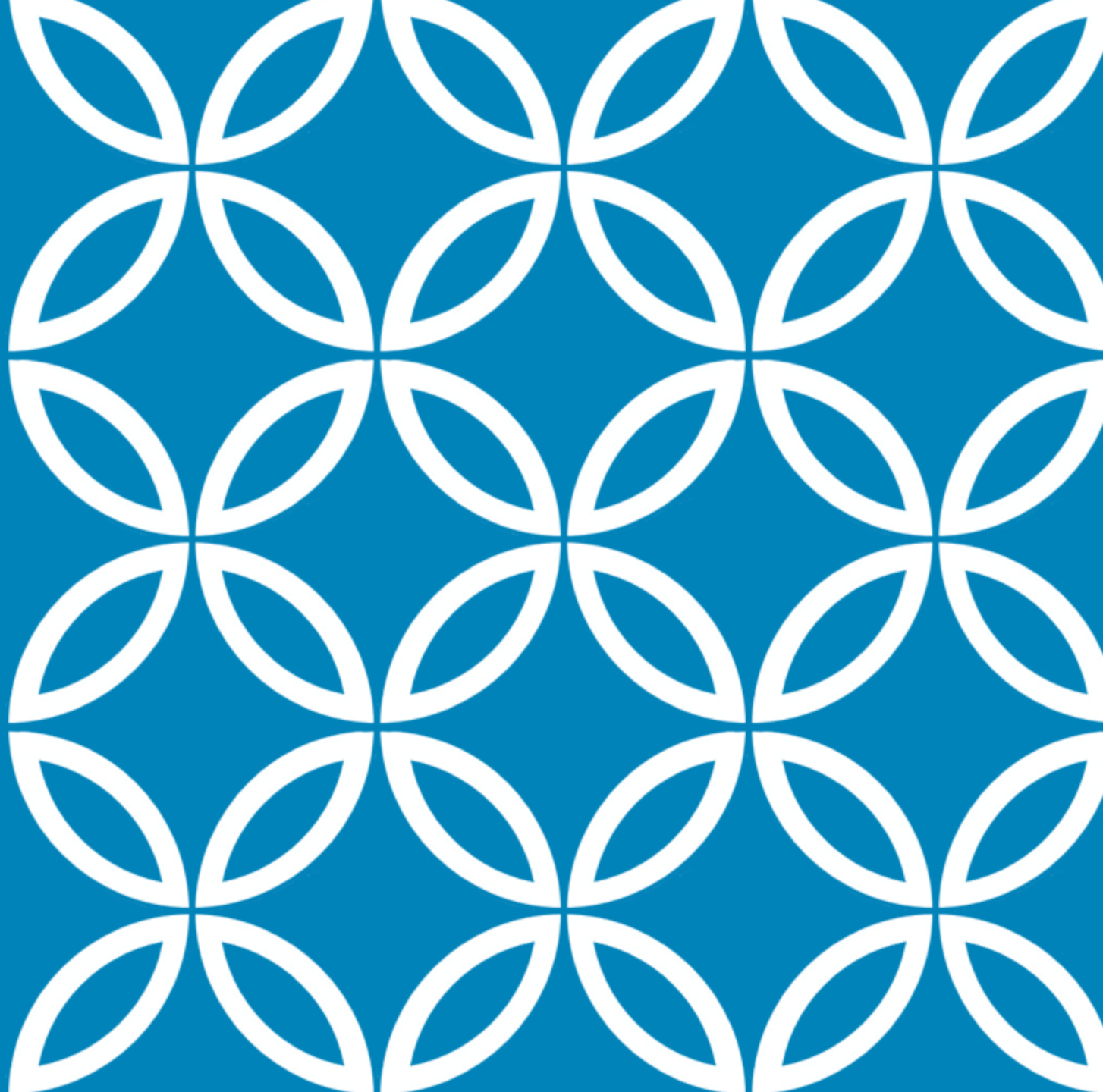
COMBINING TLS WITH ATTESTATION

Yaron Sheffer, VP of Technology, Intuit

Confidential Computing TLV, Sep. 2024



MOTIVATION

A simple TLS connection to/from a Confidential workload does not benefit from the platform's guarantees

