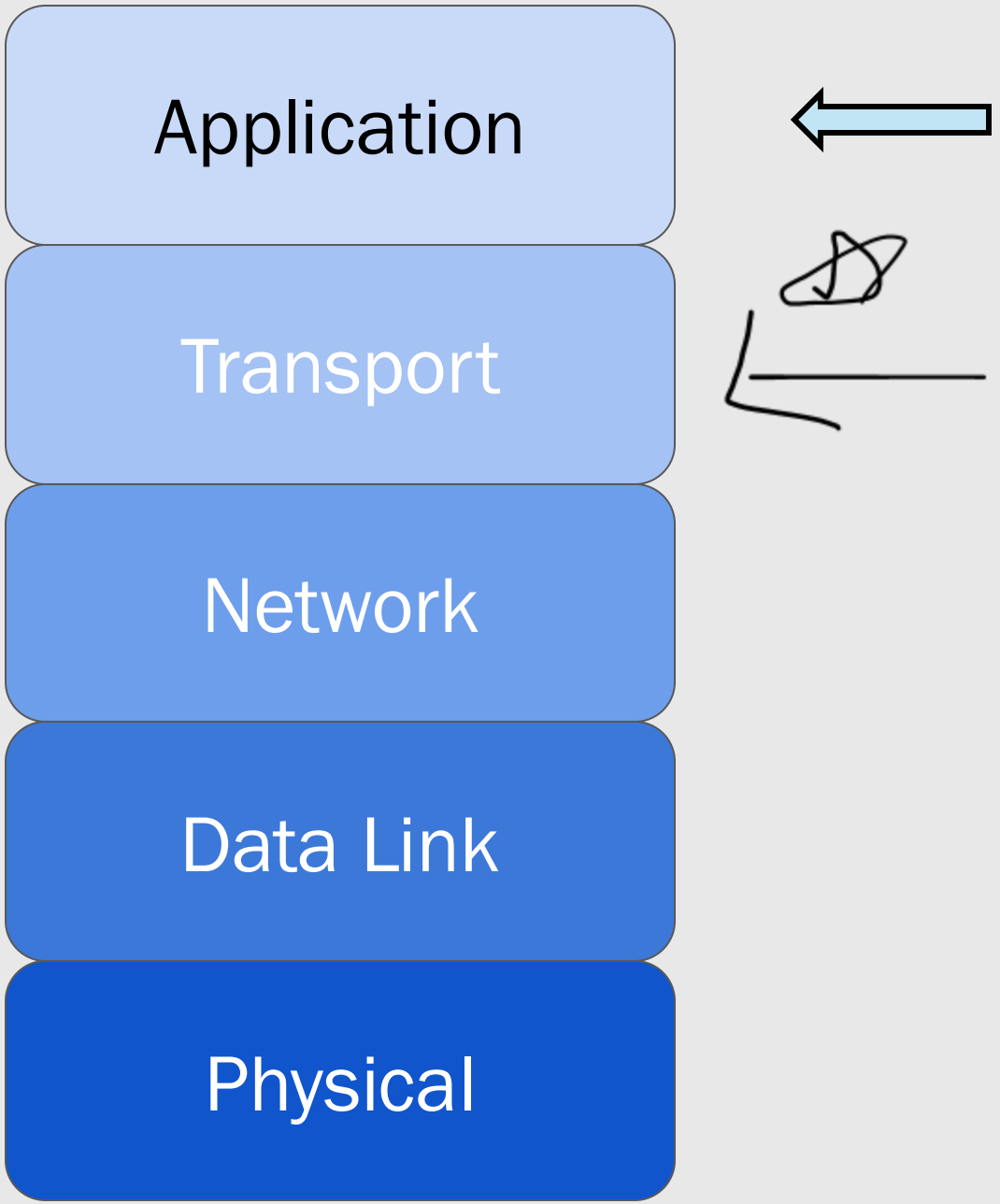
TLS/SSL

Def’n: a security protocol to provide

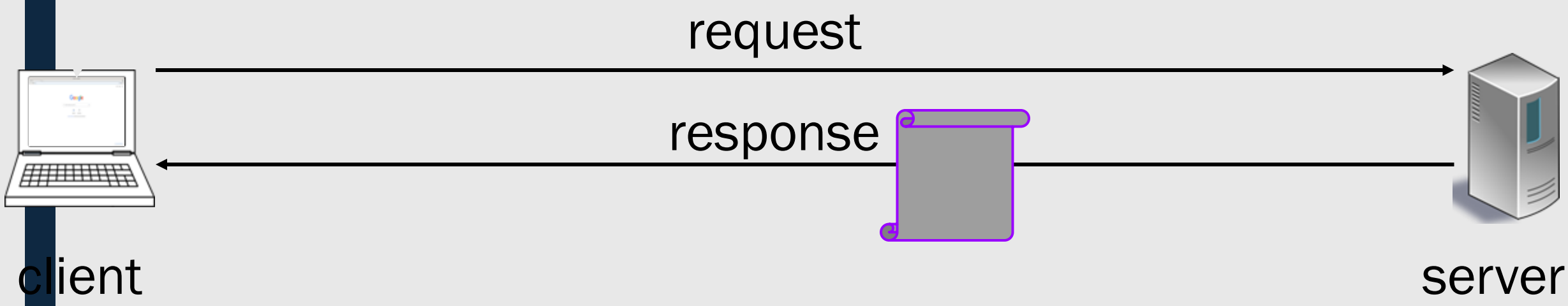
- encryption of traffic between endpoints
- authentication of a server to a client
  - *defined in 1999*
  - *replaces SSL (1994)*

TLS/SSL

https



