# Trustee

## Open Source Attestation Service

Samuel Ortiz - sameo@rivosinc.com

EuroProofNet - March 2024

# Background

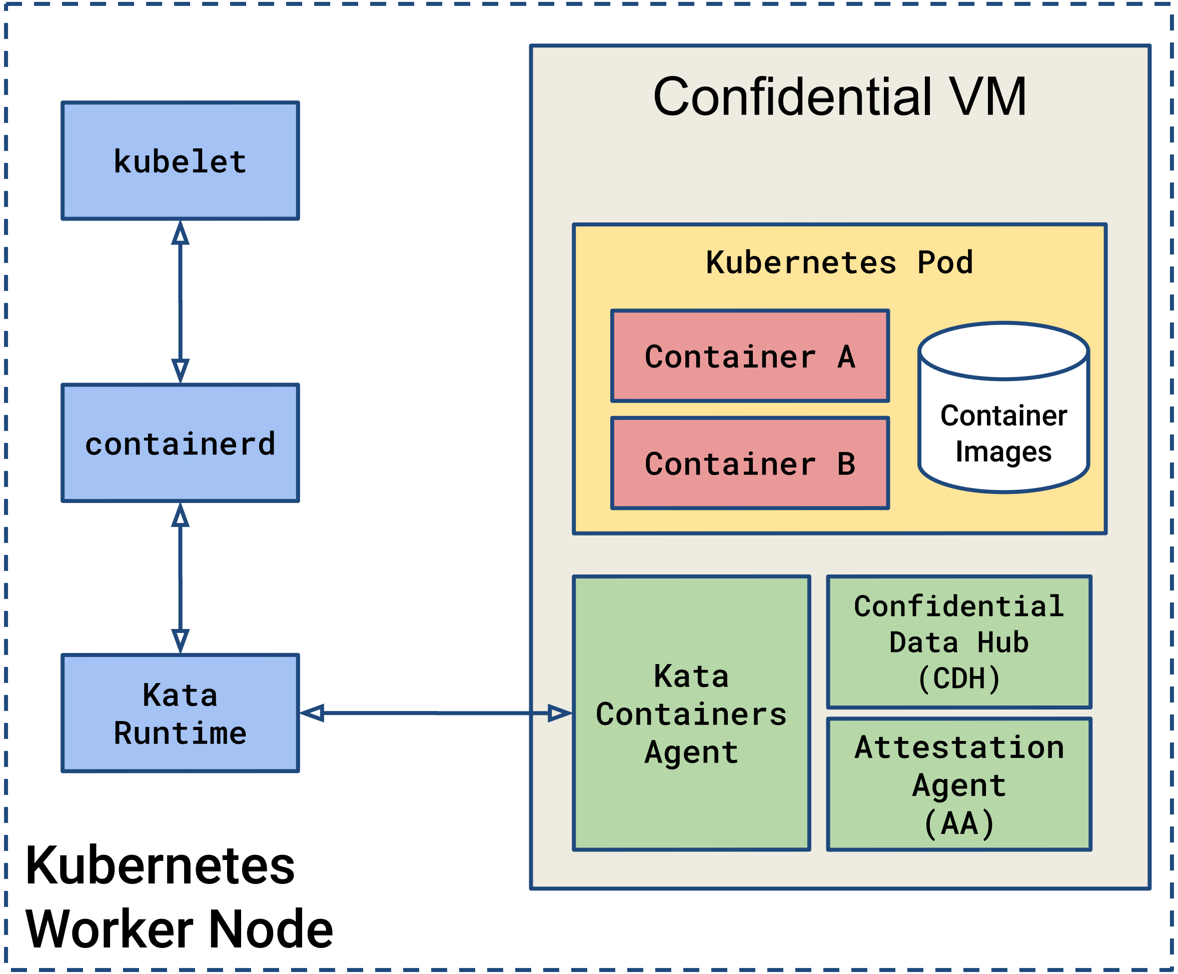
Confidential Containers

Run unmodified container workloads in TEEs

Seamless integration with Kubernetes

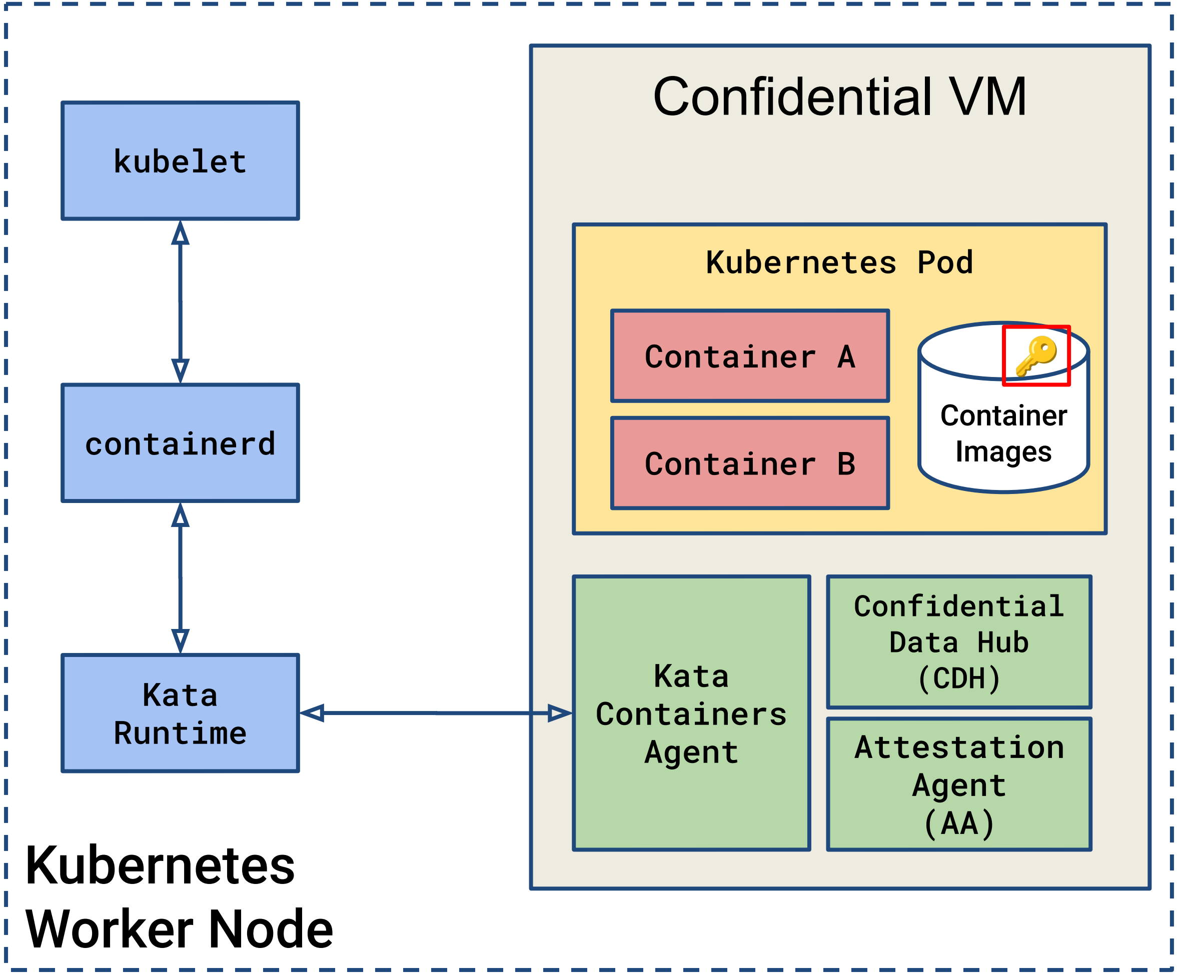
Encrypted or signed container images

# Confidential Containers Architecture



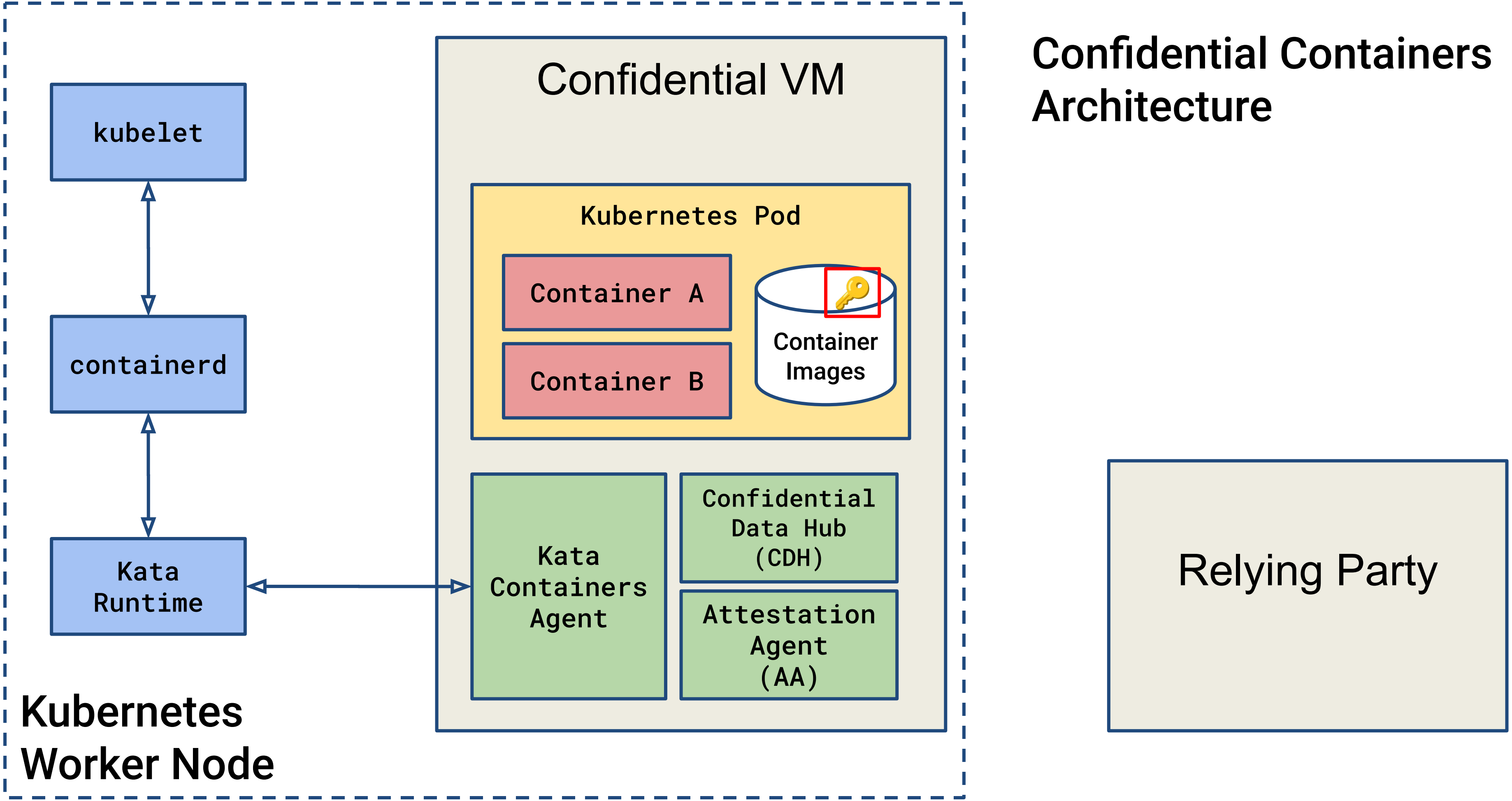
Rivos

# Confidential Containers Architecture



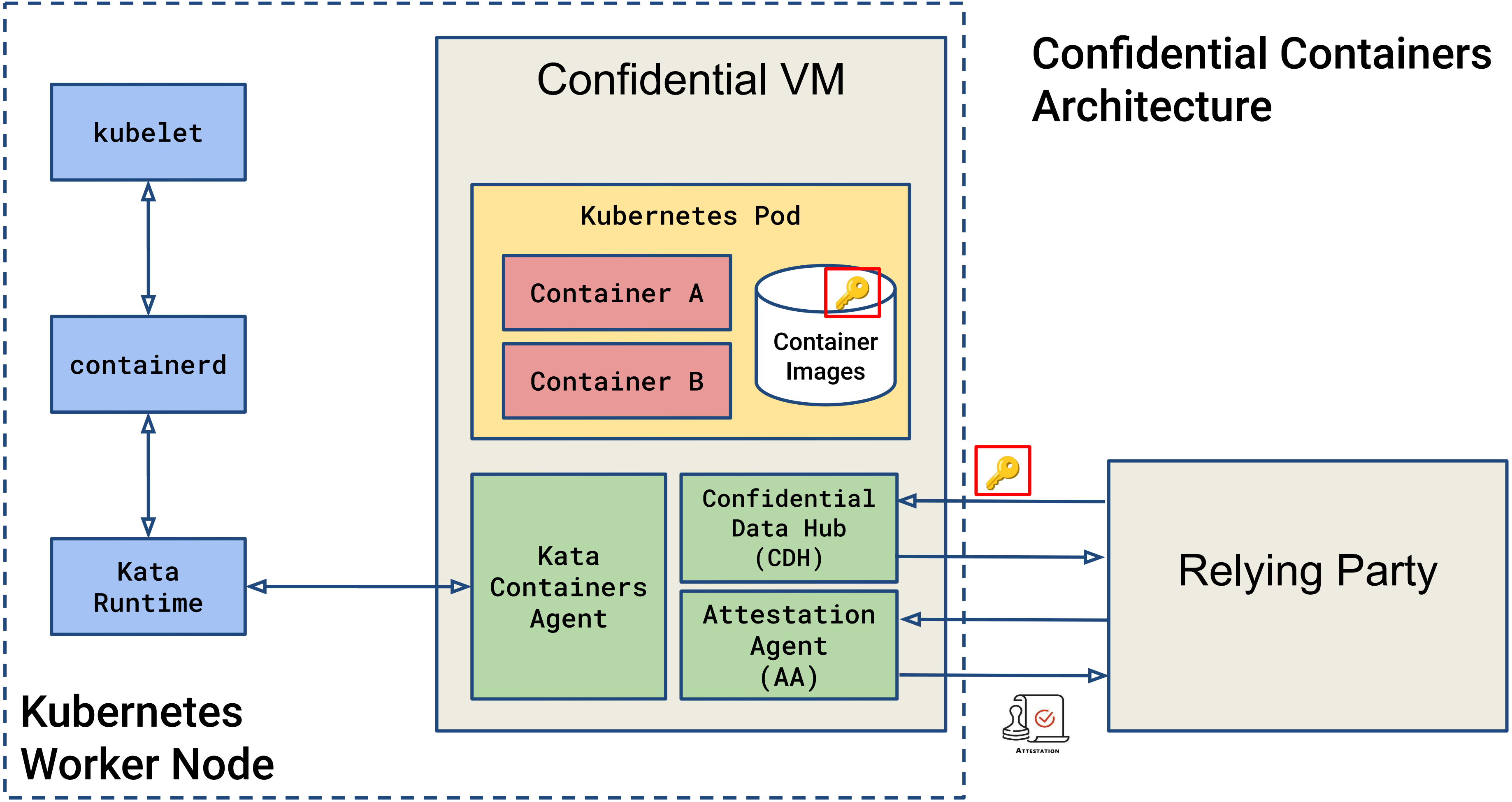
Rivos

# Confidential Containers Architecture



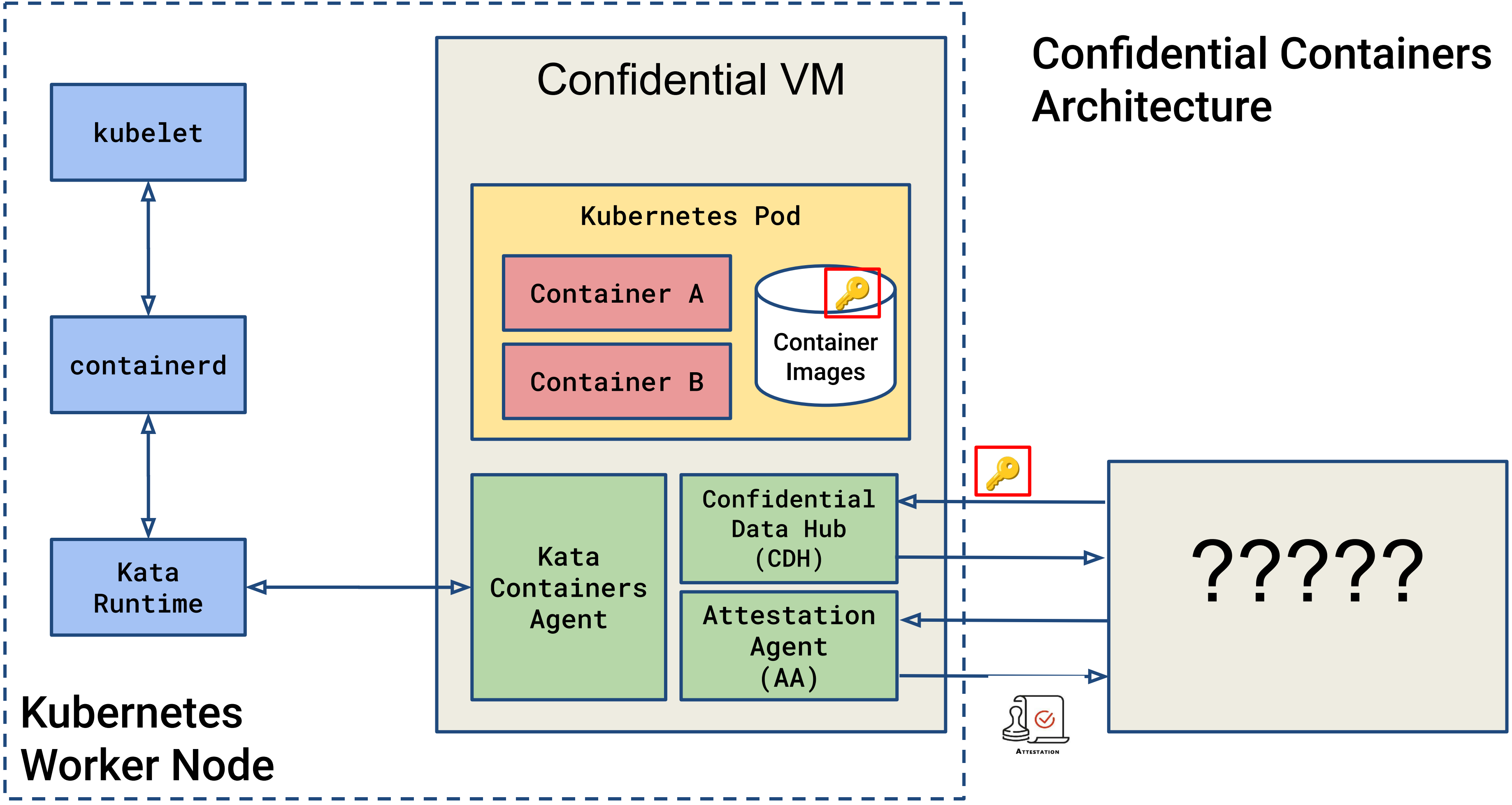
Rivos

# Confidential Containers Architecture



Rivos

# Confidential Containers Architecture



Kubernetes Worker Node

kubelet

containerd

Kata Runtime

Confidential VM

Kubernetes Pod

Container A

Container B

Container Images

Kata Containers Agent

Confidential Data Hub (CDH)

Attestation Agent (AA)

ATTESTATION

?????

