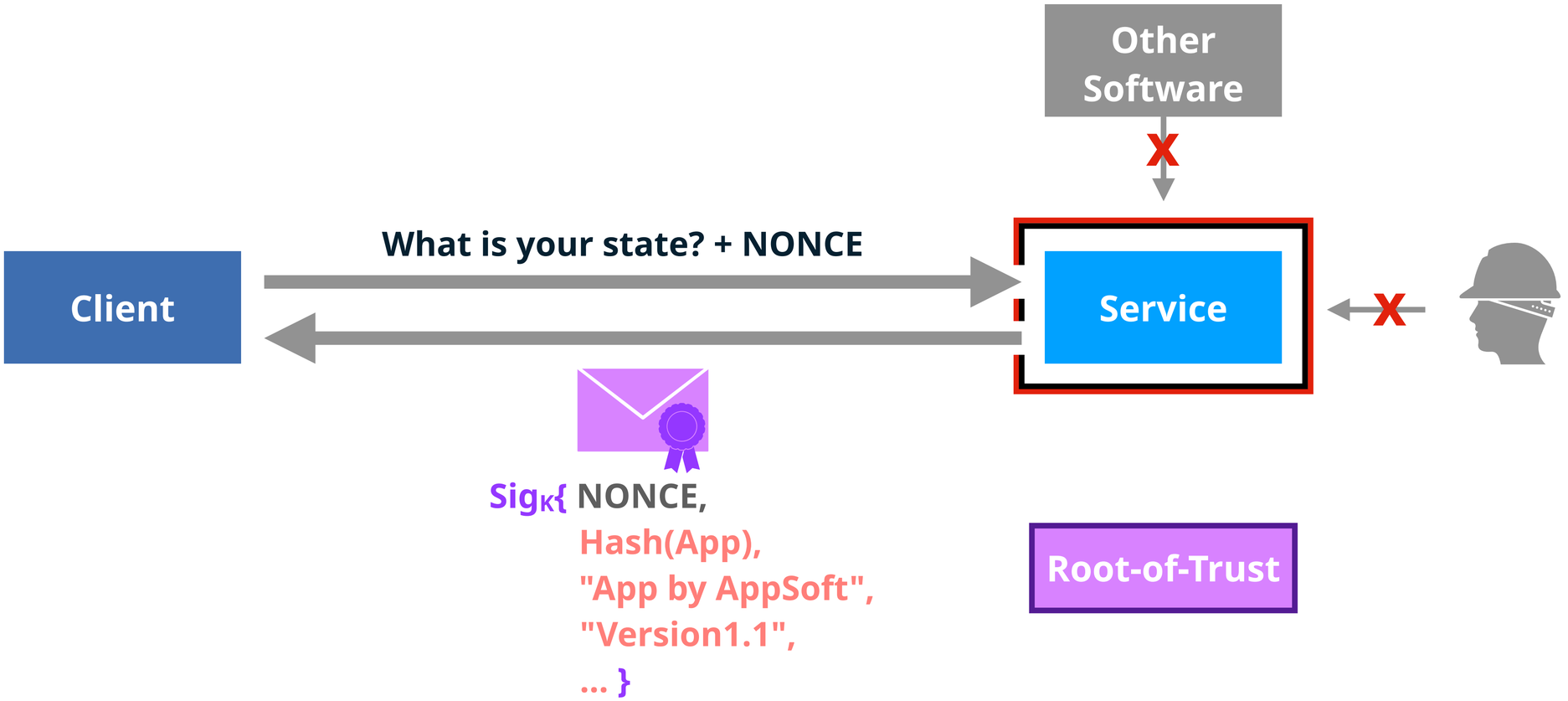
barkhauseninstitut.org

barkhausen institut

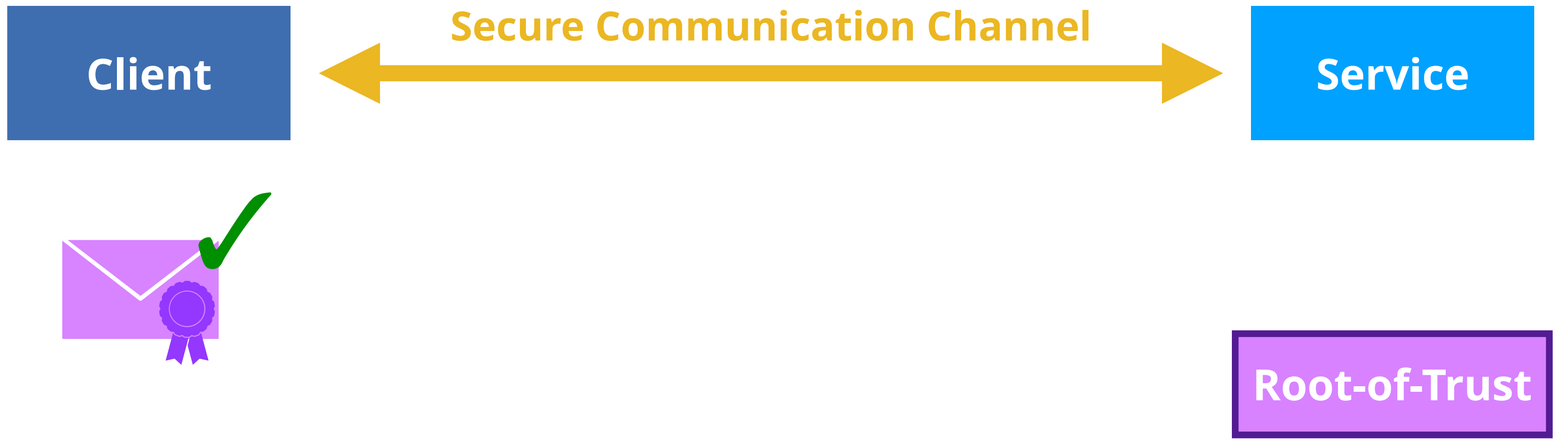
Separate but Together: Integrating Remote Attestation into TLS

