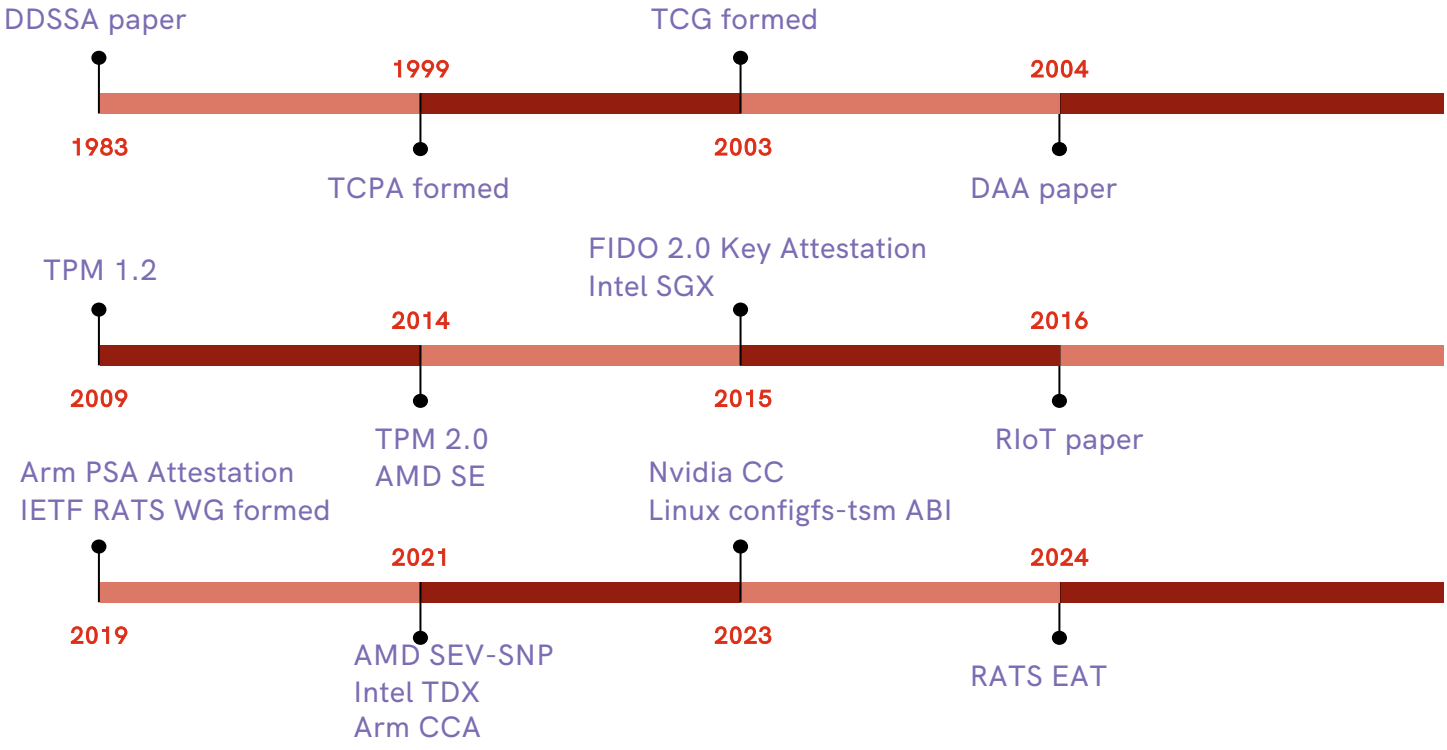
Increasing trust and preserving privacy

Advancing remote attestation

Intros

- Ionut Mihalcea (ionut.mihalcea@arm.com)
- Thomas Fossati (thomas.fossati@linaro.org)
- Hannes Tschofenig (hannes.tschofenig@gmx.net)


DDSSA paper
1983
1999
TCPA formed
TCG formed
2003
2004
DAA paper
TPM 1.2
2009
2014
TPM 2.0
AMD SE
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
Nvidia CC
Linux configfs-tsm ABI
2023
2024
RATS EAT

At an inflection point?