# The Elephant in the Room

We’re a bit handwavy about attestation services

# The Elephant in the Room

We’re a bit handwavy about attestation services

What do you do with an attestation evidence?

Who do you send it to?

How do we talk to relying parties?

Will it support my attestation evidence?

What is this attestation result that I might get back?

# Trustee

Under the Confidential Containers project - No dependencies to it

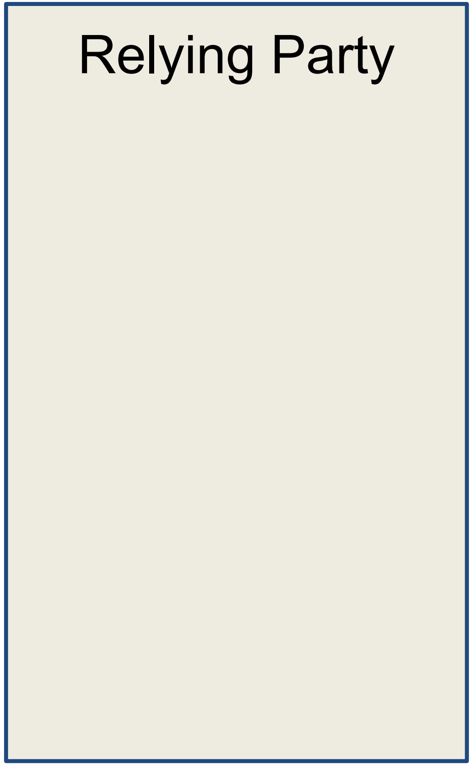
Open source, vendor agnostic attestation service

Simple, open and documented HTTPS-based protocol

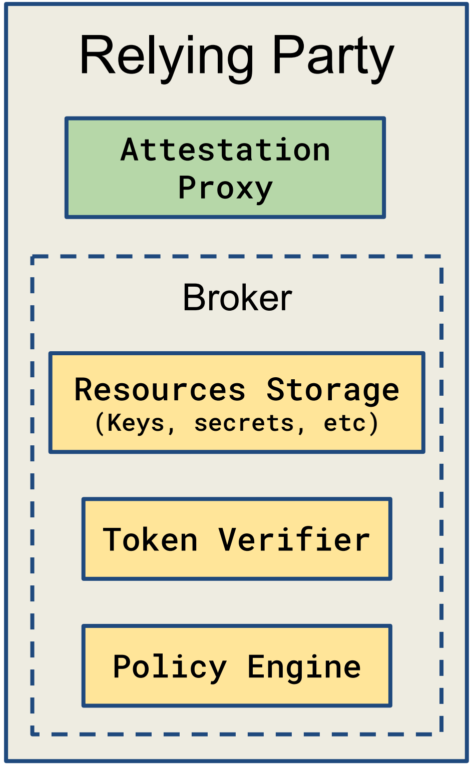
Pluggable architecture

- Support for any vendor generated attestation evidence (SNP, TDX, CCA, etc)
- Support for different verifier backends (CoCo, Veraison, etc)

Open, cloud native format for policies



Relying Party



Relying Party

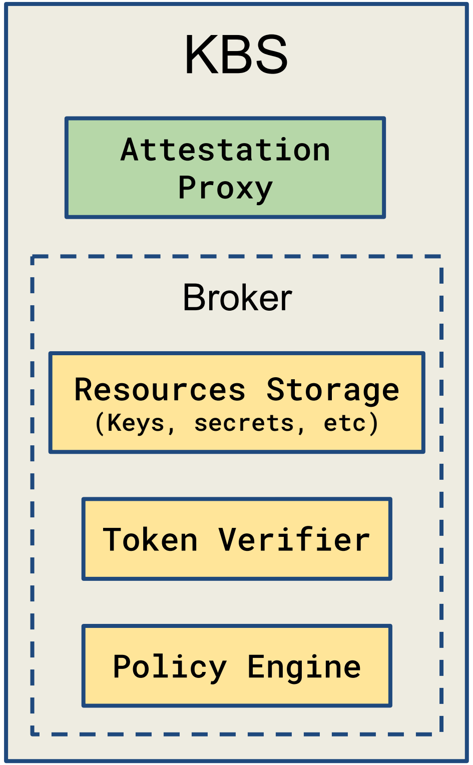
Attestation Proxy

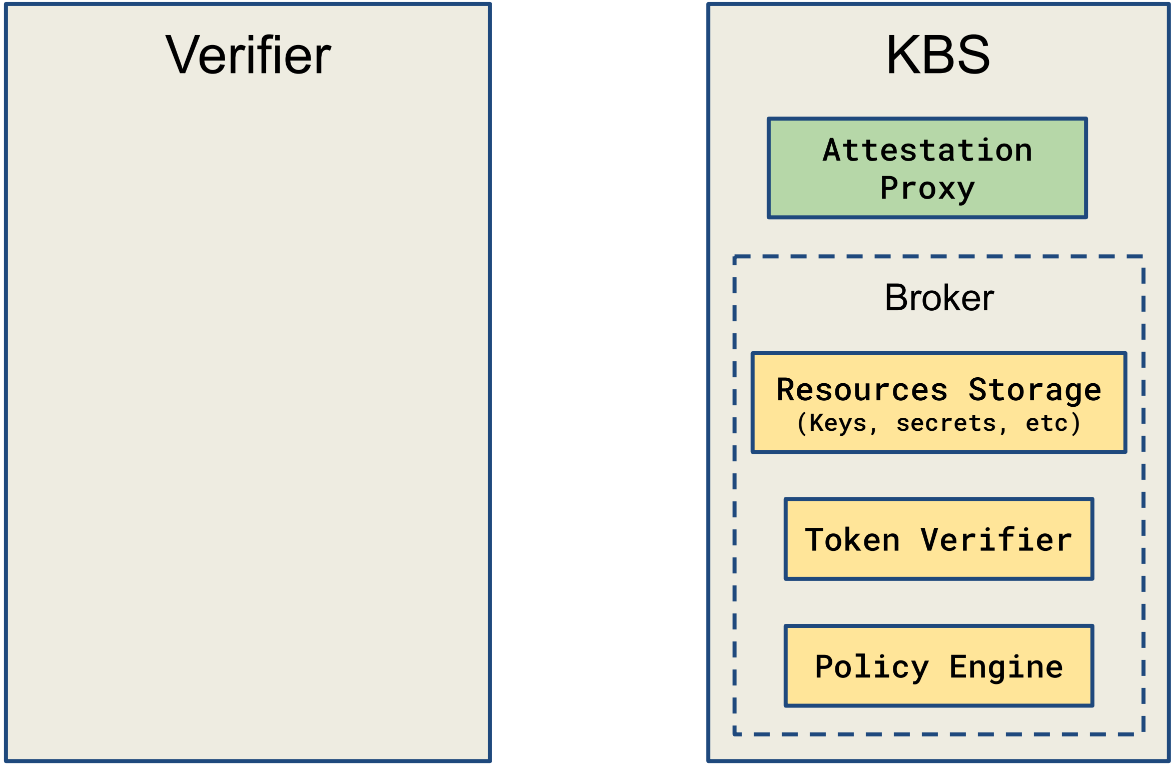
Broker

Resources Storage
(Keys, secrets, etc)