relying party



Grades for TLS Certificates

Vetting the subject and public-key association

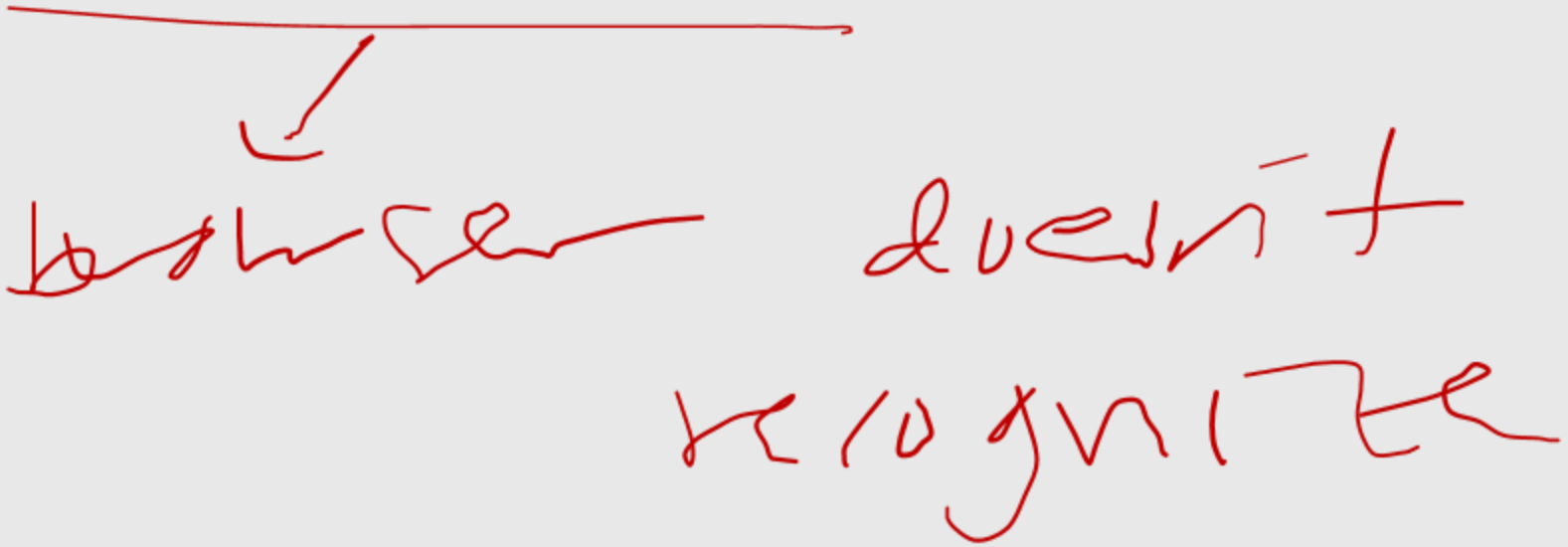
- Evidence of knowledge of the associated private key
- Evidence of control of computer-addressable identity
- Confirmation of natural-language name