- Increasingly available
- Increasingly used

“Every authentication use case is also an attestation use case” (Dave Thaler)

Centralisation & Privacy Considerations

- Verification of attestation evidence
  - & centralisation (see also RFC 9518)
  - & privacy (see also Section 11 of RFC 9334 and Section 8 or EAT)

Tackling centralisation

- User-centrism?
- A neutral Verifier?
- What else is in the toolbox?

- WEI, a cautionary tale

Tackling privacy

- Long history with Direct Anonymous Attestation (DAA)
  - Adopted by TPM v1.2 specification
  - Implemented but not widely used.
  - FIDO offered different privacy solutions
    - Variant of DAA defined but deployments lacking
    - Lightweight alternative: "group" keys shared across a set of FIDO authenticators with identical characteristics
- PrivacyPass is a recent effort
  - Uses recently standardized privacy technologies, including BBS signatures, RSA Blind Signatures and Verifiable Random Functions.
  - Deployed by Apple and Cloudflare as a CAPTCHA replacement
- Renewed excitement for privacy with “Verifiable Credentials” in OAuth/OpenID Connect
  - Selective Disclosure (SD) JSON Web Token (JWT) in OAuth working group
  - Secure Patterns for Internet CrEdentials (SPICE) BOF to create a new working group in the IETF.

Rigorous designs

- Pressure to integrate Attestation into existing auth[nz] flows
  - Moving away from organic designs…
  - … to more structured approaches

IETF

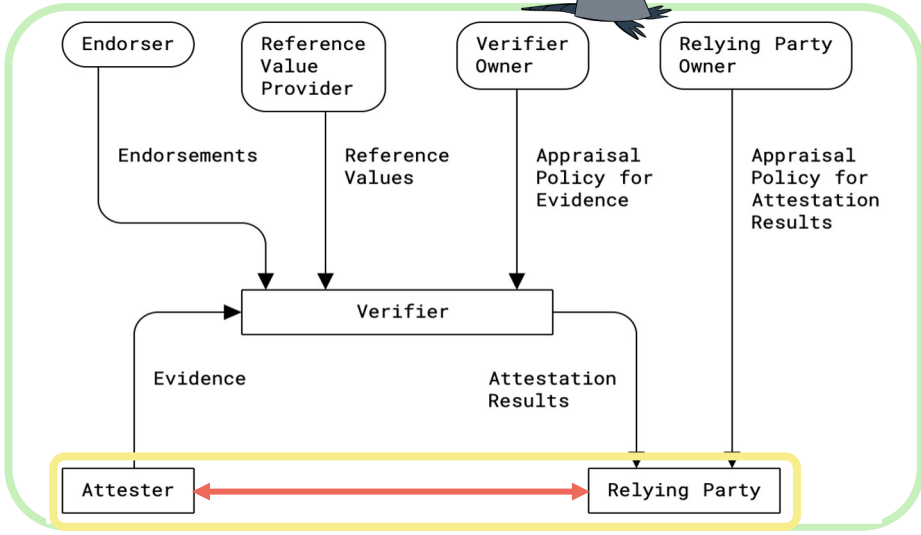
Cultivating Open Standards for an Open-Source World

IETF principles

- **Open process** - ***Any interested person can participate*** *in the work, know what is being decided, and make his or her voice heard on the issue.*
- **Technical competence** - *The issues on which the IETF produces its documents are* ***issues where the IETF has the competence needed to speak to them****, and that the IETF is willing to listen to technically competent input from any source.*
- **Rough consensus and running code** - *We make* ***standards based on the combined engineering judgement*** *of our participants* ***and our real-world experience*** *in implementing and deploying our specifications.*

