Attested TLS

10000-foot view

Thomas Fossati & Muhammad Usama Sardar

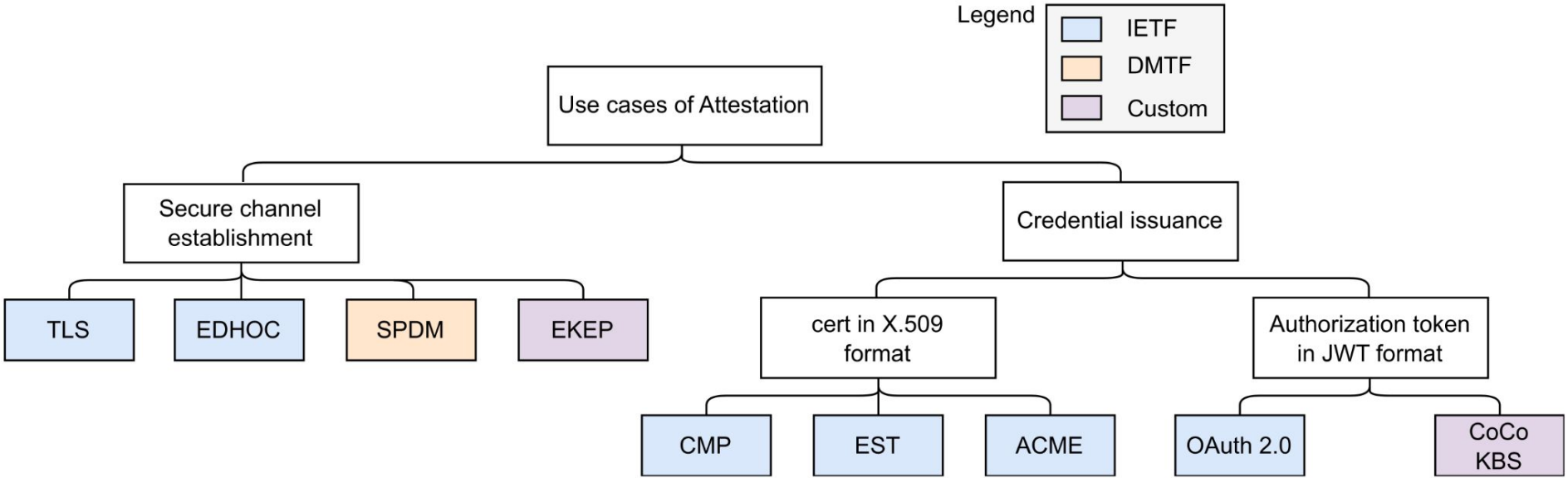
Attestation (WiP)

- The process of providing a digital signature for a set of measurements securely stored in hardware, and then having the requester validate the signature and the set of measurements.
  (Bartock et al., Trusted Geolocation in the Cloud: Proof of Concept Implementation, NISTIR 7904, 2015)

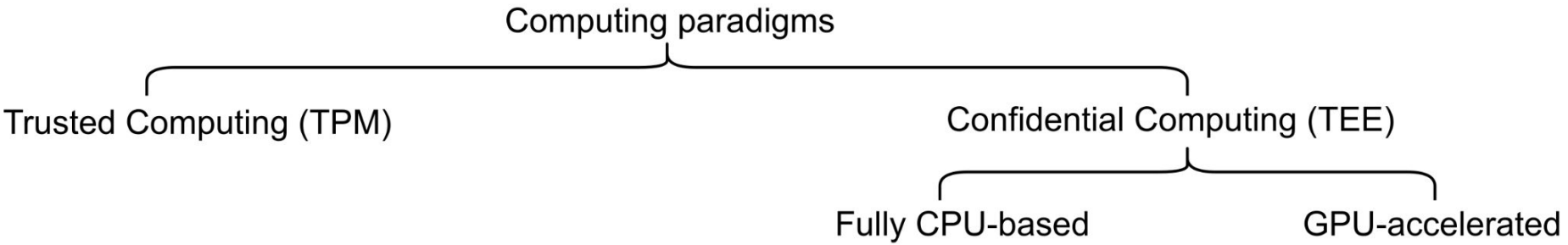
Note: wrongly attributed to NIST SP 1800-19B in NIST glossary