Token Verifier

Policy Engine


KBS
Attestation Proxy
Broker
Resources Storage
(Keys, secrets, etc)
Token Verifier
Policy Engine



Verifier

KBS

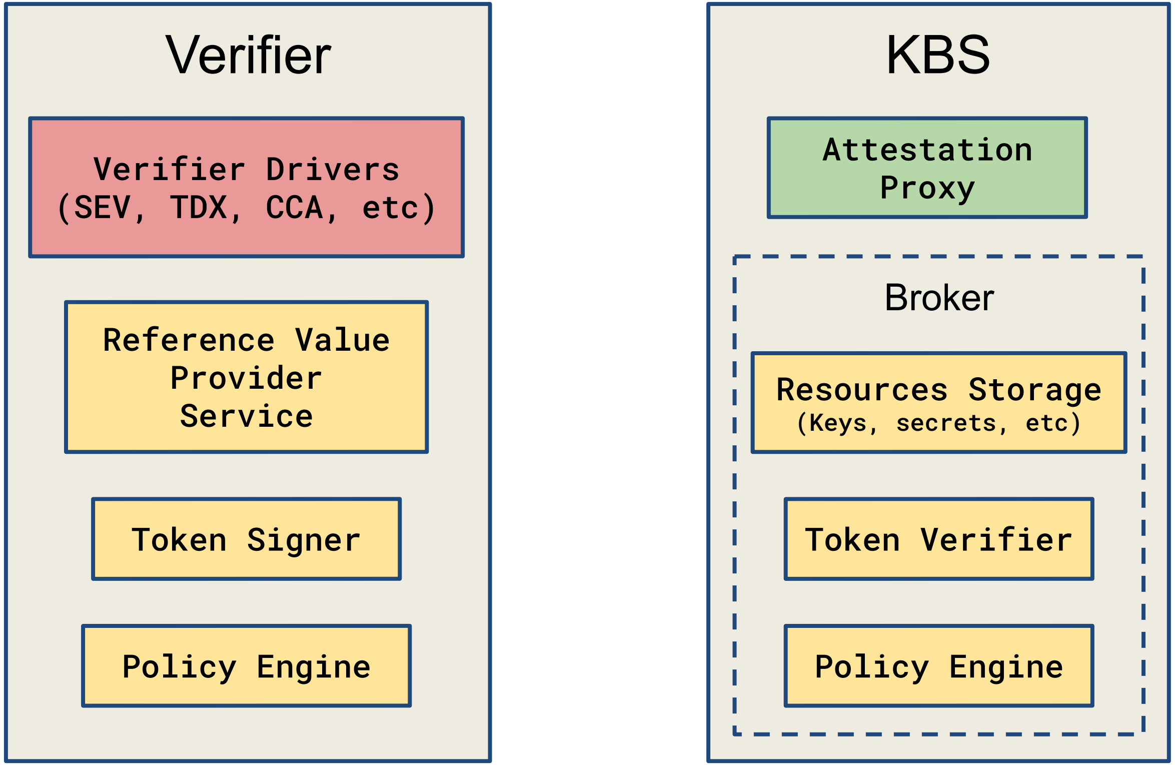
Attestation Proxy

Broker

Resources Storage
(Keys, secrets, etc)

Token Verifier

Policy Engine



Verifier

Verifier Drivers (SEV, TDX, CCA, etc)

Reference Value Provider Service

Token Signer

Policy Engine

KBS

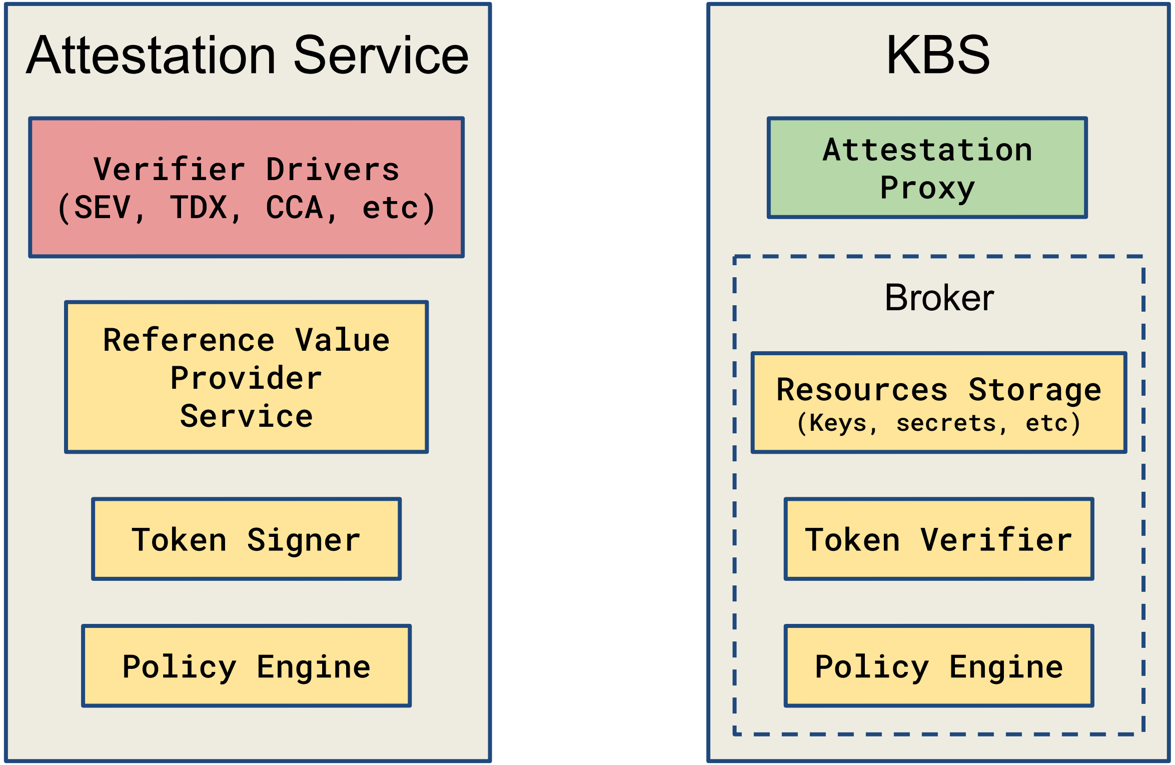
Attestation Proxy

Broker

Resources Storage (Keys, secrets, etc)

Token Verifier

Policy Engine



Attestation Service

Verifier Drivers (SEV, TDX, CCA, etc)

Reference Value Provider Service

Token Signer

Policy Engine

KBS

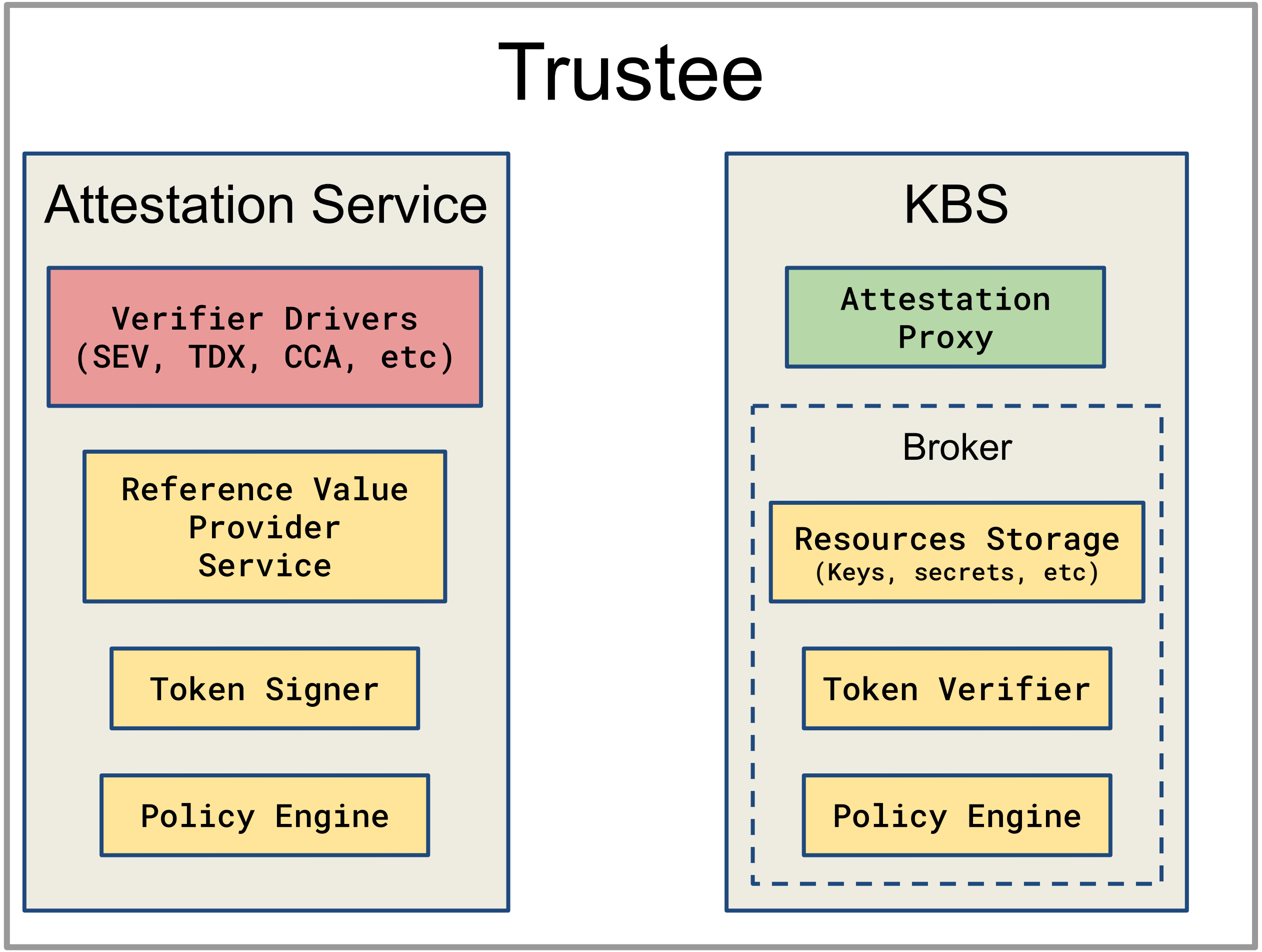
Attestation Proxy

Broker

Resources Storage (Keys, secrets, etc)

Token Verifier

Policy Engine



Trustee

Attestation Service

Verifier Drivers (SEV, TDX, CCA, etc)