Carsten Weinhold (Barkhausen Institut), Muhammad Usama Sardar (TU Dresden), Ionuț Mihalcea (Arm), Yogesh Deshpande (Arm), Hannes Tschofenig (University of Applied Sciences Bonn-Rhein-Sieg), Yaron Sheffer (Intuit), Thomas Fossati (Linaro), Michael Roitzsch (Barkhausen Institut)

How to Talk to a Trusted Execution Environment



How to Talk to a Trusted Execution Environment

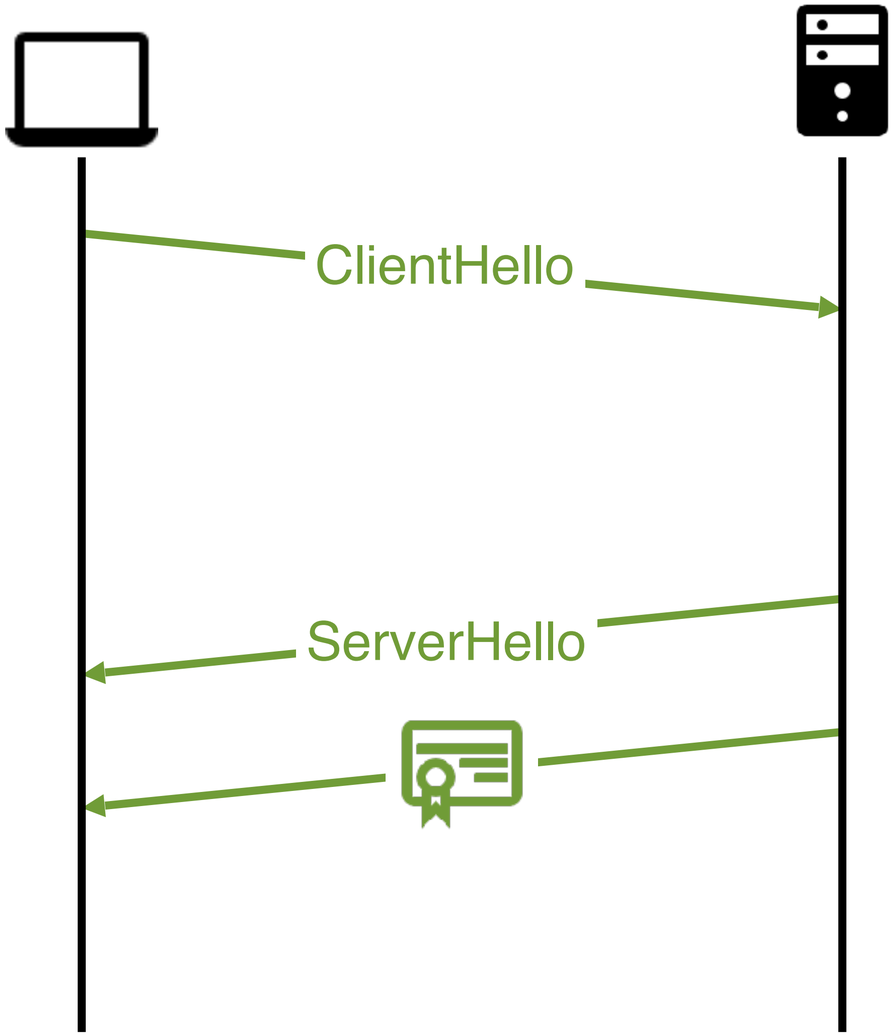


TLS+RA: Transport Layer Security (TLS) with Remote Attestation (RA)

