LIGHTNING TALK

Introduction to Project Veraison

Attestation Verification Components

Veraison: **VER**ific**A**t**I**on of atte**S**tati**ON**

Yogesh Deshpande, Principal Engineer, Arm
yogesh.deshpande@arm.com

https://github.com/veraison

VERAISON

Setting the scene:

- There are many scenarios when a user or a relying party needs to establish

  ➔ A machine's identity

  ➔ Whether the firmware or software running on it is 'trustworthy' ?

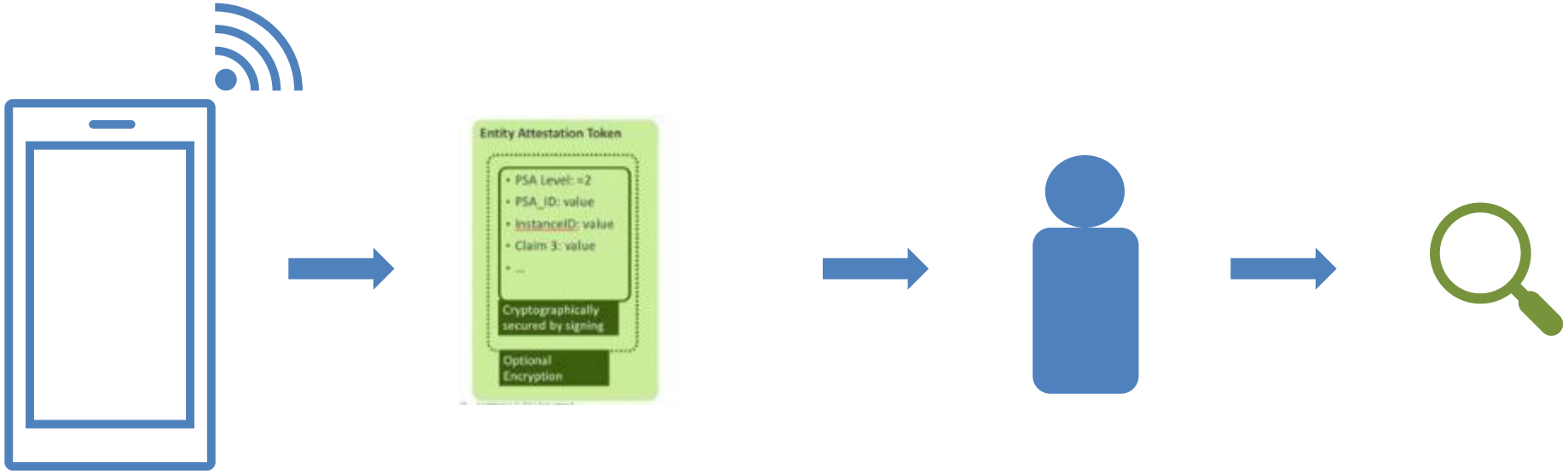
  ➔ Operating Environment is trustworthy ?

  - Enrolment – Device desiring access to network
  - Ascertain Platform state – Prior to end-to-end communication
  - Release valuable resource to an operating environment
  - Many more such use cases

VERAISON

Attestation

- A means to establishing the trustworthiness of a TEE
- Entity produces a signed Evidence (attestation report)
- Attestation report alone is insufficient
  - ➢ Must be verified by a trusted service
  - ➢ Verification is at the centre of any attestation flow