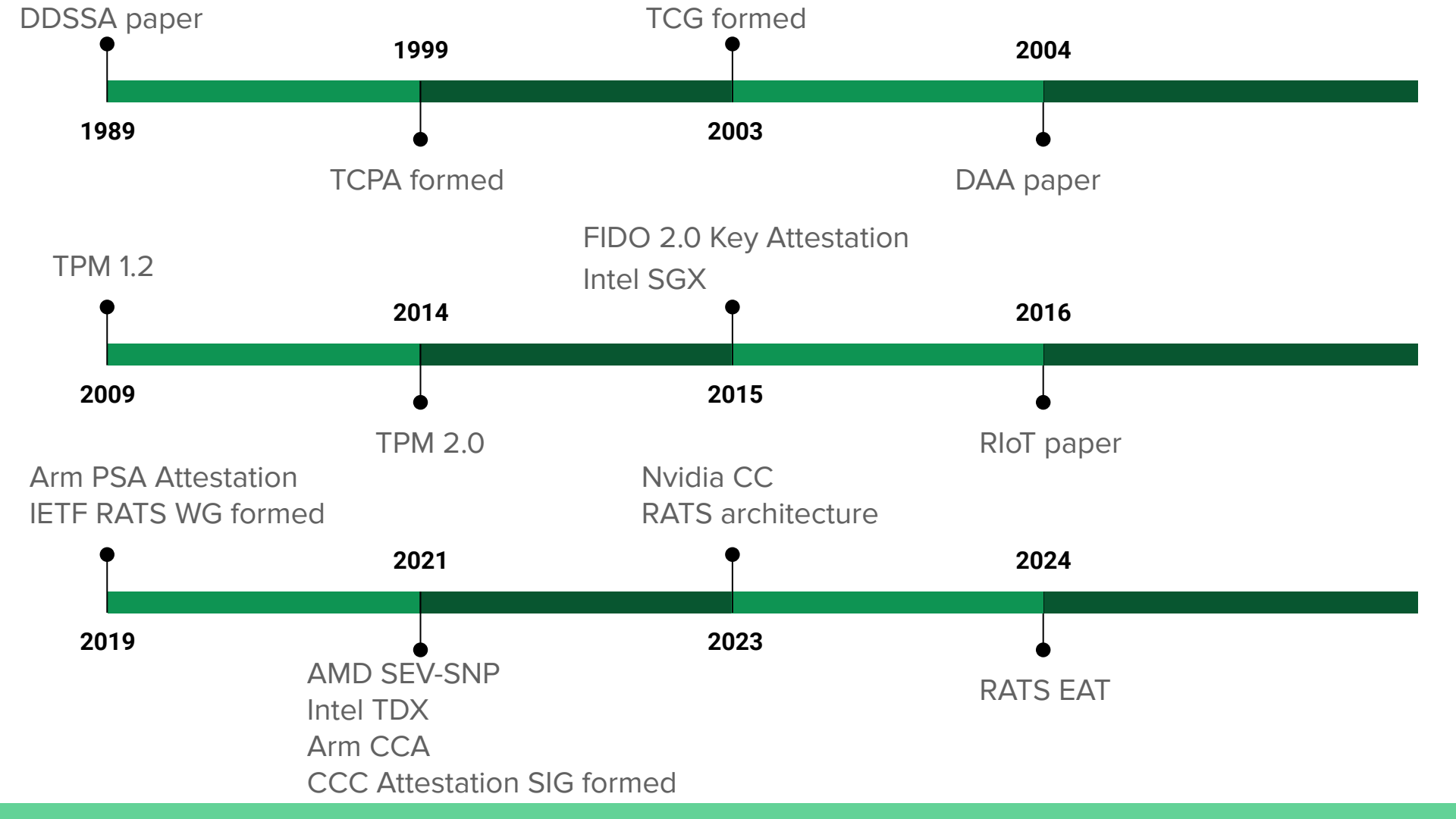
- Not necessarily *only*:
  - digital signature
  - set of measurements

