Hewlett Packard Enterprise

Secure Push Attestation

with Extensible REST APIs

Jean Snyman

FOSDEM ‘25

End-to-end solution for remote attestation

UEFI Measured Boot

IMA File Integrity


Keylime


Keylime

About me

Jean Snyman (he/him) Bristol, UK

Research Engineer within the Security Lab at Hewlett Packard Labs

- Applied research in systems architecture and platform security

MSc in Information Security, University of Surrey

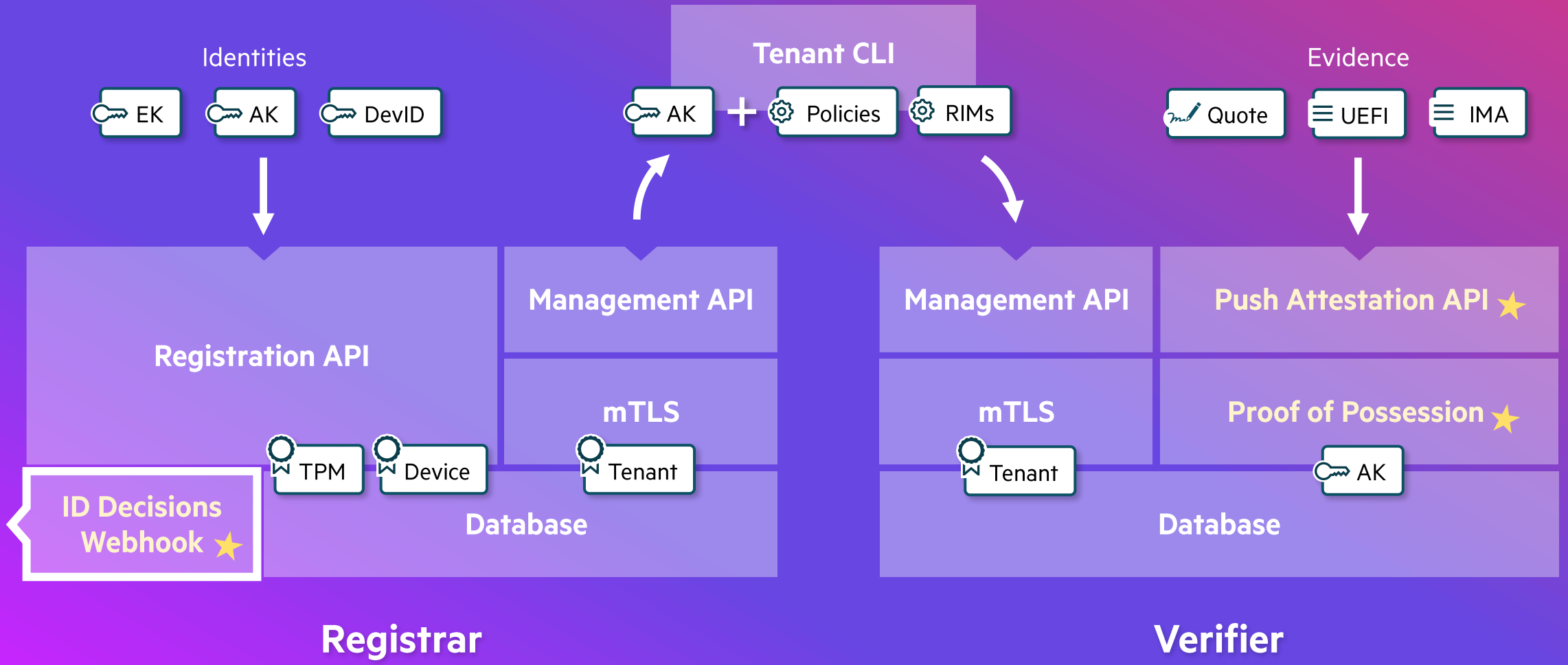
- Formal verification of security protocols
- Recipient of the Chartered Institute of Information Security's Fred Piper award as their choice for overall best student of 2023