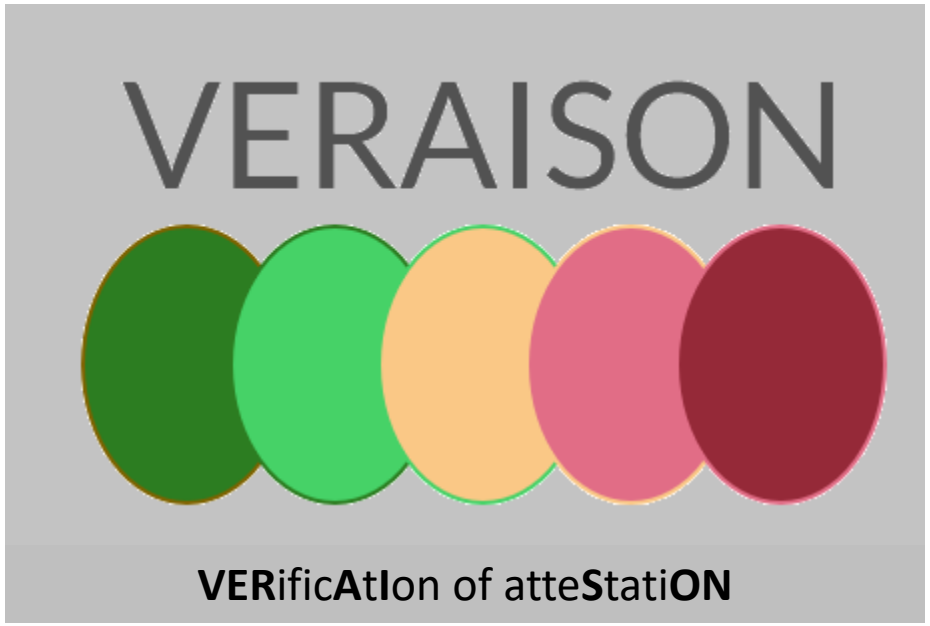
VERAISON

Building Attestation Verification Service

Challenges:

- Due to specific needs of deployments, it is difficult for a single offering to serve all use cases
  - required business relationships
  - regulation / compliance / geo-specifics
- If Verifiers have to be custom, then
  - standardisation and quality levels suffer between deployments
  - the cost of building a trustworthy infrastructure becomes a notable barrier to entry
- Solution:
  - make common components that enables building Verification Services straight forward

VERAISON



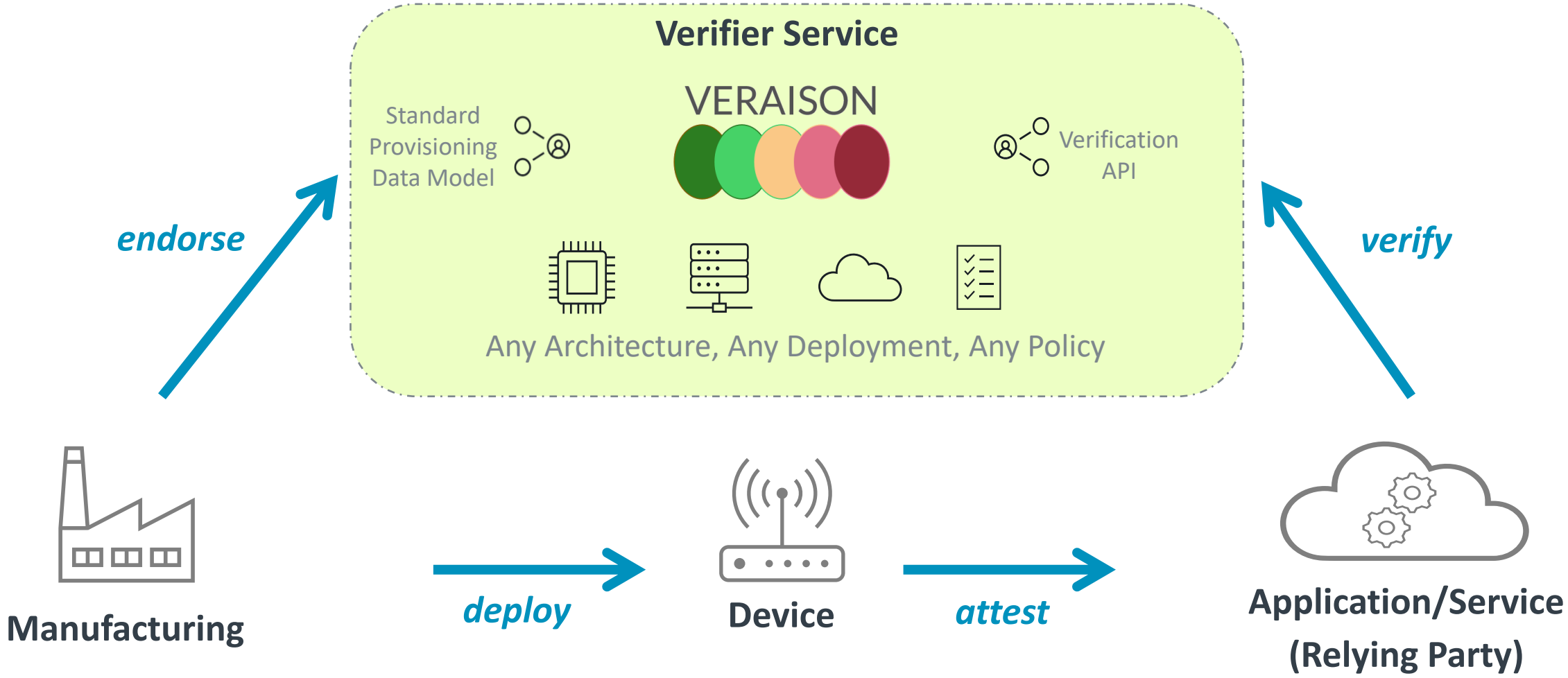
https://github.com/veraison/

Project Veraison

- **VER**ific**A**t**I**on of atte**S**tati**ON**
- Open Source (Apache v2.0) & Open Governance
- Collection of libraries and tools for implementing a remote attestation verification service
- A Confidential Computing Consortium project
- Industry wide scope
- Community Participation from multiple organizations
- Reference Docker deployment