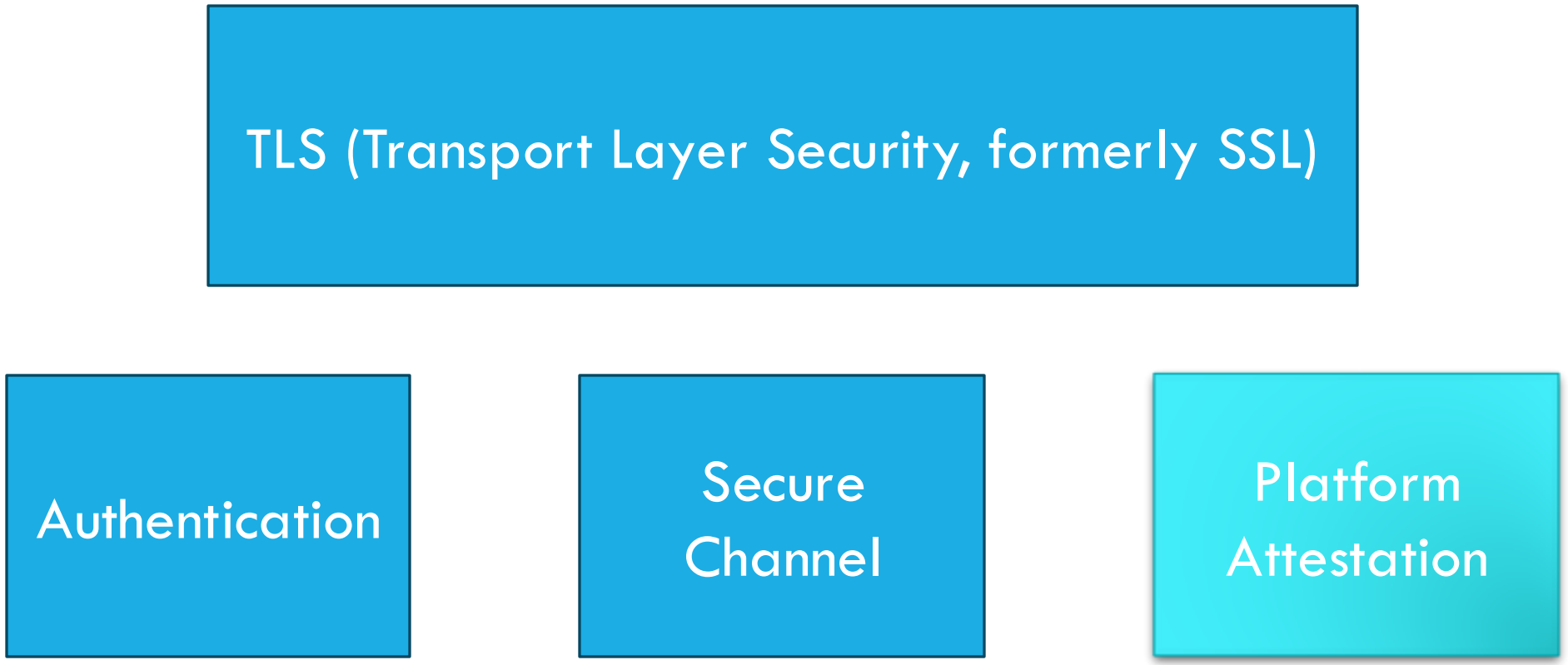
We introduce Attestation into the connection: strong guarantees regarding the security state of a device

Especially important for initial application setup

Custom solutions exist, we are working on a standard

draft-fossati-tls-attestation-07

VISUALLY…


TLS (Transport Layer Security, formerly SSL)
Authentication
Secure Channel
Platform Attestation

DETOUR: IETF

Internet Engineering Task Force

A standards organization established 1986

The main product is RFCs (“request for comments”) – these are stable standards

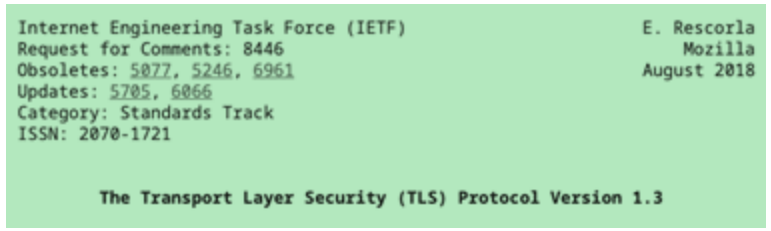
Work is carried out by Working Groups such as TLS, RATS

Network Working Group
Request for Comments: 1035

P. Mockapetris
ISI
November 1987

Obsoletes: RFCs 882, 883, 973

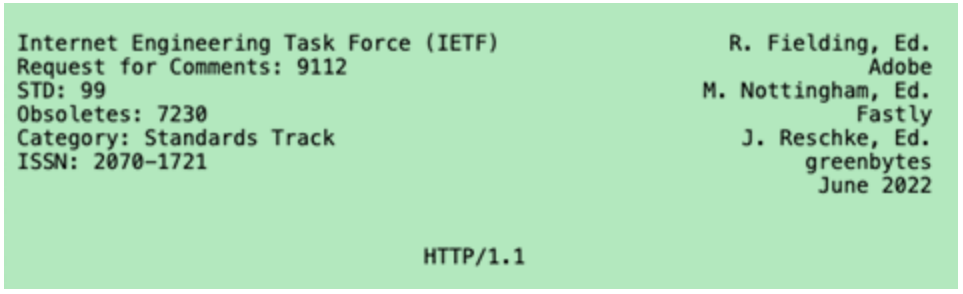
DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION



Internet Engineering Task Force (IETF)
Request for Comments: 8446
Obsoletes: 5077, 5246, 6961
Updates: 5705, 6066
Category: Standards Track
ISSN: 2070-1721

