



TLS IN THE HOMELAB: THE EASY WAY AND THE HARD WAY

Ketan Vijayvargiya

April 27, 2024

Introduction

- Principal Engineer at AWS.
- Self-hosting as a hobby.



Disclaimer: This talk is based on my own experience and understanding of the technology landscape. It does not represent policies or business practices of my current or past employers.

This talk is about ...

- 3 approaches to implement TLS, in increasing order of complexity.
- Practical, with minimal working code: <https://github.com/ketan-vijayvargiya/linuxfestnorthwest-talk-2024>

This talk is *not* about ...

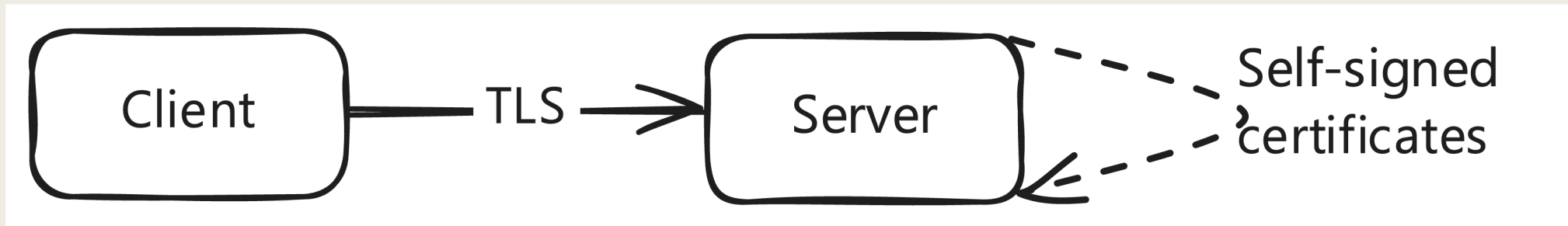
- Low-level details of TLS handshake.
- Cryptographic algorithms or math.
- Software recommendations.

Instead, we'll discuss concepts that you can replicate in your setup.

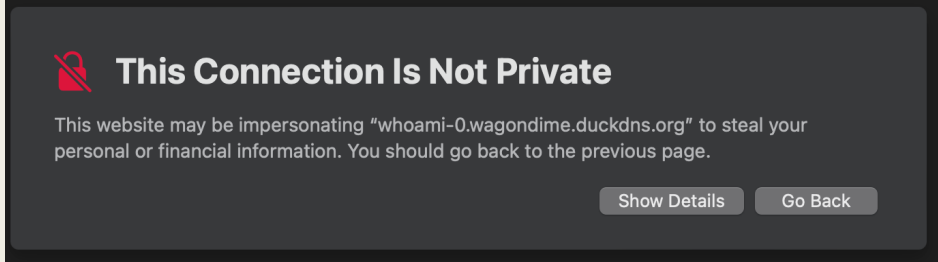
What is TLS, in brief?


- TLS == Transport Layer Security.
 - *TLS vs HTTPS.*
 - *TLS vs SSL.*
- Types of encryption:
 - *Public key cryptography == asymmetric cryptography.*
 - *Symmetric cryptography.*