Reference Value Provider Service

Token Signer

Policy Engine

KBS

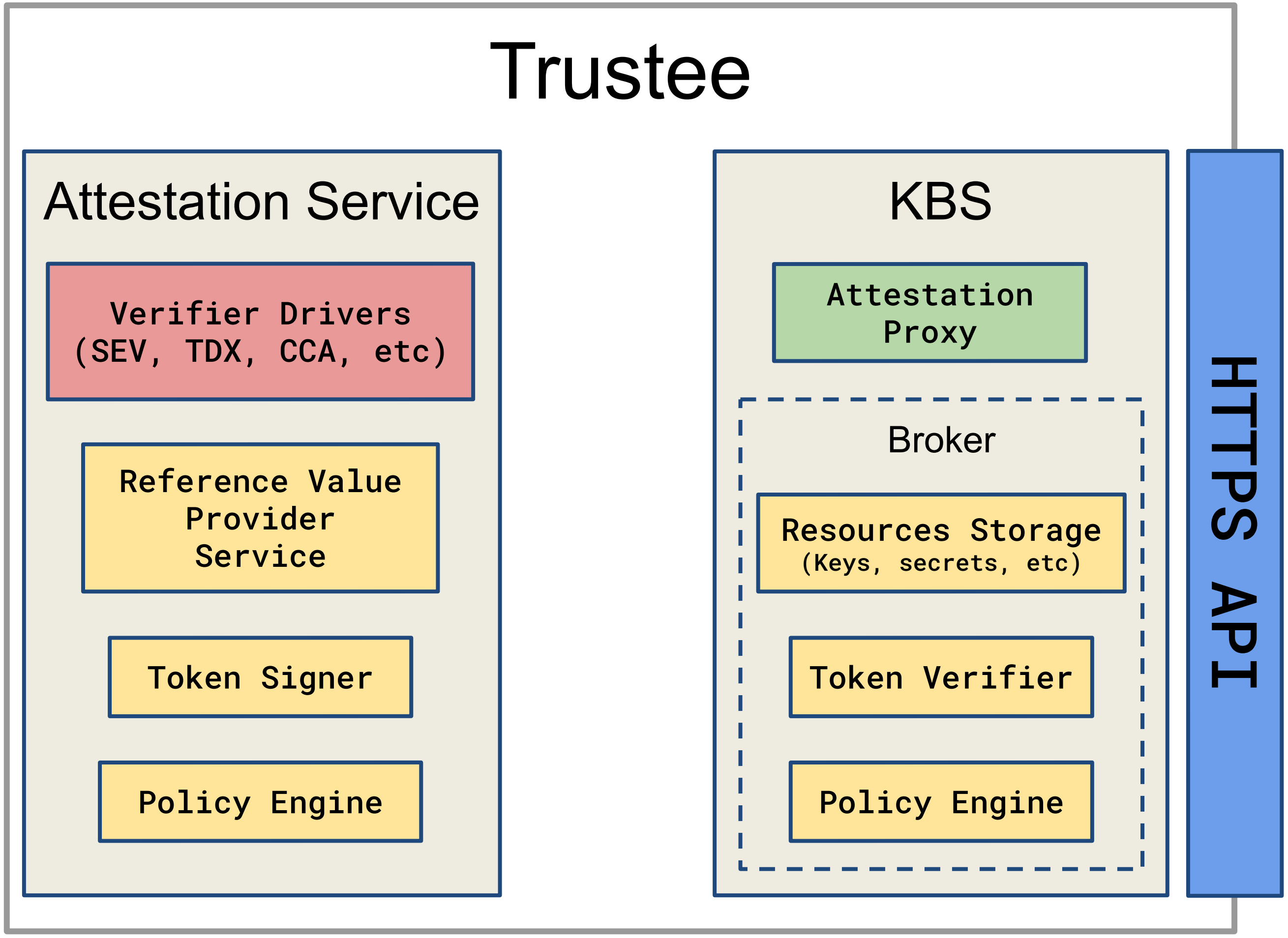
Attestation Proxy

Broker

Resources Storage (Keys, secrets, etc)

Token Verifier

Policy Engine



# Trustee

## Attestation Service

Verifier Drivers
(SEV, TDX, CCA, etc)

Reference Value Provider Service

Token Signer

Policy Engine

## KBS

Attestation Proxy

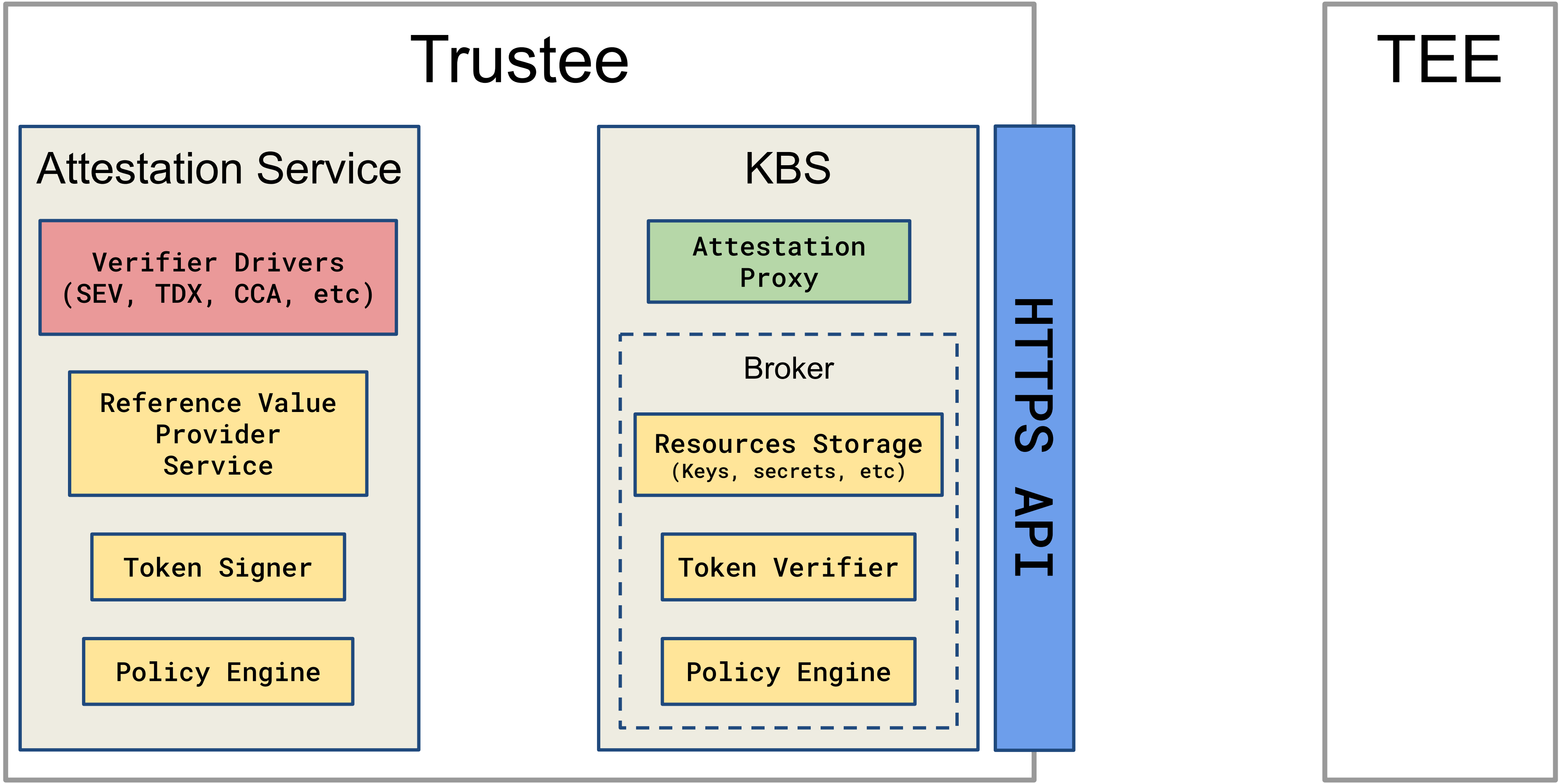
Broker

Resources Storage
(Keys, secrets, etc)

Token Verifier

Policy Engine

HTTPS API



Trustee

Attestation Service

Verifier Drivers (SEV, TDX, CCA, etc)

Reference Value Provider Service

Token Signer

Policy Engine

KBS

Attestation Proxy

Broker

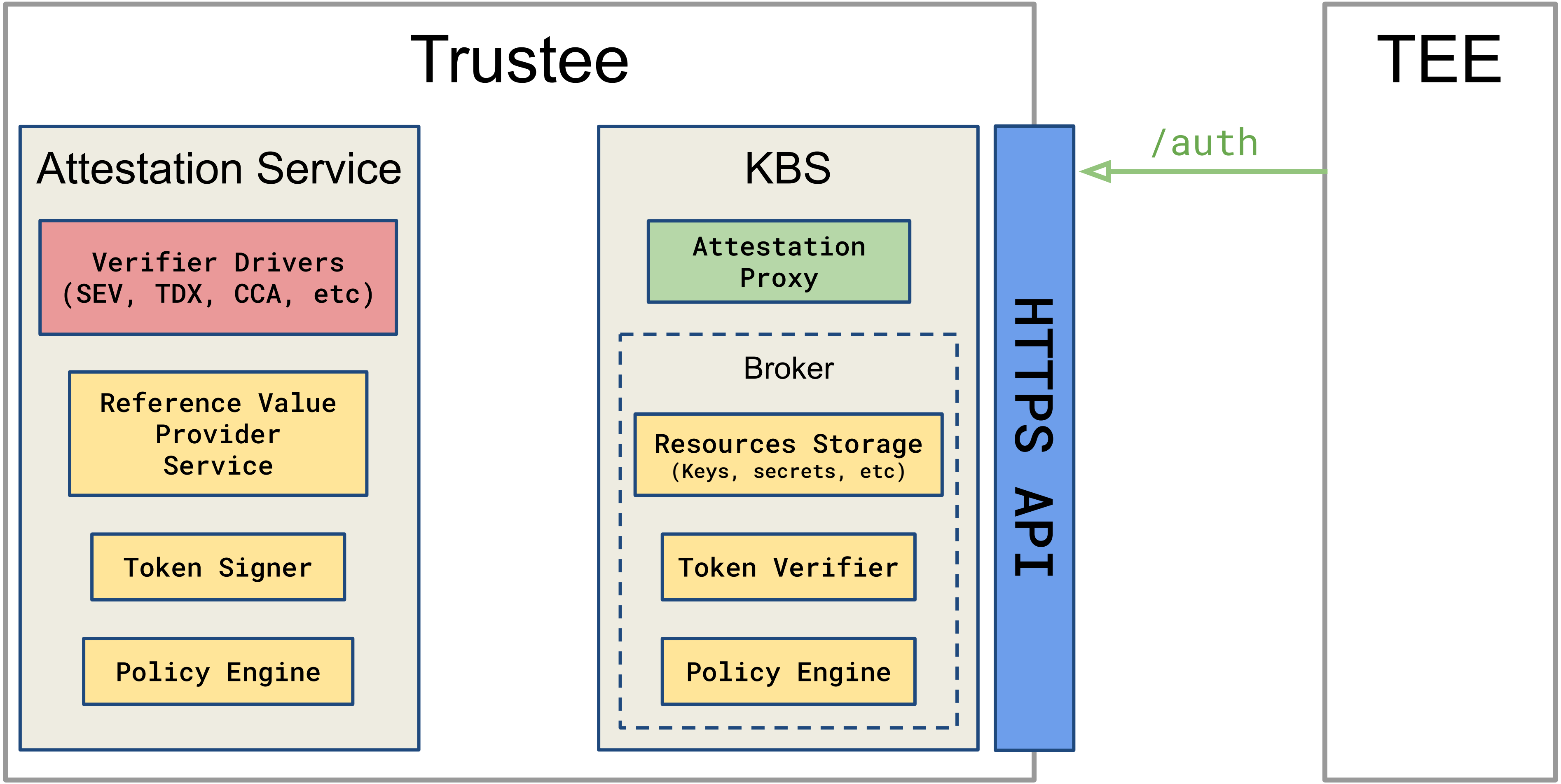
Resources Storage (Keys, secrets, etc)

Token Verifier

Policy Engine

HTTPS API

TEE



Trustee

Attestation Service

Verifier Drivers
(SEV, TDX, CCA, etc)

Reference Value Provider Service

Token Signer

Policy Engine

KBS

Attestation Proxy

Broker

Resources Storage
(Keys, secrets, etc)