Use Cases of Attestation

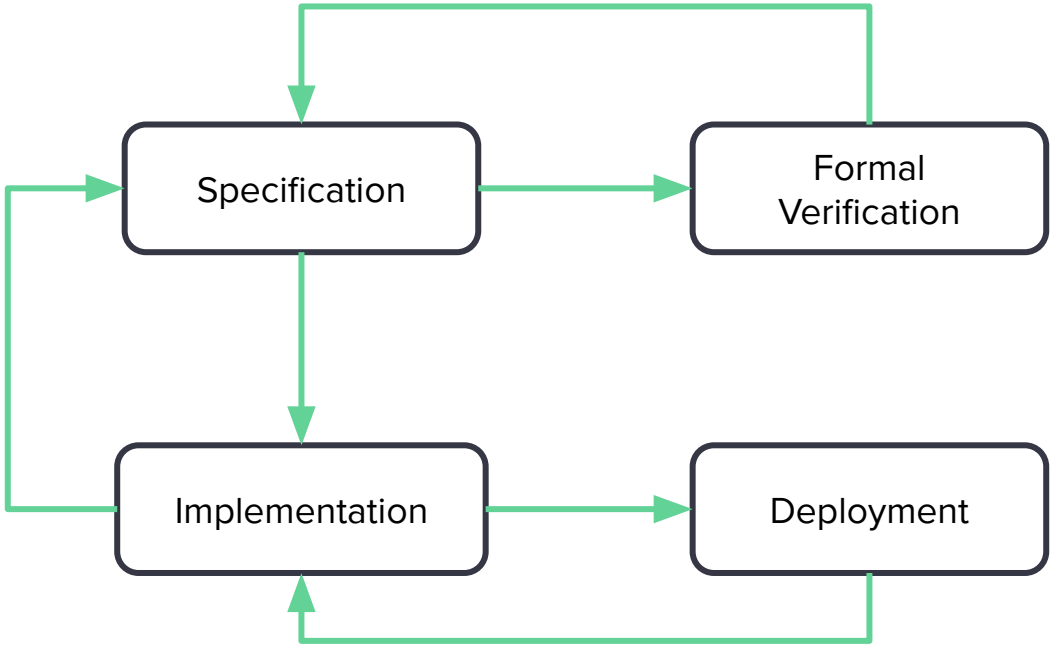


Computing Paradigms using Attestation



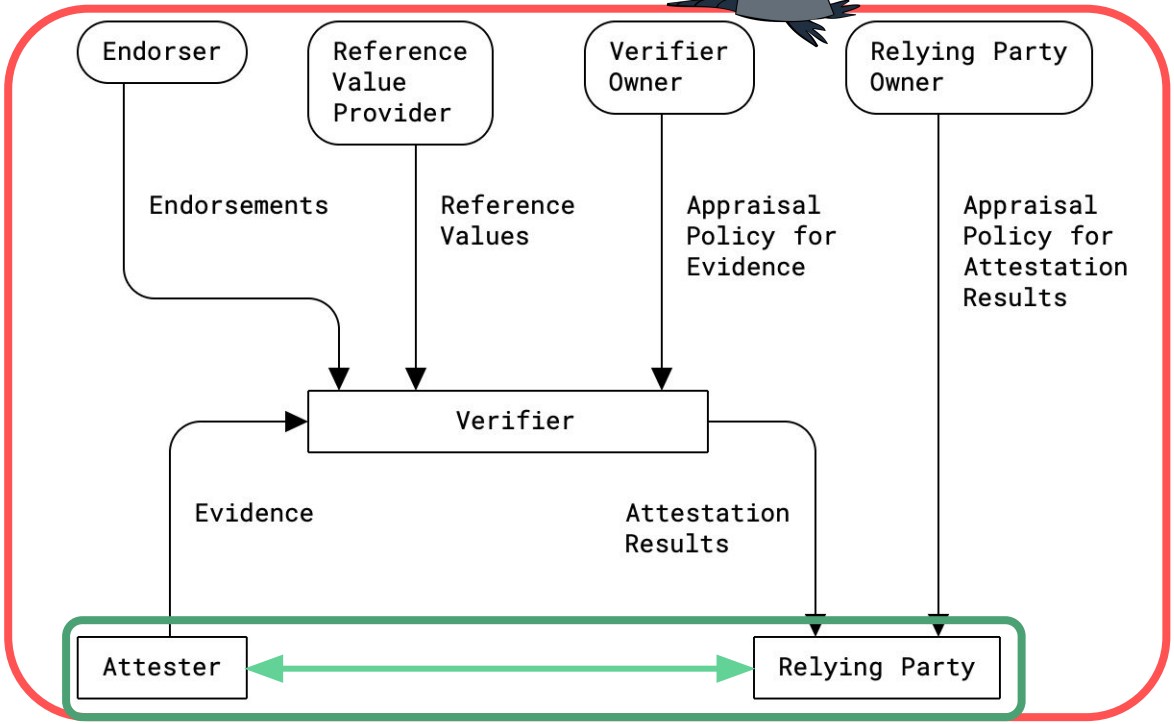

DDSSA paper
1989
1999
TCPA formed
TCG formed
2003
2004
DAA paper
TPM 1.2
2009
2014
TPM 2.0
FIDO 2.0 Key Attestation
Intel SGX
2015
2016
RIoT paper
Arm PSA Attestation
IETF RATS WG formed
2019
2021
AMD SEV-SNP
Intel TDX
Arm CCA
CCC Attestation SIG formed
Nvidia CC
RATS architecture
2023
2024
RATS EAT

Collaboration Model



Attestation in IETF

RATS WG



