

Increasing trust and preserving privacy

Advancing remote attestation

Ionut Mihalcea & Thomas Fossati
+ Hannes Tschofenig



Intros

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

DDSSA paper

TCG formed

1999

2004

1983

2003

TCPA formed

DAA paper

TPM 1.2

FIDO 2.0 Key Attestation
Intel SGX

2014

2016

2009

2015

TPM 2.0
AMD SE

RIoT paper

Arm PSA Attestation
IETF RATS WG formed

Nvidia CC
Linux configs-tsm ABI

2021

2024

2019

2023

AMD SEV-SNP
Intel TDX
Arm CCA

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

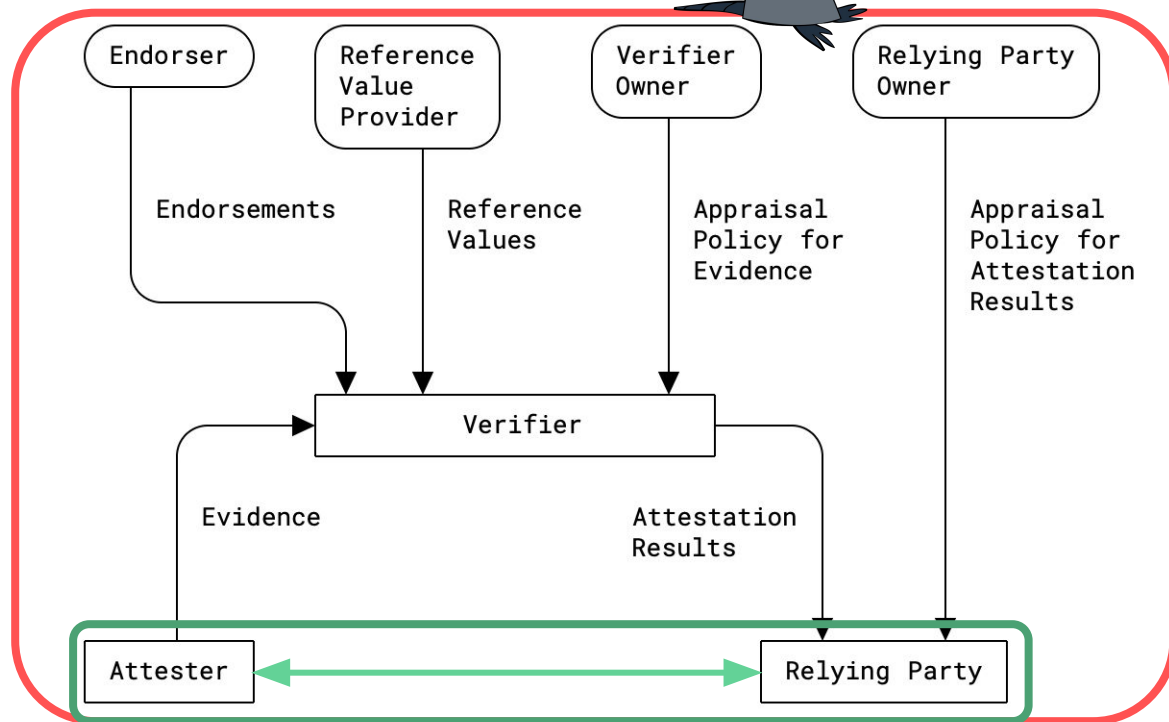
IETF principles

- **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

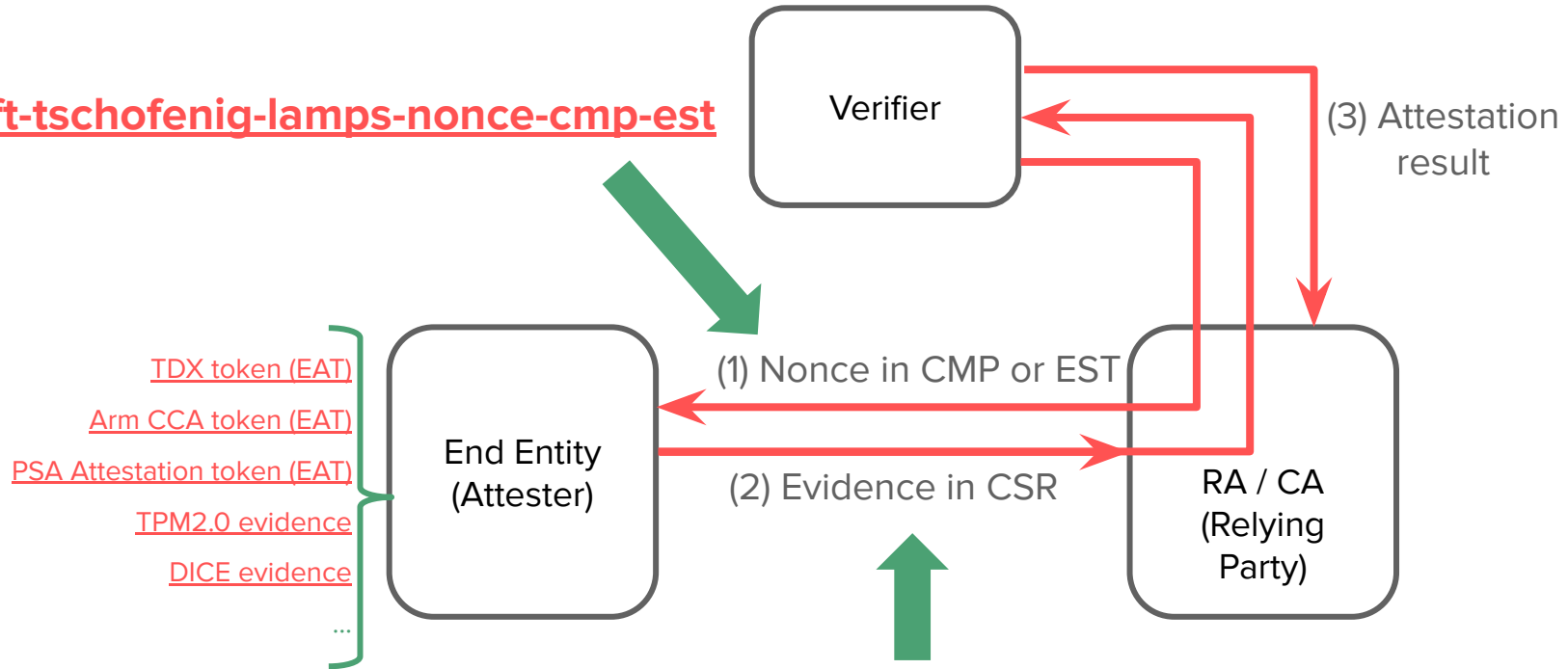


OAuth, TLS, EST, ACME, ...