Hewlett Packard Labs

Contributor to the Keylime open-source project

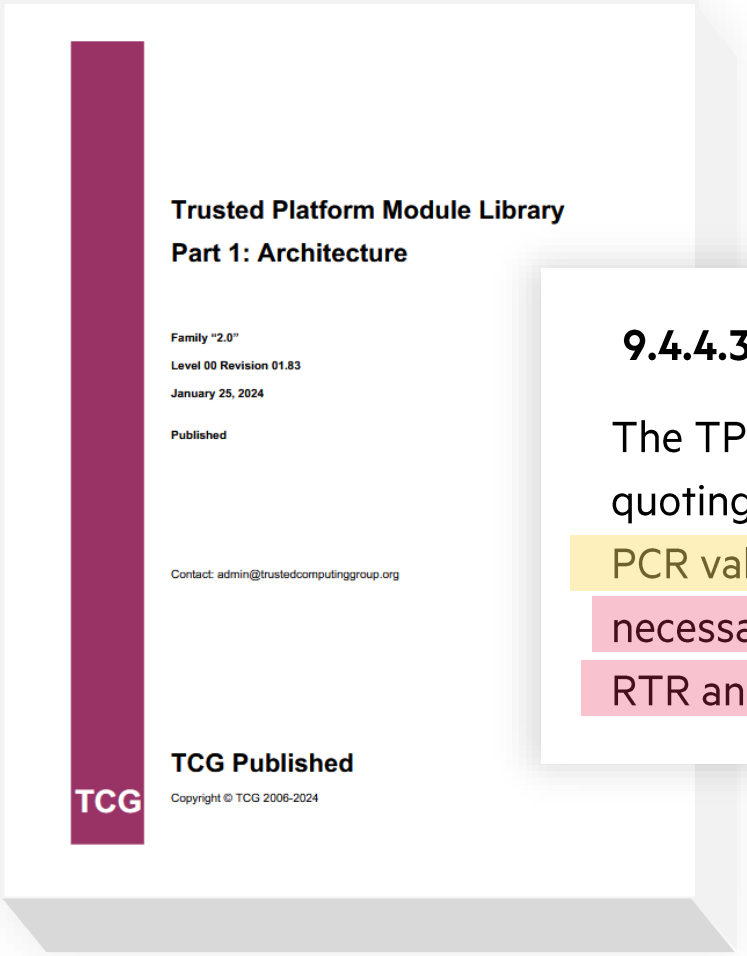
- Refactor of REST API code, agent-driven attestation, security

