IETF Hackathon
TLS & Attestation

IETF 117
22-23 July 2023
San Francisco, California

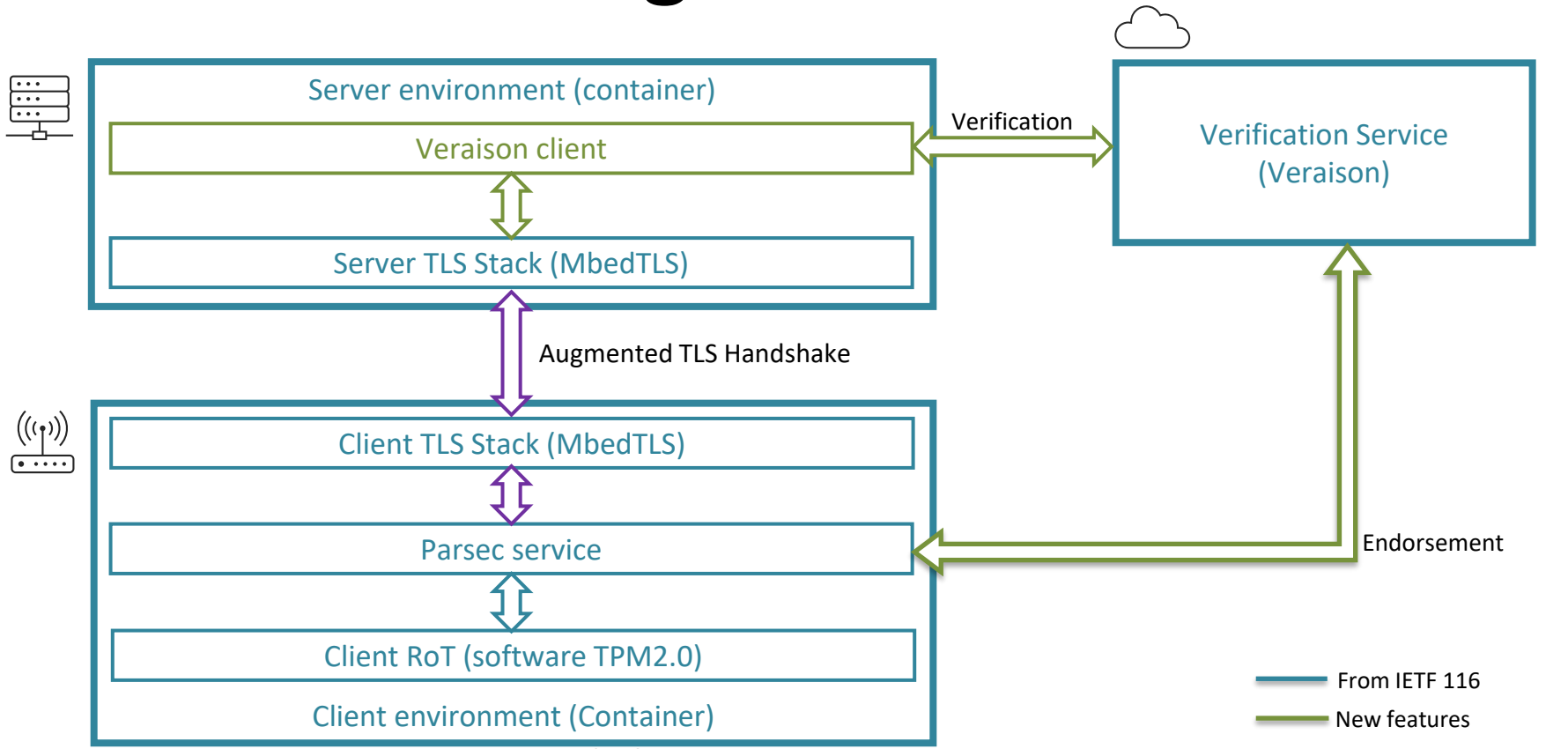
Hackathon Plan

- End-to-end prototype using remote attestation as an authentication mechanism in TLS
  - draft-fossati-tls-attestation
  - Continuing the work from IETF 116
- Goal: A prototype covering everything from Root-of-Trust to verification service

What got done

- We have a functioning, end-to-end prototype
  - Implemented the endorsement and verification sides of the attestation scheme
  - Developed some more glue layers (e.g., client libraries)
  - Assembled all container images and the orchestration between them

What got done



What we learned

- Synchronising so many moving components needs some painstaking work
- Adding new attestation schemes is much easier with the right abstractions in place

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/