OAuth, TLS, EST, ACME, ...

What is Attested TLS ?

- The Transport Layer Security (TLS) handshake protocol allows authentication of one or both peers using static, long-term credentials

- In some cases, it is also required to ensure that the peer runtime environment is in secure state

- Attested TLS introduces a series of protocol extensions to the TLS 1.3 Handshake that enables binding of TLS authentication key to a remote attestation session

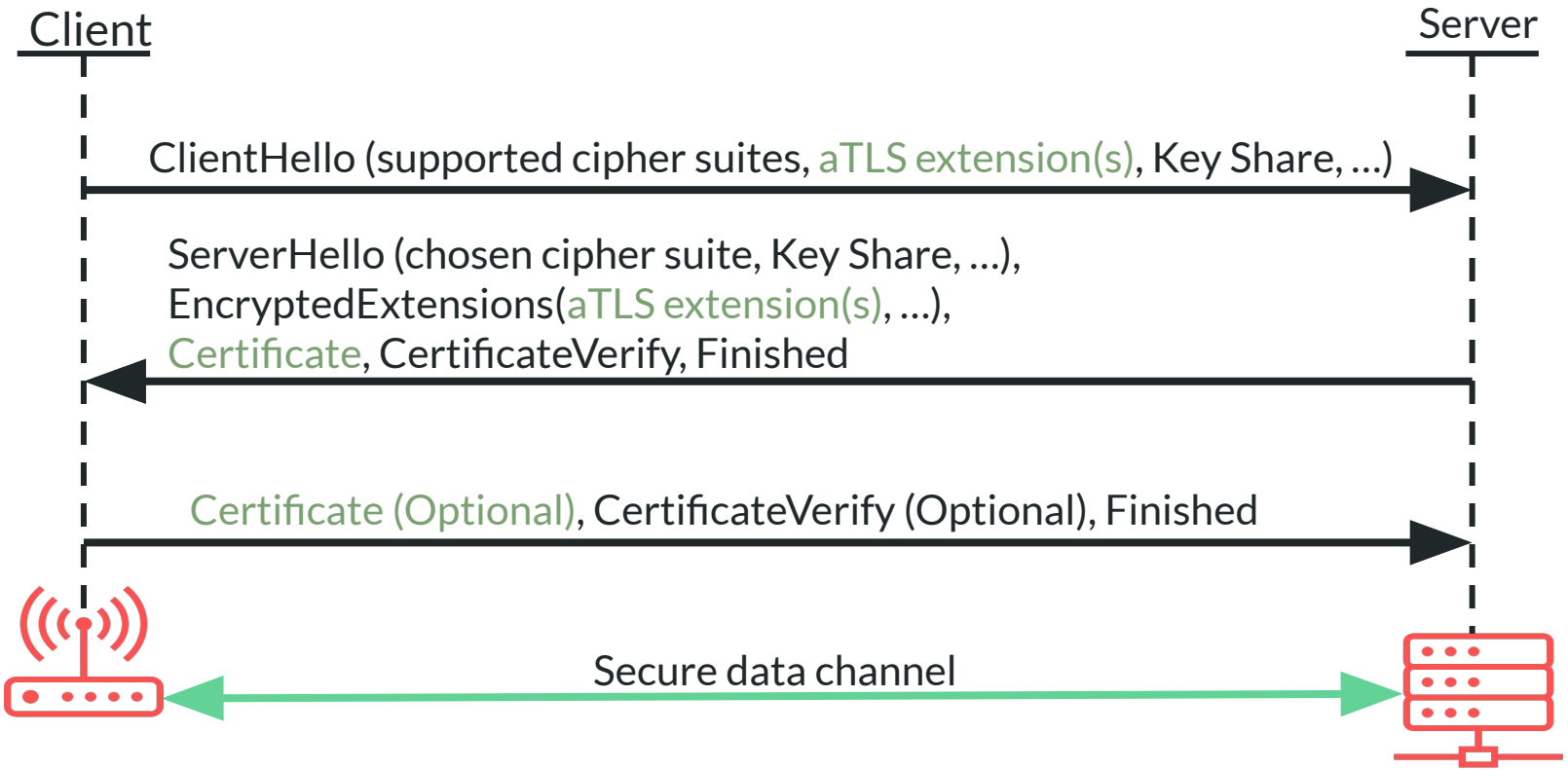
Need for Attested TLS ?