TLS Certificate Grade

Def’n: the quality of a TLS certificate, determined by how the CA validates the organization before issuing the certificate

TLS Certificate Grades

- Domain Validated (DV)
- Organization Validated (OV)
- Extended Validation (EV)
- Individual Validated (IV)



Domain Validated (DV) Certificates

- CA verifies requestor controls the listed domain
- Requestor may not correspond to any real-world entity
- Validation is cheap
- Validation is automated

admin@x.domain.com

subject: pax-paul

Organization Validated (OV) Certificates

- CA verifies requestor controls the listed domain
- CA confirms claimed street address
- CA confirms business name

Extended Validation (EV) Certificates

- CA verifies requestor controls the listed domain
- CA confirms street address
- CA confirms organization name in govt-recognized DB
- CA confirms requestor's identity
- No wildcards in listed domain (e.g., *.google.com)

TLS

TLS/SSL

Def’n: a security protocol to provide

- encryption of traffic between endpoints
- authentication of a server to a client
  - *defined in 1999*
  - *replaces SSL (1994)*

Transport Layer Security (TLS) Protocol v1.3

"TLS allows client/server applications to communicate over the Internet in a way that is designed to prevent eavesdropping, tampering, and message forgery."

-- RFC 8446

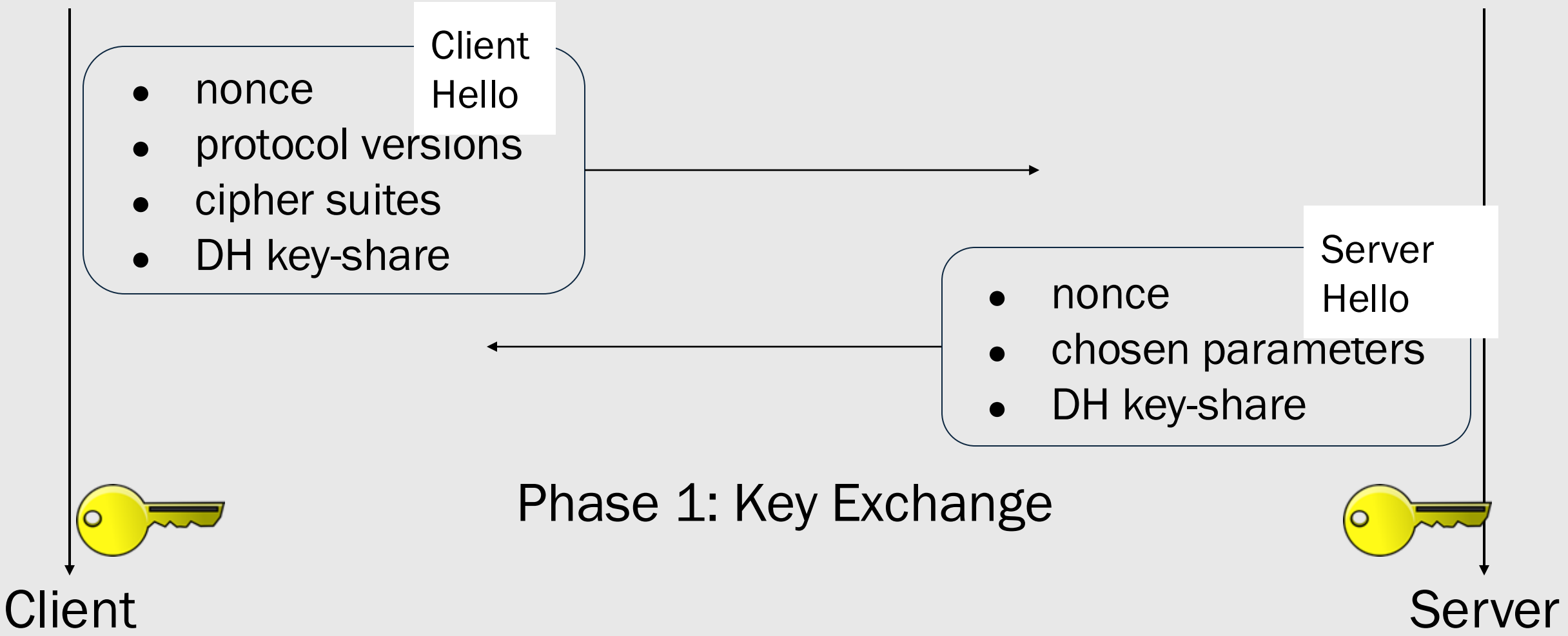
Request for Comments (RFC)