E. Rescorla
Mozilla
August 2018

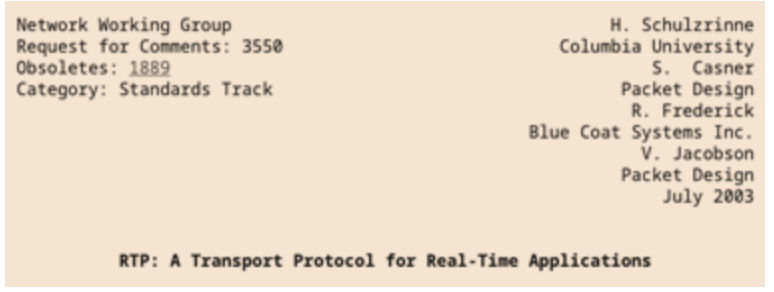
The Transport Layer Security (TLS) Protocol Version 1.3



Internet Engineering Task Force (IETF)
Request for Comments: 9112
STD: 99
Obsoletes: 7230
Category: Standards Track
ISSN: 2070-1721

R. Fielding, Ed.
Adobe
M. Nottingham, Ed.
Fastly
J. Reschke, Ed.
greenbytes
June 2022

HTTP/1.1



Network Working Group
Request for Comments: 3550
Obsoletes: 1889
Category: Standards Track

H. Schulzrinne
Columbia University
S. Casner
Packet Design
R. Frederick
Blue Coat Systems Inc.
V. Jacobson
Packet Design
July 2003

RTP: A Transport Protocol for Real-Time Applications

EXTENDING TLS

Attestation with or without authentication

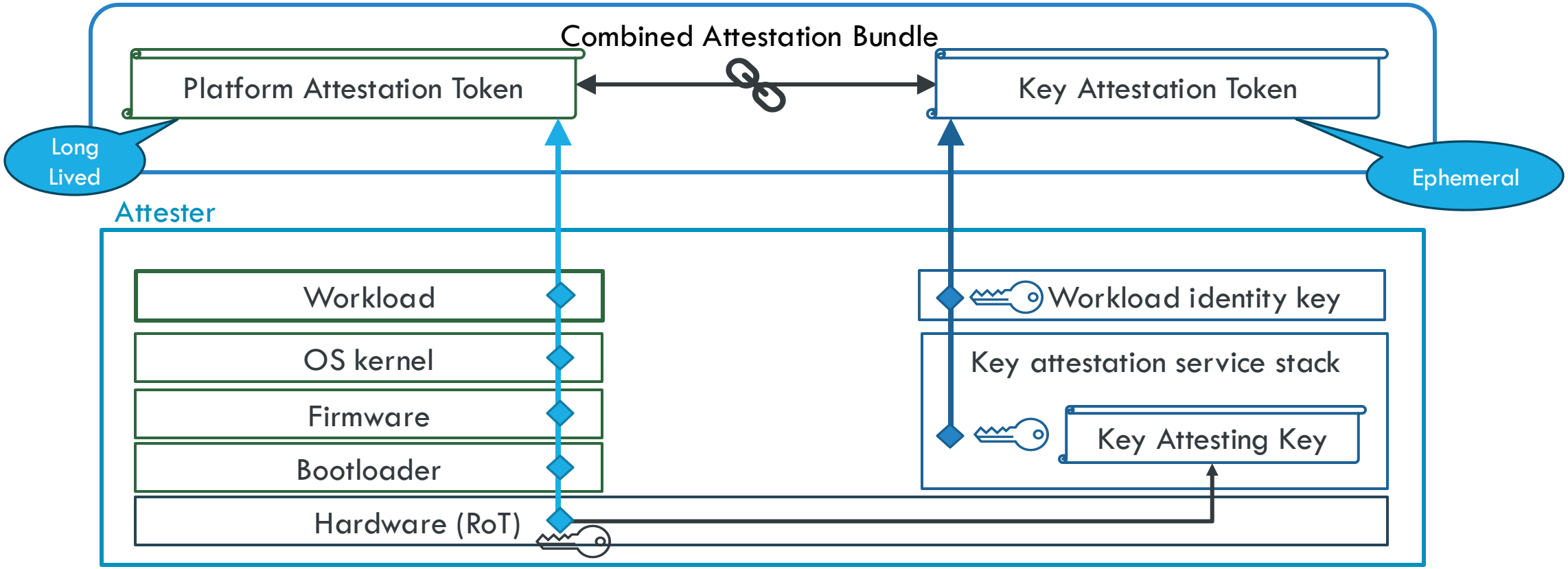
- Attestation metadata is carried instead of (or together with) an X.509 certificate
- Technically, as a new certificate type