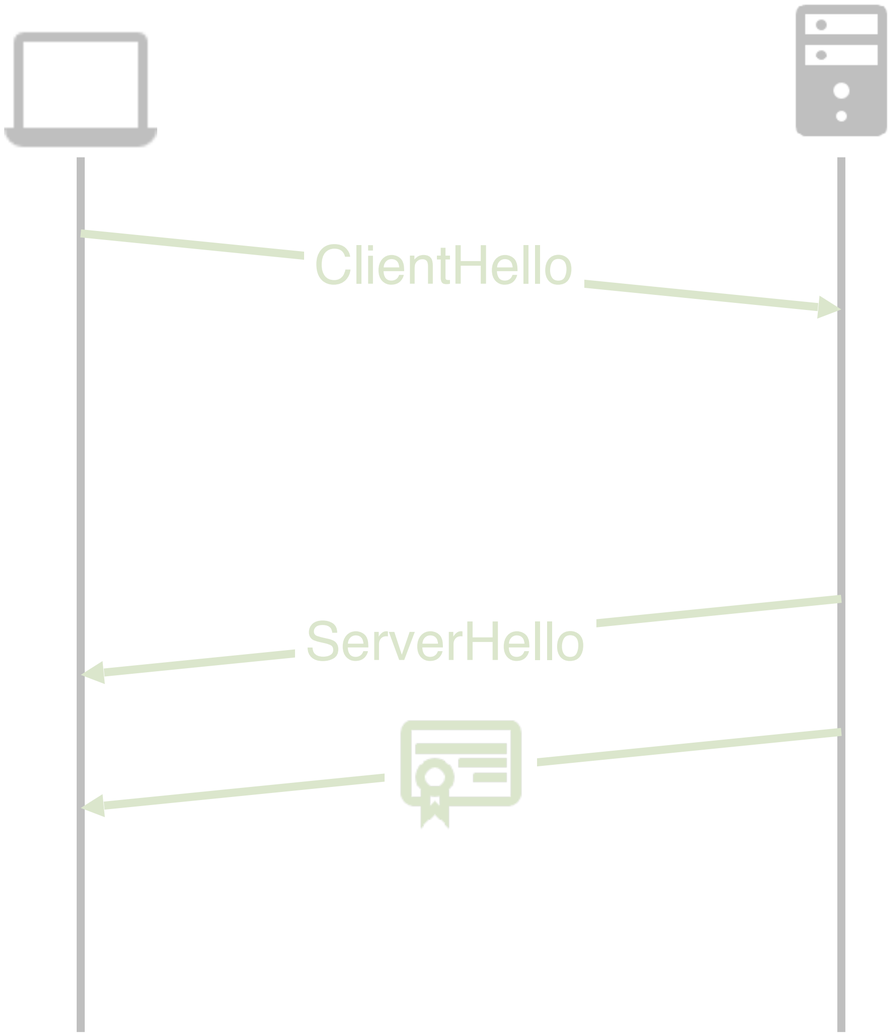
TLS+RA Design Goals

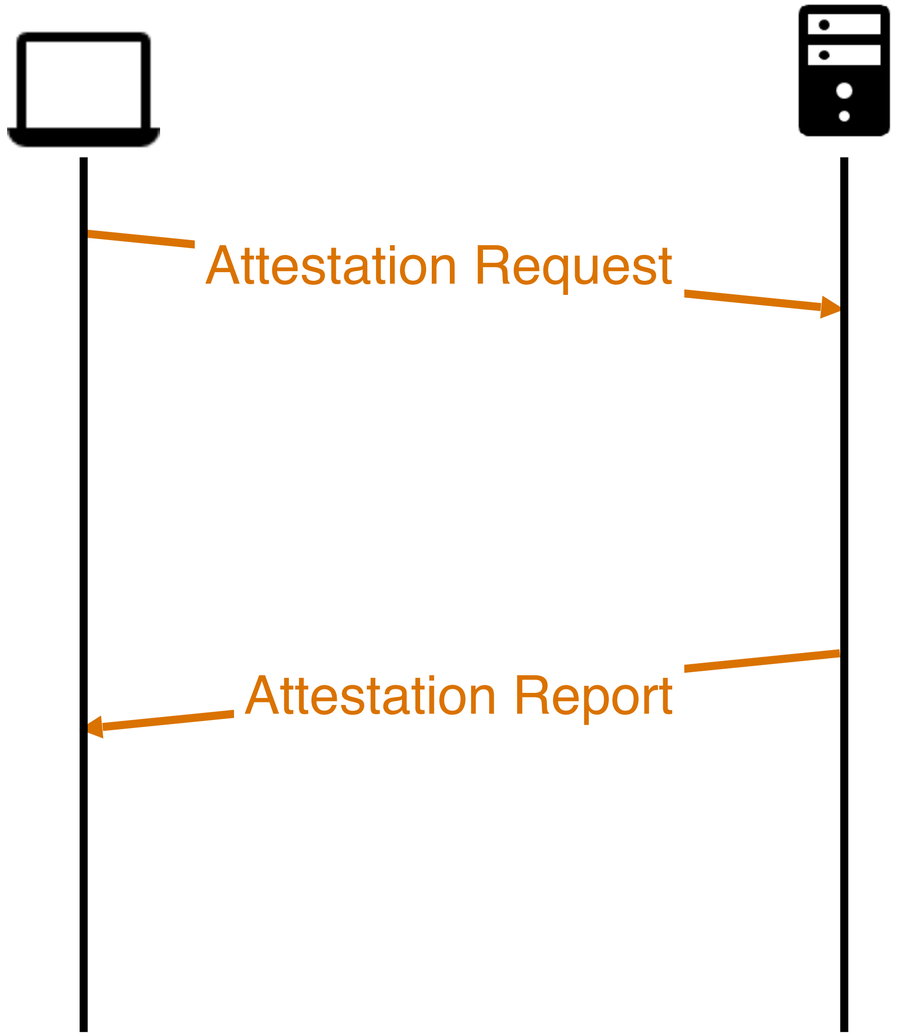
- minimize modifications to **TLS wire protocol**
- **no additional roundtrip messages** during handshake
- **no additional payload encryption** once channel is established
- **independent of root-of-trust** implementation
- resilient against **relay attacks:** channel must terminate at attested service
- **additive security:** RA validity should not hinge on TLS private key
- no changes to certificate or attestation **deployment**

