



Is Remote Attestation Relevant for Embedded Devices?"

Hannes Tschofenig

- **RIOT Summit: A Long Journey**



Communication
Security

In any distributed systems there is (naturally) interest in securing the communication between endpoints.

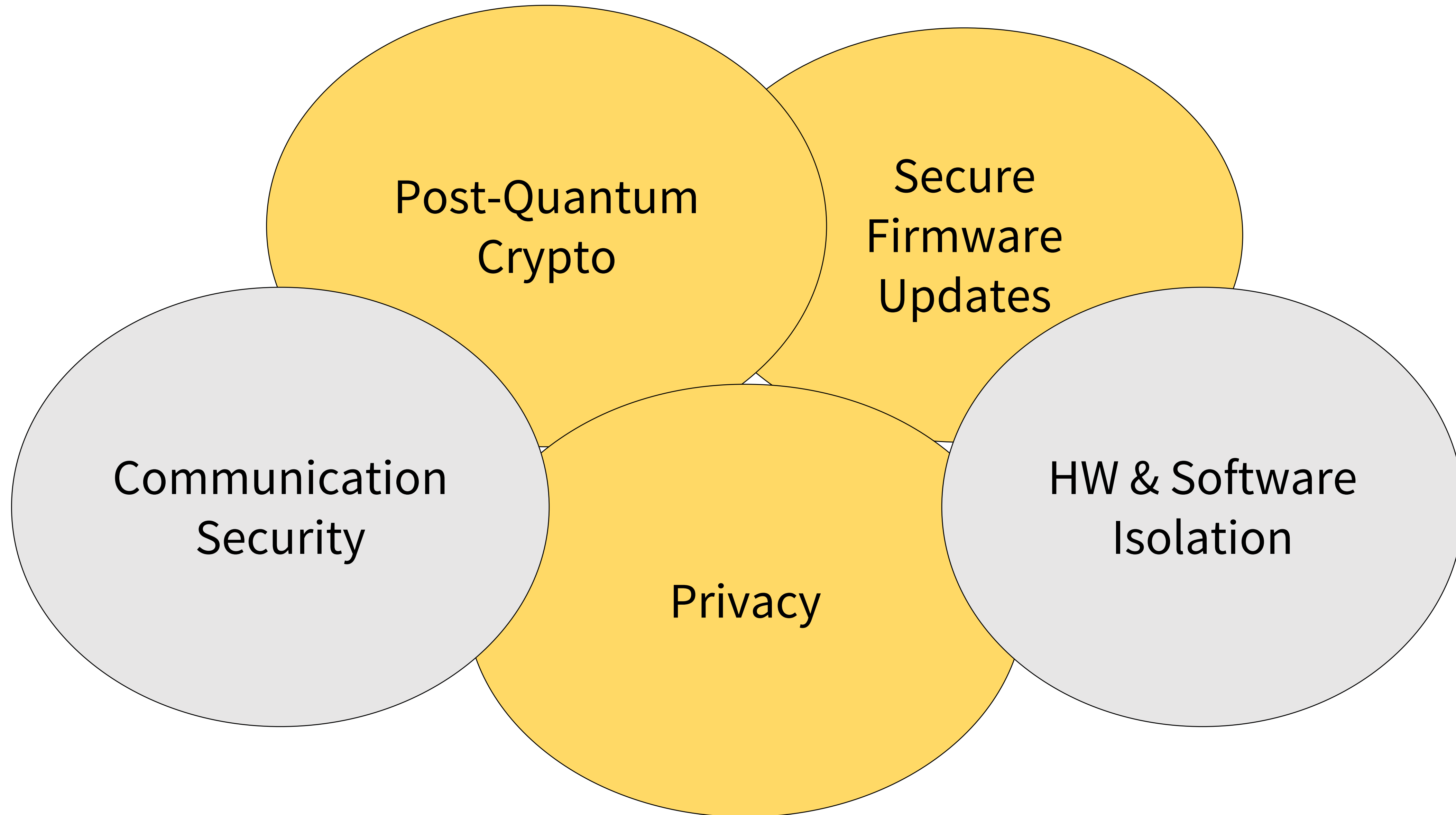
- **RIOT Summit: A Long Journey**

With the increase of vulnerabilities on the endpoints many isolation technologies were developed.



HW & Software
Isolation

- **RIOT Summit: A Long Journey**



How to communicate that the device ...

- is running the expected bootloader, firmware, application software?
- has specific security-settings?
- has been manufactured by company Y?
- uses certified hardware?
- stores keys in a secure element?
- ...