Attestation metadata is opaque to the TLS implementation

New TLS extensions to negotiate the credential type, and convey freshness

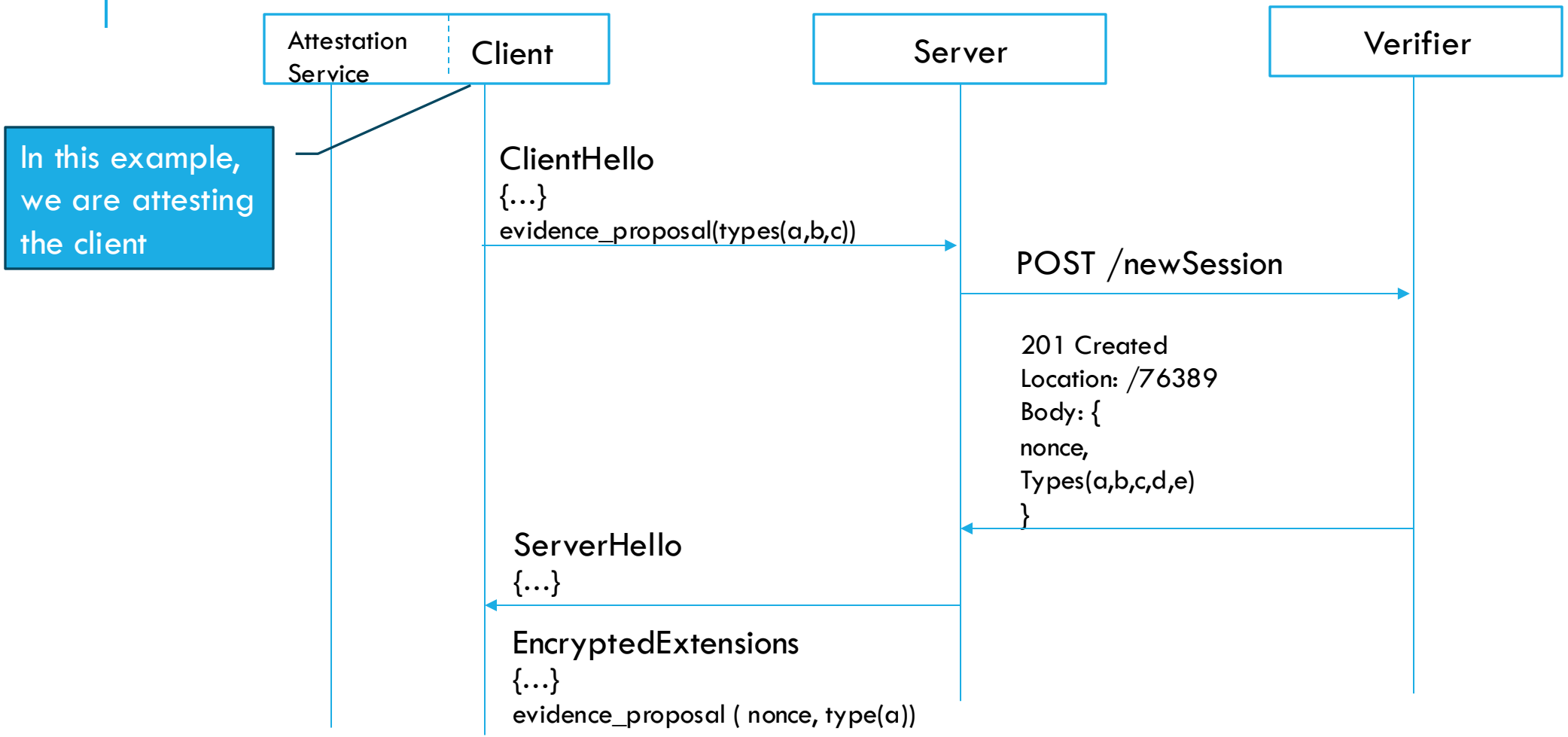
Attesting the Client, the Server or both