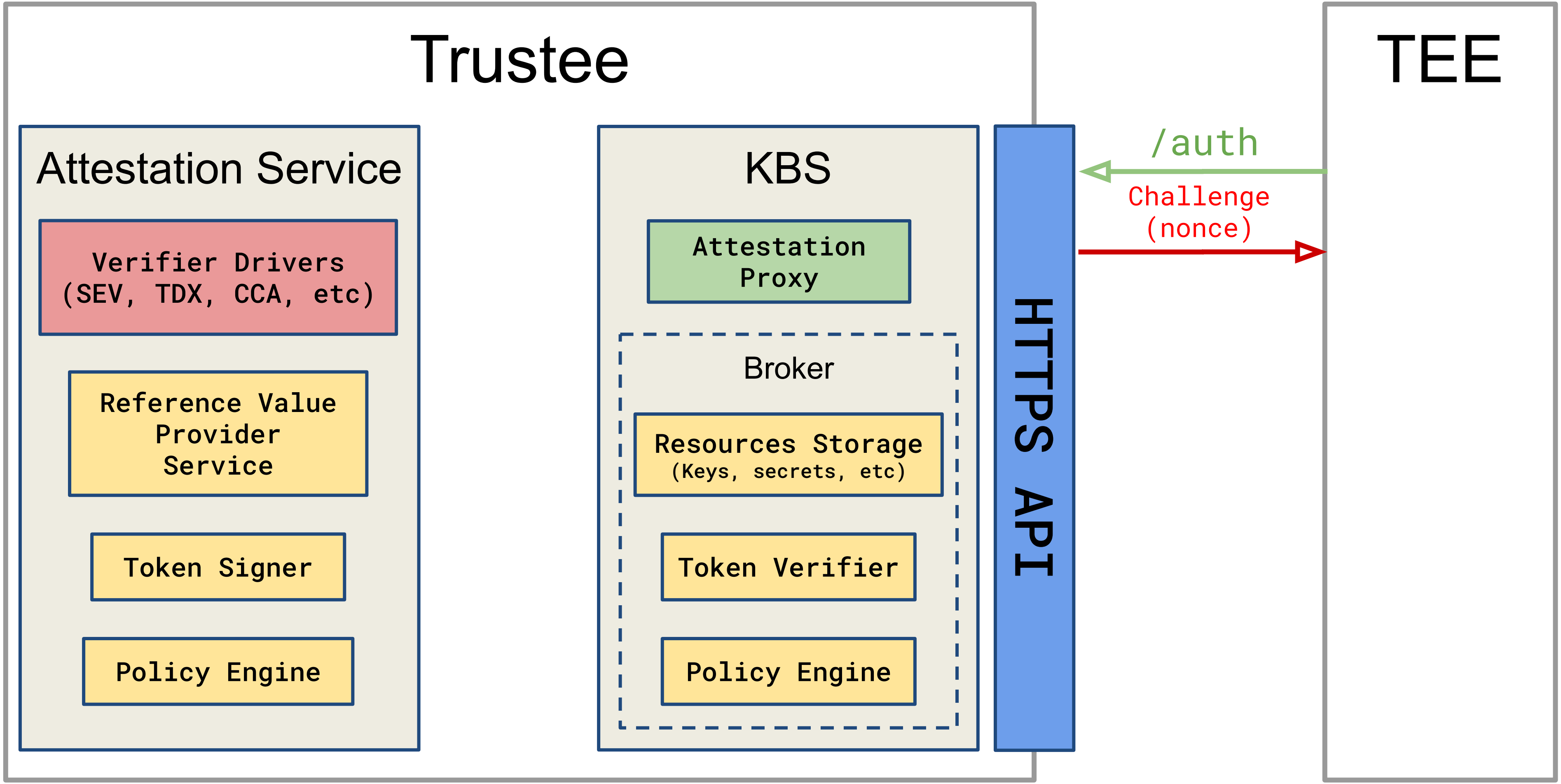
Token Verifier

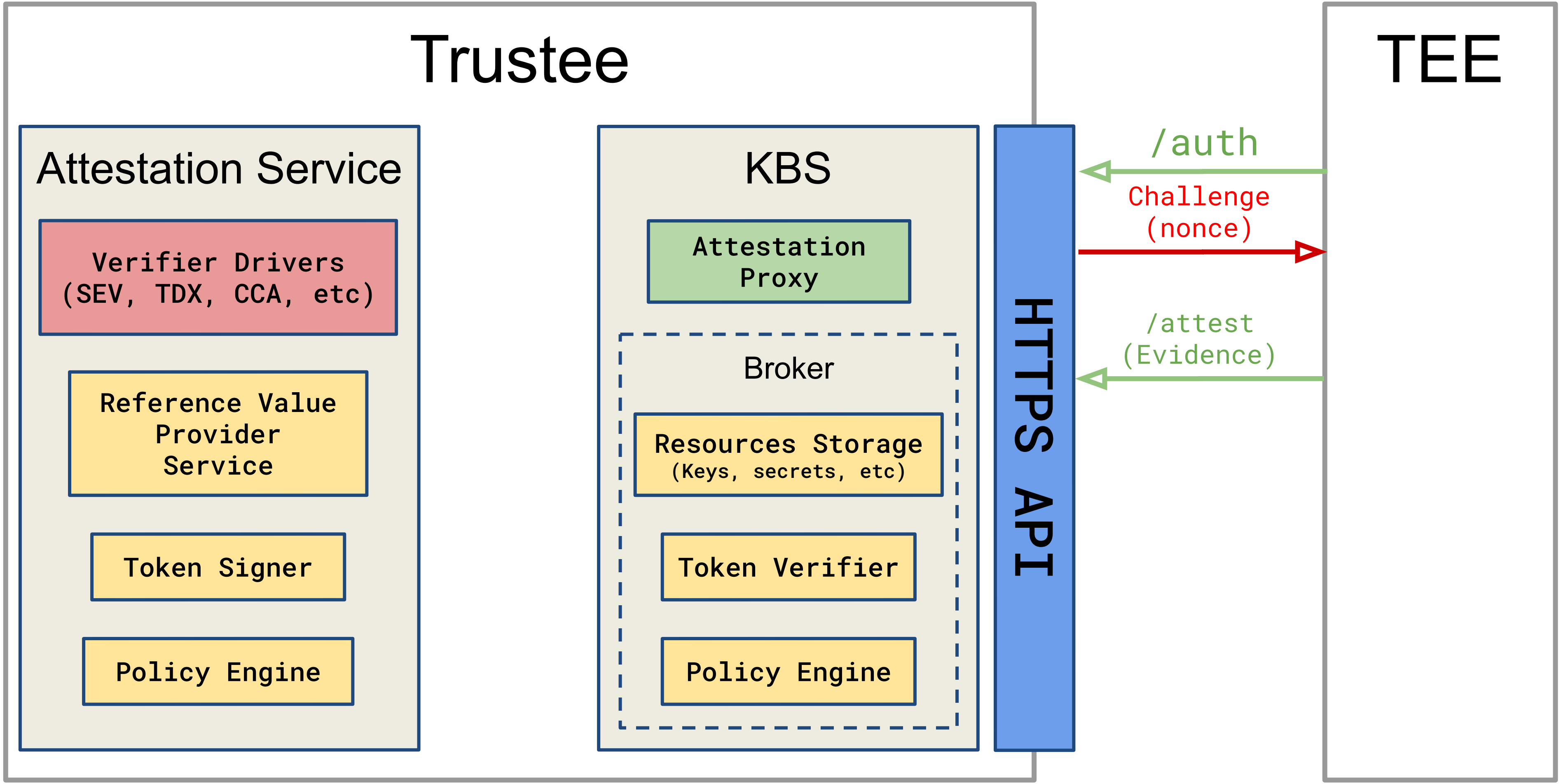
Policy Engine

HTTPS API

/auth

TEE


Trustee
TEE
Attestation Service
Verifier Drivers (SEV, TDX, CCA, etc)
Reference Value Provider Service
Token Signer
Policy Engine
KBS
Attestation Proxy
Broker
Resources Storage (Keys, secrets, etc)
Token Verifier
Policy Engine
HTTPS API
/auth
Challenge (nonce)



Trustee

Attestation Service

Verifier Drivers (SEV, TDX, CCA, etc)

Reference Value Provider Service

Token Signer

Policy Engine

KBS

Attestation Proxy

Broker

Resources Storage (Keys, secrets, etc)

Token Verifier

Policy Engine

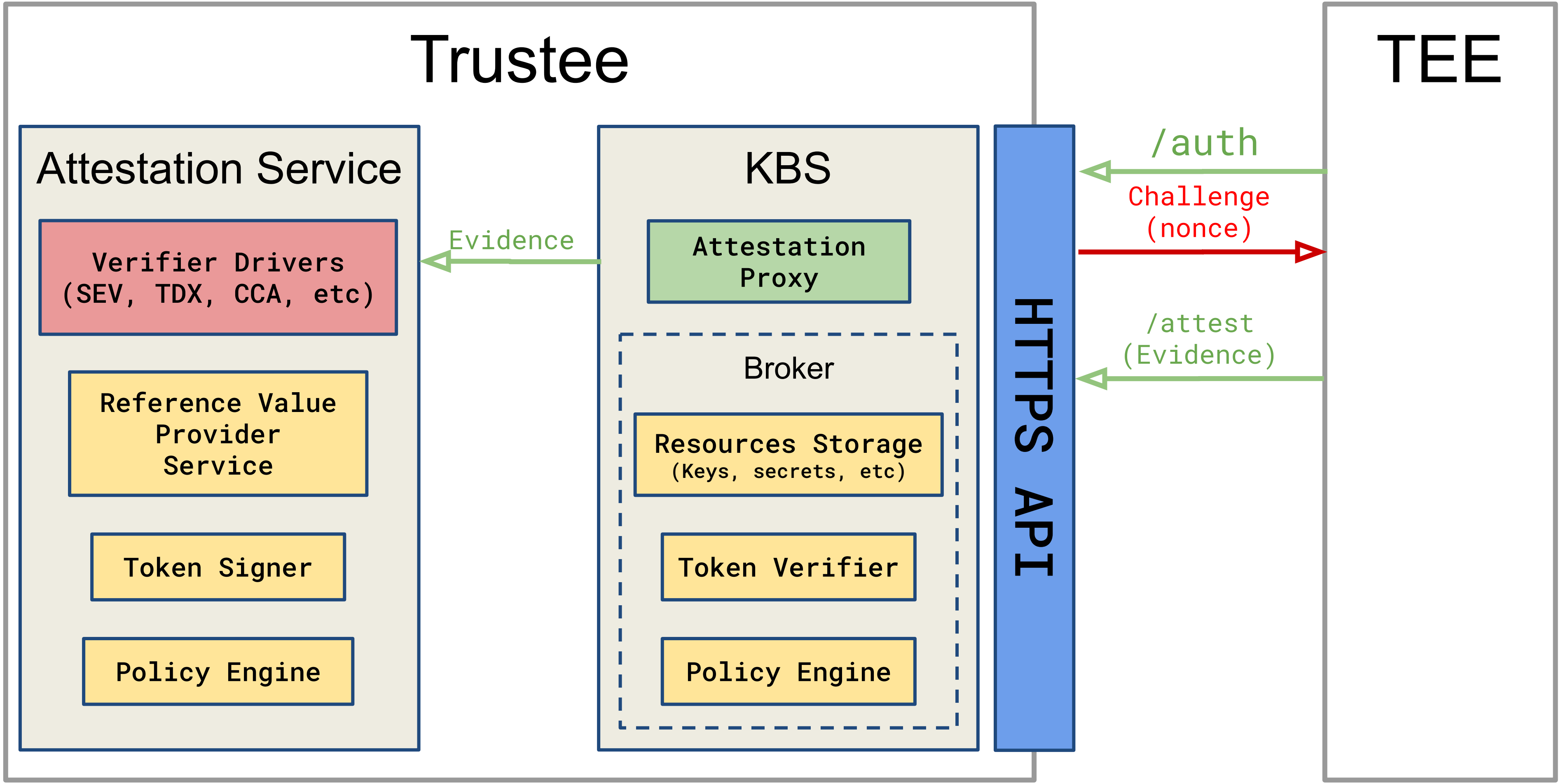
HTTPS API

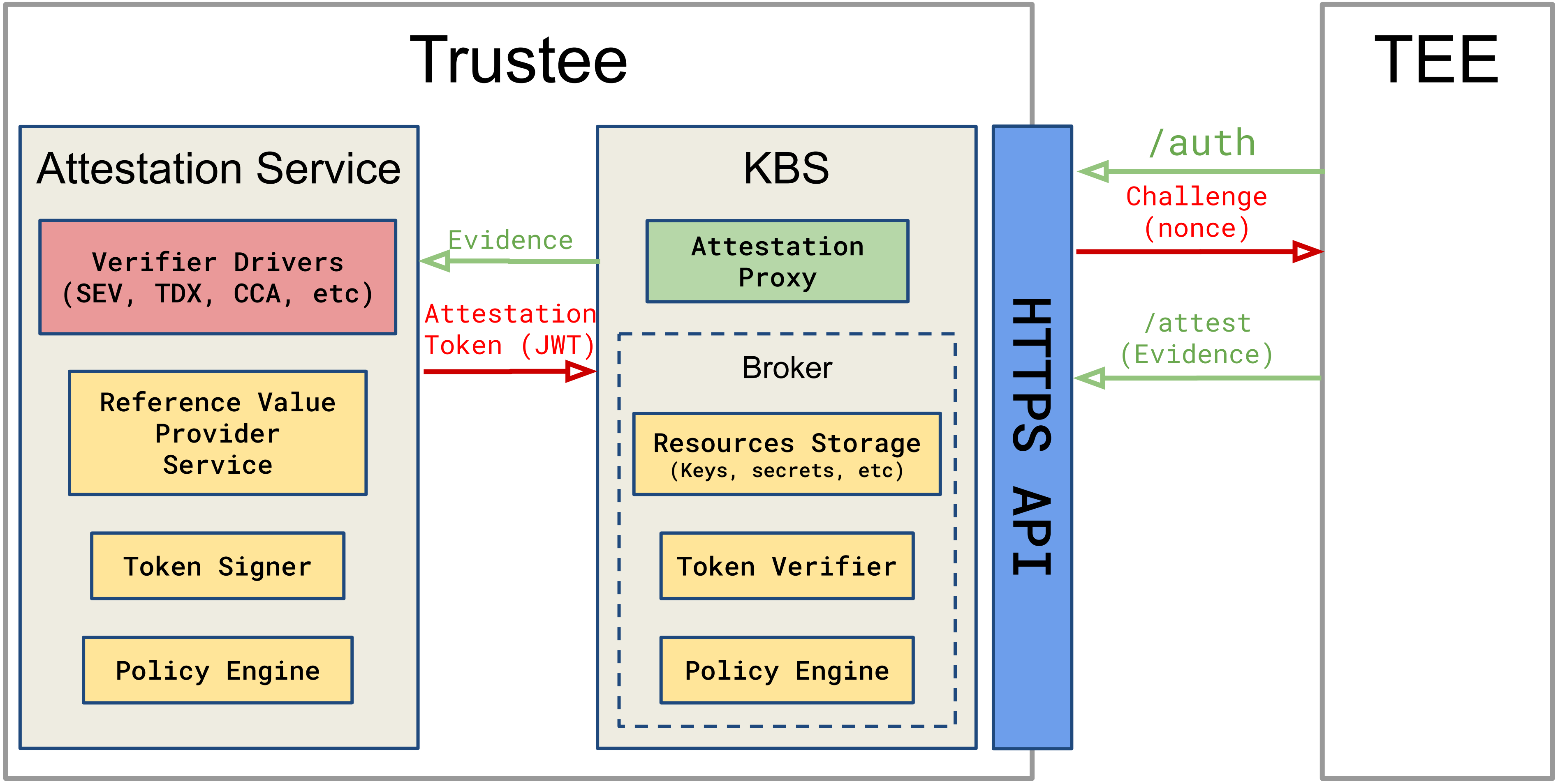
/auth

Challenge (nonce)