Use Cases

- Network Endpoint Assessment
- Confidential Computing
- Protection of confidential ML models
- Critical Infrastructure Control
- Trusted Execution Environment Provisioning
- FIDO Authenticators
- CA/Browser Forum - Code Signing
- Digital Identity Wallet
- DRM
- CAPTCHA replacement
- Device Onboarding

Use Cases

- Network Endpoint Assessment
- **Confidential Computing**
- Protection of confidential ML models
- Critical Infrastructure Control
- Trusted Execution Environment Provisioning

Provision confidential workload (code, and data) only to trusted environment.

- FIDO Authenticators
- CA/Browser Forum - Code Signing
- Digital Identity Wallet
- DRM
- CAPTCHA replacement
- Device Onboarding



**Store digital credential only on device
that offers certain security protection**

- Network Endpoint Assessment
- Confidential Computing
- Protection of confidential ML models
- Critical Infrastructure Control
- Trusted Execution Environment Provisioning
- FIDO Authenticators
- CA/Browser Forum - Code Signing
- **Digital Identity Wallet**
- DRM
- CAPTCHA replacement
- Device Onboarding

Attestation for Microcontrollers

- PSA Attestation Token represents early work.
- Offers *initial* attestation, i.e. limited set of Target Environments, namely those representing the first, foundational stages of the boot process.
- Reference implementation for devices available with Trusted Firmware M (→ attestation service) and the verification service Veraison.

Network Working Group
Internet-Draft
Intended status: Informational
Expires: 26 December 2024

H. Tschofenig

S. Frost
M. Brossard
Arm Limited
A. Shaw
HP Labs
T. Fossati
Linaro
24 June 2024

Arm's Platform Security Architecture (PSA) Attestation Token
draft-tschofenig-rats-psa-token-23

Abstract

The Arm Platform Security Architecture (PSA) is a family of hardware and firmware security specifications, as well as open-source reference implementations, to help device makers and chip manufacturers build best-practice security into products. Devices that are PSA compliant can produce attestation tokens as described in this memo, which are the basis for many different protocols, including secure provisioning and network access control. This document specifies the PSA attestation token structure and semantics.

Attester

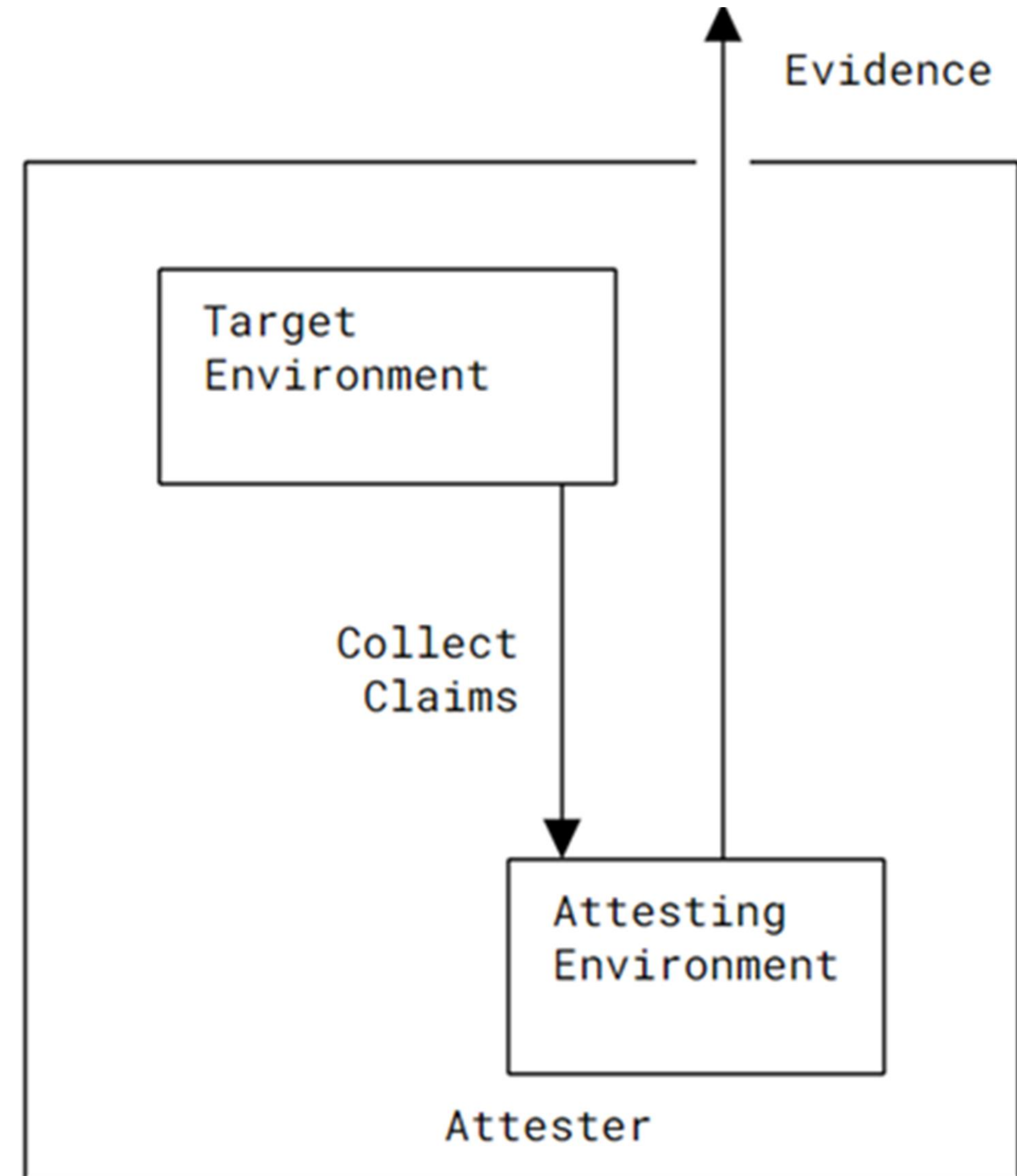
Collects information about Target Environments in form of claims.