Approach 1: Self-signed certificates



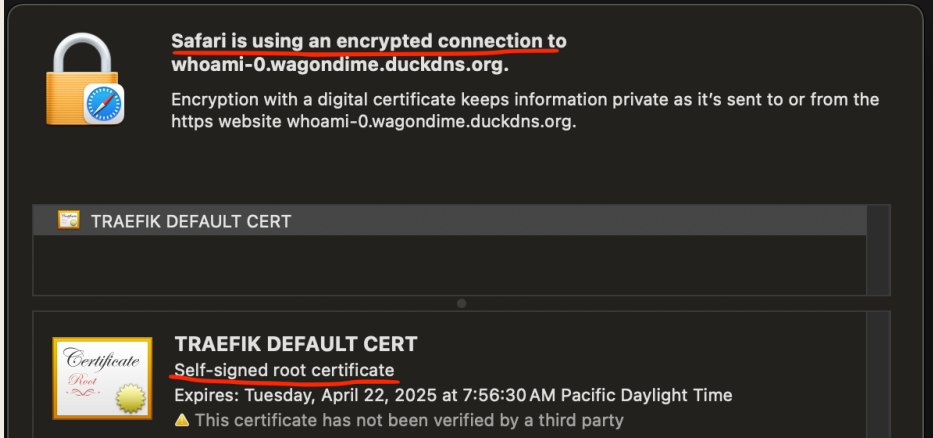
Approach 1: In practice




 **This Connection Is Not Private**


This website may be impersonating "whoami-0.wagondime.duckdns.org" to steal your personal or financial information. You should go back to the previous page.


[Show Details](#) [Go Back](#)



 **Safari is using an encrypted connection to whoami-0.wagondime.duckdns.org.**

Encryption with a digital certificate keeps information private as it's sent to or from the https website whoami-0.wagondime.duckdns.org.

 **TRAEFIK DEFAULT CERT**

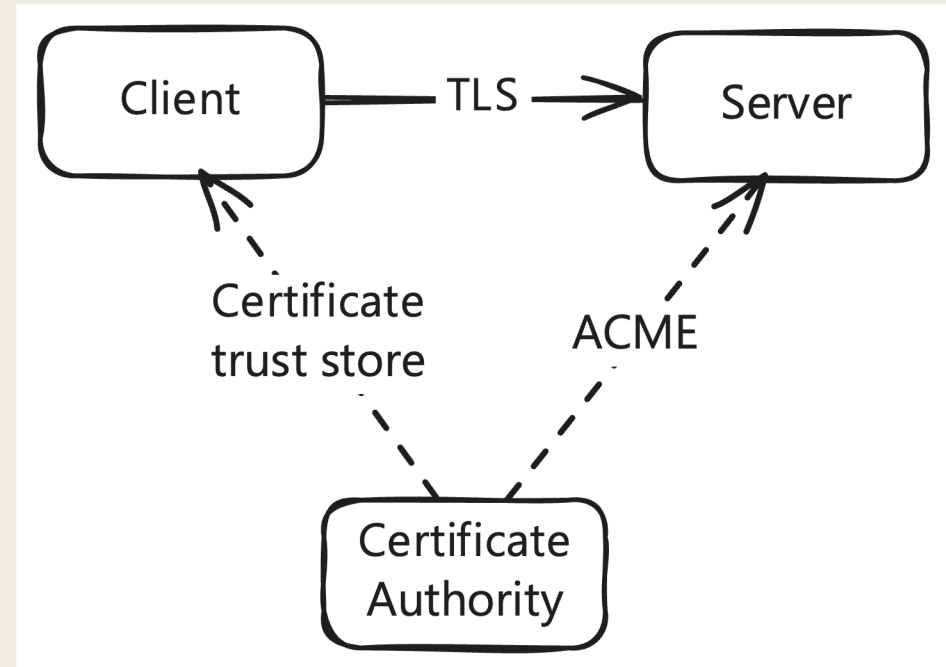
 **TRAEFIK DEFAULT CERT**
Self-signed root certificate
Expires: Tuesday, April 22, 2025 at 7:56:30 AM Pacific Daylight Time
⚠ This certificate has not been verified by a third party

Approach 1: Considerations

- Doesn't scale well.