Handshake: Transport Layer Security (TLS)

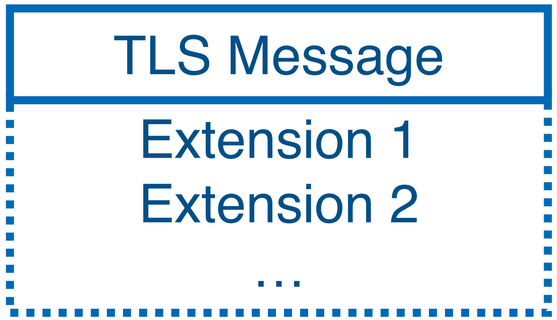


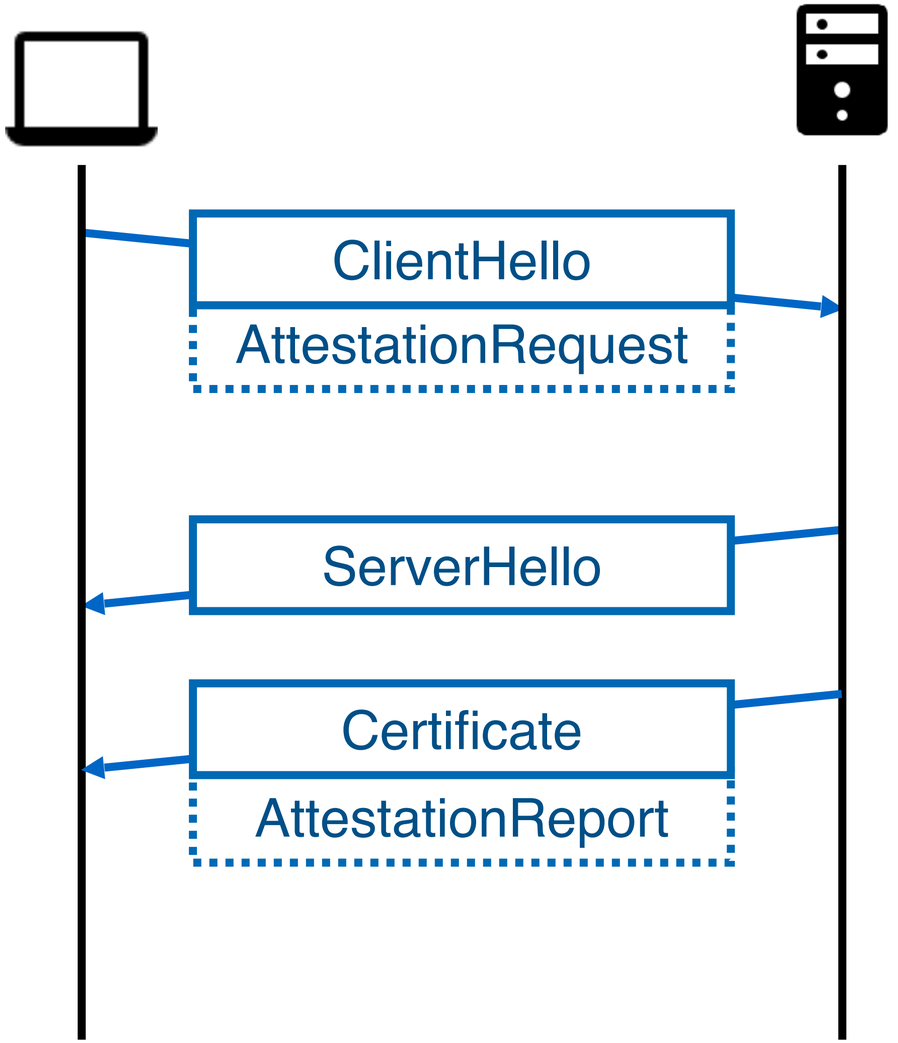
Handshake: Remote Attestation (RA)