Examples for collected information:

- Software measurements (version number, hash value)
- Device configuration (lifecycle state)

Cryptographically protects collected information (with digital signature or MAC) and releases it as Evidence.

Entities and communication patterns described in RFC 9334.



Variants of Attestation

Platform Attestation

- Foundational software (e.g., firmware & bootloader),
- Configuration (e.g., lifecycle state)
- Hardware properties

Key Attestation

- Key generation and storage attributes, i.e., how a key is stored (e.g., “secure element protected”)
- Which operations can be performed using the key(s) (e.g., signing)

Additional dimension: How often can information change?

Key Attestation: New Work on Attested CSR

- CSR = Certificate Signing Request
 - PKCS#10 – RFC 2986
 - Certificate Request Message Format (CRMF) – RFC 4211
- Developed in a design team of ~30 persons comprised of
 - **HSMs**: Entrust, Thales, Utimaco, I4P, Crypto4A, Fortanix, Intel (TPM)
 - **CAs** (and CA software vendors): Entrust, Digicert, KeyFactor, Smallstep
 - **Users of the technology**: Siemens, Bloomberg, Nokia, Ericsson
 - **Various IETF, NIST and TCG veterans**

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 9 January 2025

M. Ounsworth
Entrust
H. Tschofenig
Siemens
H. Birkholz
Fraunhofer SIT
M. Wiseman
Beyond Identity
N. Smith
Intel Corporation
8 July 2024

Use of Remote Attestation with Certification Signing Requests
draft-ietf-lamps-csr-attestation-10

Abstract

A PKI end entity requesting a certificate from a Certification Authority (CA) may wish to offer trustworthy claims about the platform generating the certification request and the environment associated with the corresponding private key, such as whether the private key resides on a hardware security module.

This specification defines an attribute and an extension that allow for conveyance of Evidence in Certificate Signing Requests (CSRs) such as PKCS#10 or Certificate Request Message Format (CRMF) payloads

Motivation CSR Attestation

To help prevent code signing keys from “walking away”, the CA/Browser Forum instituted a requirement, effective June 1, 2023 that all publicly-trusted code signing keys must be in \geq FIPS 140-2 level 2 or CC EAL 4+ hardware.

6.2.7.4 Subscriber Private Key protection and verification

The requirements in BR Section 6.2 apply equally to Code Signing Certificates.

6.2.7.4.2 Subscriber Private Key verification

Effective June 1, 2023, for Code Signing Certificates, CAs SHALL ensure that the

Subscriber's Private Key is generated, stored, and used in a suitable Hardware Crypto Module that meets or exceeds the requirements specified in [Section 6.2.7.4.1](#). One of the following methods MUST be employed to satisfy this requirement:

Motivation CSR Attestation

To help prevent code signing keys from “walking away”, the CA/Browser Forum instituted a requirement, effective June 1, 2023 that all publicly-trusted code signing keys must be in \geq FIPS 140-2 level 2 or CC EAL 4+ hardware.

6.2.7.4 Subscriber Private Key protection and verification

The requirements in BR Section 6.2 apply equally to Code Signing Certificates.