Push Attestation Overview



Identity Trust Decisions

TPM–Platform Binding

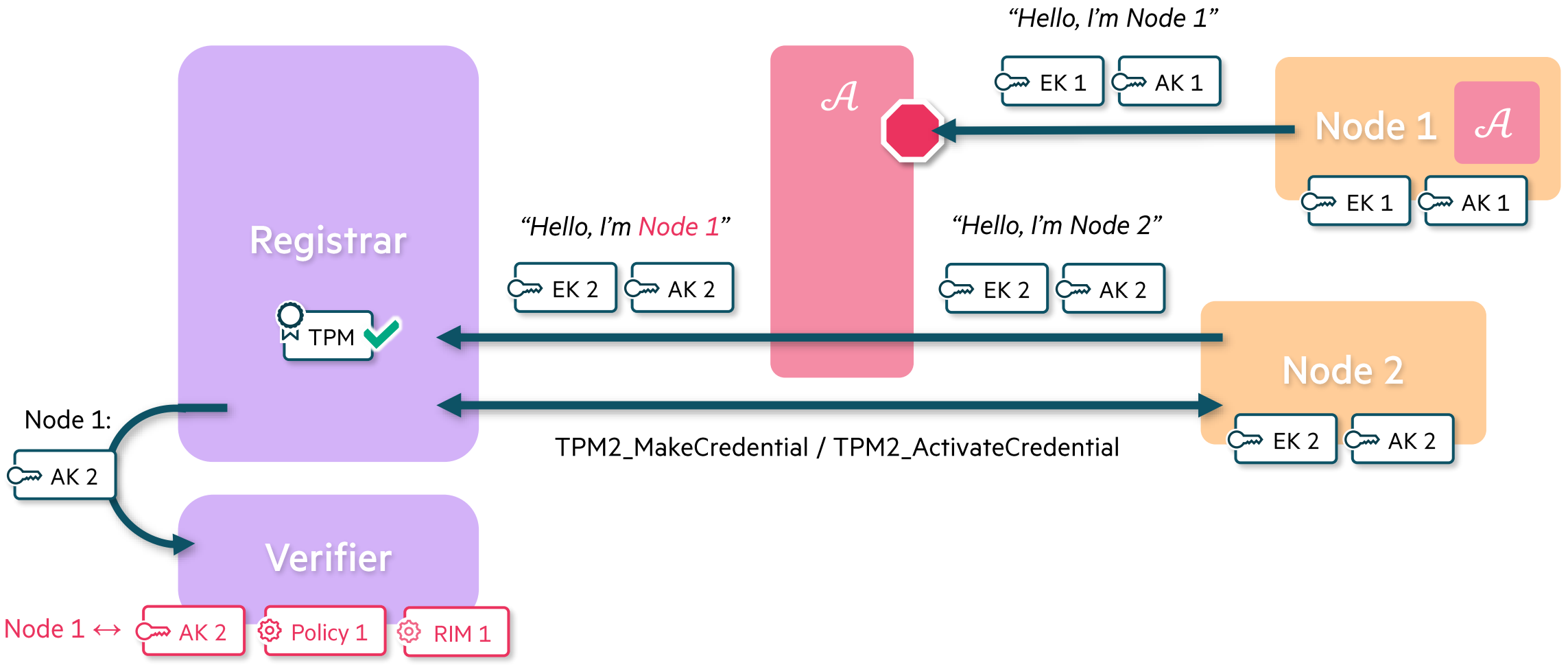


9.4.4.3 RTR Binding to a Platform

The TPM reports on the state of the platform by quoting the PCR values. For assurance that these PCR values accurately reflect that state, it is necessary to establish the binding between the RTR and the platform.