Attestation in IETF

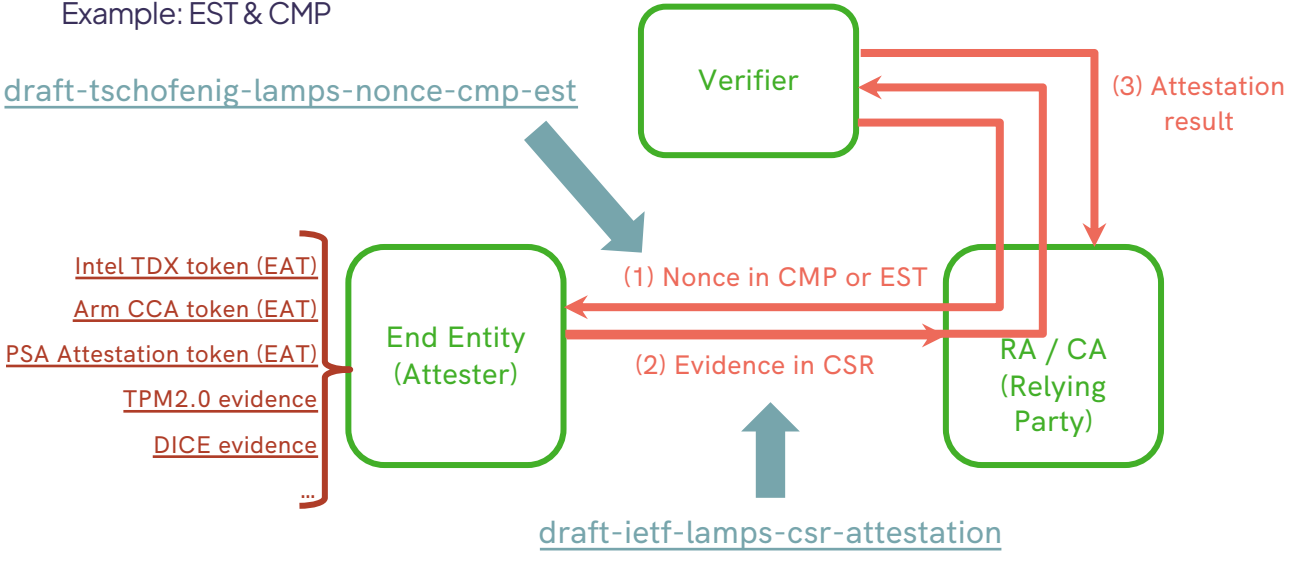
RATS WG



OAuth, TLS, EST, ACME, ...

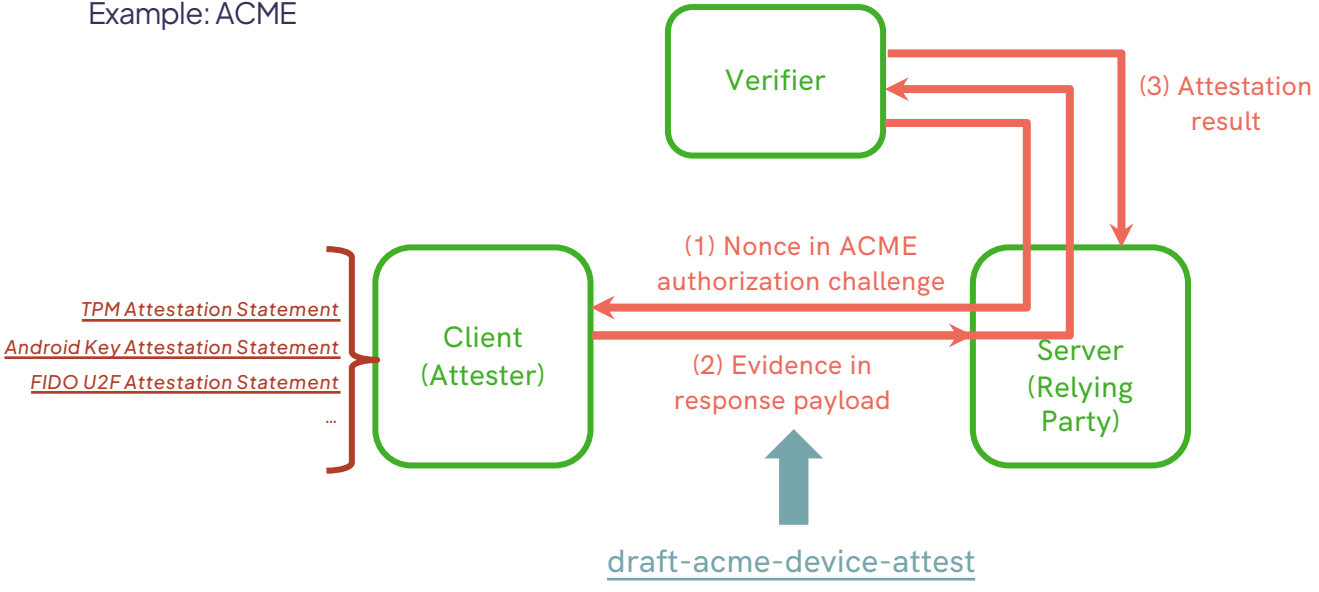
Remote attestation for credential issuance

