IETF Standards Update on Remote Attestation

Hannes Tschofenig

H-BRS

Acknowledgements

Specifications have been developed by many. I would like thank especially my co-authors (in no specific order):

- Muhammad Usama Sardar
- Thomas Fossati
- Ionut Mihalcea
- Paul Howard
- Yogesh Deshpande
- Michael Richardson
- Henk Birkholz
- Mathias Brossard
- Dionna Glaze
- Mike Ounsworth
- Monty Wiseman
- Ned Smith
- Hendrik Brockhaus
- Monty Wiseman
- Simon Frost
- Mathias Brossard
- Adrian Shaw
- Jean-Pierre Fiset
- John Kemp

Agenda

- CSR attestation and updates on the passport model
- Key attestation in RATS
- OAuth-related work on remote attestation
- WIMSE & remote attestation

Remote Attestation?

NIST SP 1800-19

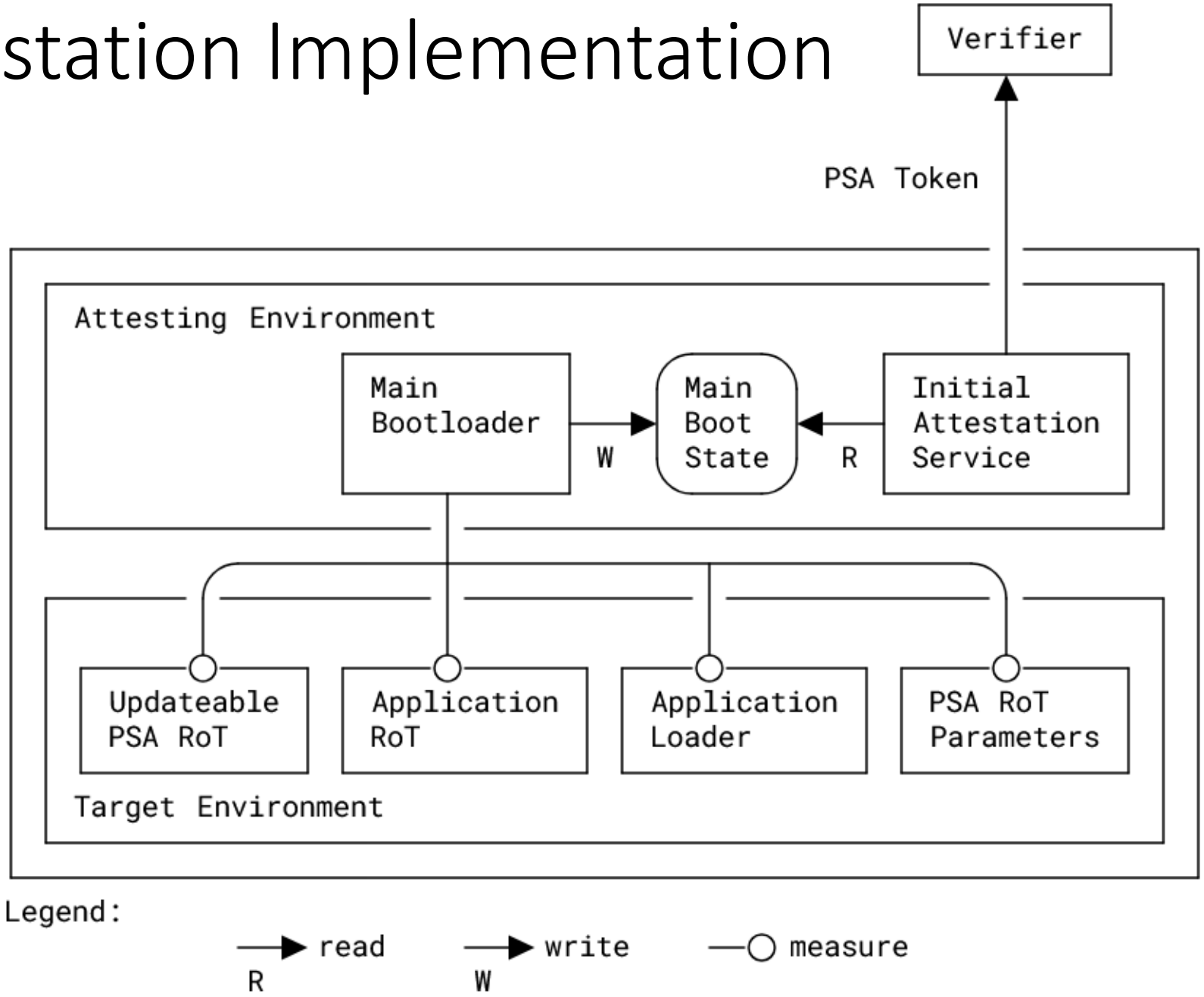
"The process of providing a digital signature for a set of measurements securely stored in hardware, and then having the requester validate the signature and the set of measurements."