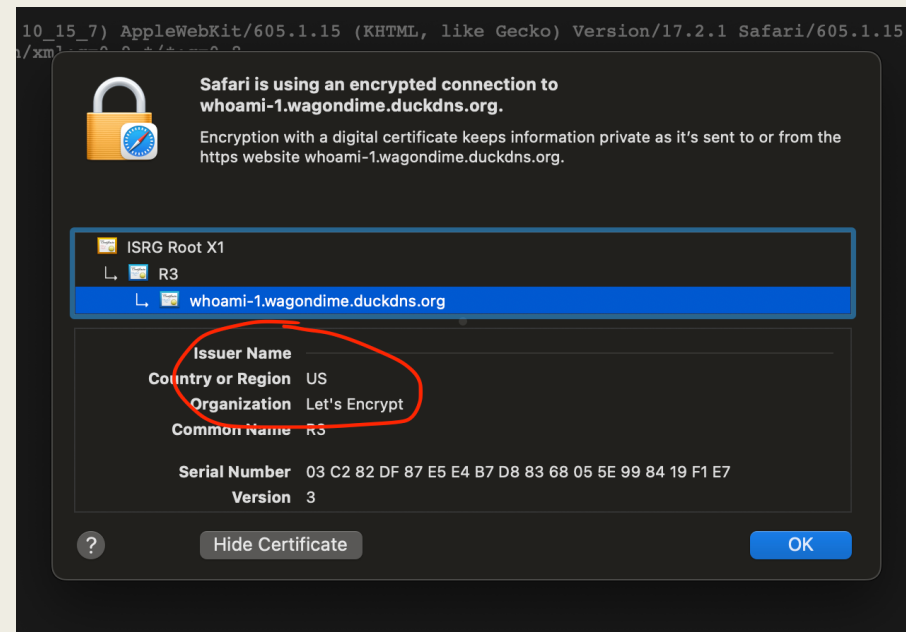
Approach 2: Certs generated by a Certificate Authority

- Noteworthy in the image:
 - *ACME protocol.*
 - *Certificate authority could be:*
 - Public, possibly free, such as Let's Encrypt.
 - Custom or self-hosted.



Approach 2.1: In practice, when using a public CA

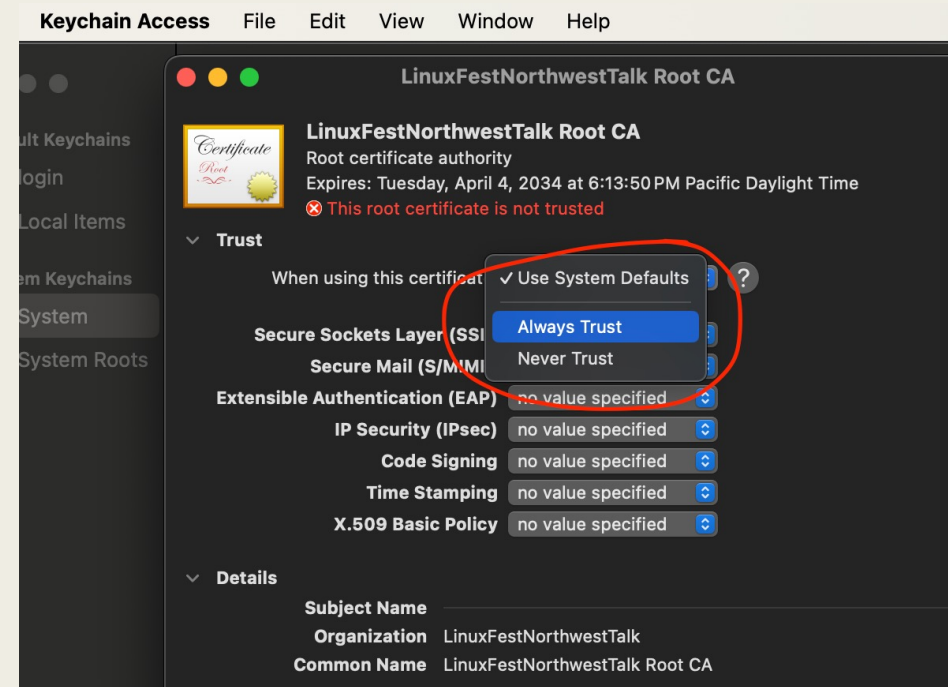
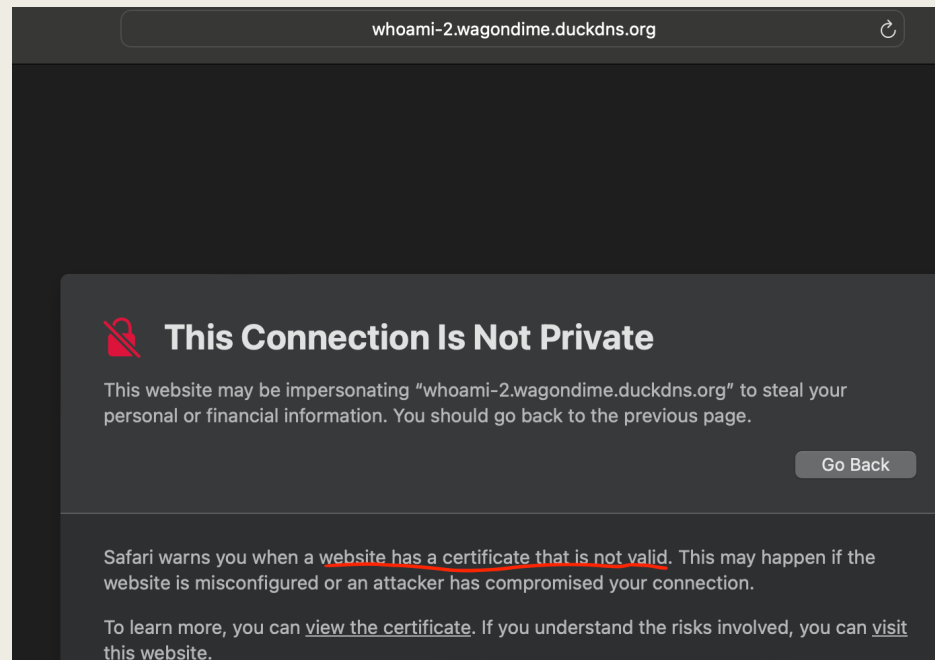
`curl https://whoami-1.wagondime.duckdns.org`