Identity Trust Decisions

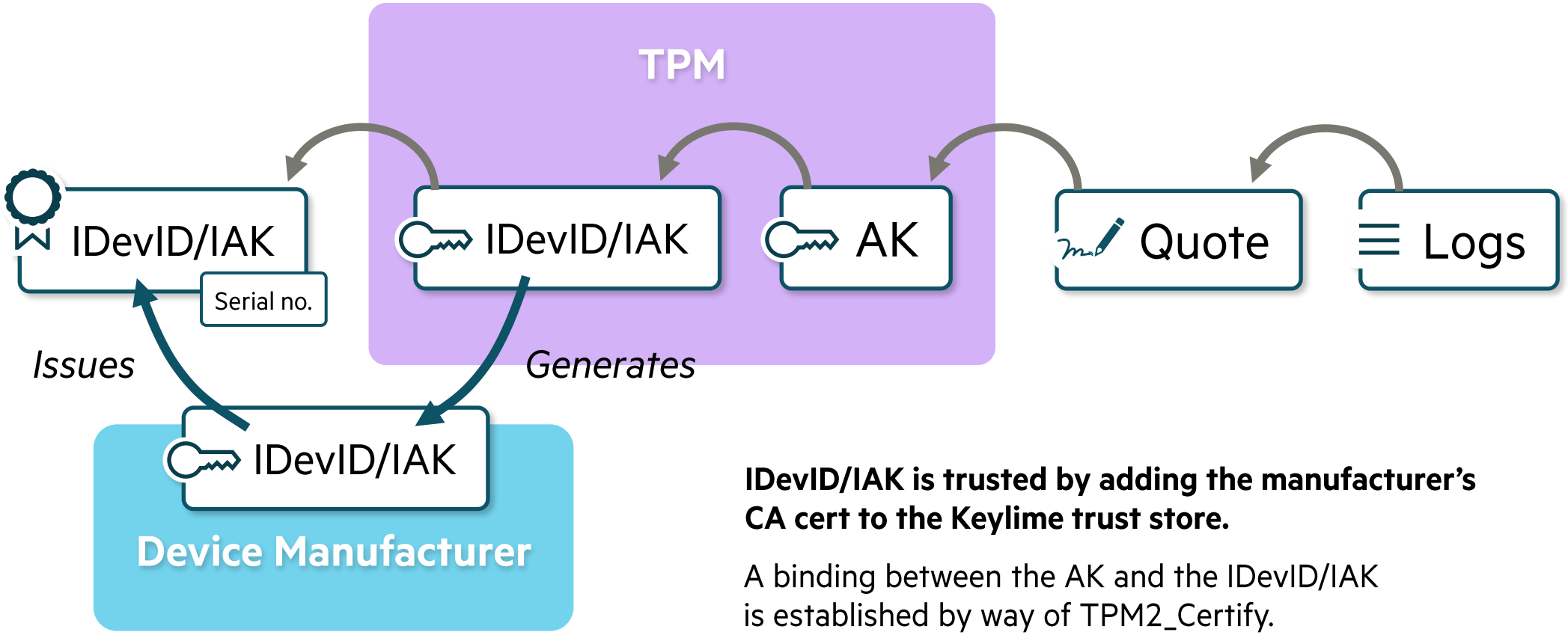
TPM–Platform Binding



Identity Trust Decisions

Option 1: Binding Using Device Identities

Existing Feature



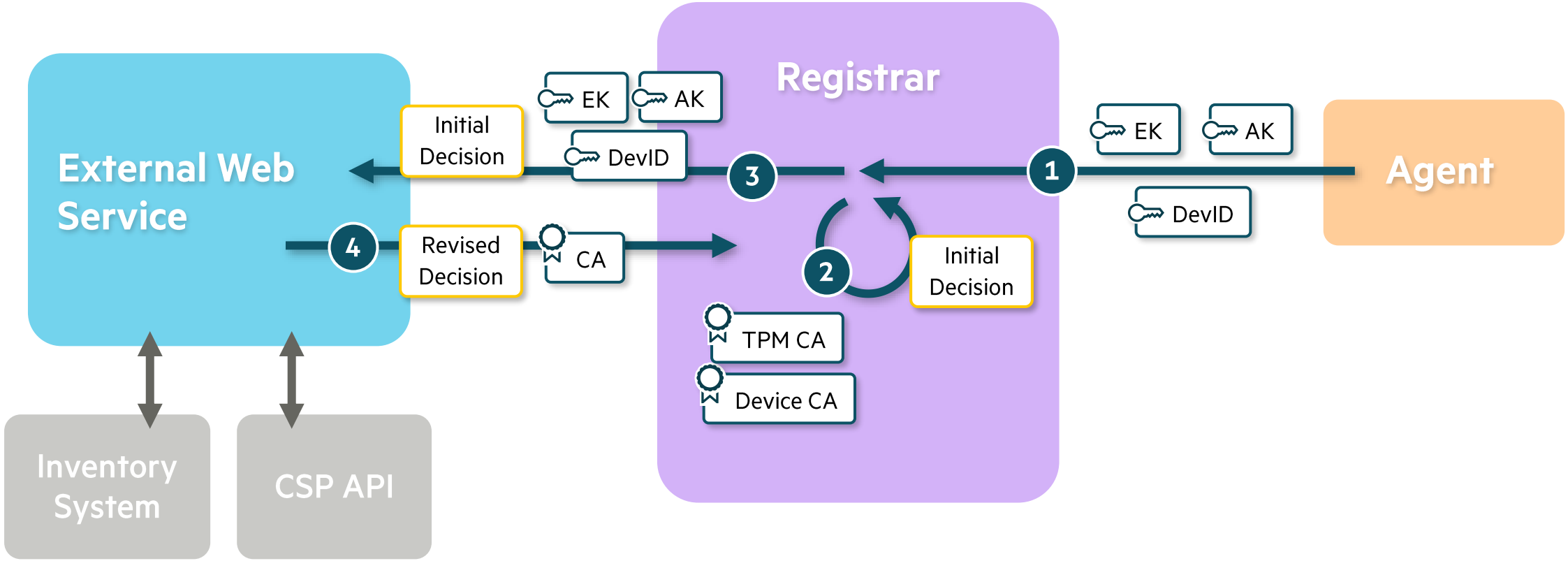
IDevID/IAK is trusted by adding the manufacturer's CA cert to the Keylime trust store.