Example: EST & CMP



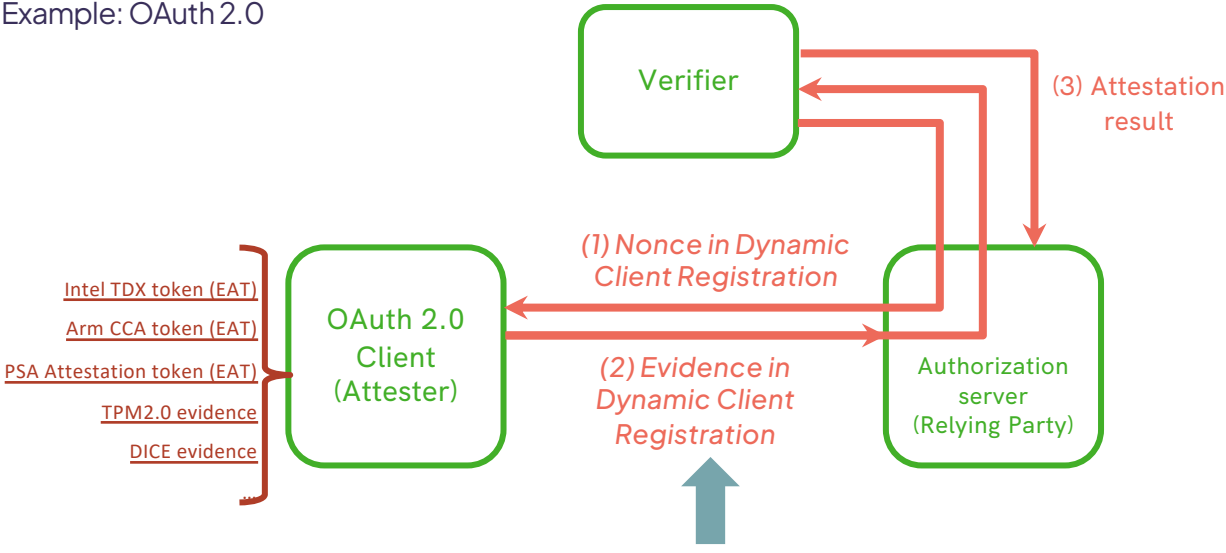
Remote attestation for credential issuance

Example: ACME



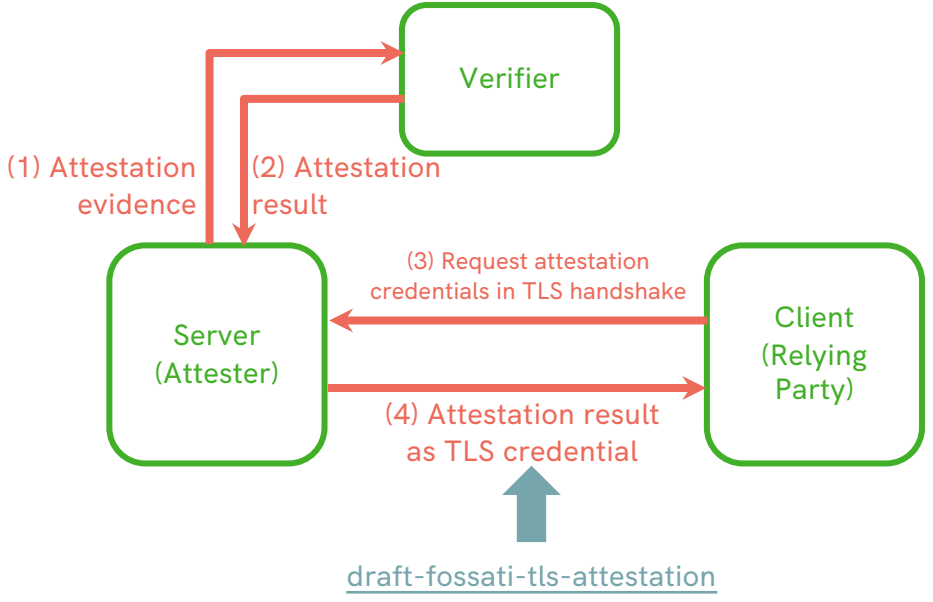
Remote attestation for credential issuance