Remote attestation for credential issuance

Example: EST & CMP

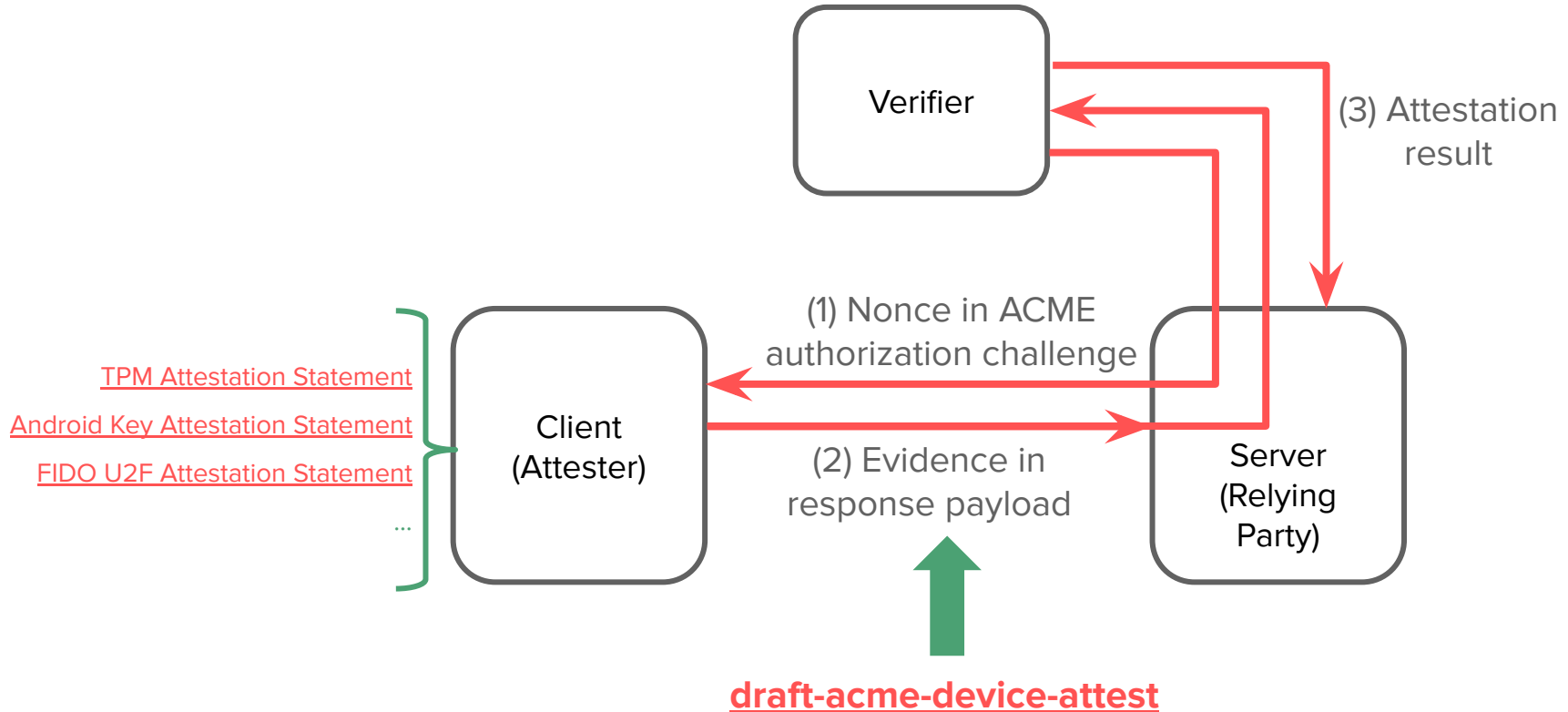
[draft-tschofenig-lamps-nonce-cmp-est](#)



[draft-ietf-lamps-csr-attestation](#)