NIST SP 1800-19 “**Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments”** copies the term NISTIR 7904 “**Trusted Geolocation in the Cloud: Proof of Concept Implementation**”.

"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."

Example Attestation Implementation

- Figure taken from [PSA Attestation Token specification](#).
- Implemented in Trusted Firmware M.
- Interaction involves bootloader and attestation service in the secure processing environment.



Dave Thaler Conjecture:

„Every authentication use case is also an attestation use case“*

Dave Thaler in IETF Datatracker

* FWIW not everyone agrees with him, see here.

Information beyond Authentication

Authentication provides information about the party issuing the credential, about the subject and potentially a lot of meta-data (such as key usage restrictions).

Platform attestation adds information about the hardware being used, configuration settings of hardware and software, firmware / software stack being executed, and much more.

Key attestation also provides information about the properties of the key, such as whether private key was generated in a secure element, can be exported in the clear, and other properties.

Field name	Contents or description
`Version`	X.509v3 or other versions
`Serial-Number`	uniquely identifies certificate, e.g., for revocation
`Issuer`	issuing CA's name
`Validity-Period`	specifies dates (`Not-Before`, `Not-After`)
`Subject`	owner's name
`Public-Key` info	specifies (`Public-Key-Algorithm`, `Key-Value`)
extension fields (optional)	`Subject-Alternate-Name/SAN-list`, `Basic-Constraints`, `Key-Usage`, `CRL-Distribution-Points` (and others)
`Signature-Algorithm`	(`algorithmID`, `parameters`)
`Digital-Signature`	signature of `Issuer`

Table 8.1: X.509v3 public-key certificate fields.

Reference

History of …

Authentication

- Identification
  (as opposed to authentication)
- Challenge/Response – one-way authentication.
- Authentication and key exchange protocols

Attestation

- Bearer token alike attestation techniques
- PSA attestation token
- Key Attestation

Granularity of the Authorization Information

- What information about the hardware/software environment should be included in the Evidence?
  - Higher in the software stack the measurements become more complex.
- How often are the measurements taken?
  - Once per boot vs. dynamically at run-time.
- How to prevent attester and verifier state to get our of sync?

Attested CSR

- CSR = Certificate Signing Request
  - PKCS#10 – RFC 2986
  - Certificate Request Message Format (CRMF) – RFC 4211
- Draft contains examples in the appendix (with source code).
- 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 — M. Ounsworth, Entrust
Internet-Draft
Intended status: Standards Track — H. Tschofenig, Siemens
Expires: 3 August 2025 — H. Birkholz, Fraunhofer SIT
M. Wiseman, Beyond Identity
N. Smith, Intel Corporation
30 January 2025

Use of Remote Attestation with Certification Signing Requests
draft-ietf-lamps-csr-attestation-15