Approach 2.1: Considerations

- Verify validity of the certificates.
- Certificates publicly logged on <https://crt.sh/>.
 - *Wildcard certs through "DNS challenge" provide some mitigation. (See accompanying code.)*

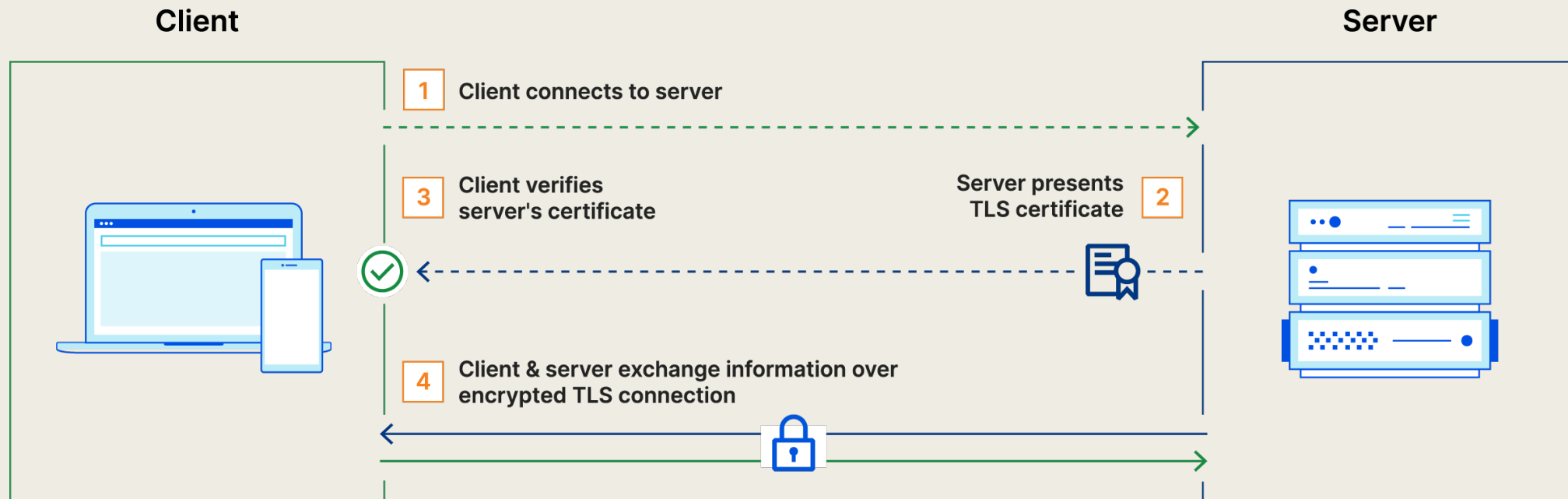
Approach 2.2: In practice, when using custom CA