RA piggy-backed in TLS message extensions





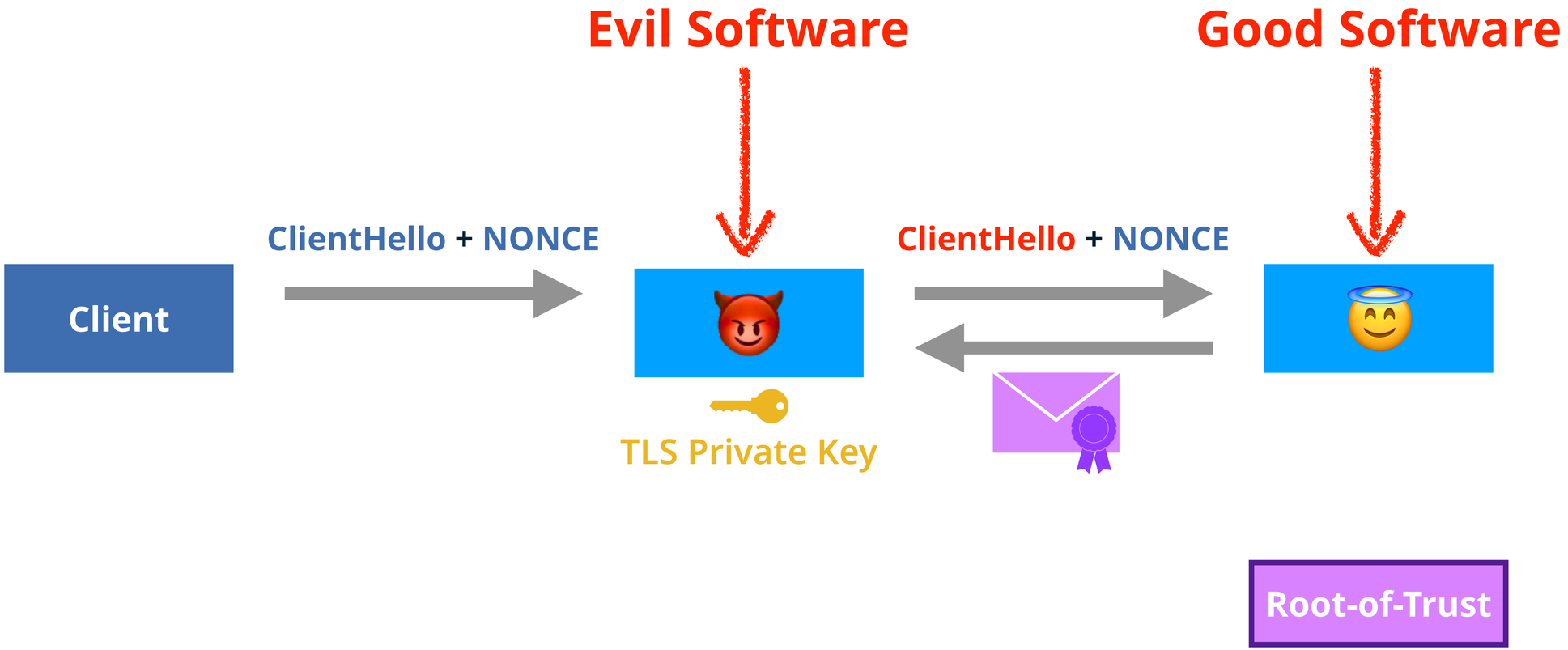
TLS+RA Design

TLS+RA uses standard TLS message extensions

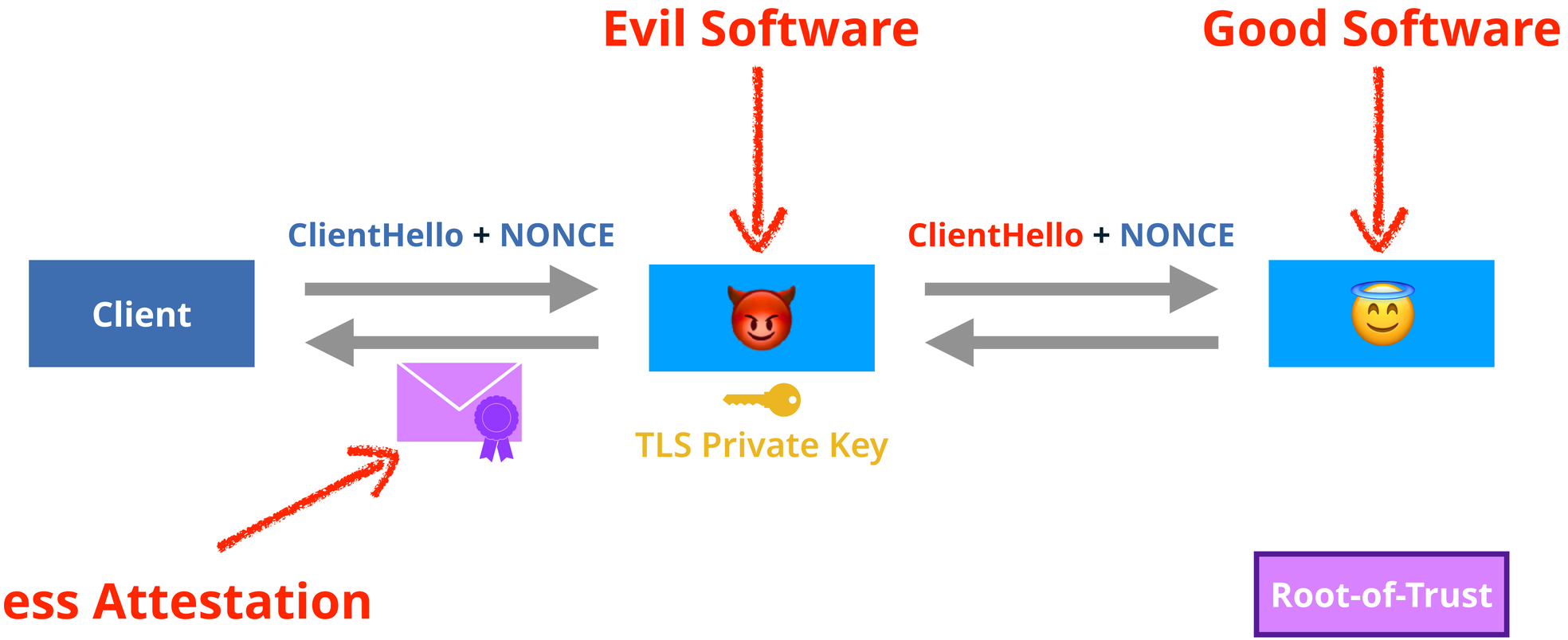
- no changes to wire protocol
- no additional roundtrips, no additional encryption
- extensions can carry any attestation report

