# Integrating Intel TDX remote attestation into SSH

Fabian Wesemann
M.Sc student, Flensburg Univ. of Applied Sciences

FOSDEM 2025

# Content

- Technology overview
- Project goal
- Protocol
- Implementation

# Intel TDX

- Confidential Computing on the virtual machine level
- Isolates a VM from software outside the trust domain, e.g. the host OS

# Intel TDX Remote Attestation

- Verify Intel TDX is enabled
- Evidence can be verified by the relying party
- On Azure CVMs: Azure Attestation Service

# SSH

- Server/Client
- Remote shell, file transfer, port forwarding, …
- Comes with encryption and authentication
- e.g. git, rsync

# Project goal

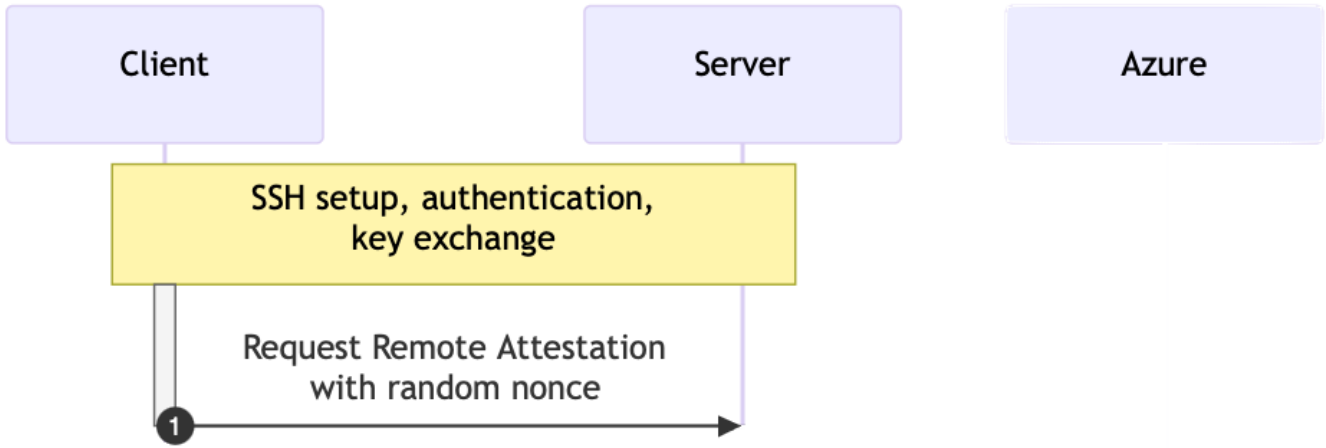
Modify OpenSSH, so that our client only connects to servers on a TDX enabled VM.