KEY & PLATFORM ATTESTATION

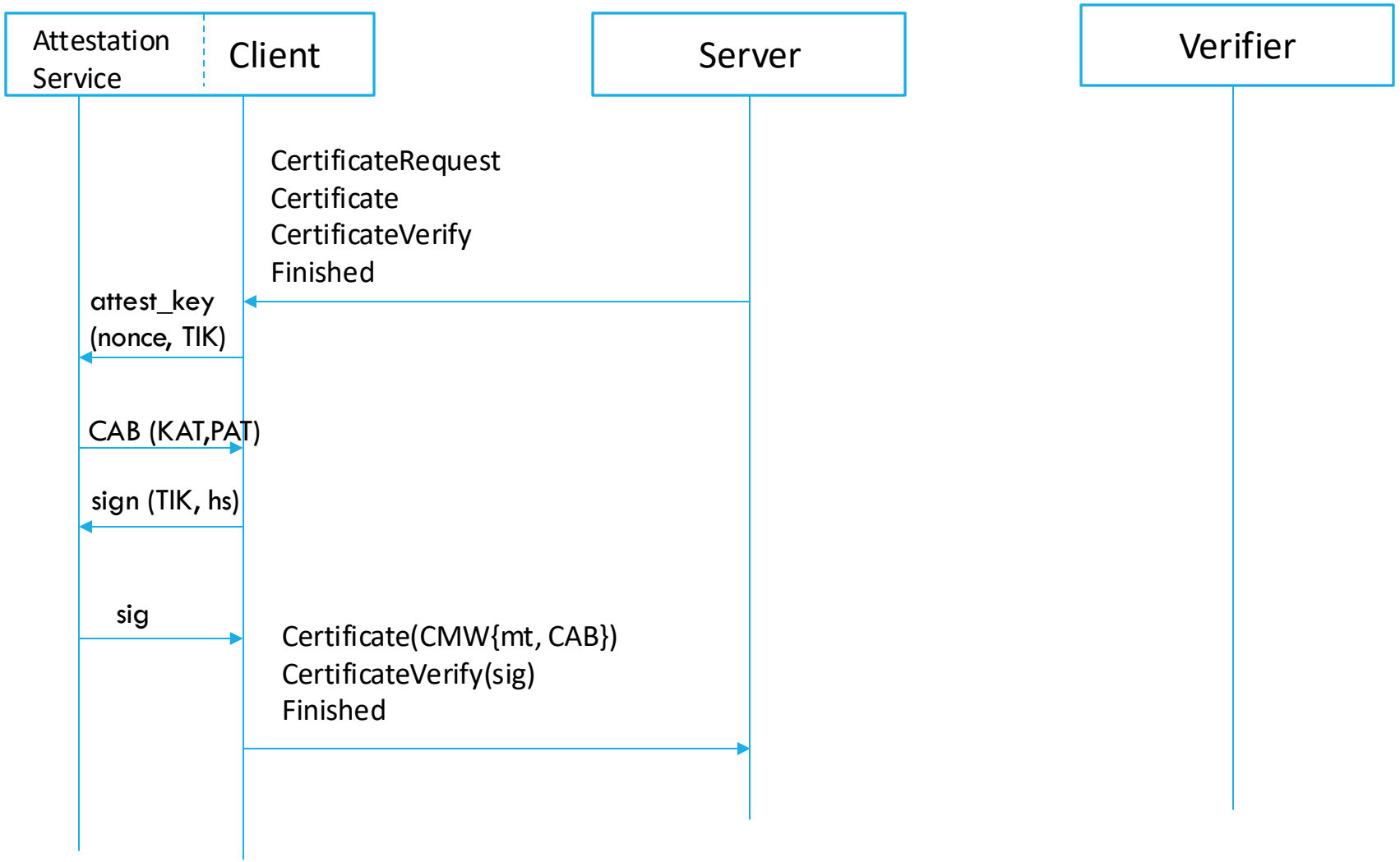


draft-bft-rats-kat-04

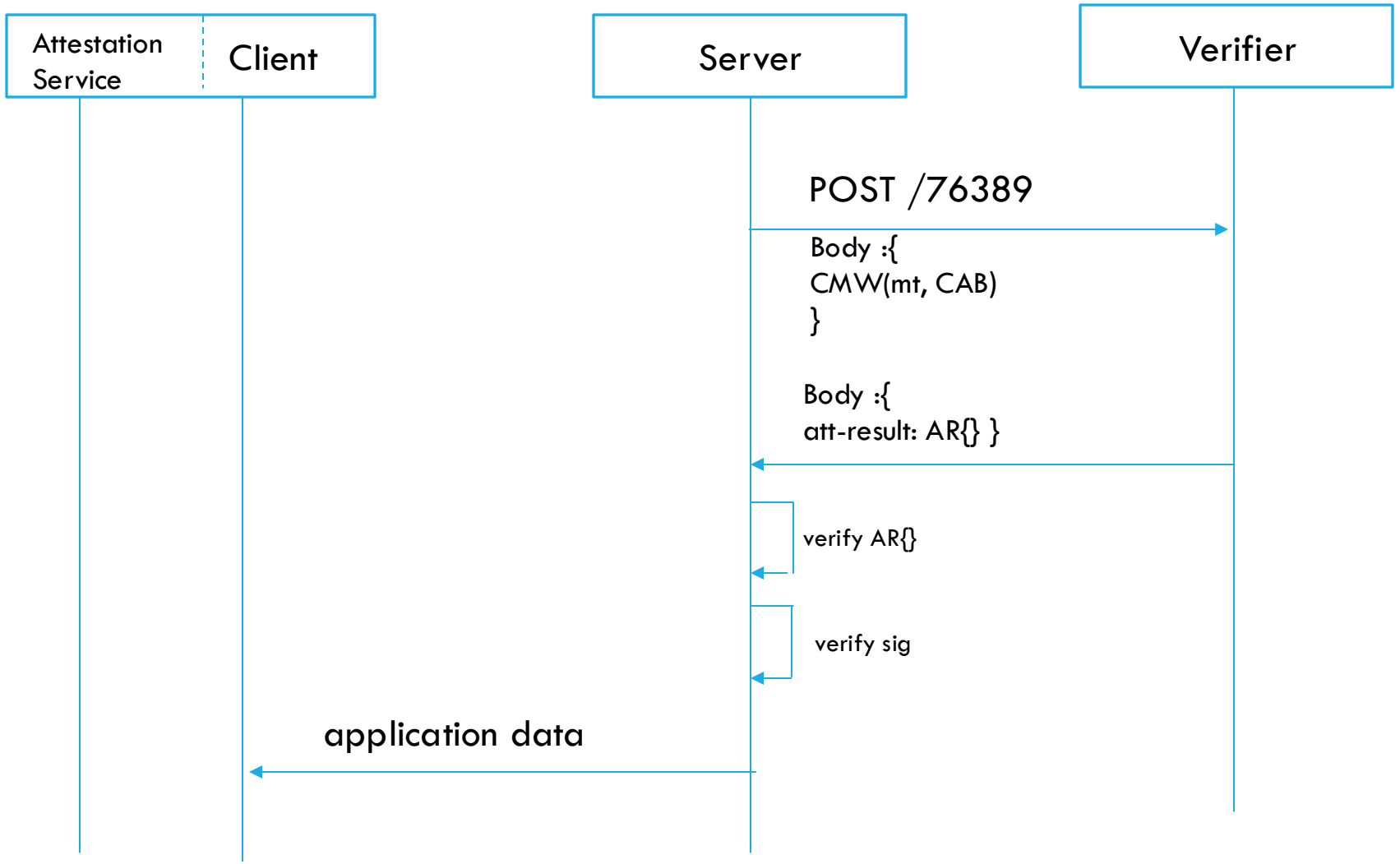
MESSAGE FLOW (1/3)