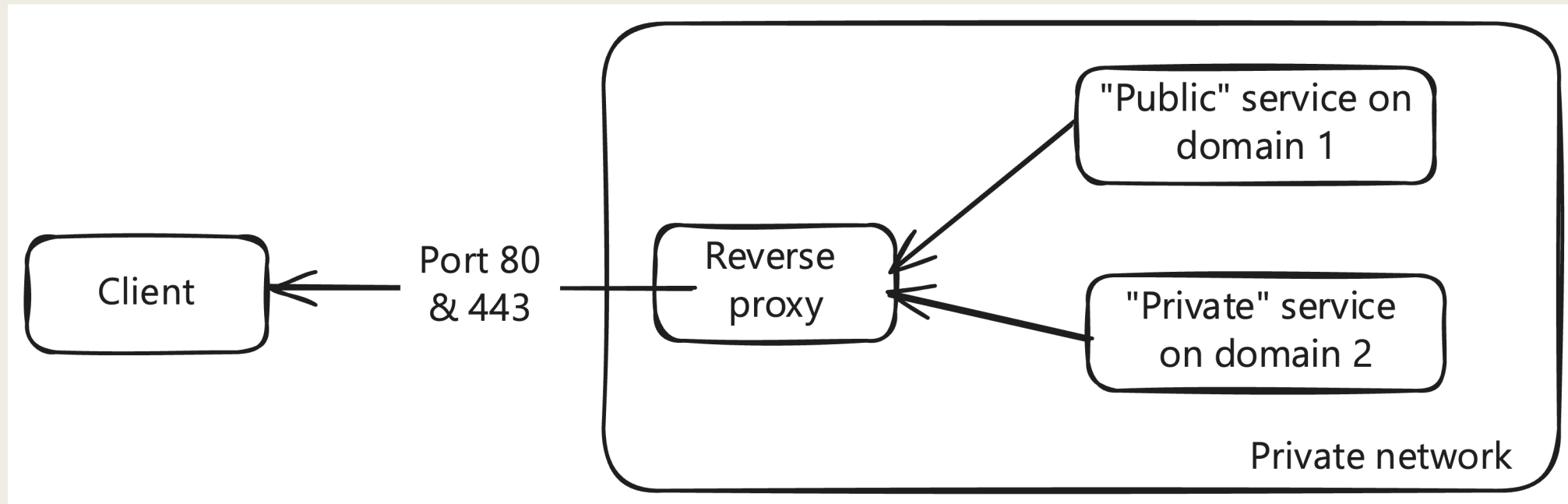
Approach 2.2: Considerations

- `curl --cacert root_ca.crt https://whoami-2.wagondime.duckdns.org` works.
- BUT `curl --insecure https://whoami-2.wagondime.duckdns.org` also works.