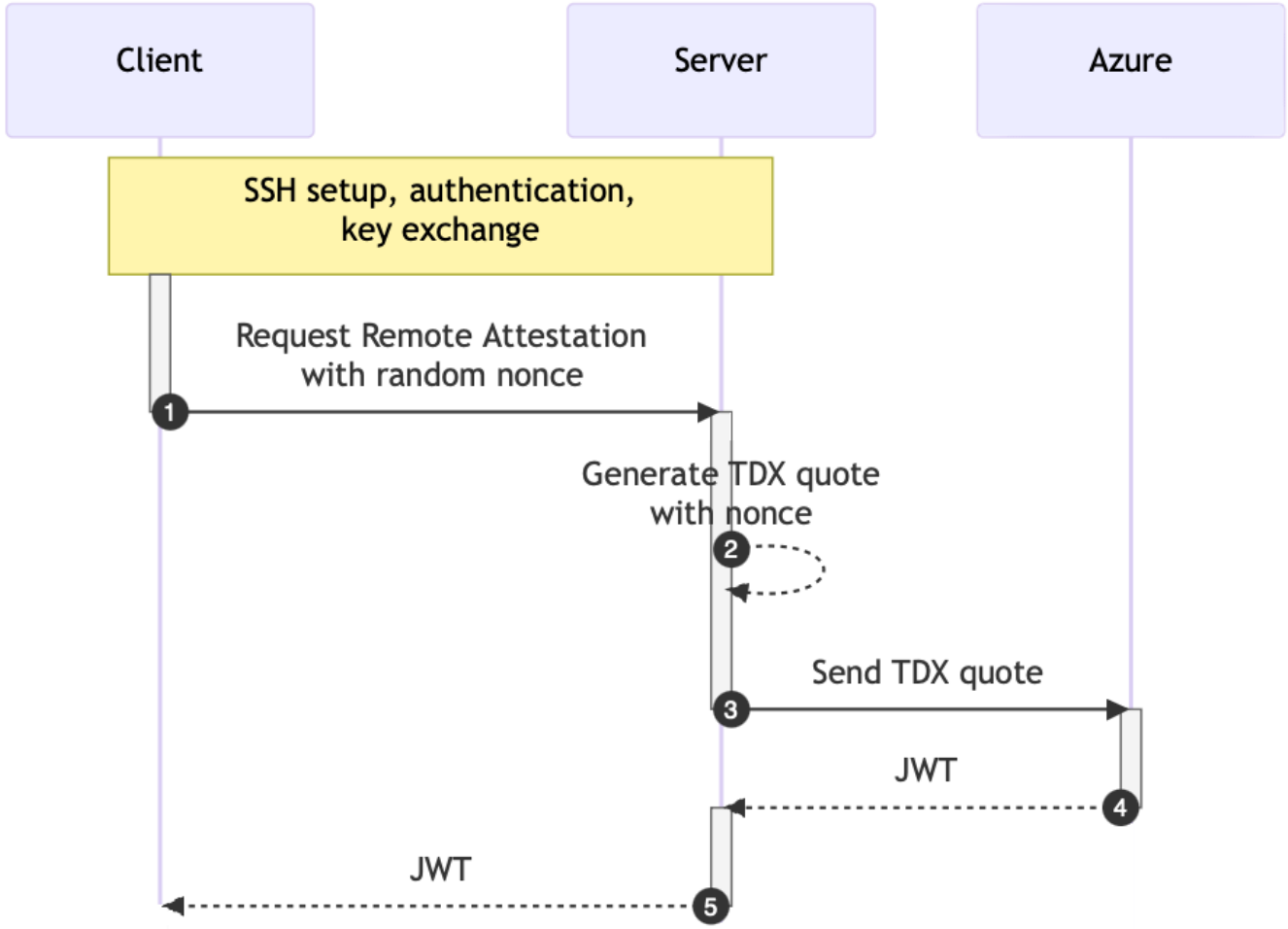
# Project goal

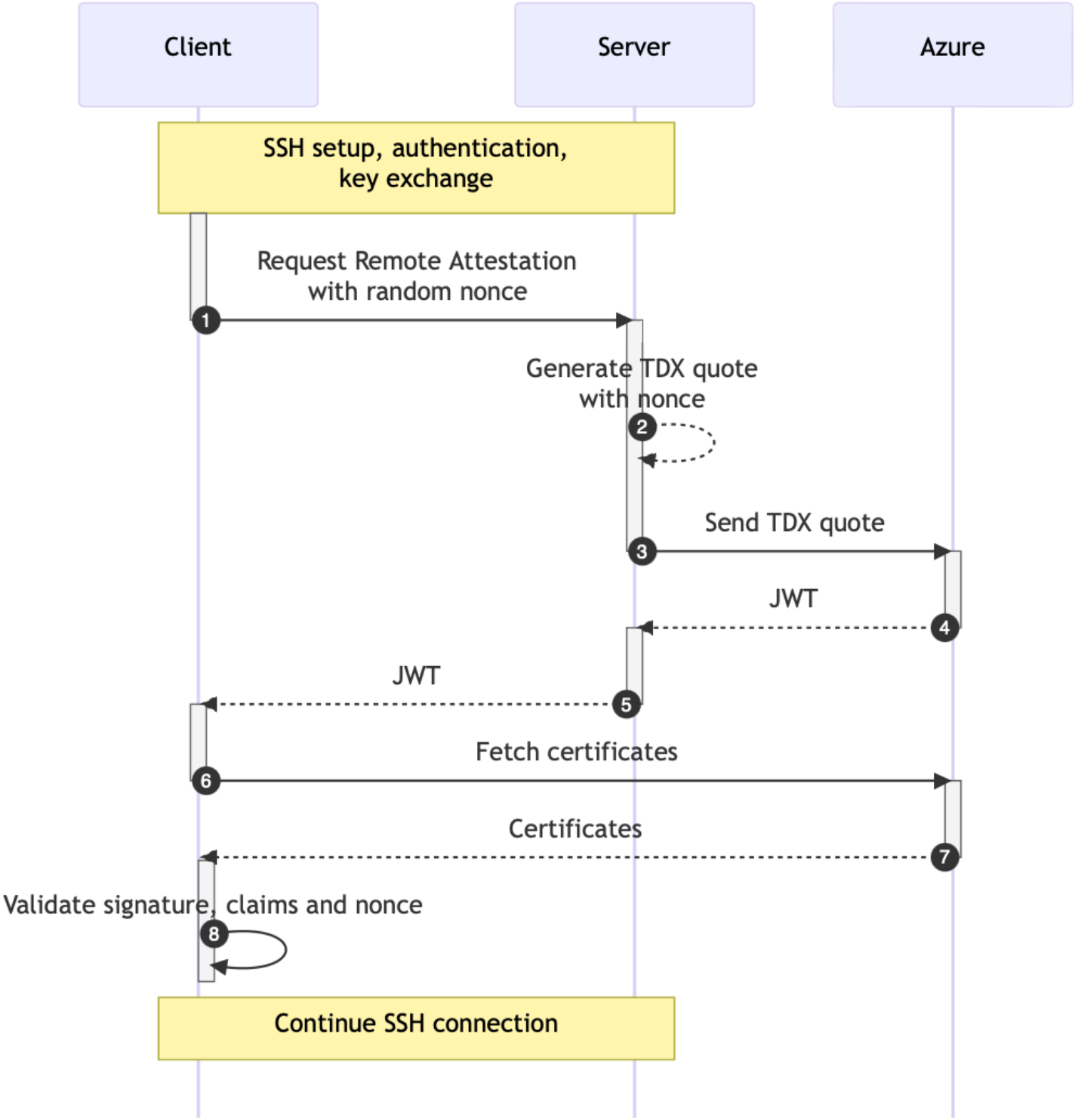
Modify OpenSSH, so that our client only connects to servers on a TDX enabled VM.