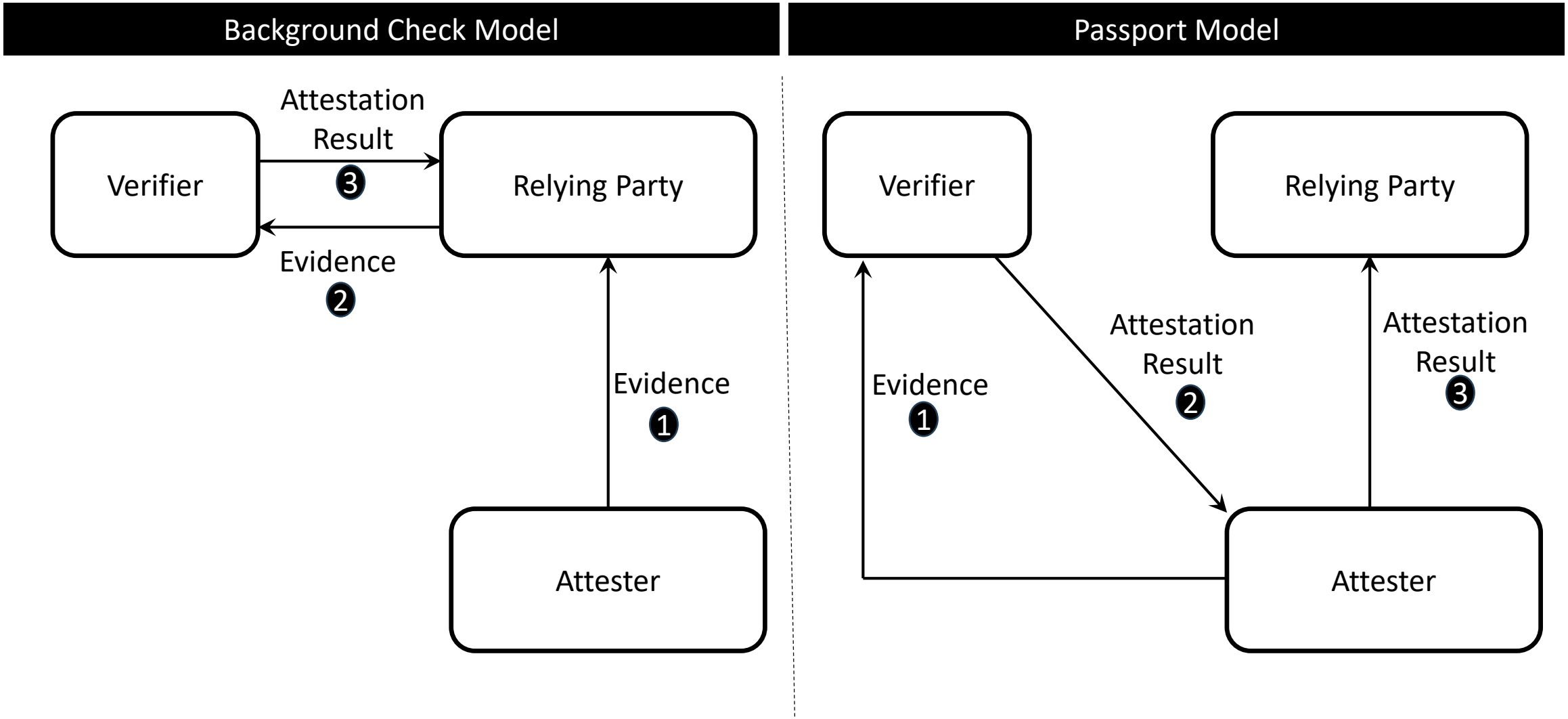
Abstract

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.