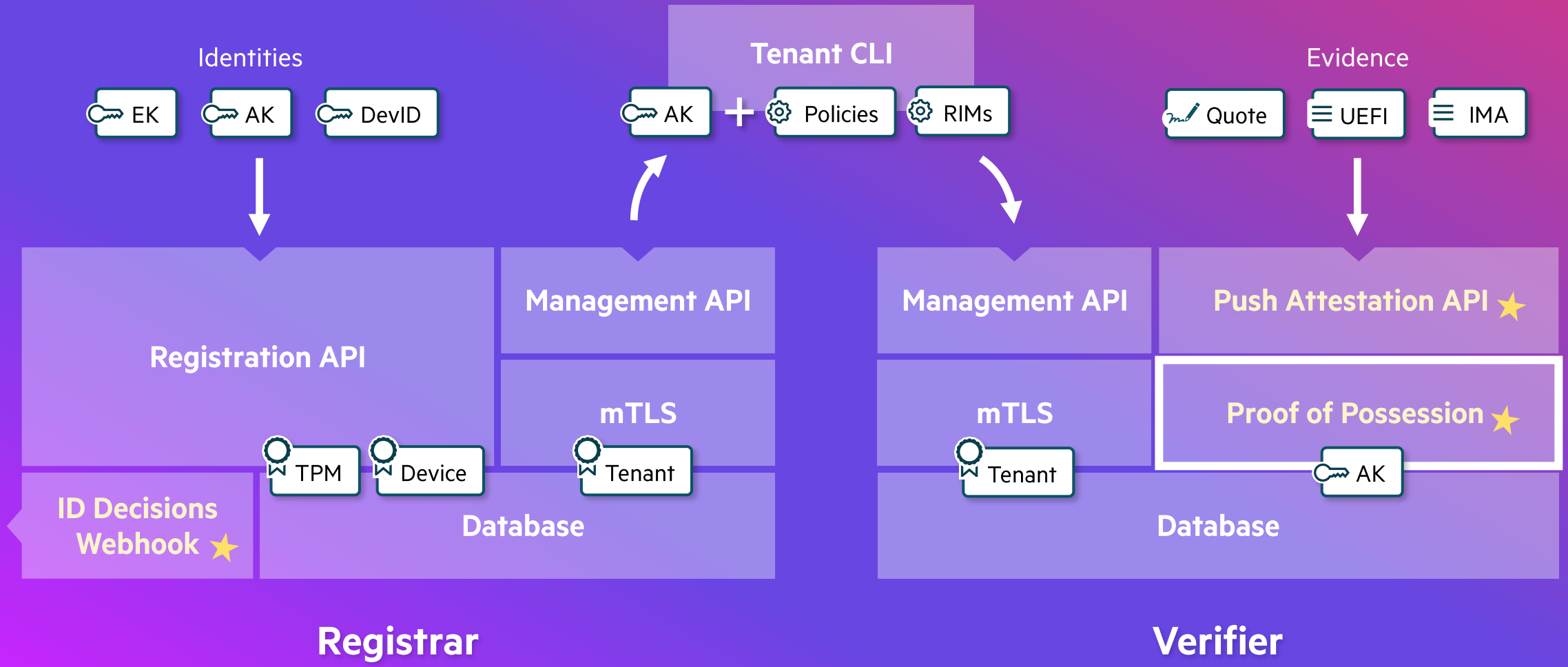
A binding between the AK and the IDevID/IAK is established by way of TPM2_Certify.

