IETF Hackathon

TLS & Attestation

IETF 116

25-26 March 2023

Yokohama, Japan

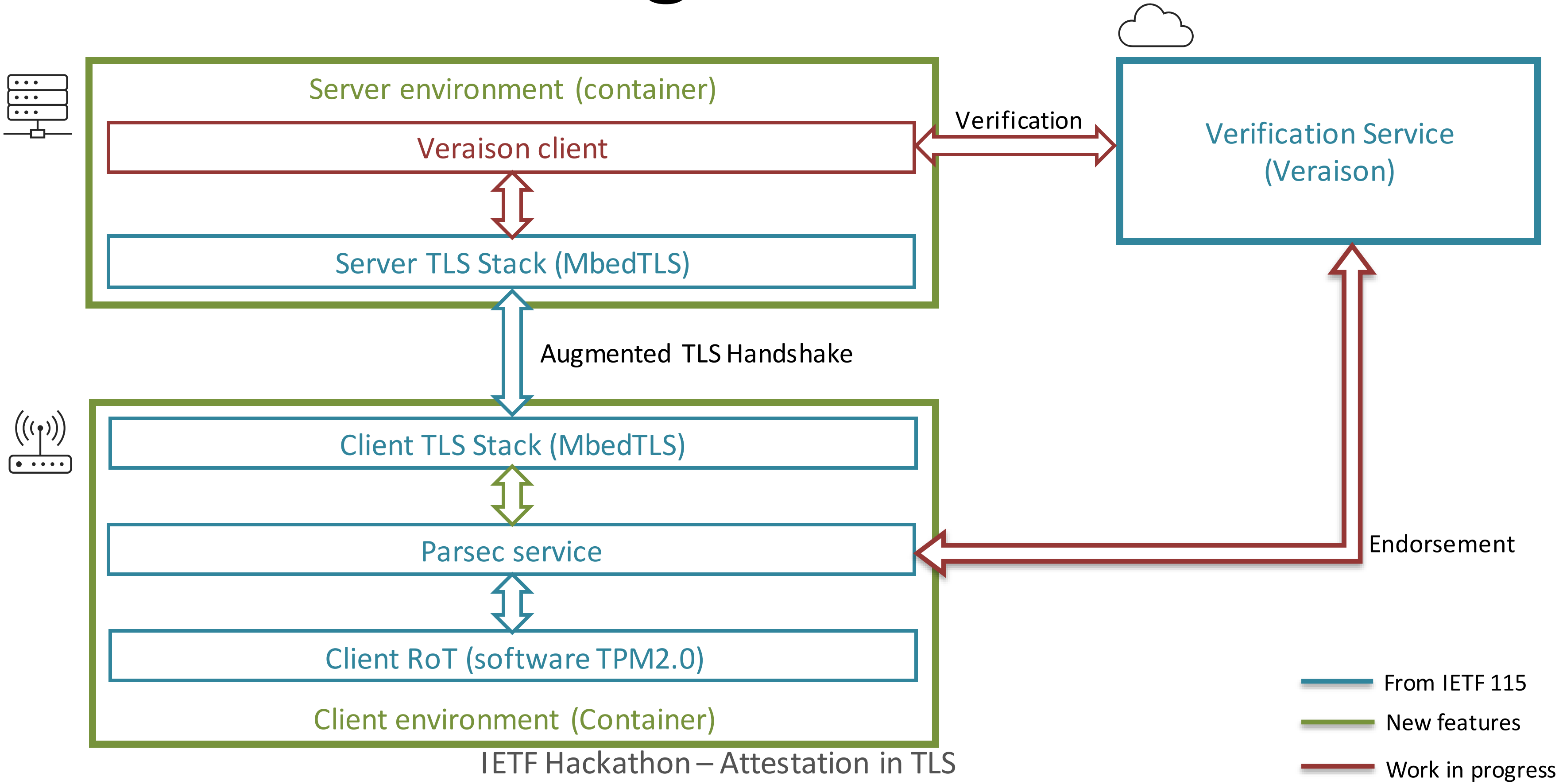
Hackathon Plan

- End-to-end prototype using remote attestation as an authentication mechanism in TLS
  - draft-fossati-tls-attestation
  - Continuing the work from IETF 115
- Goal: Hooking the TLS implementation to Root of Trust, and to Verification Service

What got done

- Filled some of the gaps in the prototype
    - Defined some of the required formats
    - Developed some of the glue layers (e.g., client libraries)
    - Started assembling container images that encapsulate the participants of the protocol

What got done



Server environment (container)

Veraison client

Server TLS Stack (MbedTLS)

Verification

Verification Service (Veraison)

Augmented TLS Handshake

Client TLS Stack (MbedTLS)

Parsec service

Client RoT (software TPM2.0)

Client environment (Container)

Endorsement

From IETF 115

New features

Work in progress

What we learned

- Many components, APIs, and formats to synchronise
- Some drafts are only now being fleshed out

Wrap Up

Team members:

- Thomas Fossati
- Paul Howard
- Yogesh Deshpande
- Ionut Mihalcea

First timers @ IETF/Hackathon:

- https://datatracker.ietf.org/doc/draft-fossati-tls-attestation/
- https://github.com/CCC-Attestation/attested-tls-poc
- https://datatracker.ietf.org/doc/html/draft-ftbs-rats-msg-wrap
- https://datatracker.ietf.org/doc/html/draft-bft-rats-kat
- https://datatracker.ietf.org/doc/draft-fv-rats-ear/