/attest (Evidence)

TEE


Trustee
TEE
Attestation Service
Verifier Drivers
(SEV, TDX, CCA, etc)
Reference Value
Provider
Service
Token Signer
Policy Engine
Evidence
KBS
Attestation
Proxy
Broker
Resources Storage
(Keys, secrets, etc)
Token Verifier
Policy Engine
HTTPS API
/auth
Challenge
(nonce)
/attest
(Evidence)



Trustee

TEE

Attestation Service

Verifier Drivers (SEV, TDX, CCA, etc)

Reference Value Provider Service

Token Signer

Policy Engine

Evidence

Attestation Token (JWT)

KBS

Attestation Proxy

Broker

Resources Storage (Keys, secrets, etc)

Token Verifier

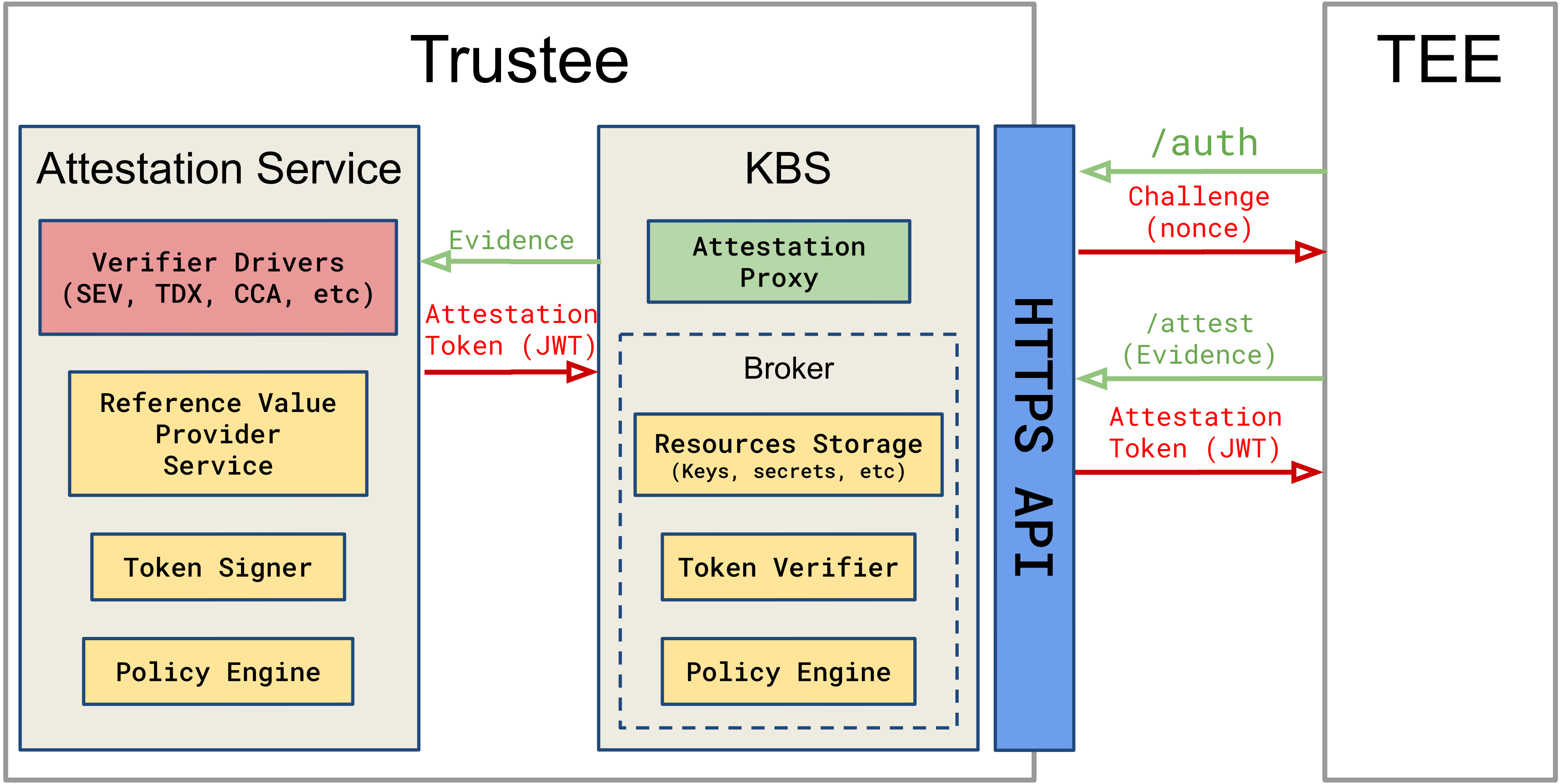
Policy Engine

HTTPS API

/auth

Challenge (nonce)

/attest (Evidence)



Trustee

TEE

Attestation Service

Verifier Drivers
(SEV, TDX, CCA, etc)

Reference Value Provider Service

Token Signer

Policy Engine

Evidence

Attestation Token (JWT)

KBS

Attestation Proxy

Broker

Resources Storage
(Keys, secrets, etc)

Token Verifier

Policy Engine

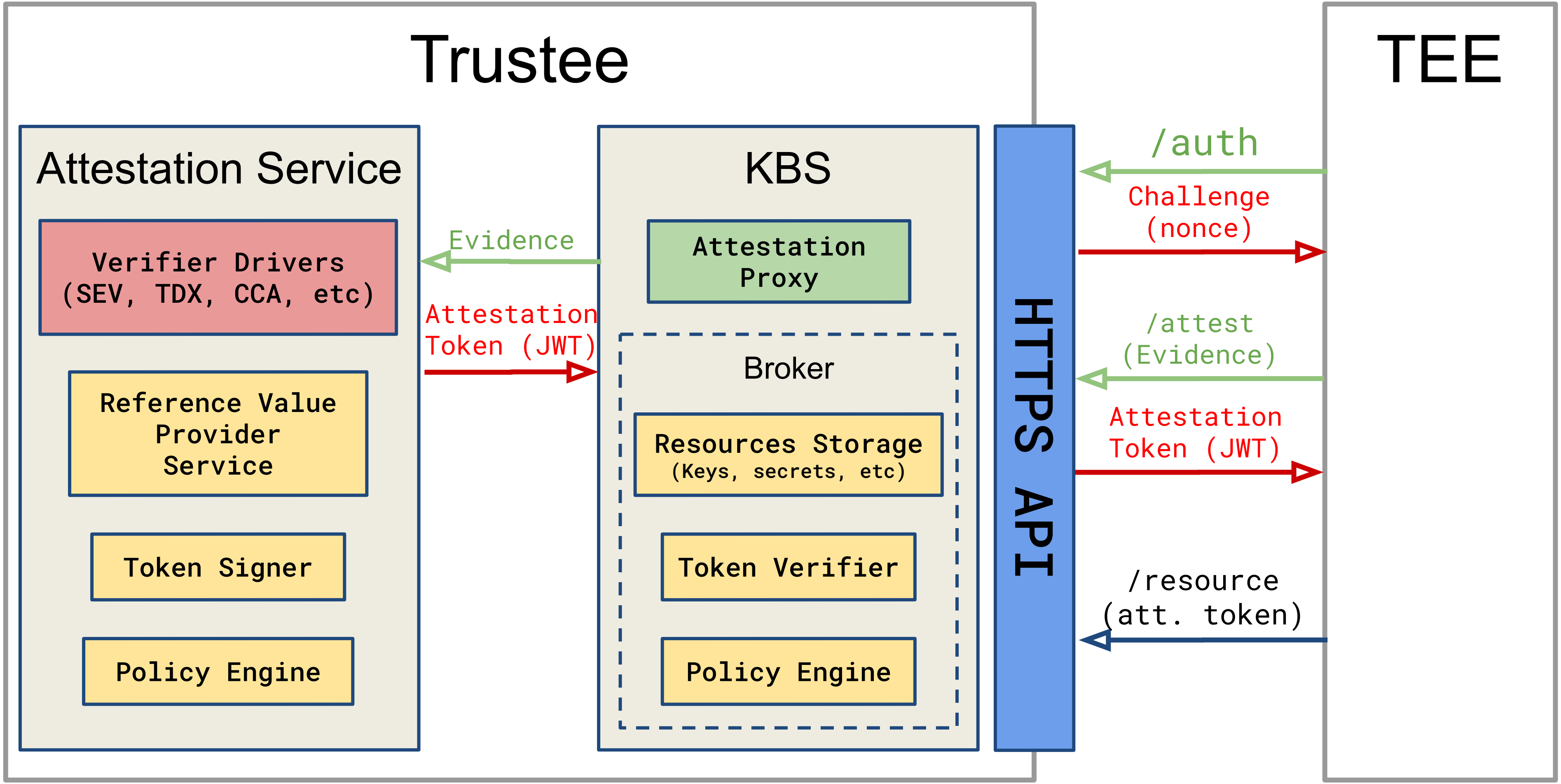
HTTPS API

/auth

Challenge (nonce)

/attest (Evidence)

Attestation Token (JWT)



Trustee

TEE

Attestation Service

Verifier Drivers
(SEV, TDX, CCA, etc)

Reference Value
Provider
Service

Token Signer

Policy Engine

Evidence

Attestation
Token (JWT)

KBS

Attestation
Proxy

Broker

Resources Storage
(Keys, secrets, etc)