Identity Trust Decisions

Option 2: Binding Using Webhook and Custom Trust Logic

NEW

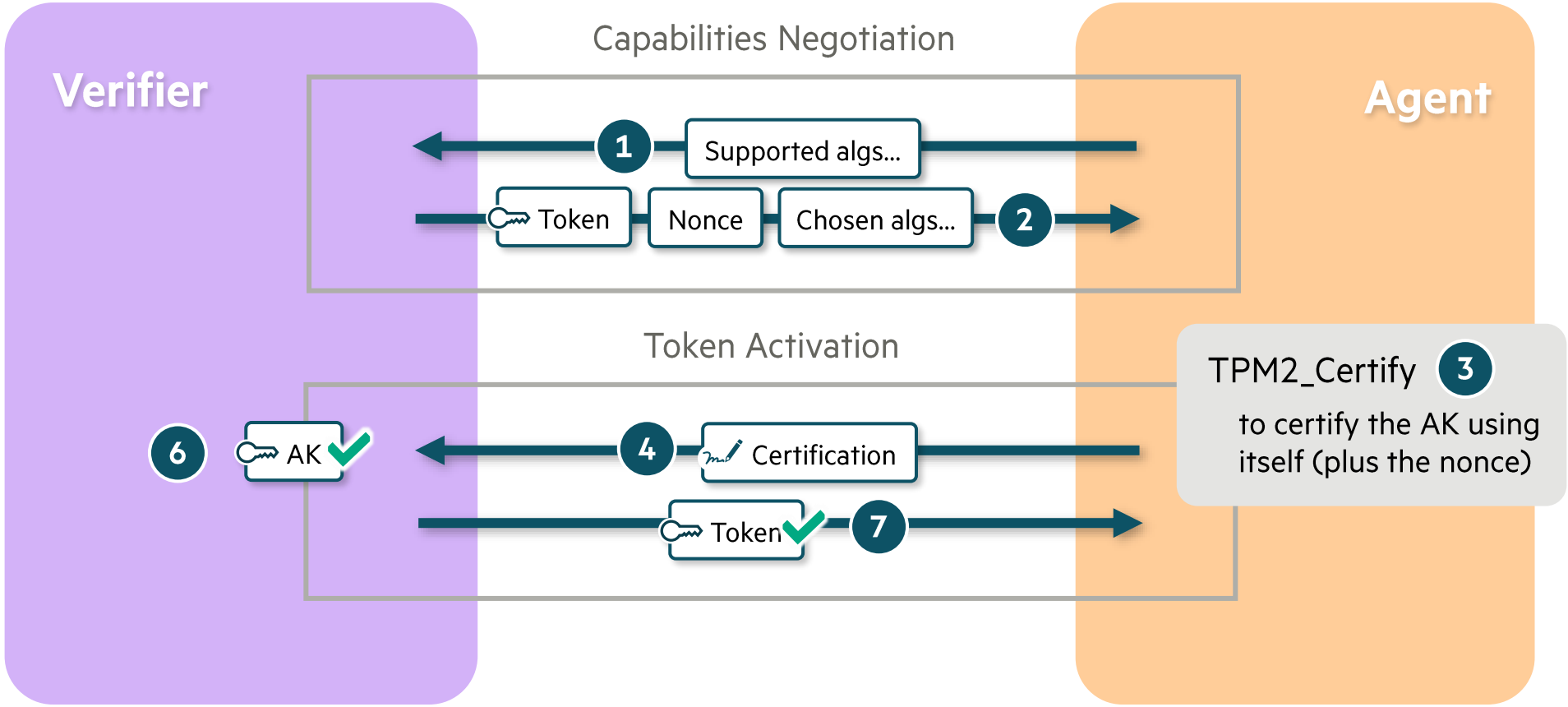


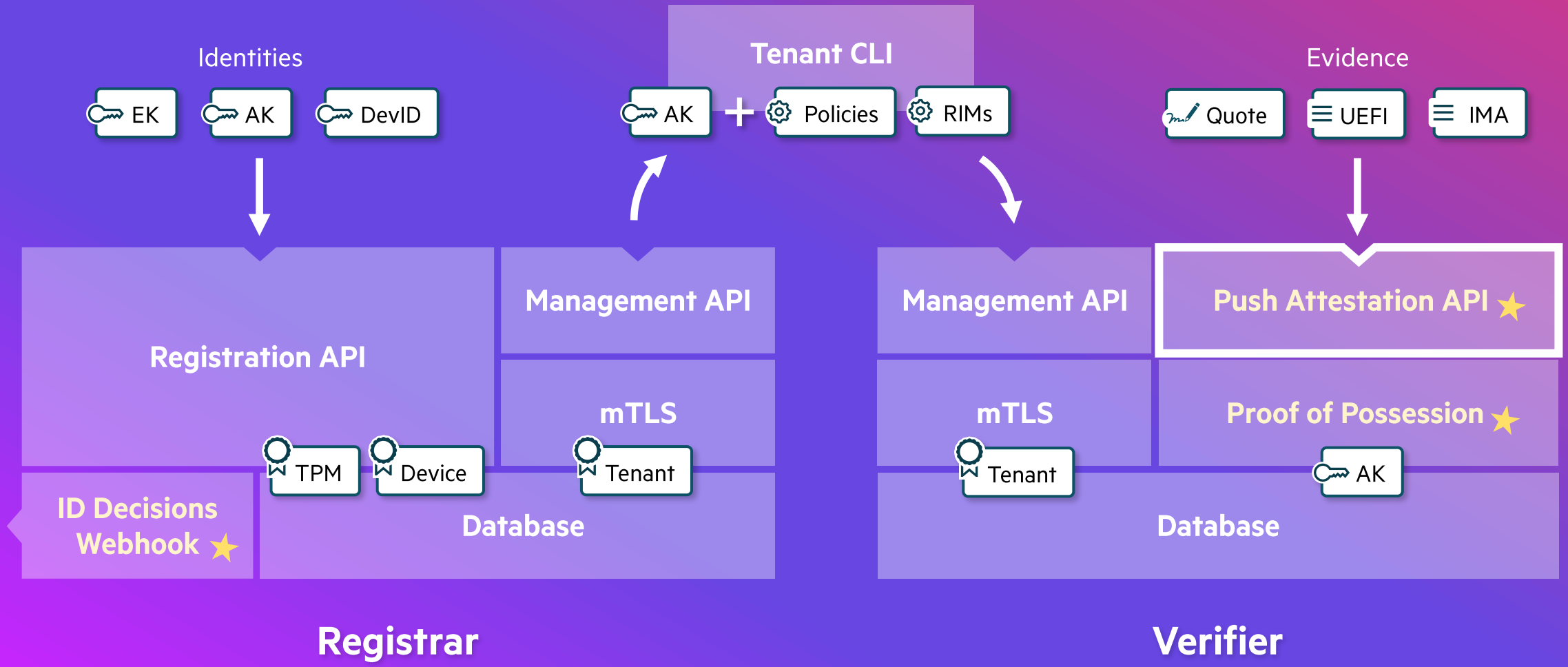

Identities
EK
AK
DevID
Tenant CLI
AK
Policies
RIMs
Evidence
Quote
UEFI
IMA
Registration API
Management API
mTLS
TPM
Device
Tenant
ID Decisions Webhook
Database
Registrar
Management API
Push Attestation API
mTLS
Proof of Possession
Tenant
AK
Database
Verifier

