

# 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 23, 2025



# Threat Model

- Standard TLS threat model (weak DH, weak hash etc.)
- Long-Term Key (**privLTK**) may be leaked
- Attestation Key (**privAK**) may be leaked (e.g., via Foreshadow<sup>1</sup>)

---

<sup>1</sup>Van Bulck, Minkin, Weisse, Genkin, Kasikci, Piessens, Silberstein, Wenisch, Yarom, and Strackx, "Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution", 2018.

# Threat Model

- Standard TLS threat model (weak DH, weak hash etc.)
- Long-Term Key (**privLTK**) may be leaked
- Attestation Key (**privAK**) may be leaked (e.g., via Foreshadow<sup>1</sup>)
- Assumptions (complementary to protocol design)
  - No weaknesses in the **generation of Claims**
  - Verifying RP provisioned with **Reference Values**
  - **TOCTOU attacks** out of the scope

---

<sup>1</sup>Van Bulck, Minkin, Weisse, Genkin, Kasikci, Piessens, Silberstein, Wenisch, Yarom, and Strackx, "Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution", 2018.

# Informal Security Goals

- Standard TLS properties, in particular Server authentication

# Informal Security Goals

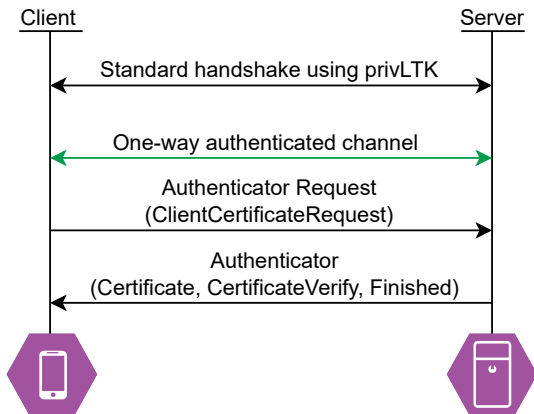
- Standard TLS properties, in particular Server authentication
- Remote Attestation
  - Integrity of *Claims*
  - Freshness of *Claims*
  - *Attestation Credential* refresh

# Informal Security Goals

- Standard **TLS** properties, in particular Server authentication
- **Remote Attestation**
  - Integrity of *Claims*
  - Freshness of *Claims*
  - *Attestation Credential* refresh
- **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.

# Exported Authenticators<sup>2</sup> (RFC 9261)

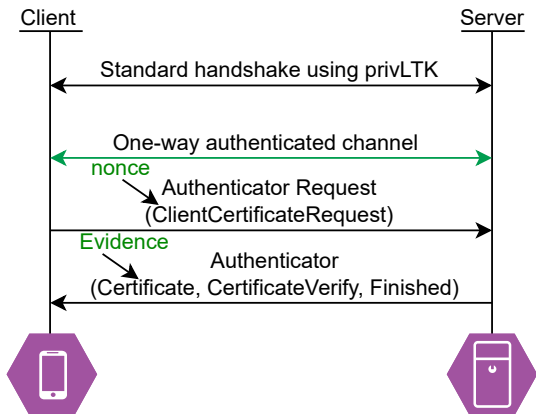
- `ClientCertificateRequest`: Similar to `CertificateRequest`
- `Authenticator Keys` via Exporters



<sup>2</sup>Sullivan, *Exported Authenticators in TLS*, 2022.

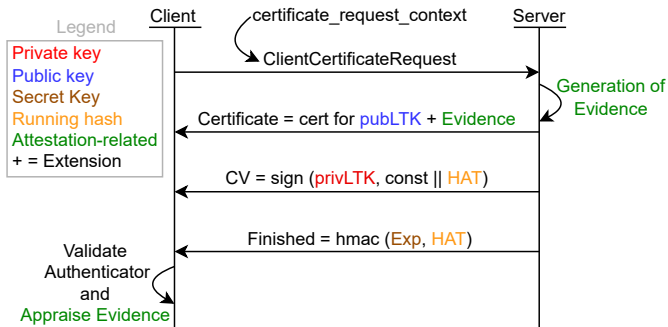
# Initial Proposal

- No change in TLS handshake protocol
- Example: **TLS Server** as **RATS Attester**



# Protocol Diagram (Post-handshake Flow)

1. Authenticator Request
  - Unique *certificate\_request\_context* within connection
2. Evidence based on this context and *Exported Keying Material (EKM)*
3. Authenticator
  - Certificate message extended with Evidence
  - CertificateVerify as in RFC 9261
  - Finished as in RFC 9261
4. Validation: additionally appraise Evidence



# Key References



Sullivan, Nick. *Exported Authenticators in TLS*. RFC 9261. July 2022. DOI: 10.17487/RFC9261. URL: <https://www.rfc-editor.org/info/rfc9261>.



Van Bulck, Jo, Marina Minkin, Ofir Weisse, Daniel Genkin, Baris Kasikci, Frank Piessens, Mark Silberstein, Thomas F. Wenisch, Yuval Yarom, and Raoul Strackx. "Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution". In: *Proceedings of the 27th USENIX Security Symposium*. USENIX Association, Aug. 2018.