Relay attacks?

Relay Attacks



Relay Attacks

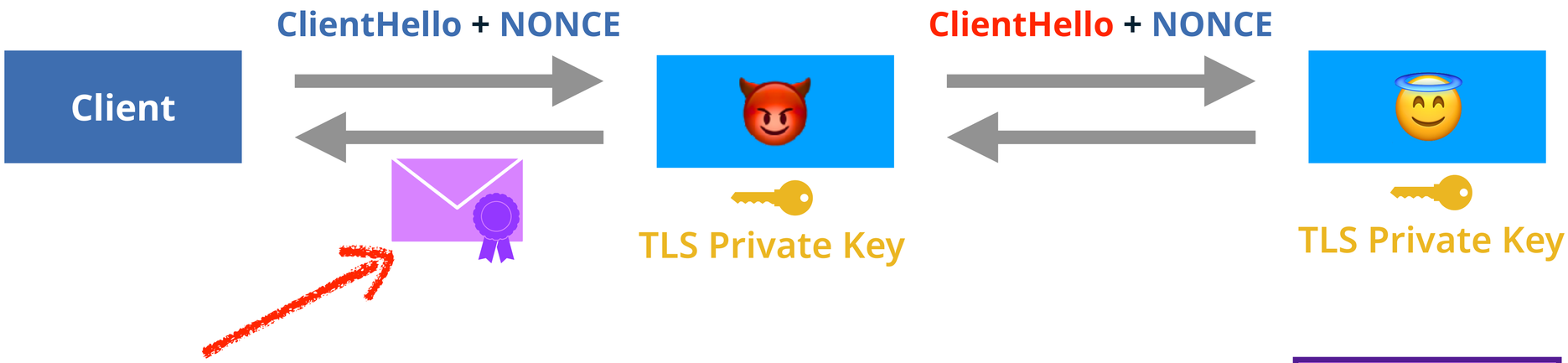


Must link attestation to TLS channel!