Agent API Authentication

Proof-of-Possession (PoP) Protocol

NEW

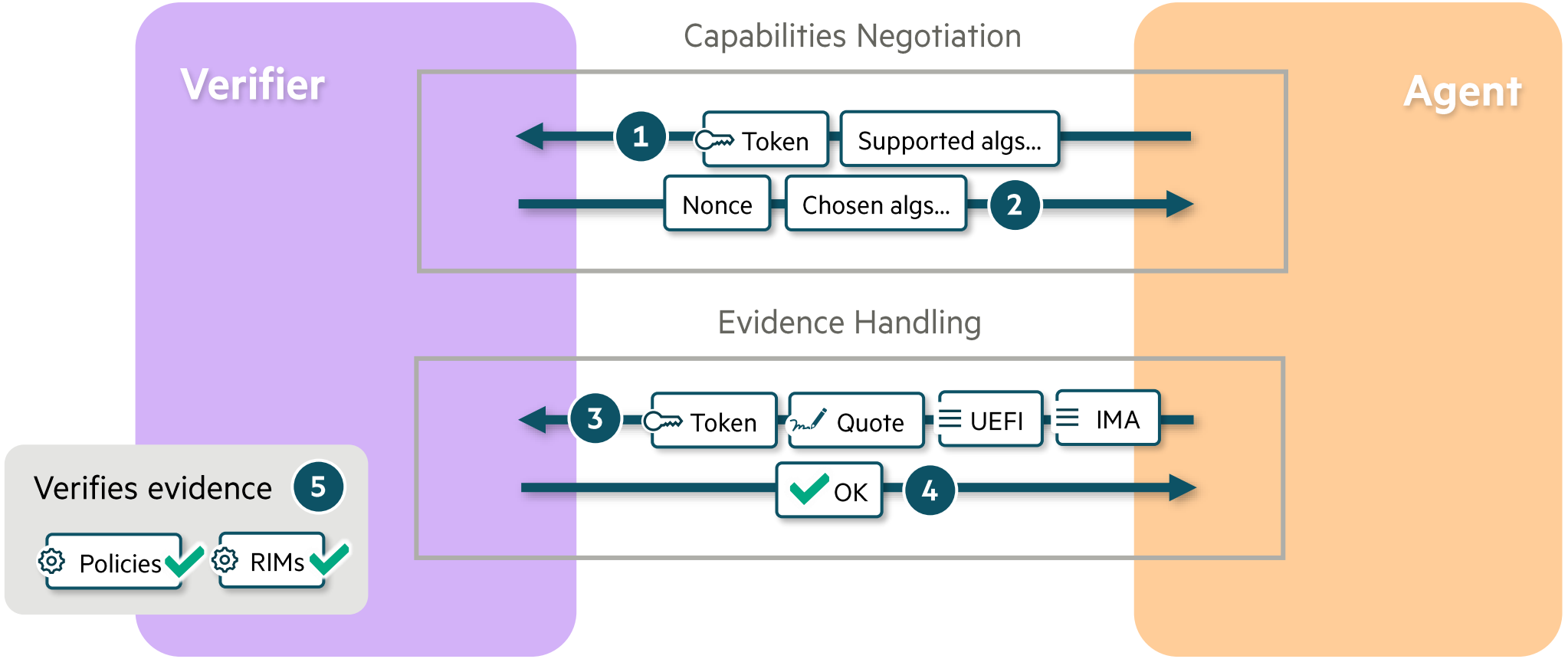



Identities
EK
AK
DevID
Tenant CLI
AK
Policies
RIMs
Evidence
Quote
UEFI
IMA
Registration API
Management API
mTLS
TPM
Device
Tenant
ID Decisions Webhook
Database
Registrar
Management API
Push Attestation API
mTLS
Proof of Possession
Tenant
AK
Database
Verifier

Push Attestation API

Attestation Protocol

NEW



Push Attestation API

Example Request Body

NEW

1 POST /v3.0/agent/1/attestations


```
{
    "data": {
        "type": "attestation",
        "attributes": {
            "evidence_supported": [
                {
                    "evidence_class": "certification",
                    "evidence_type": "tpm_quote",
                    "capabilities": {
                        "spec_version": "2.0",
                        "hash_algorithms": [ "sha3_512", "sha3_384", "sha3_256", "sha512", "sha384", "sha256", "sha1" ],
                        "signature_schemes": [ "rsassa", "rsapss", "ecdsa", "ecdaa", "ecschnorr", "sm2" ],
                        "attestation_keys": [
                            {
                                "key_class": "private_key",
                                "key_identifier": "...",
                                "key_algorithm": "rsa",
                                "public_hash": "..."
                            }
                        ]
                    }
                },
                {
                    "evidence_class": "log",
                    "evidence_type": "mb_log"
                },
```

Push Attestation API

Example Request Body

NEW

1 POST /v3.0/agent/1/attestations

```
                    "attestation_keys": [
                        {
                            "key_class": "private_key",
                            "key_identifier": "...",
                            "key_algorithm": "rsa",
                            "public_hash": "..."
                        }
                    ]
                }
            },
            {
                "evidence_class": "log",
                "evidence_type": "mb_log"
            },
            {
                "evidence_class": "log_partial",
                "evidence_type": "ima_entries"
            }
        ],
        "boot_time": "2024-11-12T16:21:17Z"
    }
}
```

Status

PR #1523	Foundational refactor of registrar web layer ✔
PR #1670	Identity trust decisions webhook
PR #1693	Push attestation protocol
PR #1731	PoP agent authentication protocol

Server-side changes

Agent implementation to follow

PR #1704	Adversarial model used in the design of the push protocols

Thank you

LinkedIn: Jean Snyman
GitHub: stringlytyped
Email: jean.snyman@hpe.com

Credits

City 3D render by Sketchfab user “abhayexe”, used under Creative Commons Attribution license.

Illustrations of business interiors by Freepik user “vectorpouch”.