VERAISON

Endorse, Attest, Verify

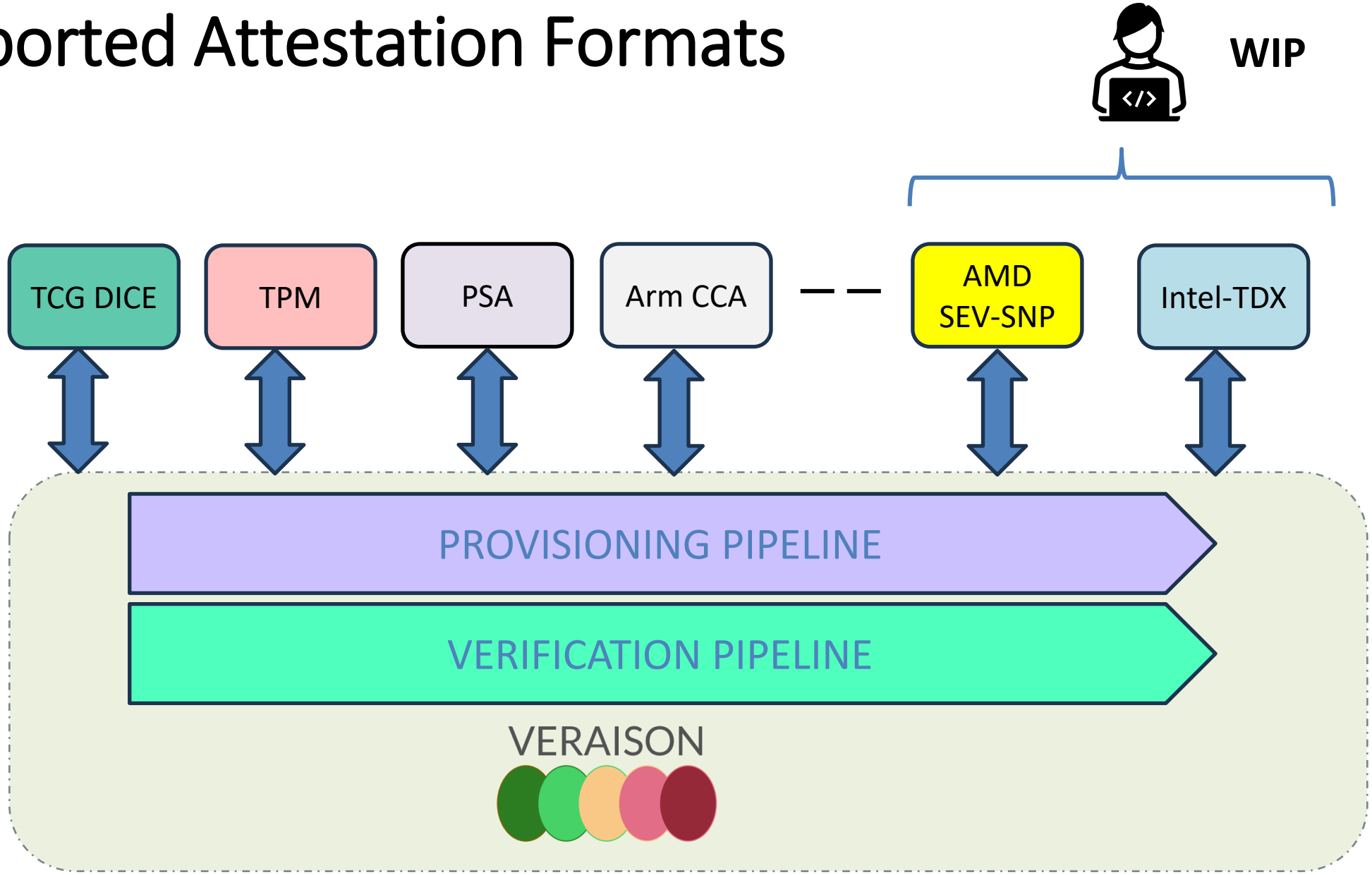


Design Highlights

- Model supply chain interaction with Verifier
- Flexible deployment models
  - Public, private, hybrid, multi cloud service
  - Single or multiple tenants
  - Potential to deploy `locally' e.g. in adjacent isolation such as Trust Zone
- Industry standards used where possible
  - IETF RATS (RFC 9334) Architecture & Information model
  - TCG DICE Endorsement data format working group
- API Driven
- Policy driven and Extensible via Plugins

