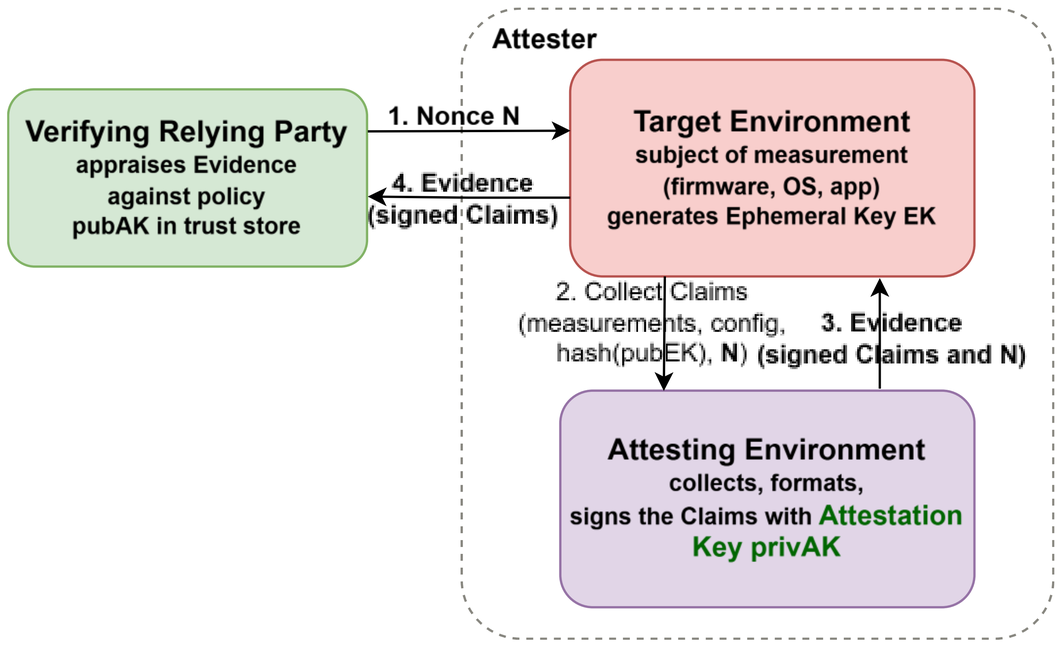
[1]TU Dresden, [2]Aalto University

Muhammad Usama Sardar[1], Mariam Moustafa[2], Tuomas Aura[2]