6.2.7.4.2 Subscriber Private Key verification

Effective June 1, 2023, for Code Signing Certificates, CAs SHALL ensure that the

Subscriber's Private Key is generated, stored, and used in a suitable Hardware Crypto Module that meets or exceeds the requirements specified in Section 6.2.7.4.1. One of the following methods MUST be employed to satisfy this requirement:

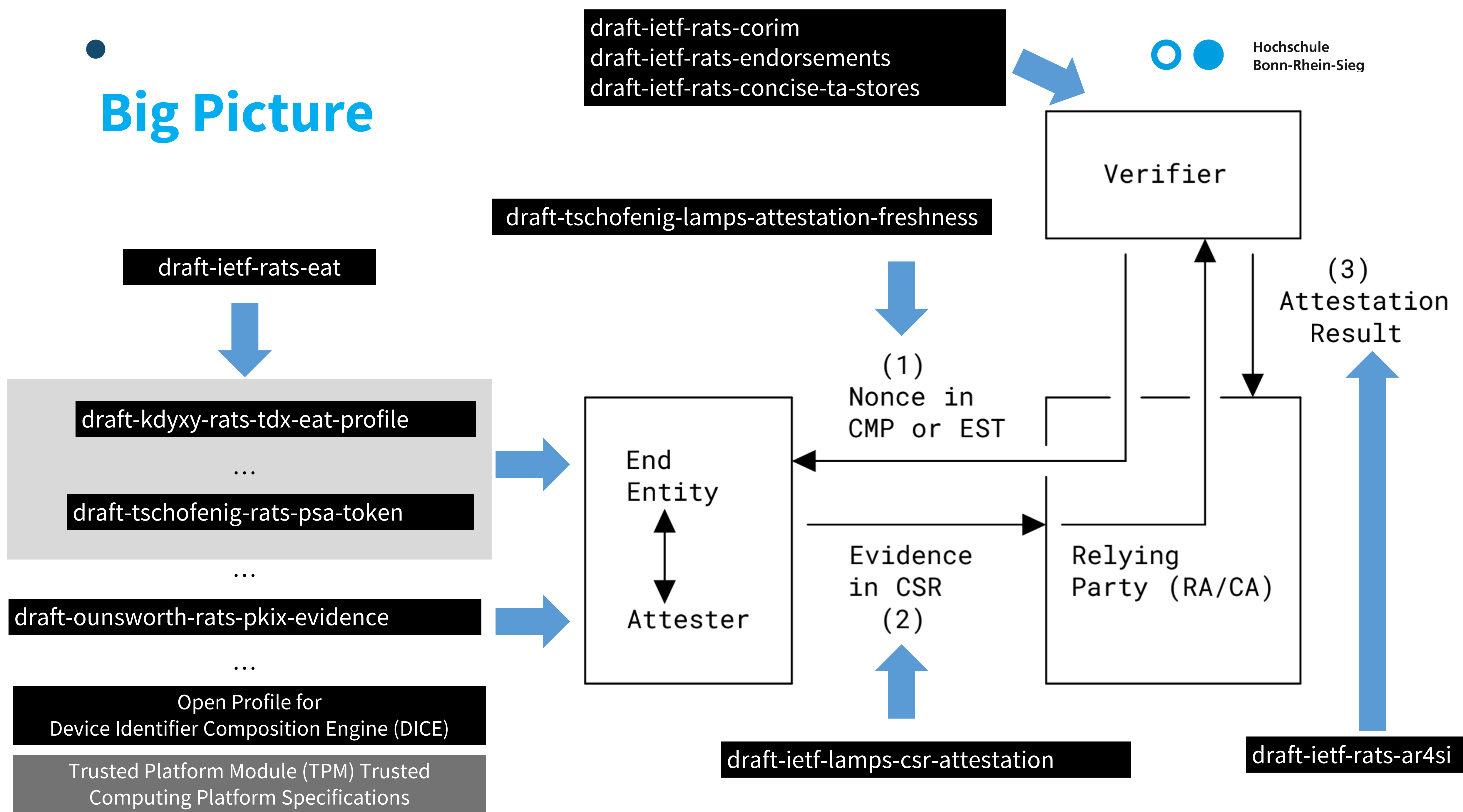
Remote Attestation

Problem #1: How is an HSM operator supposed to prove this to a CA?

Problem #2: How is a CA supposed to decide what evidence counts and what doesn't?

Verifier Configuration

Big Picture



Attestation for Embedded Devices

Where is it useful?

Device-to-Device
Communication
Pattern

Device
Onboarding
Use Cases

Dynamic
Attestation
Information

Confidential AI

Microcontroller
is part of an SoC
design

Device uses
Measured Boot



Next Steps

Call for Support: Your Input is needed

CSR Attestation

- Draft in last call for comments: <https://datatracker.ietf.org/doc/draft-ietf-lamps-csr-attestation/>
- For TPM-based key attestation, scripts for use with CSRs are available at: <https://github.com/mwiseman-byid/csr-attestation-tpm-example>

PKI-based Evidence

- Evidence format that is tailored to PKI deployments: <https://datatracker.ietf.org/doc/draft-ounsworth-rats-pkix-evidence/>

Use of attestation in TLS

- Draft: <https://datatracker.ietf.org/doc/draft-fossati-tls-attestation/>
- Reference implementation (part of the attested TLS implementation):
<https://github.com/veraison/services/tree/demo-attested-tls>
<https://github.com/CCC-Attestation/attested-tls-poc>