- PKI Certificates used in TLS handshake are good at conveying a (network) identity of a service
- Remote Attestation is good at conveying the security state of a service, i.e. whether the execution environment is trustworthy ?
- We can combine them efficiently to get the security benefits of both

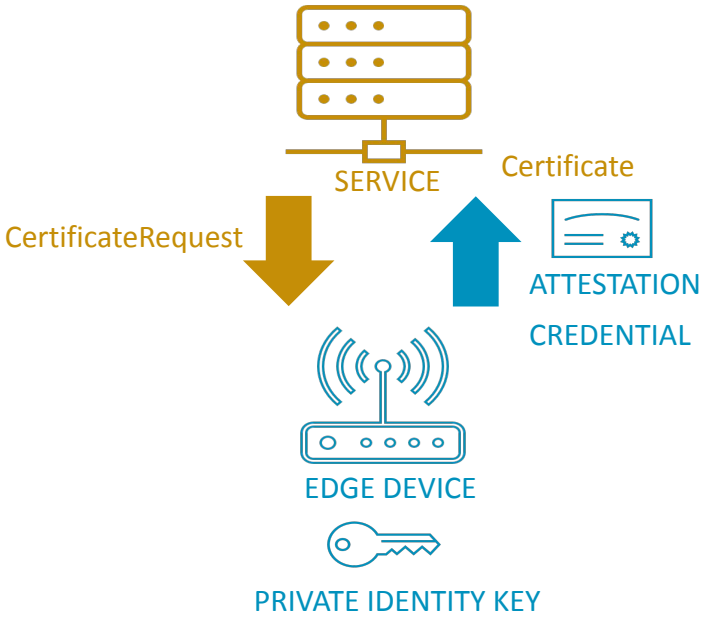
Proposed Design

- Proposed Design uses Remote Attestation information as a first-class credentials in a TLS Handshake
- Attestation information (Evidence or Results), from any scheme, carried as extensions alongside X.509 certificate or using a new certificate type
- This approach has following benefits
  - Better security
  - Better performance – No need to run channel establishment and remote attestation sequentially