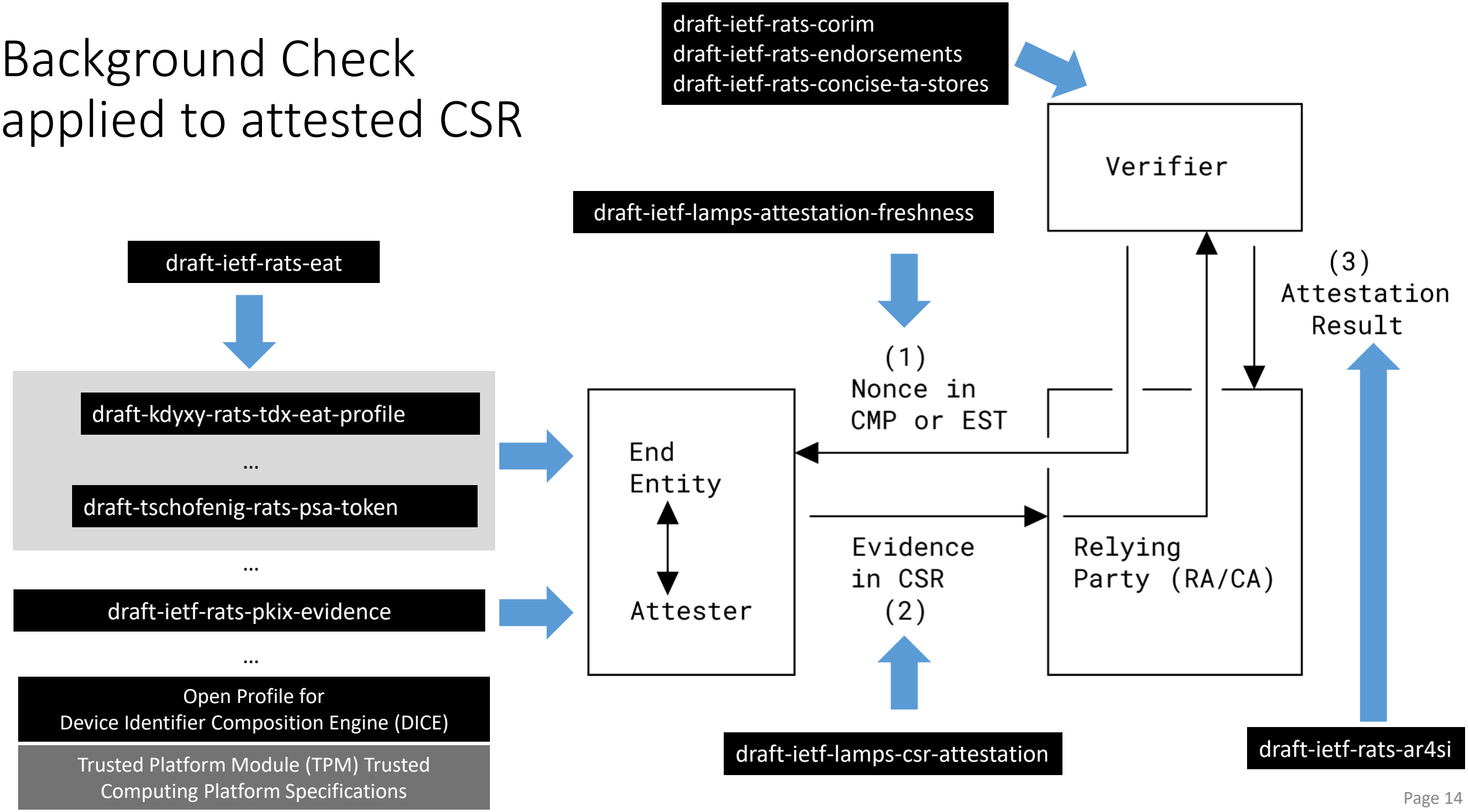
This specification defines an attribute and an extension that allow for conveyance of Evidence and Attestation Results in Certificate Signing Requests (CSRs), such as PKCS#10 or Certificate Request

Reference

Reminder: IETF RATS Communication Patterns



Background Check applied to attested CSR



Passport Model applied to attested CSR

(added with draft version -15)