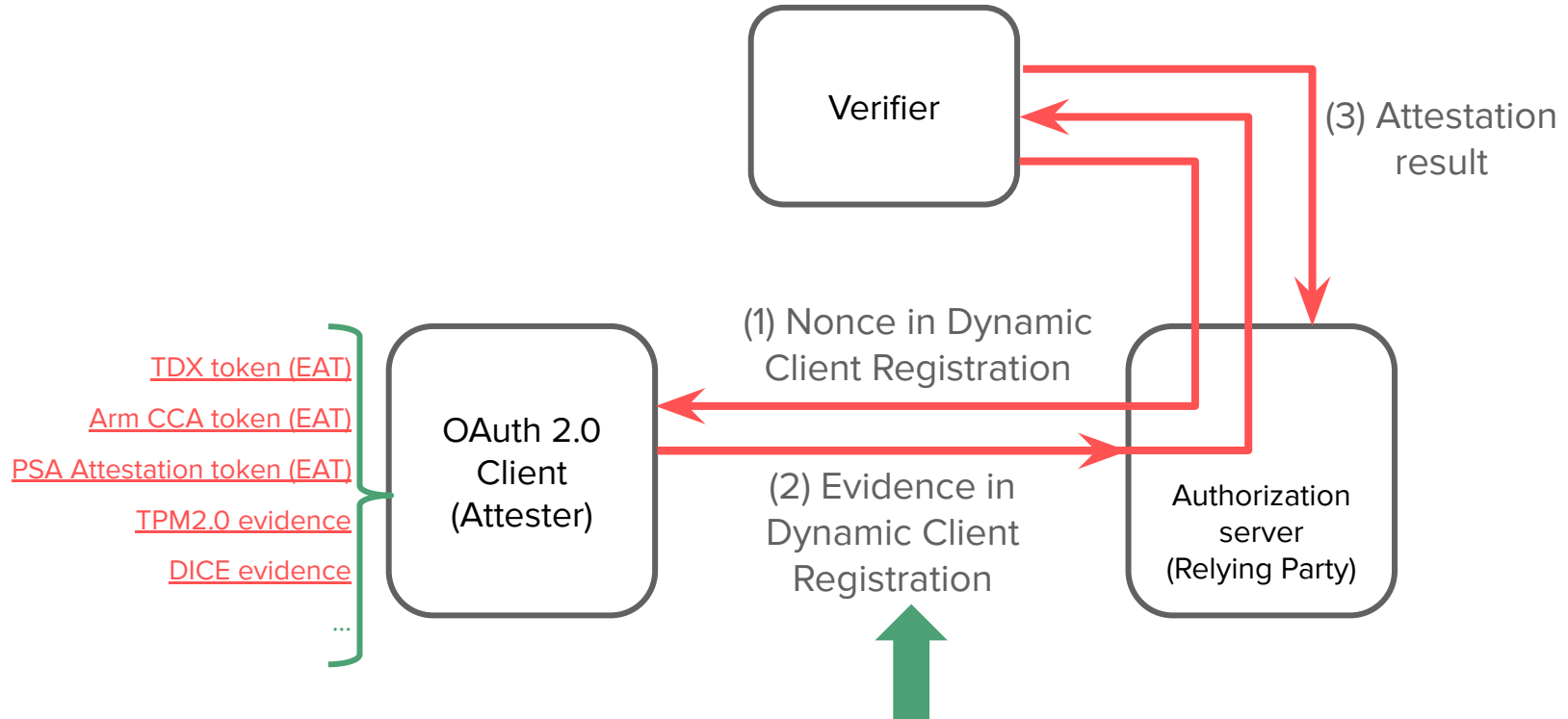
Remote attestation for credential issuance