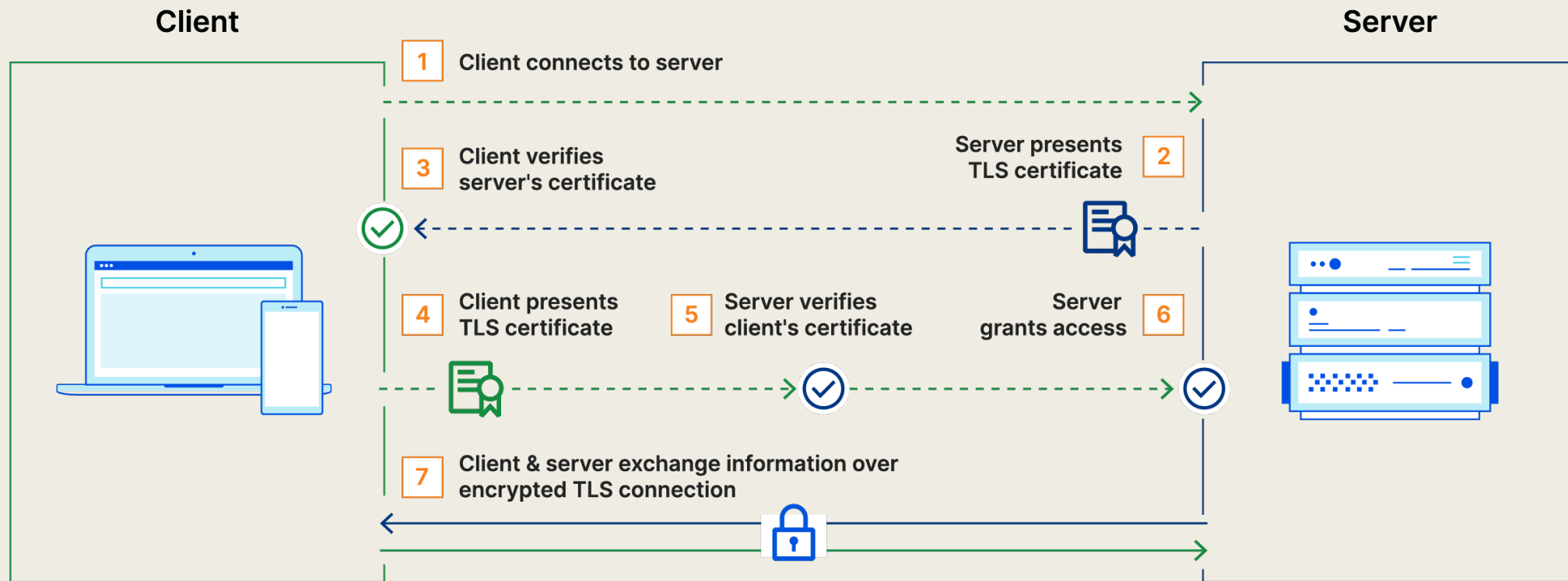
How does TLS handshake work, in brief?