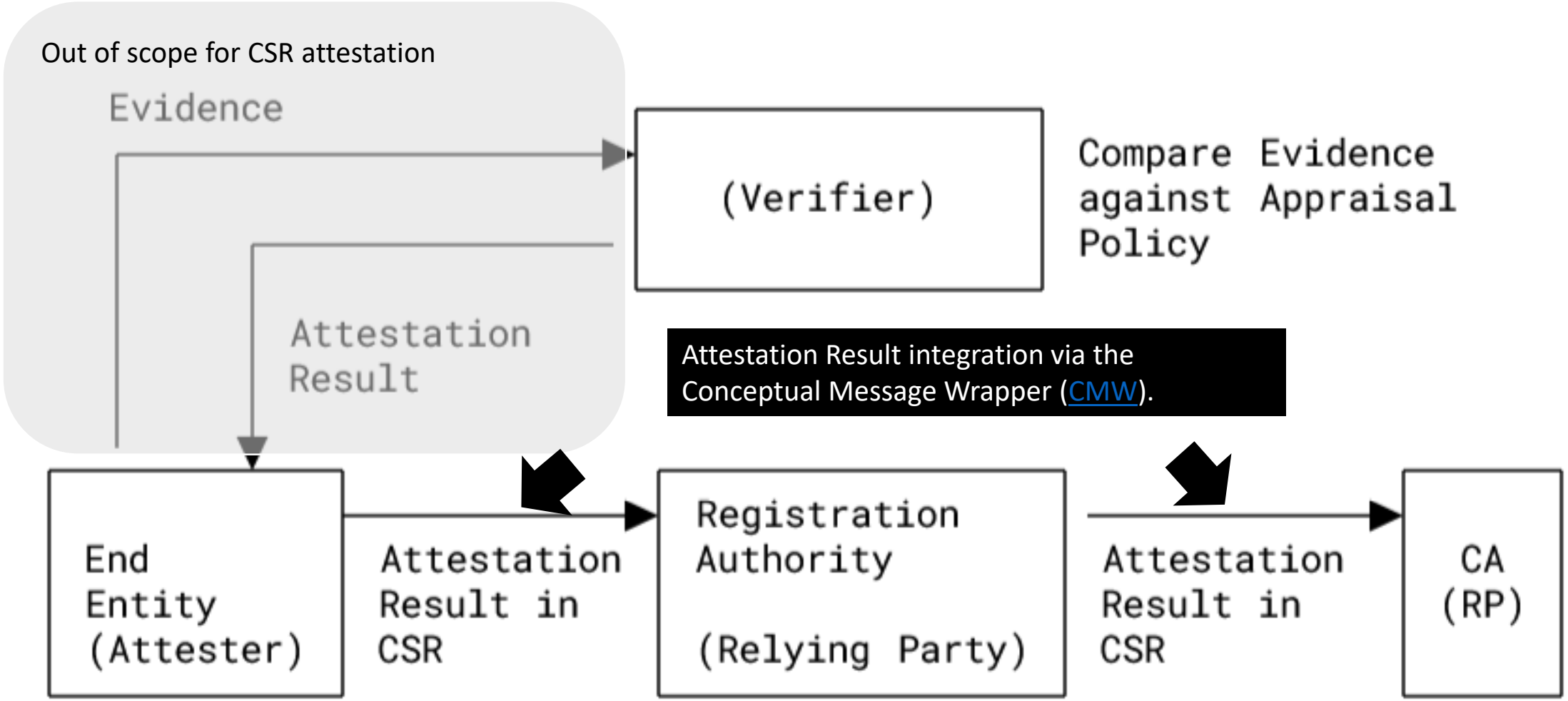


Figure 2 of draft-ietf-lamps-csr-attestation-15

ASN.1/DER-based Evidence

- Motivation: The CA/Browser Forum instituted a requirement, effective June 1st 2023 that all publicly-trusted code signing keys must be in >= FIPS 140-2 level 2 or CC EAL 4+ hardware.
- HSM vendors prefer ASN.1/DER encodings (rather than CBOR/COSE or JOSE/JOSE).
- PKIX Evidence (see draft-ietf-rats-pkix-evidence) offers
  - A mapping of EAT claims to ASN.1
  - Defines additional claims for key attestation
  - A means to embed Attestation Results in an X.509 certificate.
- Code available.

ASN.1/DER-based Evidence, cont.

- For better readability we decided to split the document into three parts:
  1. DER Web Token (DWT)
  2. Key Attestation
  3. X.509-Attestation Result (AR)
- All of this is work in progress done in the IETF LAMPS attestation design team.
- It is a good time to participate in the work.