Example: ACME



Remote attestation for credential issuance

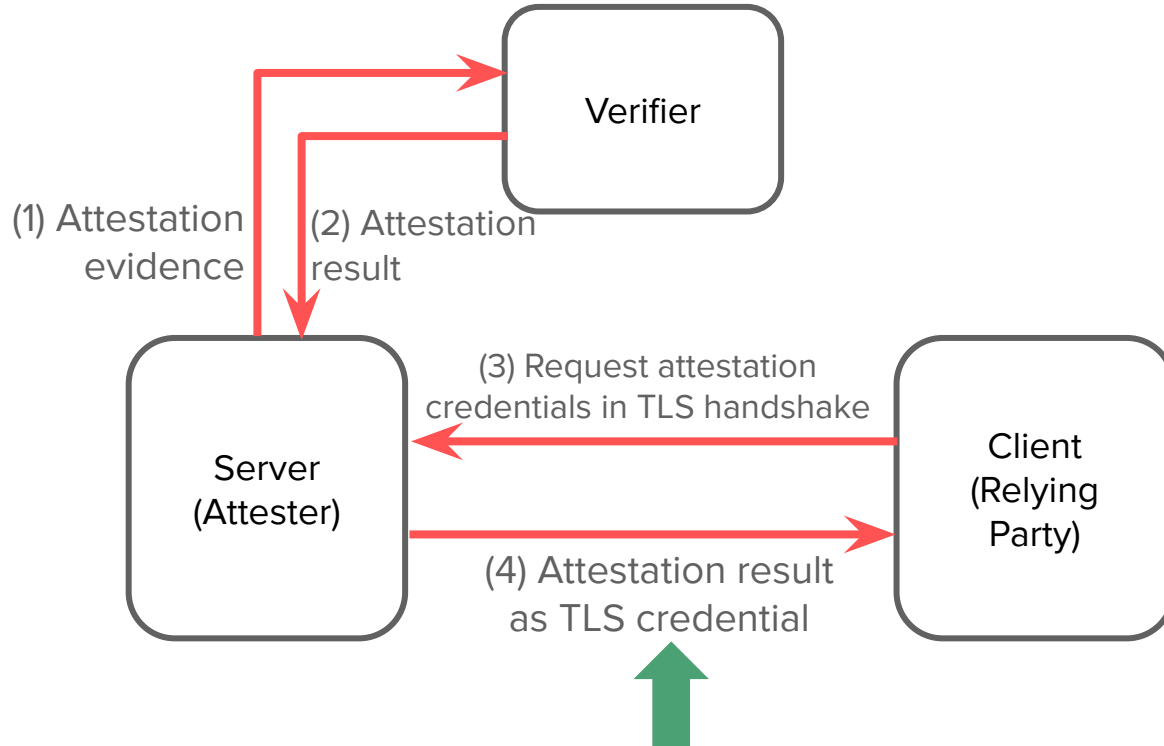
Example: OAuth 2.0



[draft-tschofenig-oauth-attested-dclient-reg](#)

Remote attestation for secure channel establishment

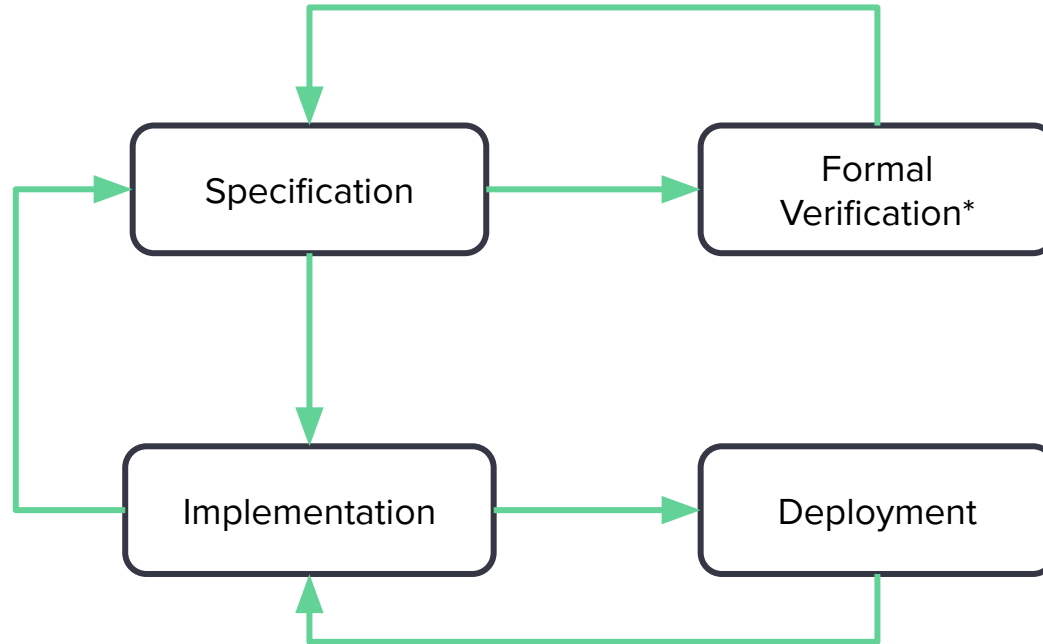
Example: TLS



[draft-fossati-tls-attestation](#)