- Memo detailing and specifying a standard
- Published by the Internet Engineering Task Force (IETF)
- Made public for peer review
- Can be adopted as a standard by IETF

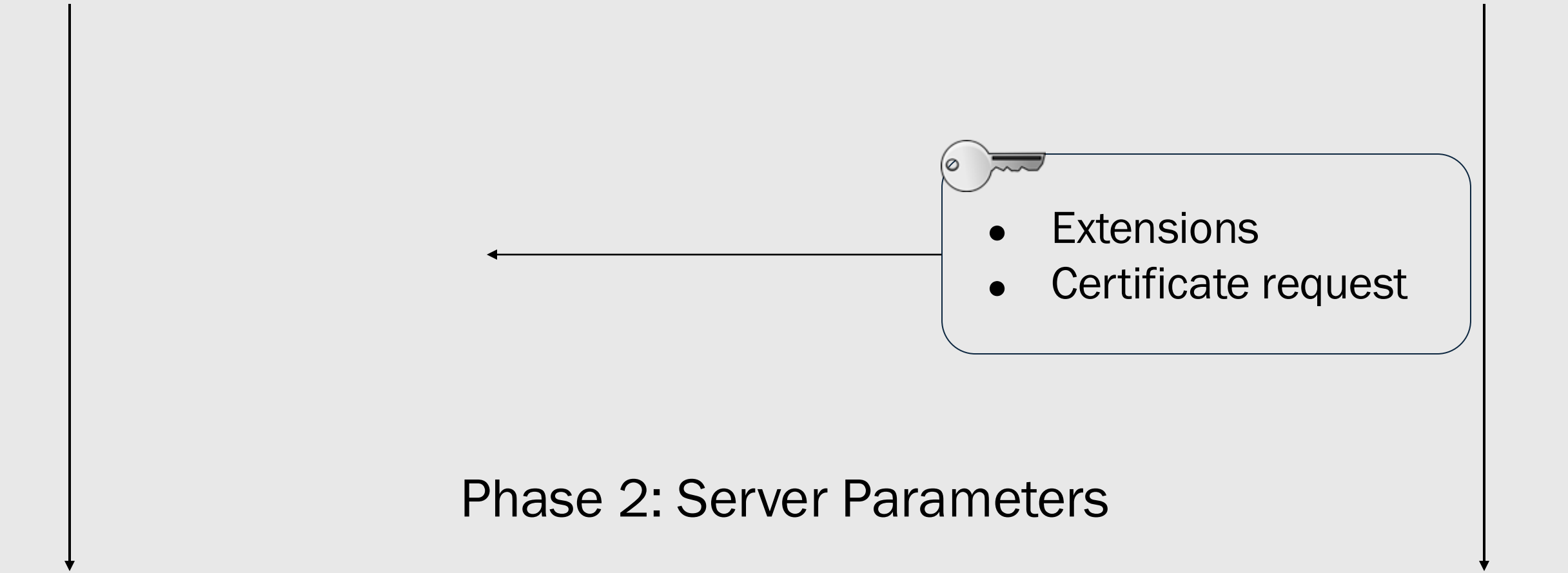