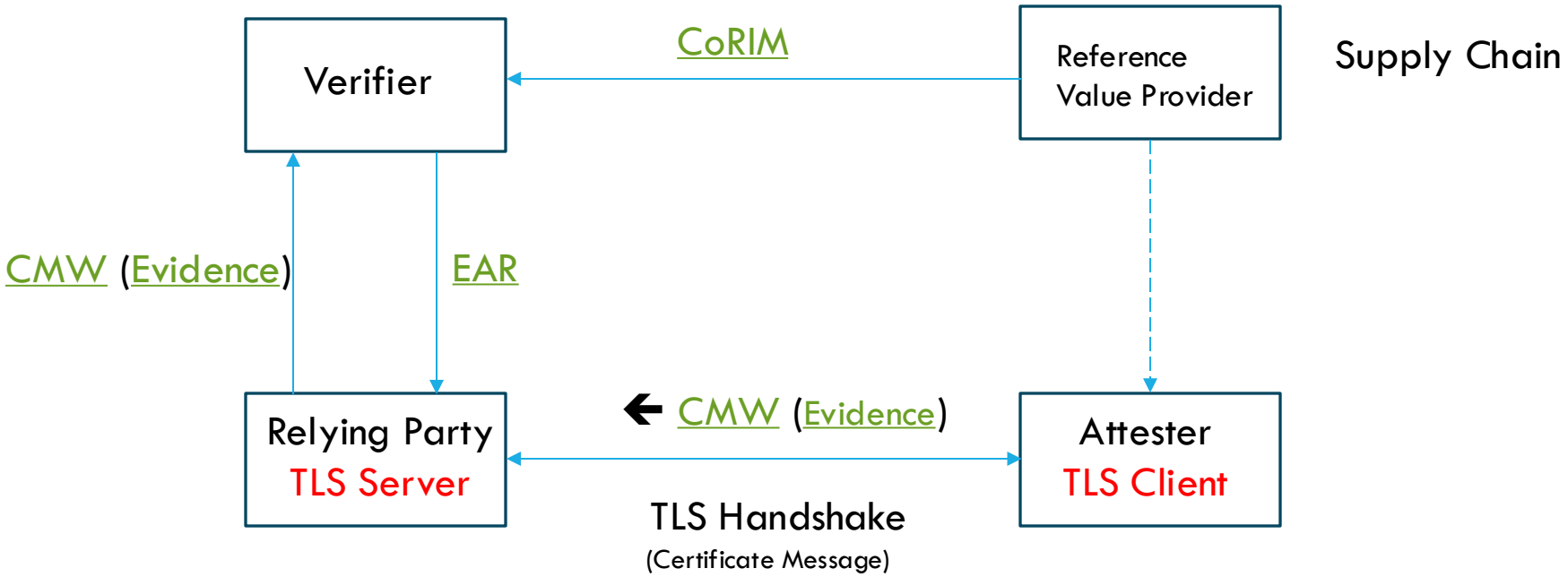
MESSAGE FLOW (2/3)



MESSAGE FLOW (3/3)