Key Attestation Approaches

Combined Platform Key Attestation Token

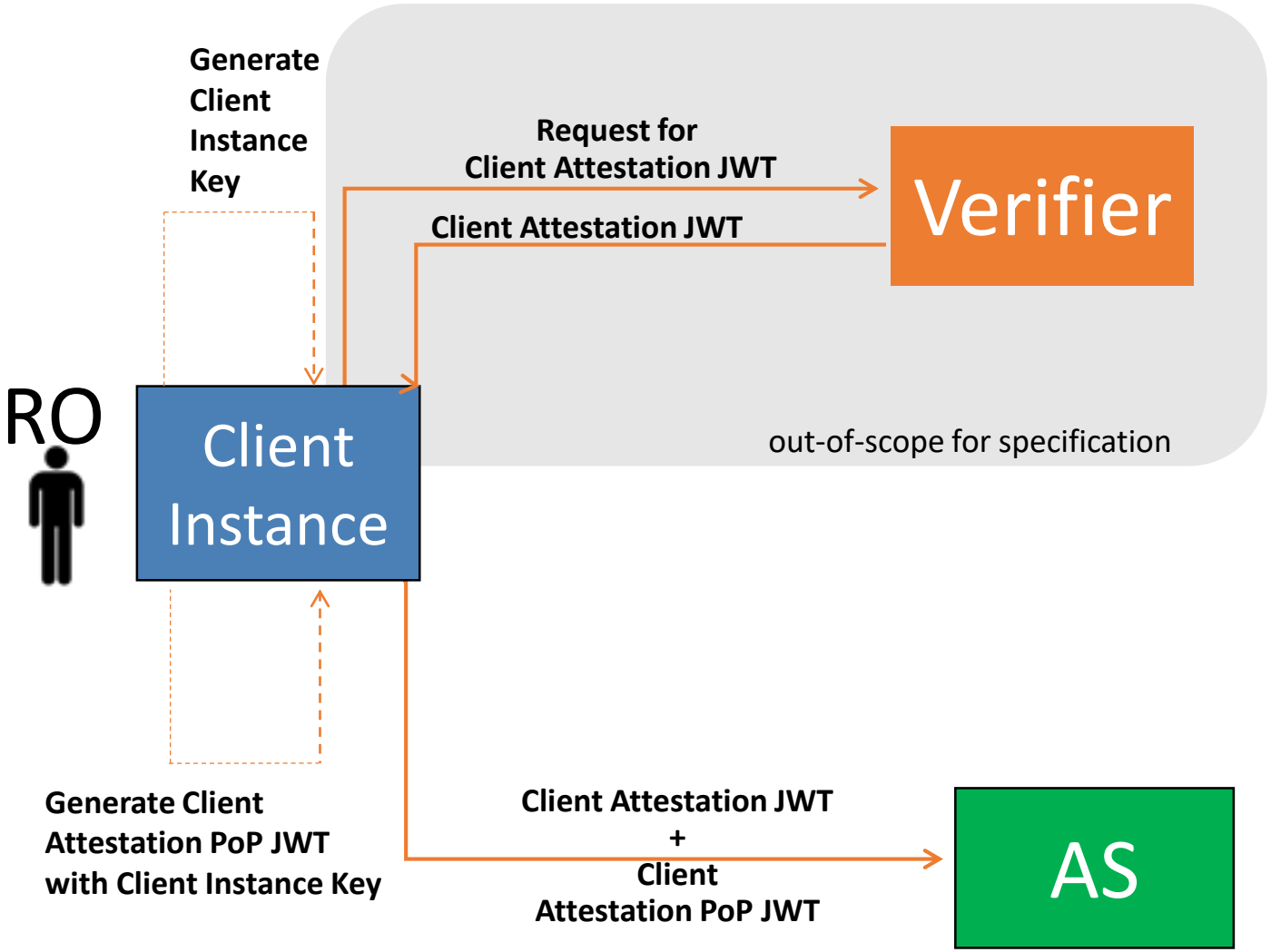
- Single attestation token only.
- Requires foundational attestation service to be updated.
- Design could use nested tokens: Platform attestation is embedded inside the Key Attestation Token.

Linked Platform and Key Attestation Token

- Platform attestation token (PAT) remains unchanged.
- Nonce of the PAT is the hash of the public key of the Key attestation token (KAT).
- KAT contains the nonce, the public key and key attributes.
- KAT will be signed by another attestation key.

From LAMPS to OAuth

OAuth Attestation Architecture



- Defined in [draft-ietf-oauth-attestation-based-client-auth]
- Uses the passport model.
- Requires that Attestation Results are encoded as JWTs but does not mandate any AR claims.
- Binds a key to the Attestation Result but does not require key attestation.

Client Attestation JWT

- Encoded as a PoP token with a cnf claim according to RFC 7800
- Sub claims contains the client id and must contain issuer claim and the expiry claim.
- Type indicates „oauth-client-attestation+jwt“

```
{
 "typ": "oauth-client-attestation+jwt"
 "alg": "ES256",
 "kid": "11"
}
.
{
 "iss": "https://client.example.com",
 "sub": "https://client.example.com",
 "nbf":1300815780,
 "exp":1300819380,
 "cnf": {
   "jwk": {
      "kty": "EC",
      "use": "sig",
      "crv": "P-256",
      "x":
"18wHLeIgW9wVN6VD1Txgpqy2LszYkMf6J8njVAibvhM",
      "y": "-V4dS4UaLMgP_4fY4j8ir7cl1TXlFdAgcx55o7TkcSA"
   }
 }
}
```

Example of a Client Attestation JWT without signature.

Client Attestation PoP JWT

- Used to demonstrate possession of the private key to the relying party.
- Encoded as a JWT with several mandatory claims:
  - The audience claim must specify a value that identifies the authorization server as an intended audience
  - Expiry claim
  - Issuer claim containing the client_id
  - Type claim indicates „oauth-client-attestation-pop+jwt“
- May contain iat, nbf, and nonce.