Token Verifier

Policy Engine

HTTPS API

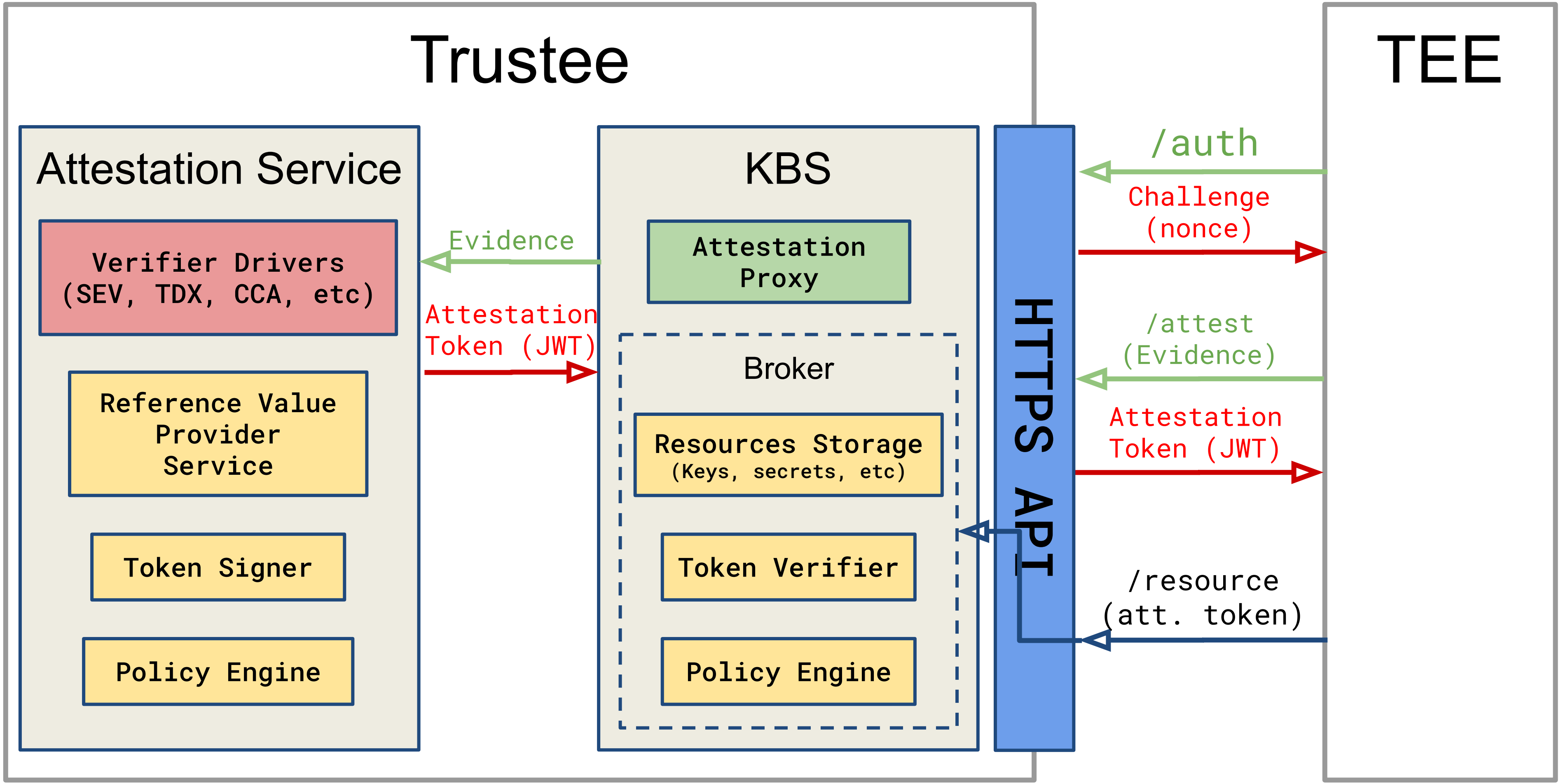
/auth

Challenge
(nonce)

/attest
(Evidence)

Attestation
Token (JWT)

/resource
(att. token)



Trustee

Attestation Service

Verifier Drivers (SEV, TDX, CCA, etc)

Reference Value Provider Service

Token Signer

Policy Engine

Evidence

Attestation Token (JWT)

KBS

Attestation Proxy

Broker

Resources Storage (Keys, secrets, etc)

Token Verifier

Policy Engine

HTTPS API

/auth

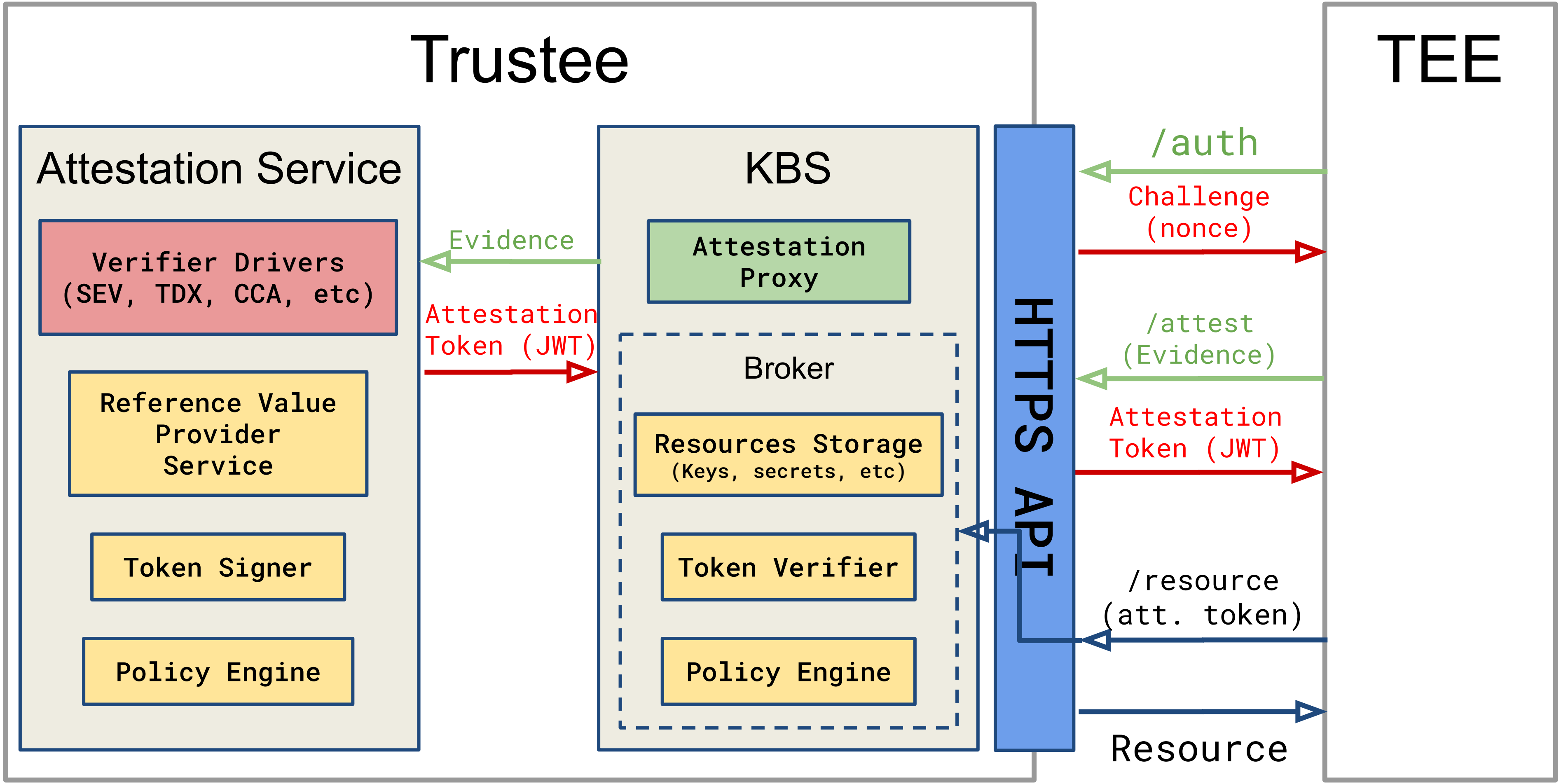
Challenge (nonce)

/attest (Evidence)

Attestation Token (JWT)

/resource (att. token)

TEE



Trustee

TEE

Attestation Service

Verifier Drivers (SEV, TDX, CCA, etc)

Reference Value Provider Service

Token Signer

Policy Engine

Evidence

Attestation Token (JWT)

KBS

Attestation Proxy

Broker

Resources Storage (Keys, secrets, etc)

Token Verifier

Policy Engine

HTTPS API

/auth

Challenge (nonce)

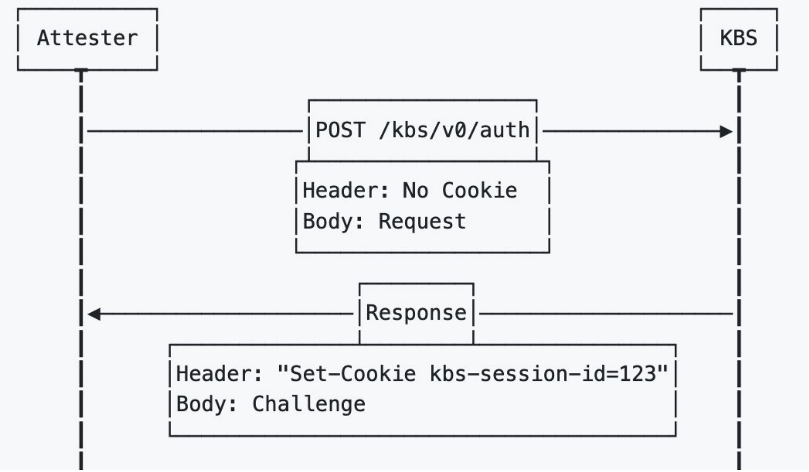
/attest (Evidence)

Attestation Token (JWT)

/resource (att. token)

Resource

# Attestation Protocol - POST /auth



## TEE Request (Request Payload)

Protocol version

Optional extra params

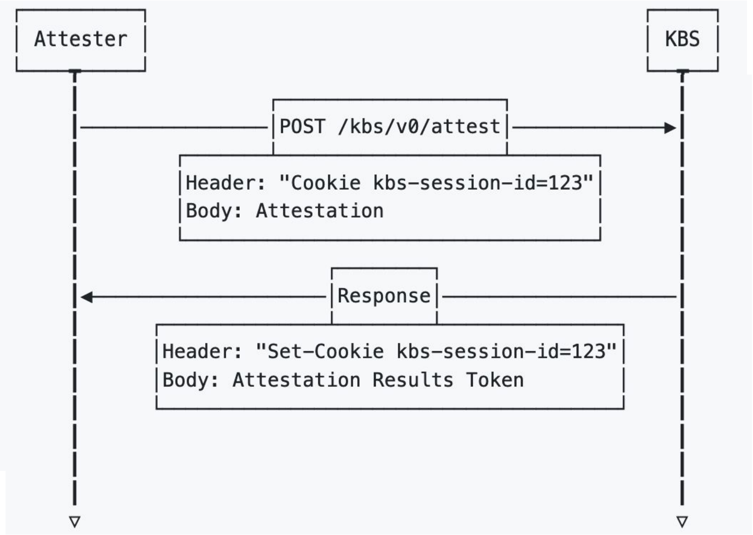
## KBS Response (Challenge Payload)

Attestation challenge

- Nonce

HTTP Cookie session identifier

# Attestation Protocol - POST /attest



Header: "Cookie kbs-session-id=123"
Body: Attestation

Header: "Set-Cookie kbs-session-id=123"
Body: Attestation Results Token

## TEE Request (Attestation Payload)

**Ephemeral public key (tee_pubkey)**

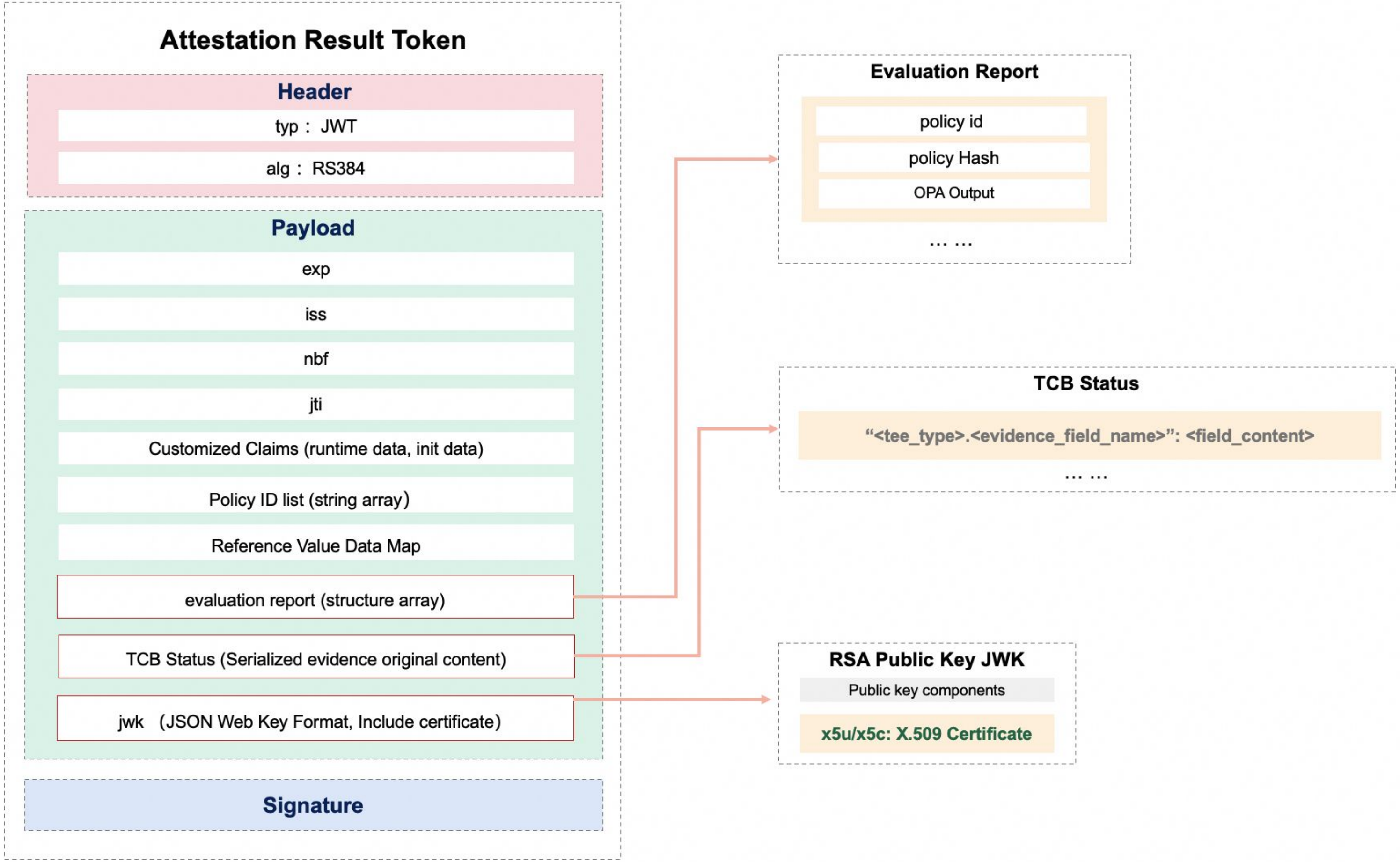
**Attestation Evidence (nonced)**

## KBS Response (Attestation Token Payload)

**JWT**

- Registered and custom claims
- Custom claims
    - Attestation evaluation
    - AS endorsed key