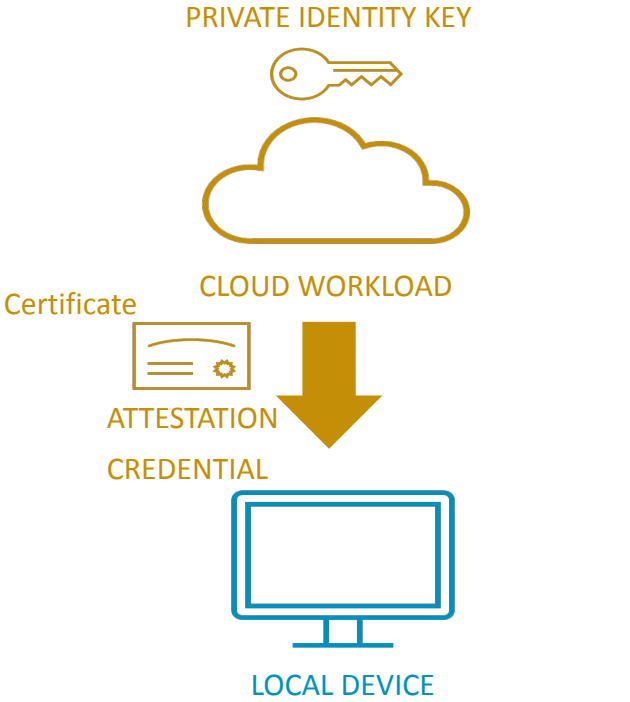
Augmented TLS v1.3 Handshake



Initial Use Cases

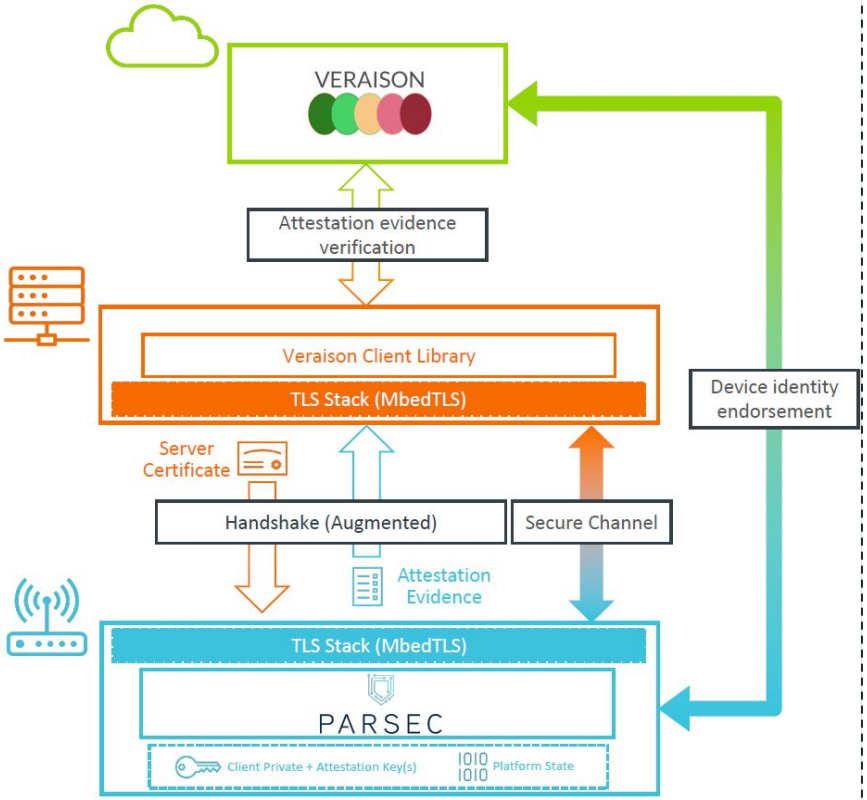


IoT/Edge Device Onboarding



Confidential Computing

PROTOTYPE



- Open-source End to End System Prototype operated under CCC – Attestation SIG
- Consists of Interconnected Docker Containers to simulate entire System
- Attester is TPM 2.0
- Fully symmetrical (both Client AND/OR Server can be the Attester)
- https://github.com/CCC-Attestation/attested-tls poc

Open standards and Open-Source Links

Description	Link
IETF TLS Extension Draft	https://datatracker.ietf.org/doc/draft-fossati-tls-attestation/
IETF EAT based Key Attestation Token	https://datatracker.ietf.org/doc/draft-bft-rats-kat/
Conceptual Message Wrapper(CMW) draft	https://datatracker.ietf.org/doc/draft-ftbs-rats-msg-wrap/
CCC Project Repository	https://github.com/CCC-Attestation/attested-tlspoc
Parsec	https://parsec.community/
Project Veraison	https://github.com/veraison
MbedTLS	https://www.trustedfirmware.org/projects/mbed-tls/

Current Community Contributors

- Linaro
- TU Dresden
- Arm
- Siemens
- Intuit
- Barkhausen Institute
- Huawei

Join us:

- **Via Slack – ietf.slack.com # attested-tls**
- **Participate via Biweekly Community meeting@ 4 PM CET (Monday and Thursday)**