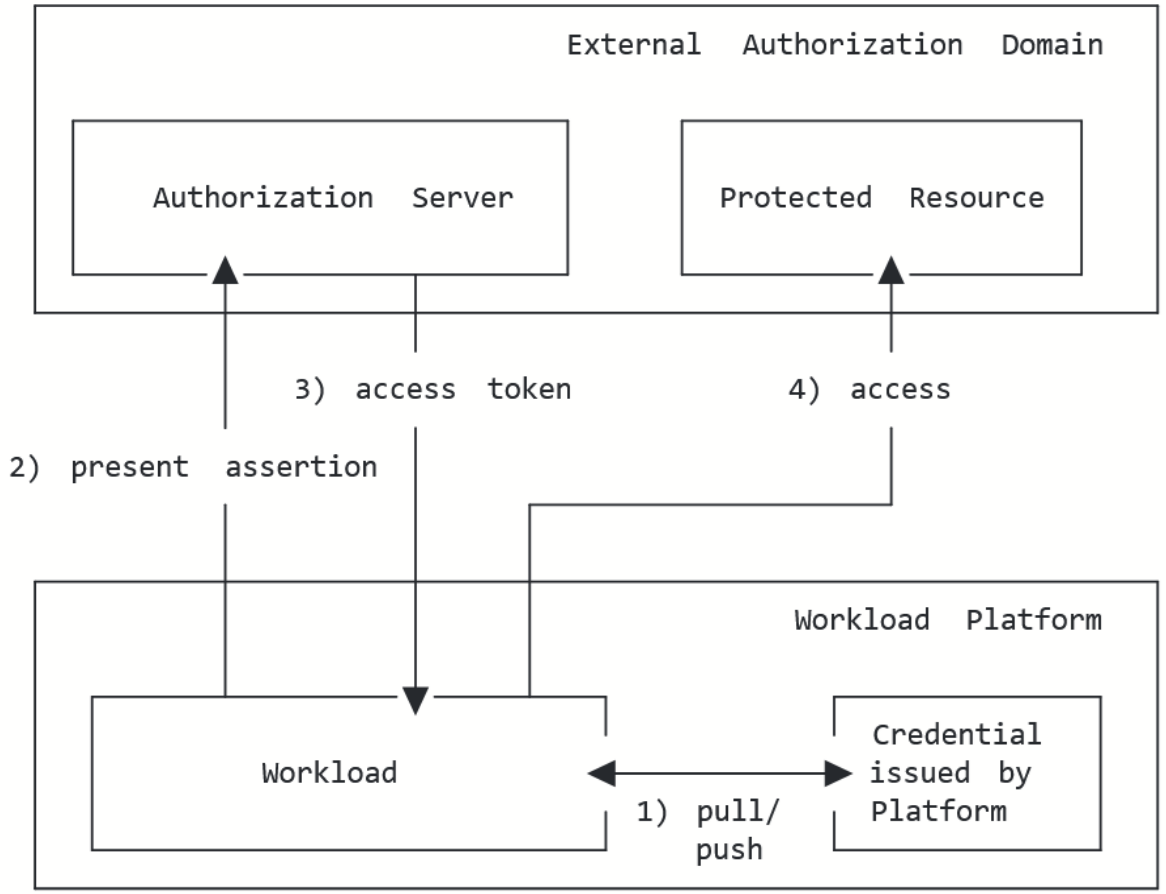
```
{
 "typ": "oauth-client-attestation-pop+jwt",
 "alg": "ES256"
}
.
{
 "iss": "https://client.example.com",
 "aud": "https://as.example.com",
 "nbf":1300815780,
 "exp":1300819380,
 "jti": "d25d00ab-552b-46fc-ae19",
 "nonce" : "5c1a9e10-29ff-4c2b-ae73"
}
```

Example of a Client Attestation PoP JWT without signature.

Workload Identity

Remote Attestation in WIMSE

- Workloads needs to present assertion to Authorization Server to obtain access token.
- This assertion is obtained from the Workload Platform in form of a credential.
- Attestation verifies that a workload is running on trusted infrastructure and has not been tampered with.
- Workloads use different types of credentials: X.509 certs and JWTs
- Terminology is still in flux → architecture draft.



Reference to Workload Identity Practices draft

Summary

Summary

- Work on remote attestation ongoing for a number of years and we are seeing deployment results
- New requirements and applications (digital wallets, (confidential) containers) have created the need for key attestation and attestation to be integrated into different applications.
- We need your input → reviews, specification, implementations, applications
- Groups: LAMPS, RATS, OAuth, WIMSE