# Identity Crisis in Confidential Computing: Formal Analysis of Attested TLS

AsiaCCS'26

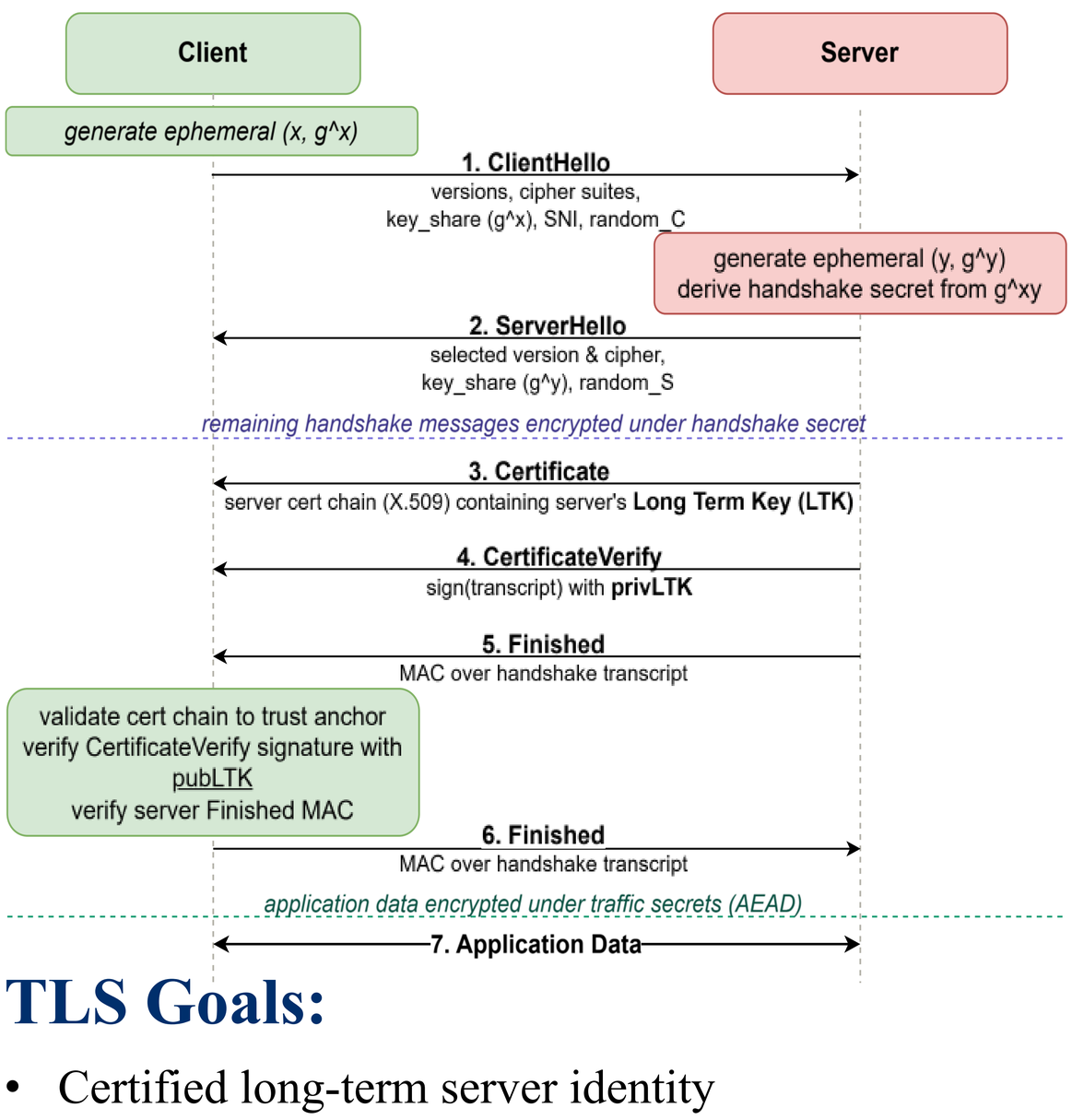
## Remote Attestation




## Remote Attestation Goals:

- Integrity of the Evidence about server configuration
- Bind evidence to an ephemeral server key
- Freshness of the Evidence

