Remote Attestation with Exported Authenticators (draft-fossati-tls-exported-attestation)

Thomas Fossati, Muhammad Usama Sardar, Tirumaleswar Reddy, Yaron Sheffer, Hannes Tschofenig and Ionut Mihalcea

July 25, 2025

CONFIDENTIAL COMPUTING CONSORTIUM

GENXT

Teleport

Thank you all!

$$\text{expat} = \text{RATS++}$$

Informal Security Goals of Attested TLS

- Standard TLS properties, in particular Server authentication

- Remote Attestation
  - Integrity of *Claims*
  - Freshness of *Claims*
  - *Attestation Credential* refresh
    - Discussion: concrete use case?

Informal Security Goals of Attested TLS

- Standard TLS properties, in particular Server authentication
- Remote Attestation
  - Integrity of *Claims*
  - Freshness of *Claims*
  - *Attestation Credential* refresh
    - Discussion: concrete use case?
- Composition goals
  - Binding of Remote Attestation and TLS
    - Binding *Evidence* to TLS session: *Evidence* should not be usable in other sessions.
  - *Evidence* is generated by the same server that is authenticated.
- What else?