# Trustee Attestation Token



### Attestation Result Token

**Header**

typ : JWT

alg : RS384

**Payload**

exp

iss

nbf

jti

Customized Claims (runtime data, init data)

Policy ID list (string array)

Reference Value Data Map

evaluation report (structure array)

TCB Status (Serialized evidence original content)

jwk (JSON Web Key Format, Include certificate)

**Signature**

### Evaluation Report

policy id

policy Hash

OPA Output

… …

### TCB Status

“<tee_type>.<evidence_field_name>”: <field_content>

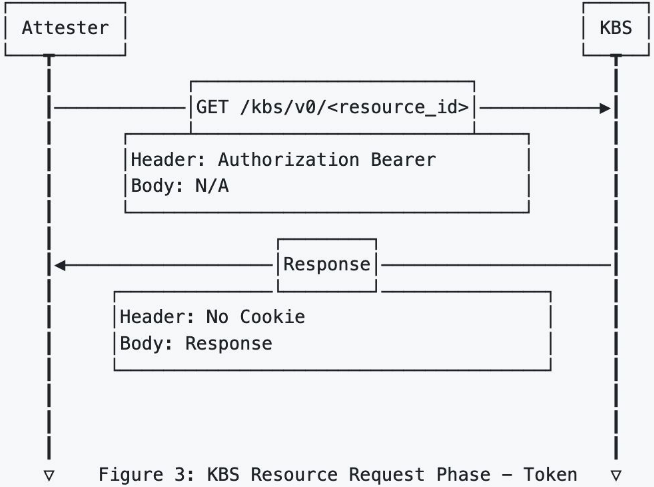
… …

### RSA Public Key JWK

Public key components

x5u/x5c: X.509 Certificate

# Attestation Protocol - GET `/resource`



Attester

KBS

GET /kbs/v0/<resource_id>

Header: Authorization Bearer
Body: N/A

Response

Header: No Cookie
Body: Response

Figure 3: KBS Resource Request Phase – Token

## TEE Request (No Payload)

**HTTP Authorization Bearer**

Attestation Results token

## KBS Response (Response Payload)

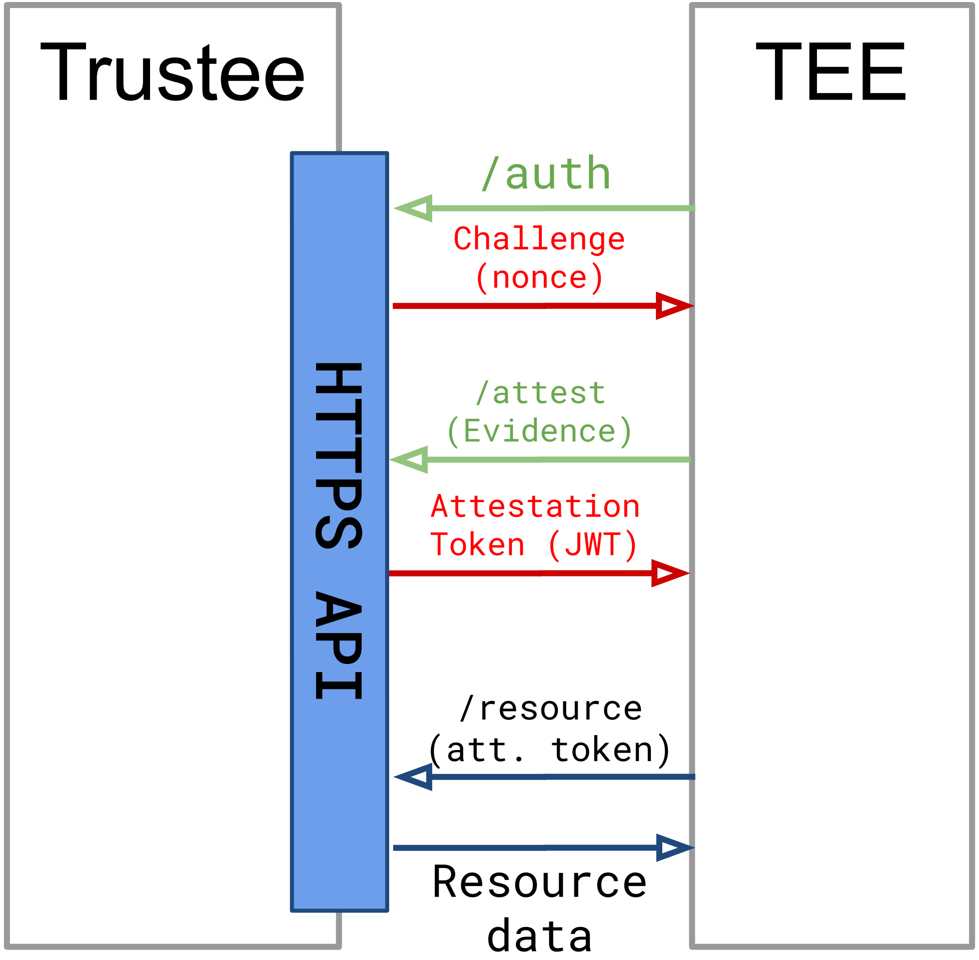
**JWE**

Ciphertext (Resource)
Encrypted key (with the tee_pubkey)

# Background Check

Trustee is the Relying Party

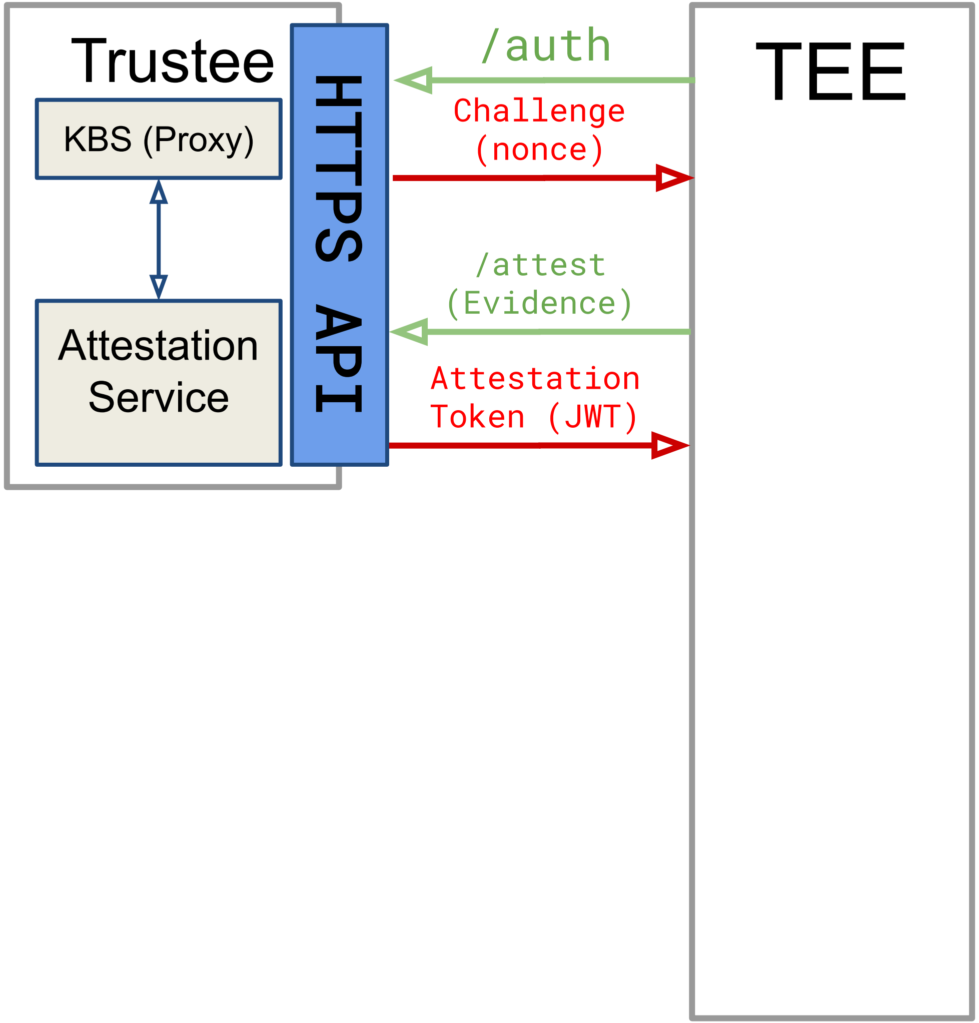
Trustee is the Verifier



# Passport

## Verifier

- KBS is a simple proxy
- TEE gets an attestation token



# Passport

## Verifier

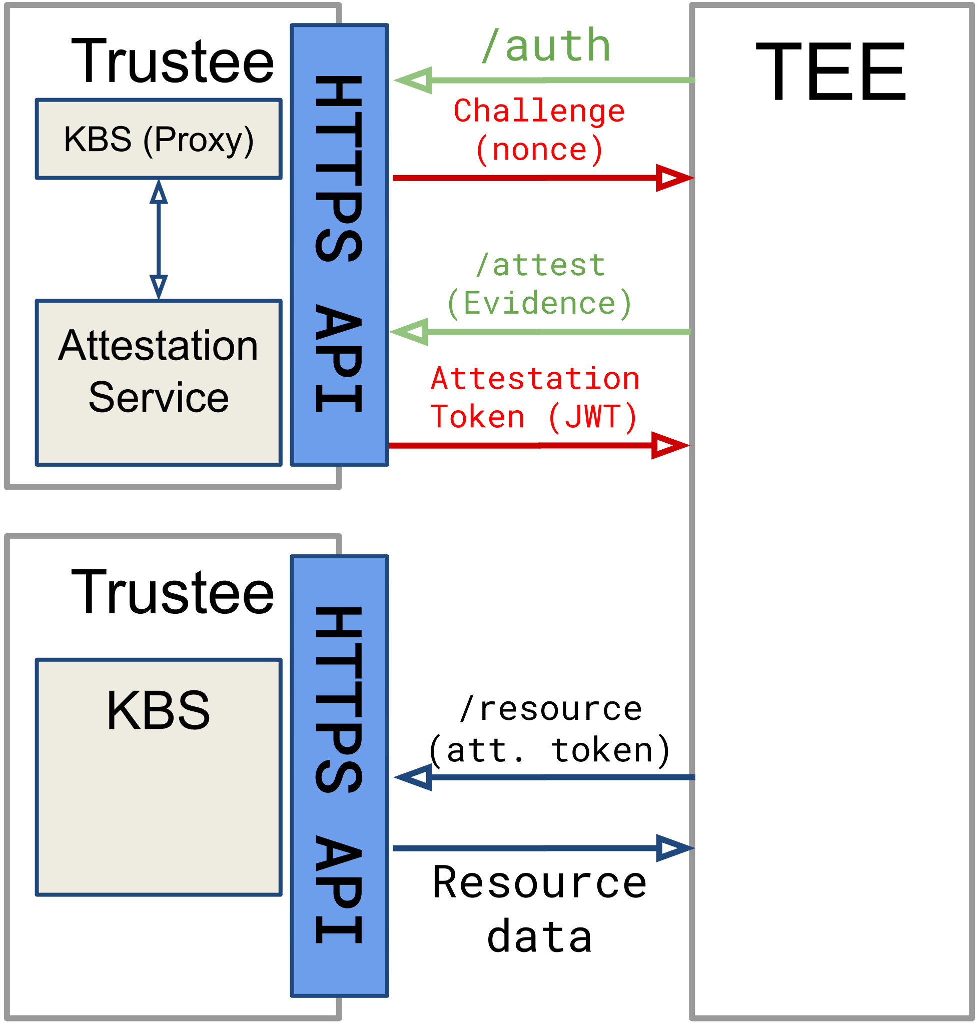
KBS is a simple proxy

TEE gets an attestation token

## Relying Party

KBS verifies the attestation result

KBS releases resources/secrets



# Opens

Reference Values provisioning

Attestation token format

InitData

# References

Trustee

Attestation Protocol

Trustee Verifier Framework