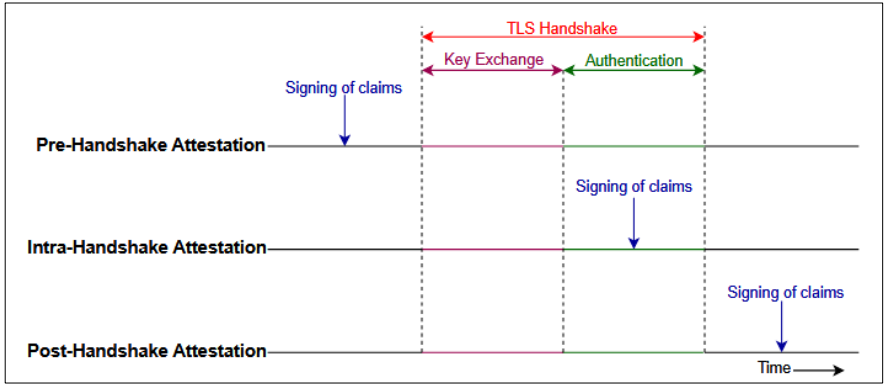
Attestation and TLS

TLS WG, IETF 121, Dublin

Status

- Full exploration of the design space
  - Pre-handshake: attested CSR
  - Intra-handshake: attested TLS
  - Post-handshake: application layer and based on Exported Authenticators (RFC9261)
- Formal verification (Usama)
- Implementations exist



Use Cases

- The use of remote attestation in TLS is applicable to these use cases:

- **Confidential computing** (main priority)
- **Device onboarding**

The web is not a use case for this document!

Next Steps

- Aiming for experimental status
- Adopt?