VERAISON

Supported Attestation Formats



VERAISON

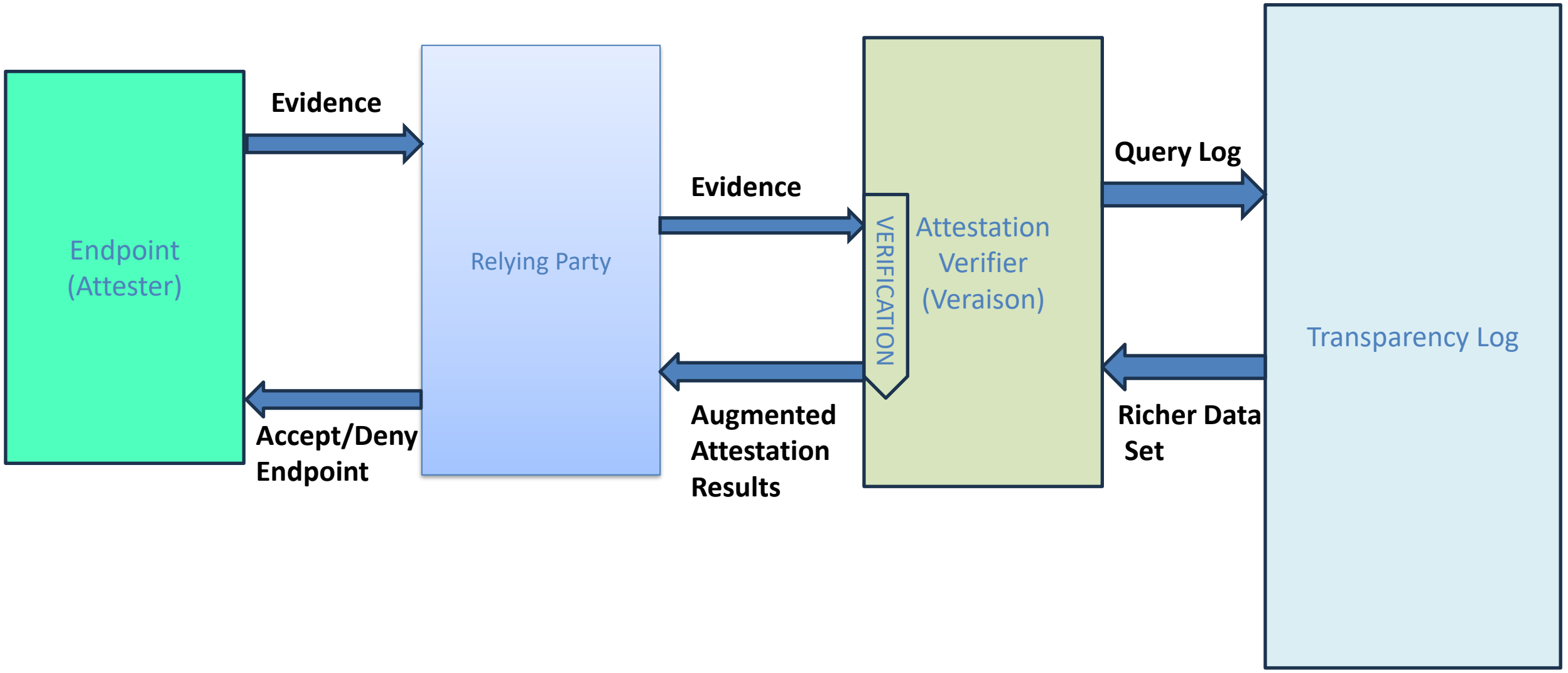
Intersection with Transparency

Using Attestation of Transparency Entities

- Establishing trustworthiness of the operating environment running a Transparency Log
- Attestation of Transparency Log itself!
- Can assist other key roles in a Transparency system, for example running the Witness in a TEE which is attested

VERAISON

Transparency augmenting Attestation



VERAISON

Get Involved

- We would be very interested in further collaboration
  - Principles/Assumptions
  - Design Aspects
  - Extend Veraison to support a new scheme to match the use case
  - Consumption/Reference deployments

- Joins us on Zulip at https://veraison.zulipchat.com/
- Welcome to discuss @ Weekly Community Meet (every Tuesday 4PM UK)

VERAISON

https://github.com/veraison/