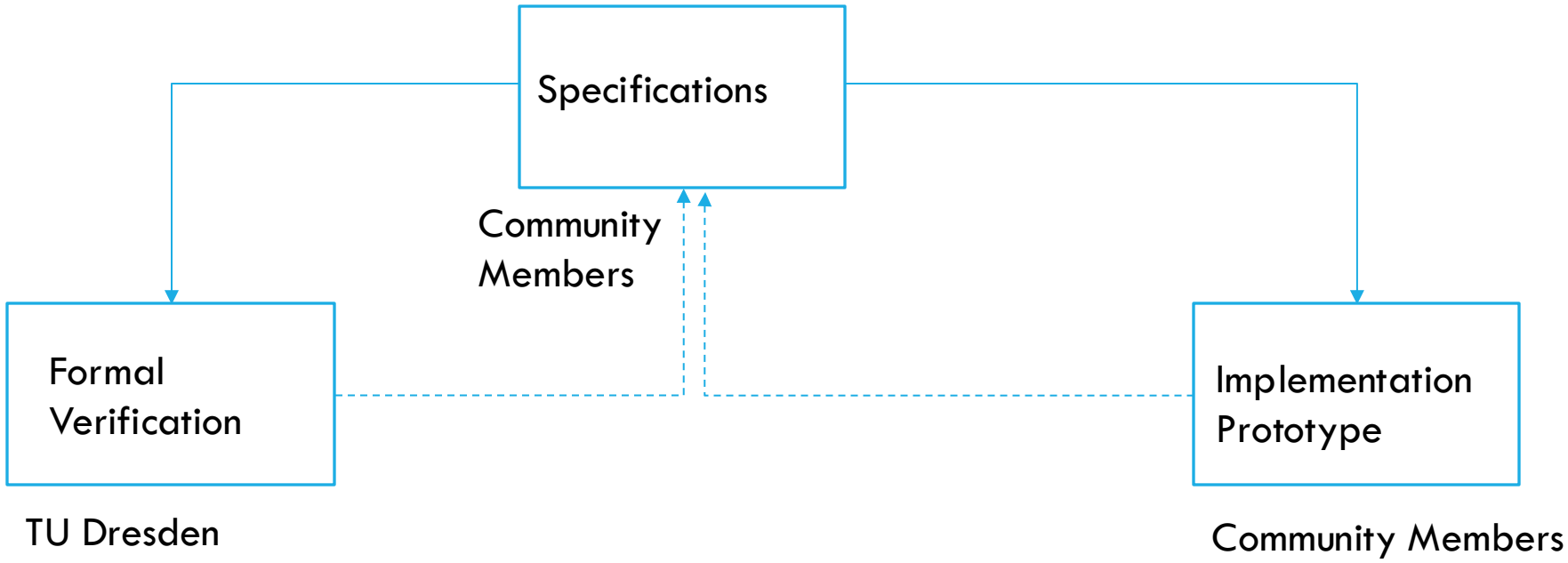


MAPPING TO THE RATS ARCHITECTURE



RATS Architecture: RFC 9334

CURRENT ACTIVITIES AND COLLABORATIONS



STATUS OF IMPLEMENTATION

An end-to-end working proof of concept is available

- From Attester through a TLS implementation, to a Verifier
- Uses Background Check model, with TPM 2.0 as a RoT

Open-Source availability of entire stack

- The components themselves are open-source software
- Project harbored under CCC-Attestation SIG

Work In Progress on a Confidential Computing (CC) version of Attester running in a confidential environment: ARM-CCA

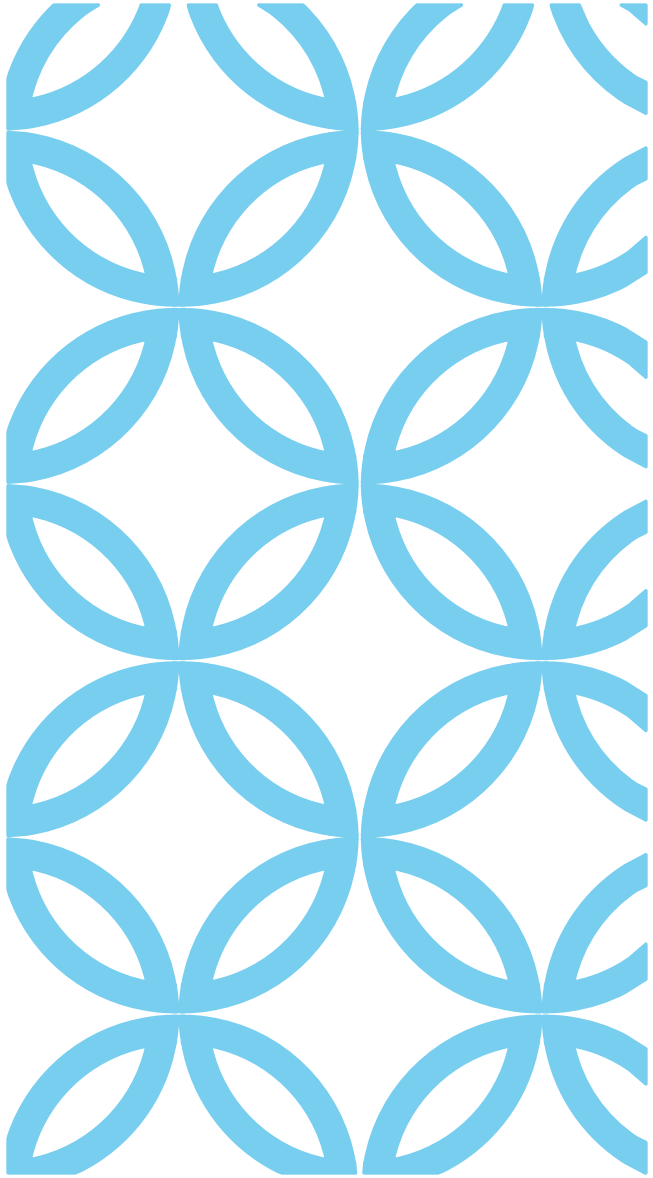
OPEN-SOURCE IMPLEMENTATIONS

Multiple (different) implementations of TLS with attestation:

- Open Enclave Attested TLS (Microsoft)
- Split-Trust Encryption Tool (Google)
- Gramine RA-TLS
- Attested TLS PoC (Attested TLS Internet Draft)

Commercial Projects

- Attestation within TLS handshake in Constellation (by Edgeless Systems)

