Attested TLS

Microsoft Azure Confidential Compute Team

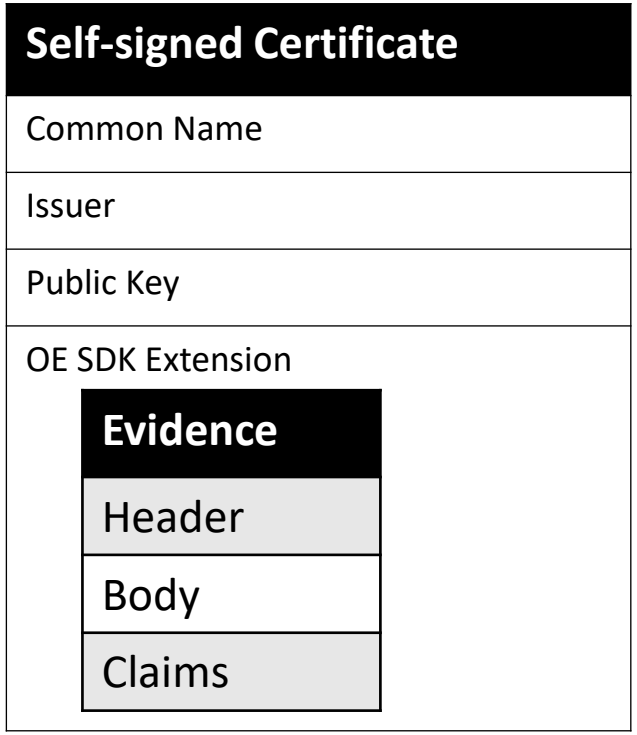
Presented by Andy Chen

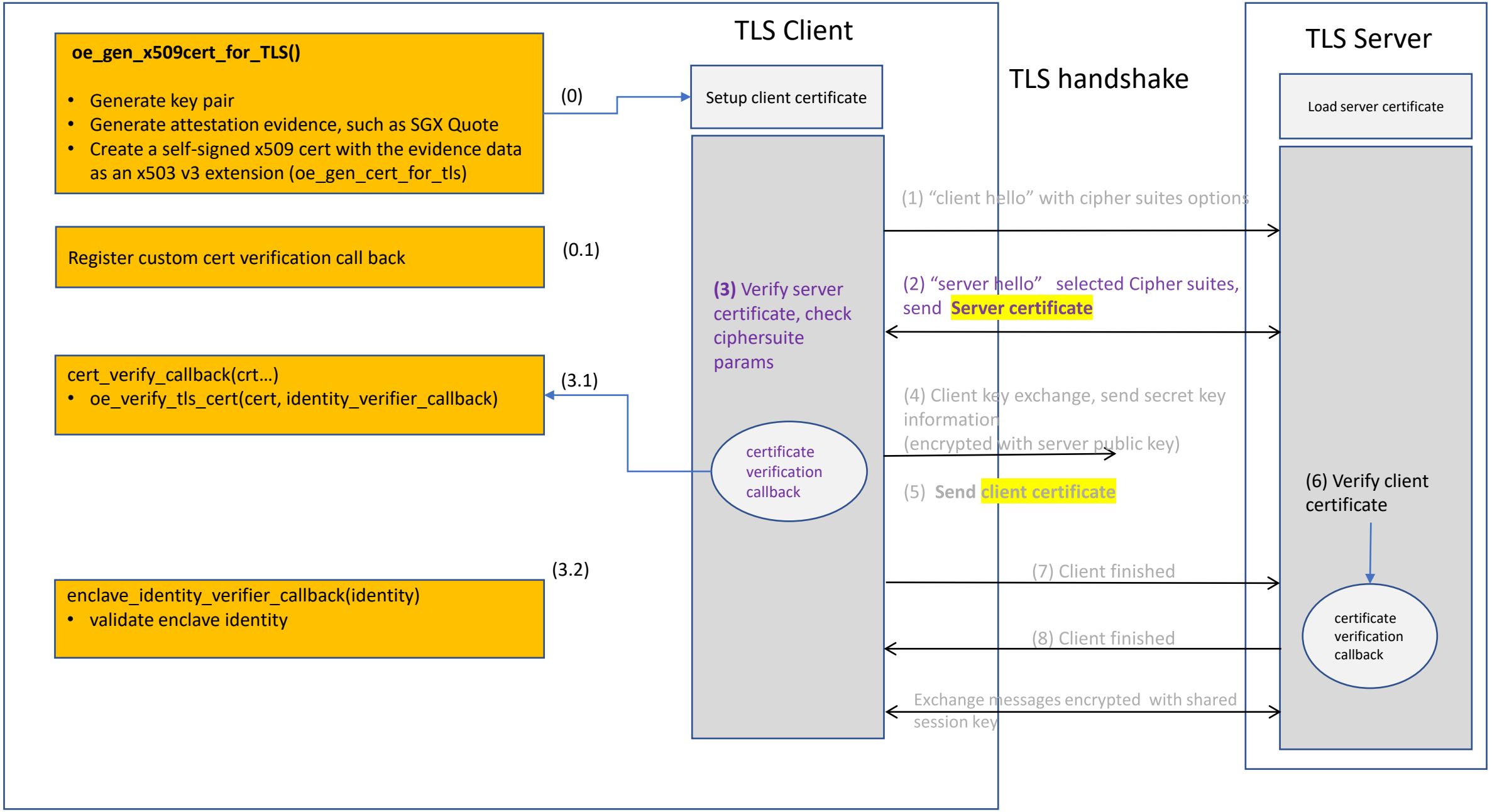
Agenda

- TLS channel setup with attestation
- Attestation Extensions

Certificates for TLS channel setup

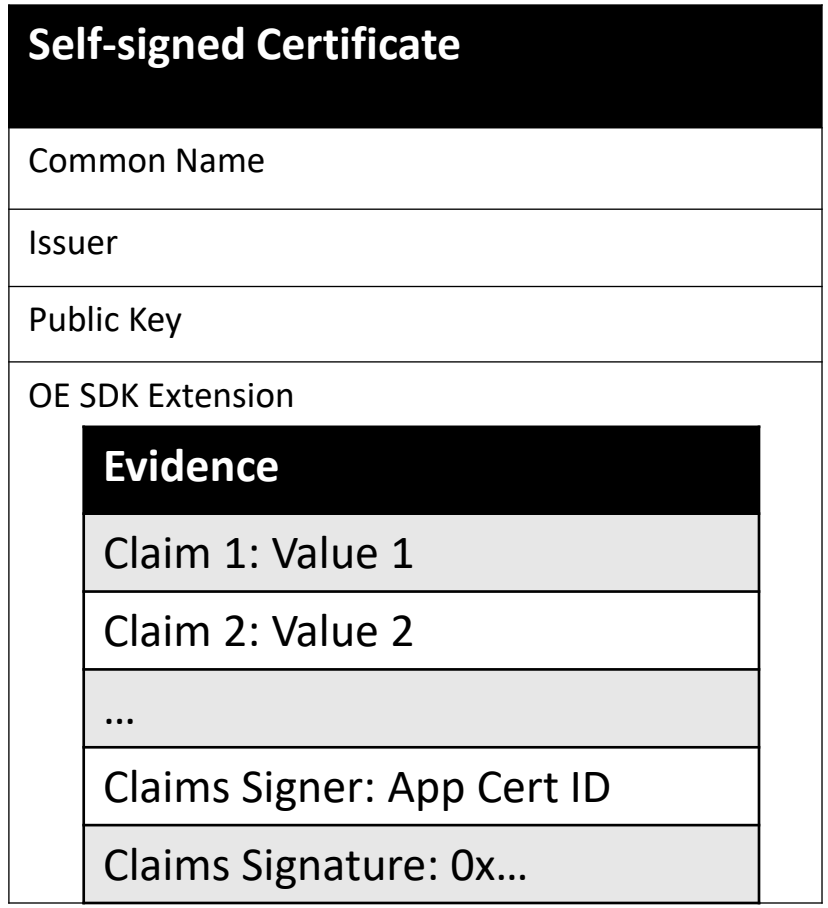
- Server & Client Certificates
  - Includes attestation evidence
    - Microsoft defines a unique OID for it
    - A data package for attestation, such as SGX report
  - Created during the TLS channel setup
  - Self-signed




TLS Client
TLS handshake
TLS Server
oe_gen_x509cert_for_TLS()
• Generate key pair
• Generate attestation evidence, such as SGX Quote
• Create a self-signed x509 cert with the evidence data as an x503 v3 extension (oe_gen_cert_for_tls)
(0)
Setup client certificate
Load server certificate
Register custom cert verification call back
(0.1)
(1) "client hello" with cipher suites options
(3) Verify server certificate, check ciphersuite params
(2) "server hello" selected Cipher suites, send Server certificate
cert_verify_callback(crt…)
• oe_verify_tls_cert(cert, identity_verifier_callback)
(3.1)
(4) Client key exchange, send secret key information (encrypted with server public key)
certificate verification callback
(5) Send client certificate
(6) Verify client certificate
(3.2)
(7) Client finished
enclave_identity_verifier_callback(identity)
• validate enclave identity
certificate verification callback
(8) Client finished
Exchange messages encrypted with shared session key

Attestation Extensions by OpenEnclave SDK

- Claims in evidence
  - A set of data that attached to the evidence
  - Claimed by the host and signed as part of attestation report, such as SGX.
  - OE SDK verifies the integrity of data
  - Application verifies the truth of the claims



Resources

- RA-TLS
  - RA-TLS-whitepaper v2.3 no copyright.docx (arxiv.org)
- Attested TLS Source Code
  - openenclave/samples/attested_tls at master · openenclave/openenclave (github.com)