TLS Handshake

- Key Exchange
- Server Parameters
- Authentication

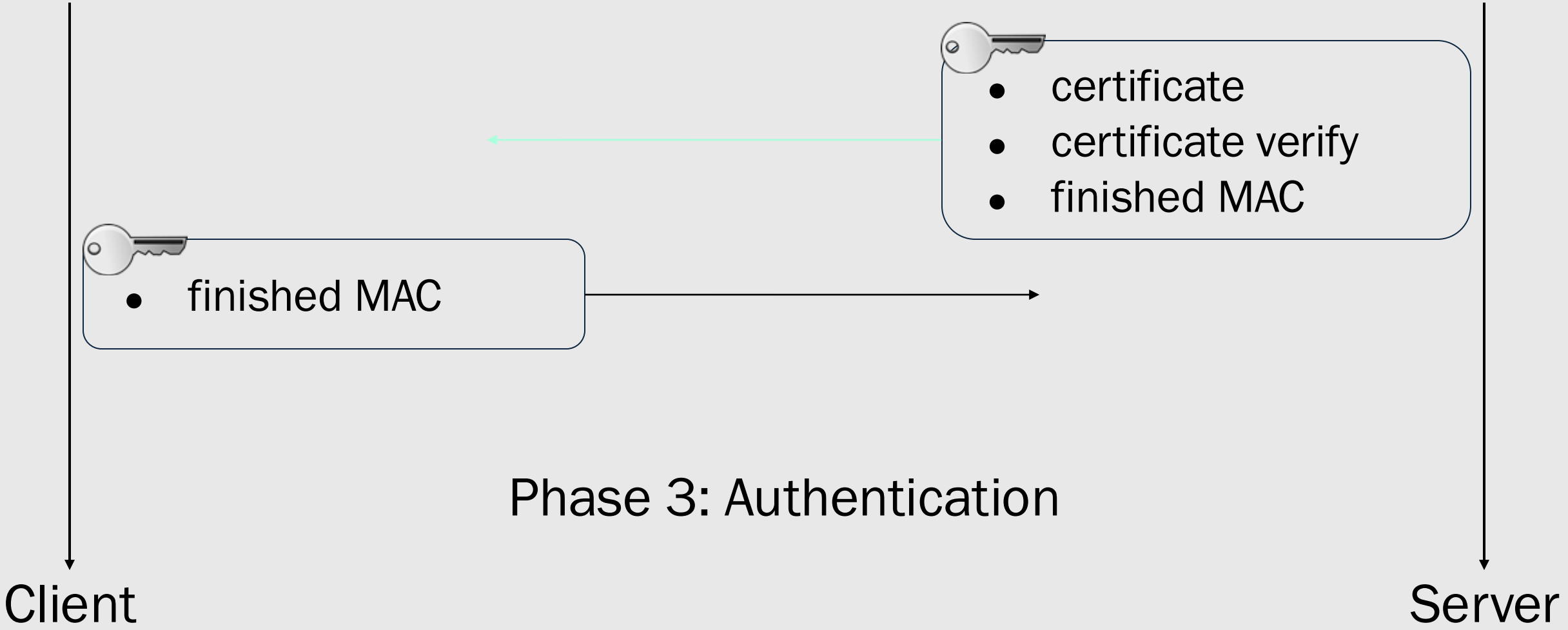
TLS Handshake



TLS Handshake



TLS Handshake



HTTP over TLS