- client → challenger / relying party
- server → attester

# Protocol


Client
Server
Azure
SSH setup, authentication,
key exchange
Request Remote Attestation
with random nonce
1


Client
Server
Azure
SSH setup, authentication, key exchange
Request Remote Attestation with random nonce
1
Generate TDX quote with nonce
2
Send TDX quote
3
JWT
4
JWT
5


Client
Server
Azure
SSH setup, authentication, key exchange
Request Remote Attestation with random nonce
1
Generate TDX quote with nonce
2
Send TDX quote
3
JWT
4
JWT
5
Fetch certificates
6
Certificates
7
Validate signature, claims and nonce
8
Continue SSH connection

# Implementation

- Based on OpenSSH
- New *ra-ssh* Service for attestation
- *trustauthority-cli* for TDX quote generation
  - Needs privileged process
  - *monitor* messages between *sshd* and the session

Server

# Quote generation

```
trustauthority-cli quote -u <nonce>
```

```
Quote:
BAACAIEAAAAAAAAAk5pyM/ecTKmUCg2zlX8GByxxGNDcfxhLFr0pGDnEuPoAAAAAB
runtime_data:
eyJrZXlzIjpbeyJraWQiOiJIQ0xBa1B1YiIsImtleV9vcHMiOlsic2lnbiJdLCJrd
user_data: ZmFiaWFu # base64(userdata)
```

Server

# Azure JWT creation

```
POST https://sharedeus2e.eus2e.attest.azure.net/attest/TdxVm?
api-version=2023-04-01-preview
```

```
{
  "quote": "BAACAIEAAAAAAAAAk5pyM...AAAAAA=",
  "runtimeData": {
    "data": "eyJrZXlzIjp...IyMCJ9",
    "dataType": "JSON"
  }
}
```

# Azure JWT

```
{
  "alg": "RS256",
  "jku": "https://sharedeus2e.eus2e.attest.azure.net/certs",
  "kid": "6qubGPaYpJMjCD9chNyuh/ztq87166pwivQJz1quFRQ=",
  "typ": "JWT"
}
```

```
{
"attester_tcb_status": "UpToDate",
"x-ms-attestation-type": "tdxvm",
"x-ms-compliance-status": "azure-compliant-cvm",
"x-ms-runtime": {
    "user-data": "2F1B...5B20",// base64(sha512(nonce))
    "vm-configuration": {
      "console-enabled": true,
      "secure-boot": true,
    ...
}
...
}
```

Full version on jwt.io

Mail: fabian.wesemann at stud.hs-flensburg.de

Implementation and Demo: github.com/tufteddeer/openssh-tdx-remote-attestation

Slides: tufteddeer.github.io/remote-attestation-ssh-slides/

Paper: tufteddeer.github.io/remote-attestation-ssh-slides/TDX-remote-attestation-in-SSH.pdf

# Interesting stuff

- OpenSSH: openssh.com
- Intel Trustauthority CLI: github.com/intel/trustauthority-client-for-go
- Azure JWTs: thomasvanlaere.com/posts/2023/03/azure-confidential-computing-verifying-microsoft-azure-attestation-jwt-tokens/
- EAT profile: learn.microsoft.com/en-us/azure/attestation/trust-domain-extensions-eat-profile