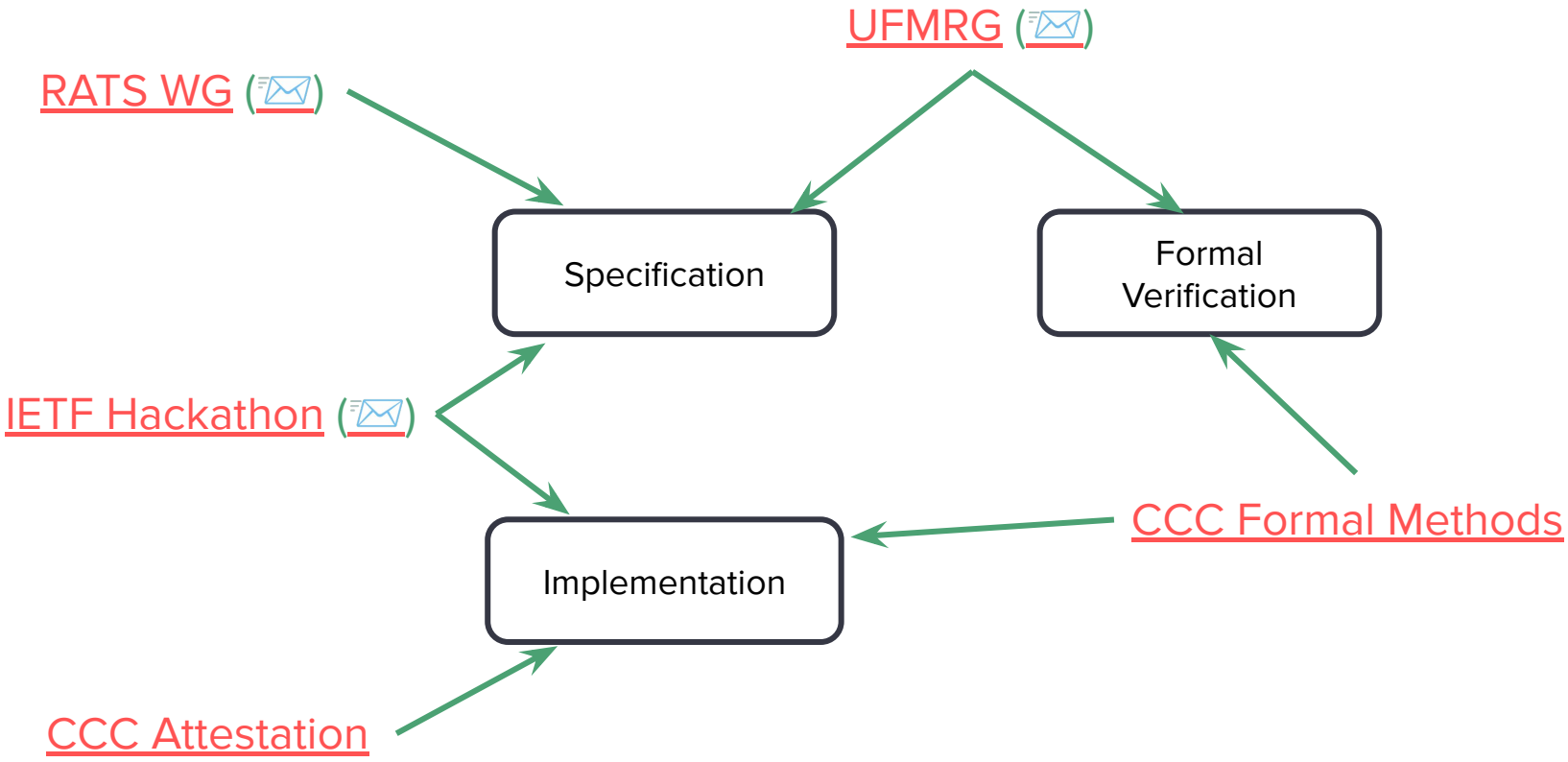
Zoom Meeting Details:

Meeting link

Meeting ID: 926 3098 5214

Passcode: 794083

Join us!


UFMRG (✉)
RATS WG (✉)
Specification
Formal Verification
IETF Hackathon (✉)
CCC Formal Methods
Implementation
CCC Attestation

Join us!

RATS WG

CCC Attestation