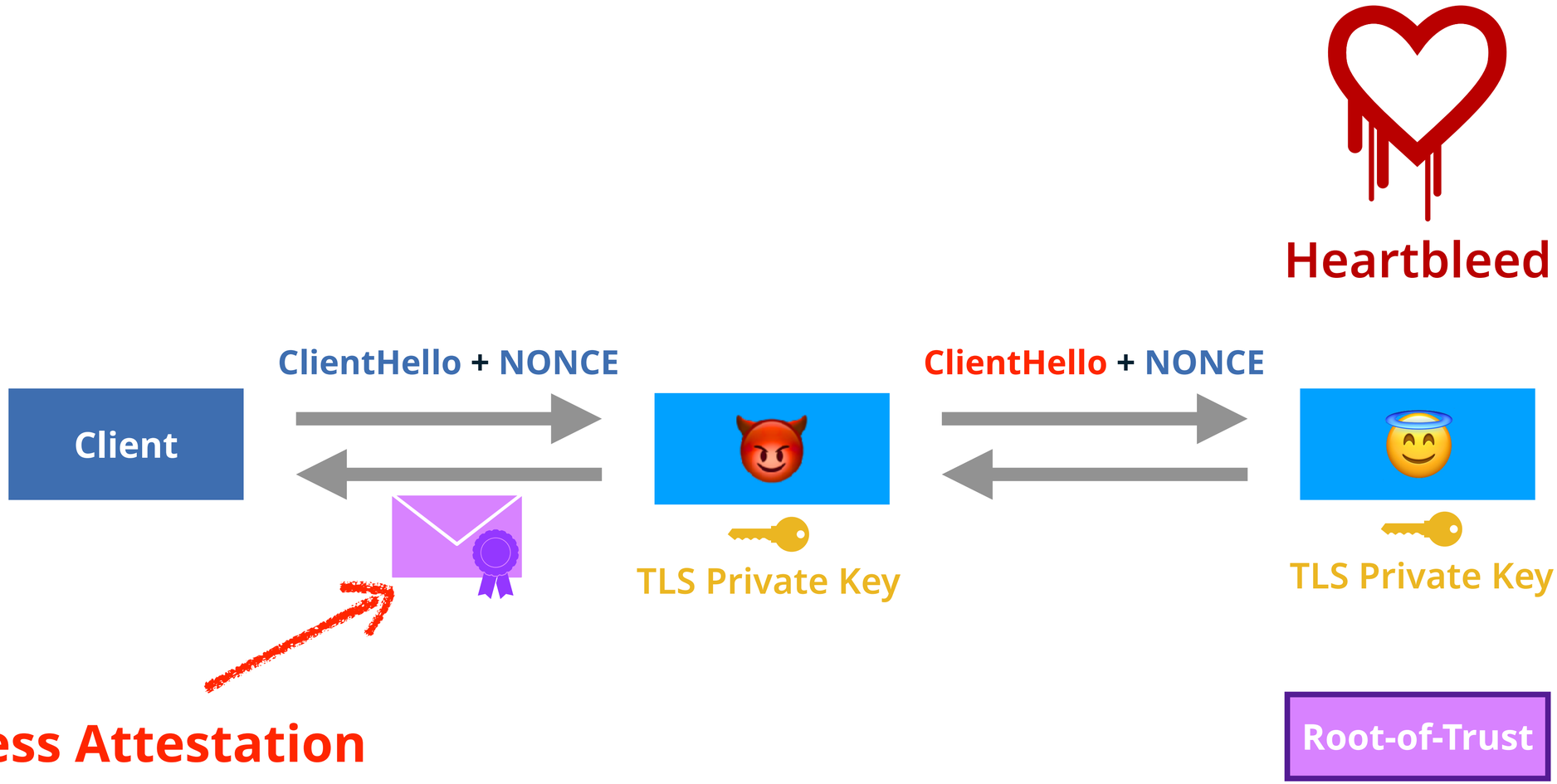
Relay Attacks



Relay Attacks

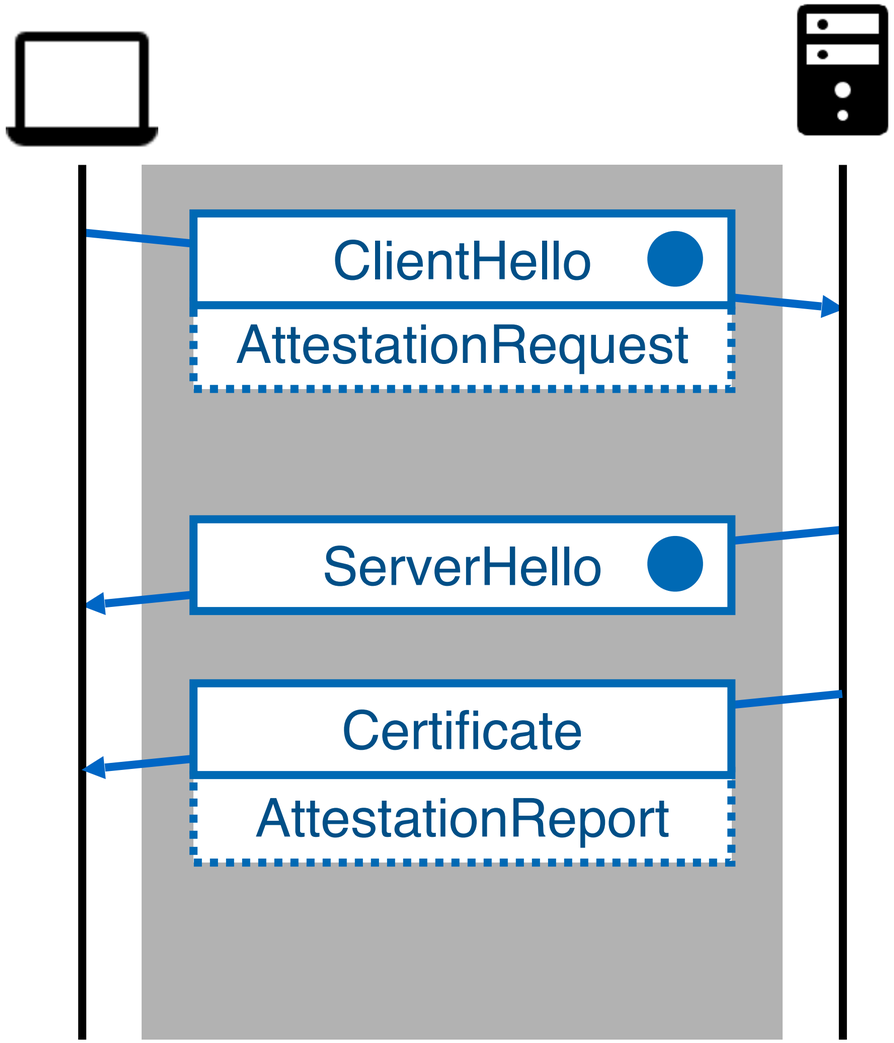


Relay Attacks



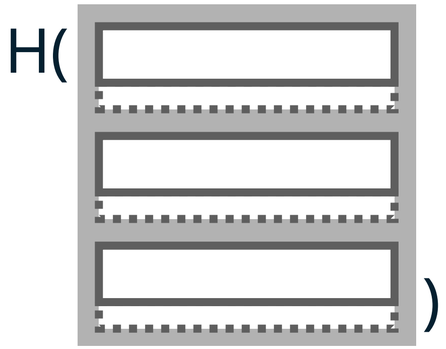
Attestation relies on residency of TLS private key!