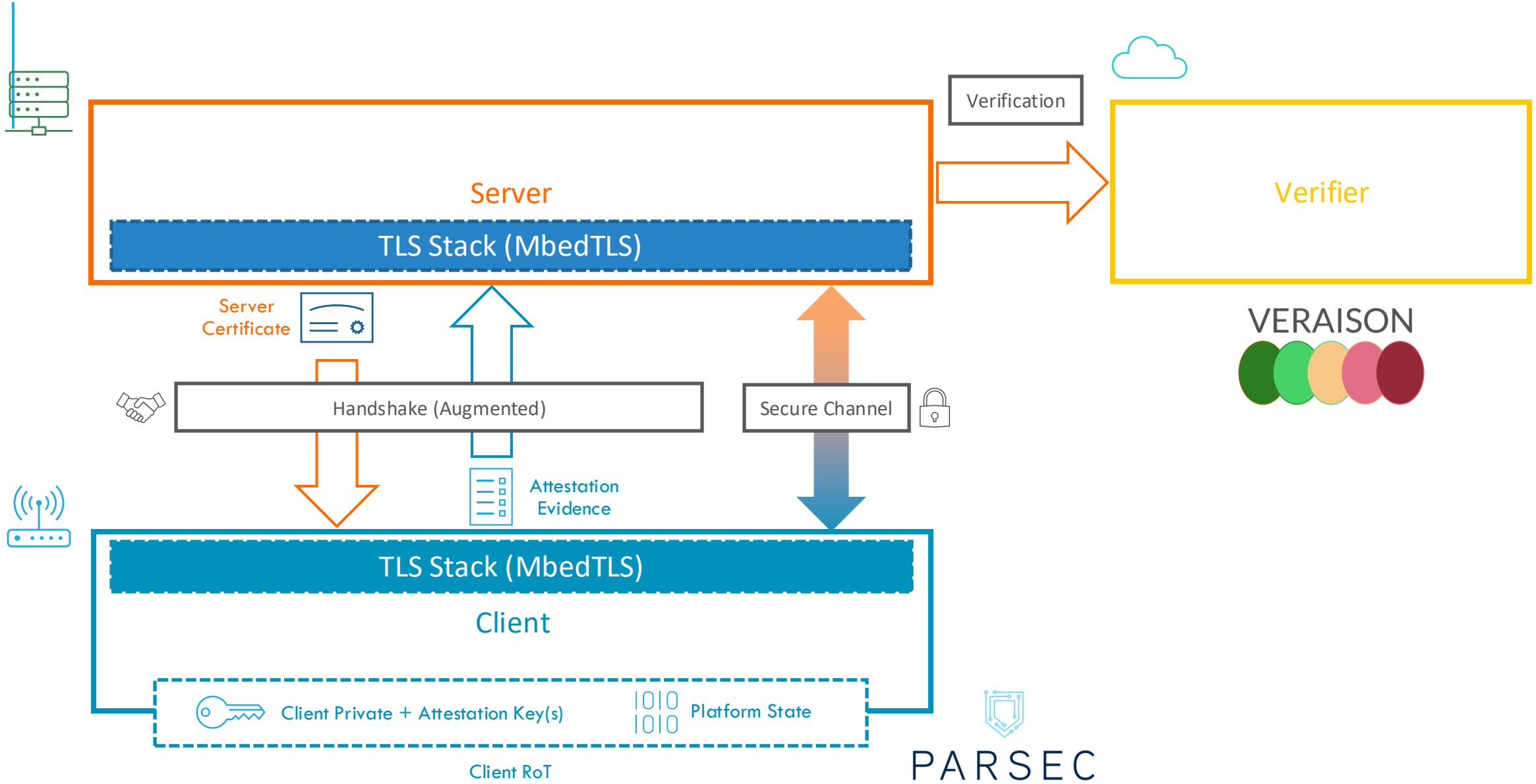


Yaron Sheffer, yaronf@intuit.com

THANK YOU!

BACKUP

PROTOTYPE ARCHITECTURE



USAGE OF RATS DRAFTS

Draft Name	Describes
Attestation in TLS and DTLS	Describes TLS extensions to use attestation for authentication
EAT based Key attestation Token	Evidence format of combined key and platform attestation
CoRIM	Concise Reference Integrity Manifest (CoRIM), a standardised way to convey Reference Values and Endorsed Values to a Verifier
EAT Attestation Results (EAR)	An EAT profile for conveyance of Attestation Results
CMW	A format used to Wrap RATS Messages in a protocol agnostic way
EAT Collection Types	An extension to EAT allowing the top-level token to consist of a collection of otherwise defined tokens

MAIN OPEN-SOURCE REPOSITORIES

Repository Name(link)	Contains
CCC Attested TLS PoC	Central space for open collaboration on the proof of concept
Parsec	Library to abstract Attester Evidence Formats
Mbed TLS library	TLS Library
Veraison	Attestation Verification deployment
ctoken	A C library to implement EAT, CWT and UCCS
t_cose	A C Library to implement COSE RFC 9052

INTRODUCTION

Historically Transport Layer Security (TLS) protocol has relied on Public Key Infrastructure (PKI) for authentication

Remote Attestation presents an enhancement to PKI, leveraging hardware features to provide comprehensive information about the security state of the device

Our work is focused on standardising remote attestation as a native authentication mechanism in TLS

Also backed by an Open-Source proof of concept project, supported by the Confidential Consortium Attestation Special Interest Group