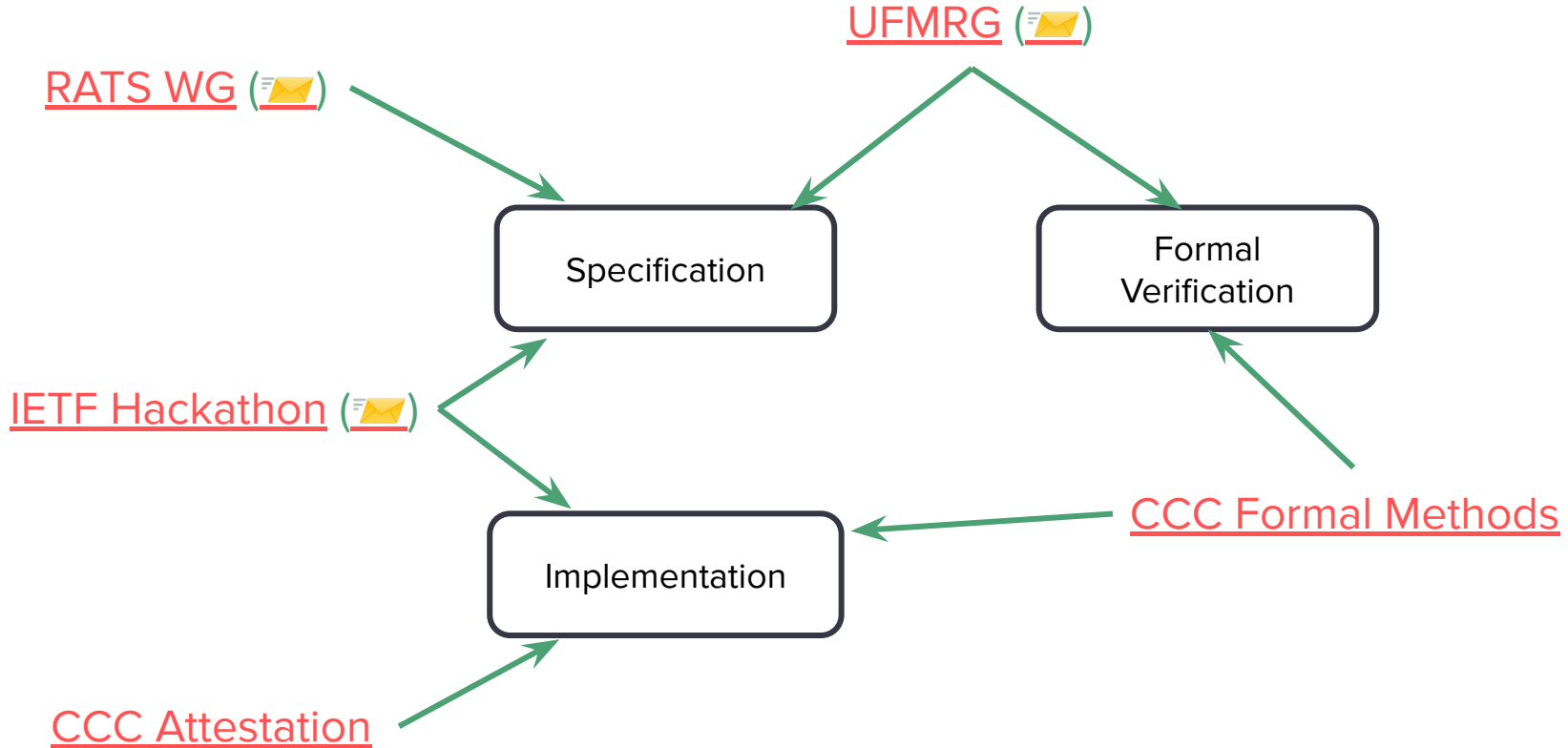


Formal verification



* [Usable Formal Methods Proposed Research Group](#)

Join us!



Join us!

RATS WG



CCC Attestation