Linking Attestation to Session Secrets



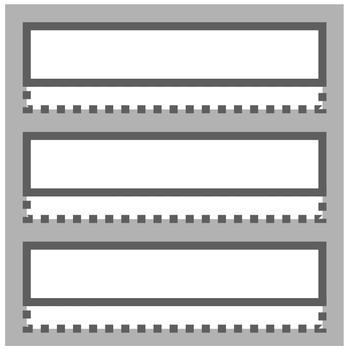
Ephemeral Diffie-Hellman Key Exchange

Transcript hash:



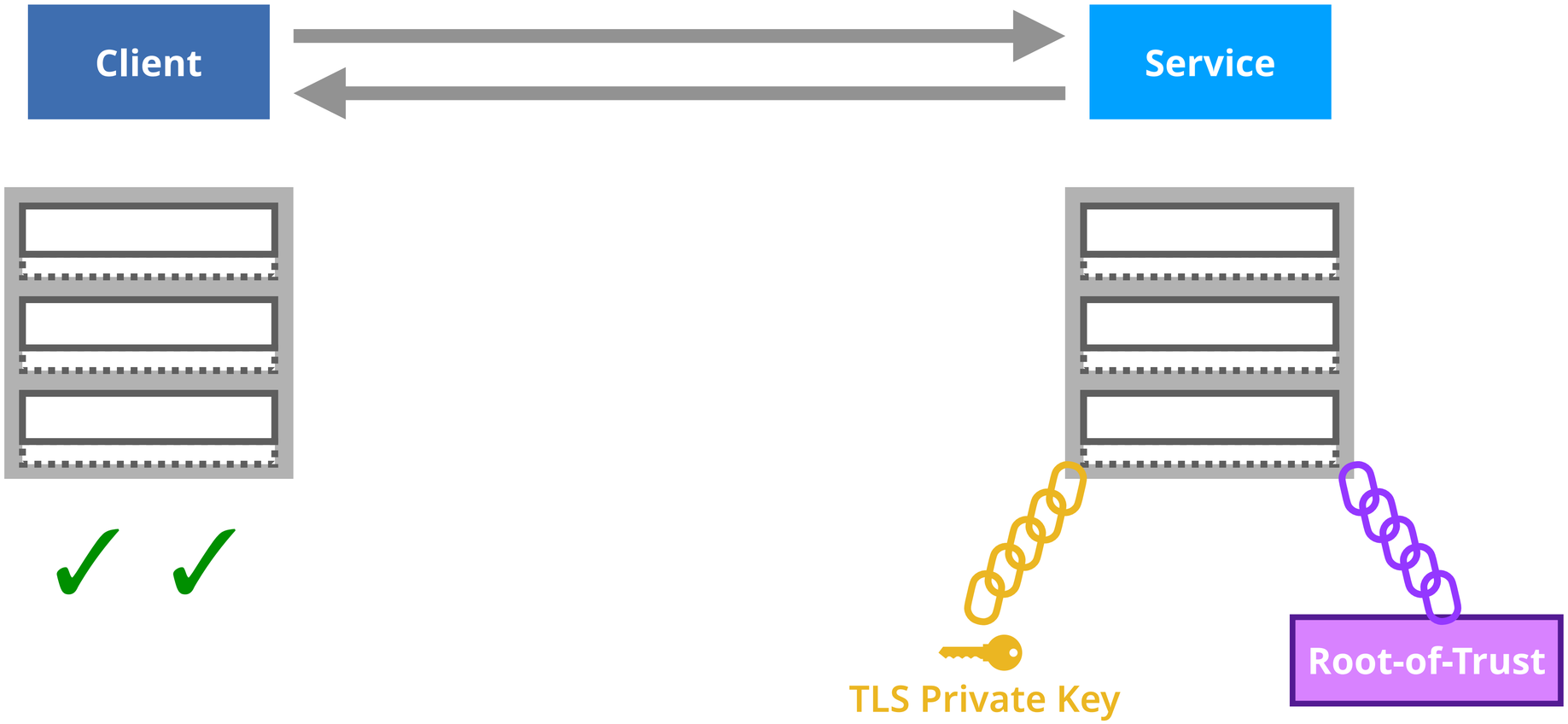
TLS Private Key

Linking hash:



Root-of-Trust

TLS+RA: Additive Security



Summary



TLS+RA combines TLS with Remote Attestation

- uses TLS standard extensions, no changes to wire protocol
- no additional roundtrips, no additional encryption
- extensions can carry any attestation report

Relay attacks prevented by linking attestation to handshake messages

- independent deployment: no changes to RA and TLS infrastructure
- independent failure: RA does not rely on TLS key residence

TLS+RA provides additive security of TLS and RA

CORENEXT CYMEDSEC inenious SACHSEN