## Server Authentication in TLS 1.3



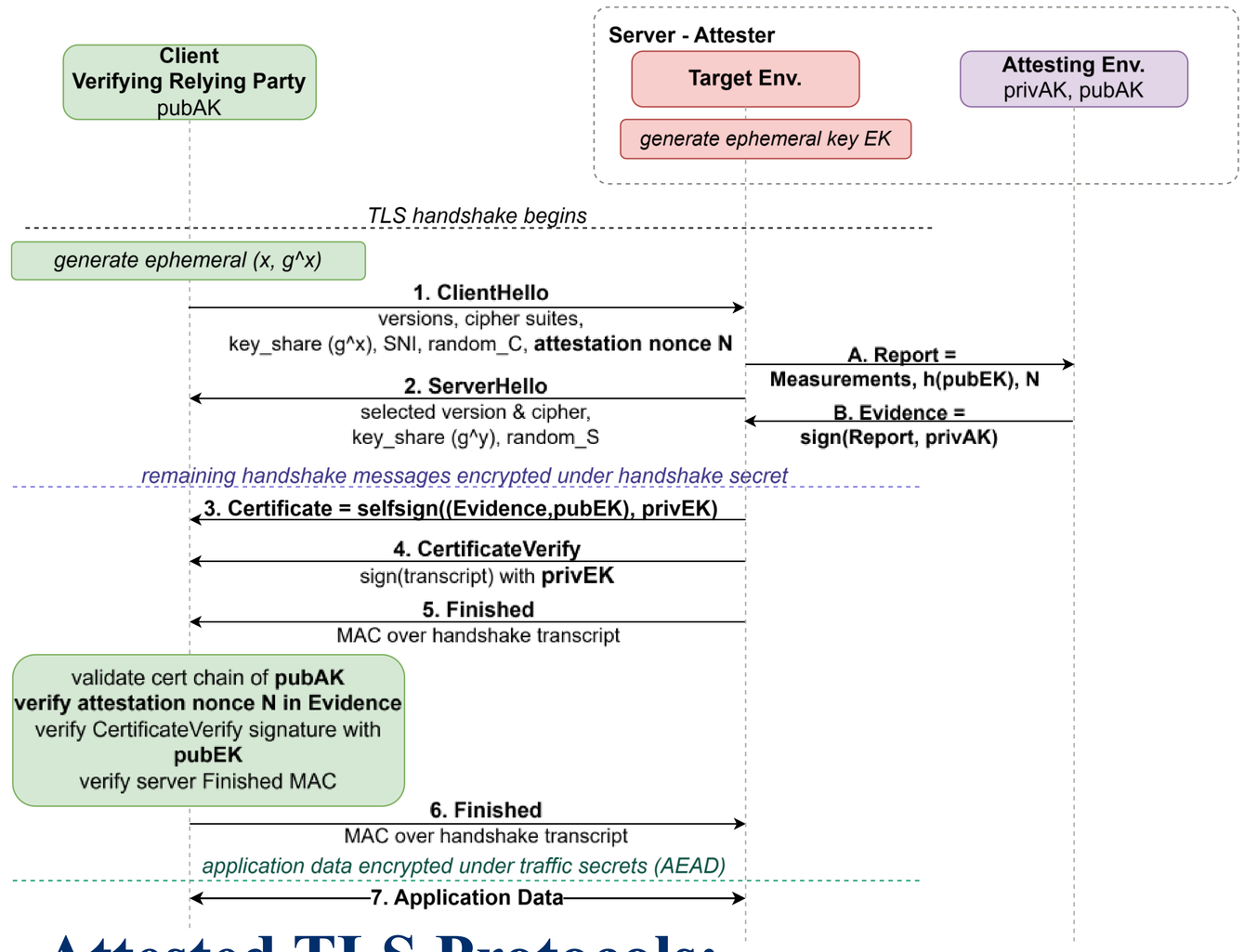

## TLS Goals:

- Certified long-term server identity
- Server authentication in TLS handshake

**Can TLS be used to communicate Evidence?**

The Intel RA-TLS protocol uses TLS to send attestation Evidence. The IETF working group propose TLS-a which adds freshness to the Evidence.

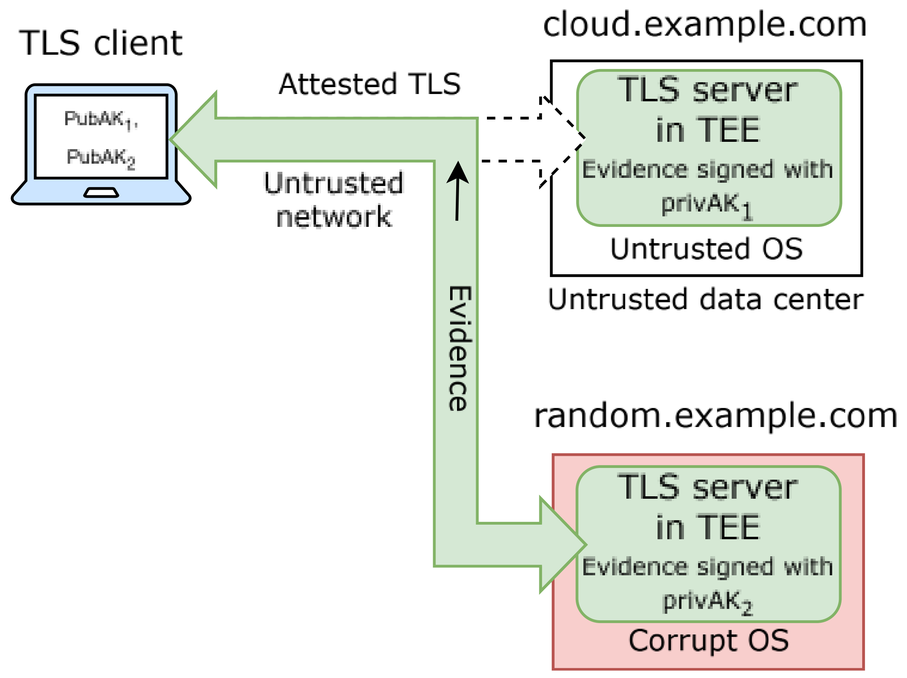
## IETF draft: TLS-a




## Attested TLS Protocols:

- Both, Intel RA-TLS and TLS-a send the Attestation Evidence instead of X.509 Certificate as TLS Certificate message
- Use Ephemeral Key EK to sign TLS CertificateVerify message
- Replace TLS goals with Attestation goals

## Attack: Diversion to a different Server




- In all attested TLS protocols, the server identity is not verified.
- Attested TLS connections can be redirected to any server anywhere that runs the same software in TEE
- If one TEE somewhere in the world is compromised, it could be used to break the security of all attested TLS connections.

Aalto University

Contact: muhammad_usama.sardar@tu-dresden.de, mariam.moustafa@aalto.fi, tuomas.aura@aalto.fi