Example: OAuth 2.0

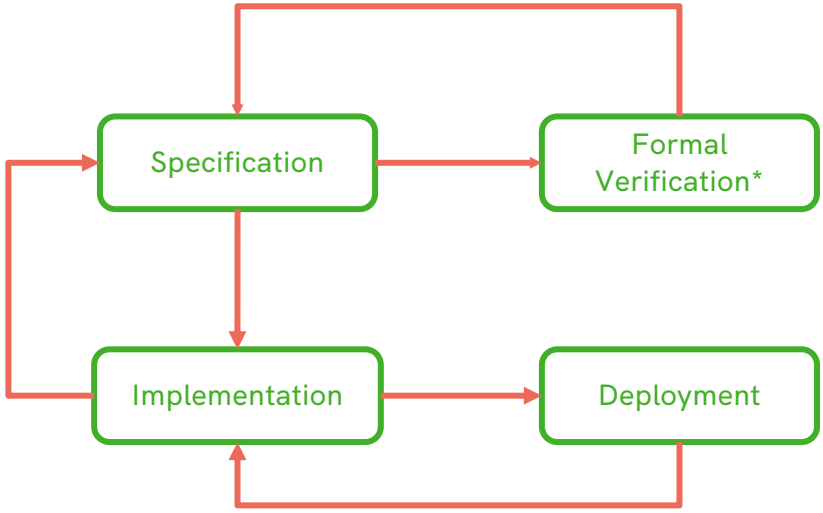


Remote attestation for secure channel establishment

Example: TLS

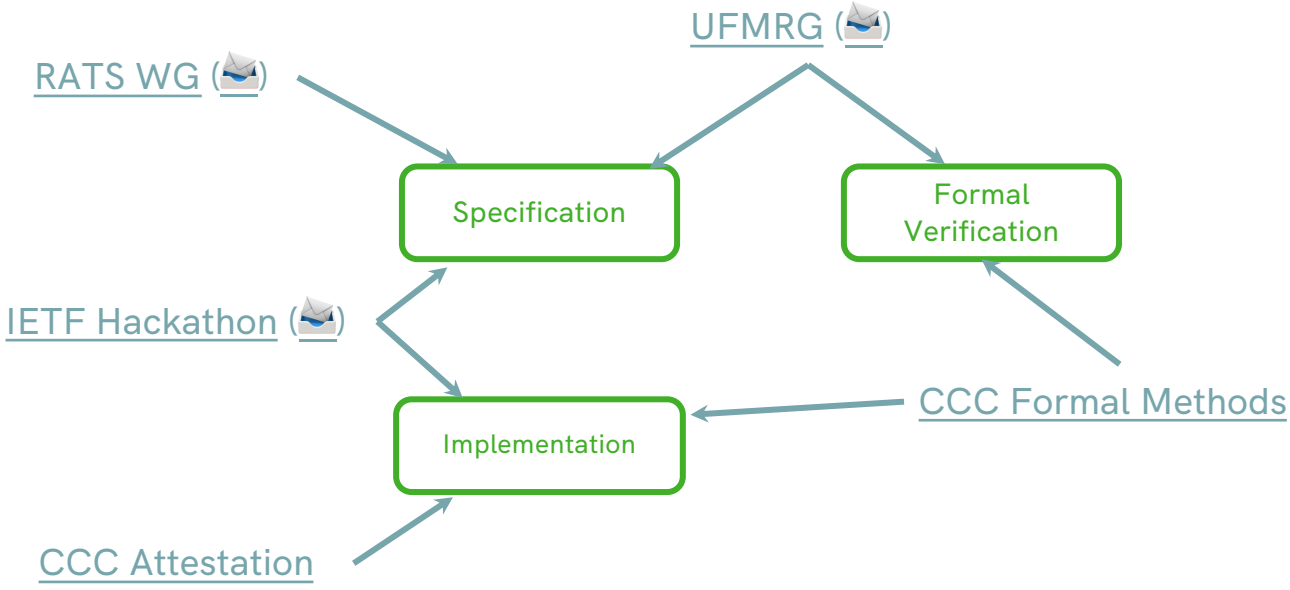


Formal verification



* *Usable Formal Methods Proposed Research Group*

Join us!


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

Join us!

RATS WG

CCC Attestation