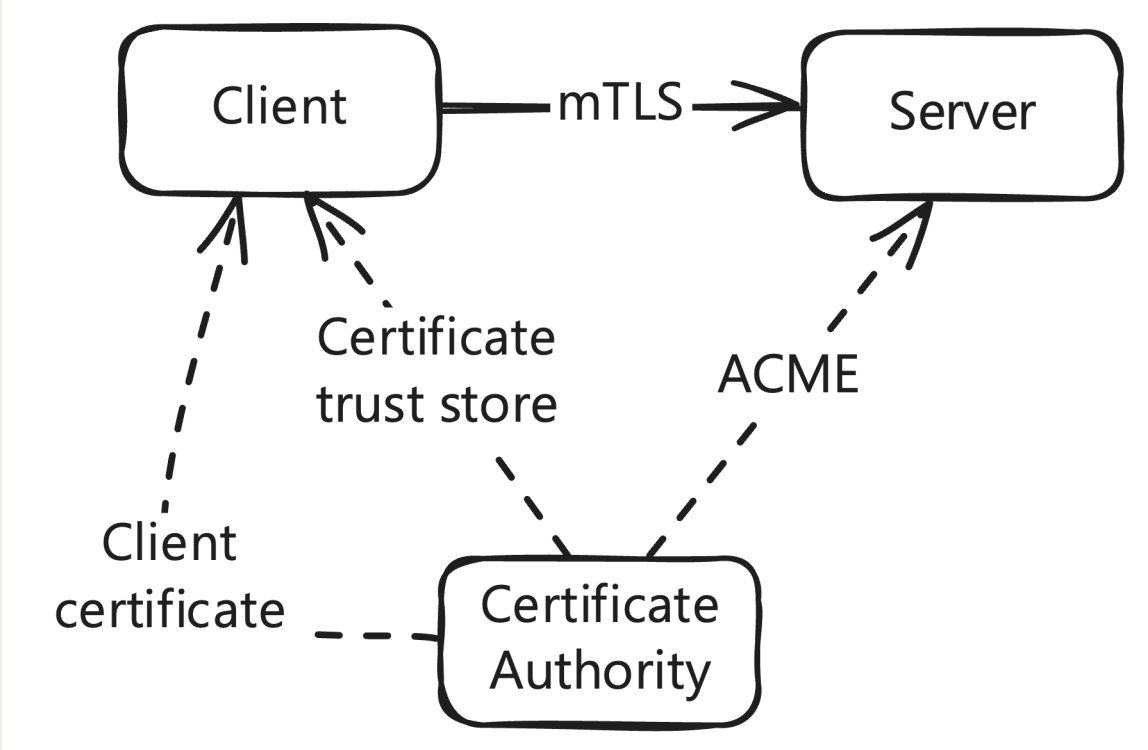
Motivation for approach 3



How does mTLS handshake work, in brief?

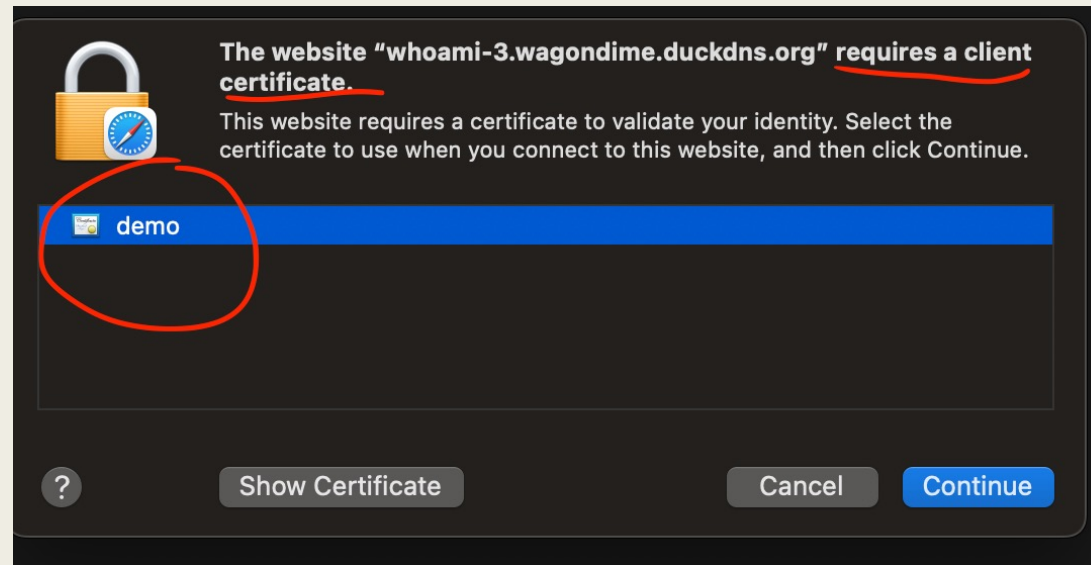


Approach 3: mTLS (== mutual TLS)



Approach 3: In practice

```
curl --cert client.crt --key client.key --cacert root_ca.crt \  
https://whoami-3.wagondime.duckdns.org
```



Considerations while setting up a custom CA

- Manage root certificate on all clients.
 - *Additionally, client certificates for mTLS.*
- Rumors that:
 - *Some reverse proxies don't play well with public and custom CA together.*
 - *Some Android apps don't work.*

Accompanying code

<https://github.com/ketan-vijayvargiya/linuxfestnorthwest-talk-2024>. (Scan the QR code.)

- Traefik: reverse proxy.
- Docker: service management.
- Domain: free from Duck DNS.
- Let's Encrypt: public CA.
- Step CA: custom CA.



Thanks!

Contact: <https://ketanvijayvargiya.com/>
(Scan the QR code.)



Questions?

