Project Veraison

Attestation Verification Components

Building Attestation Verification componentry

*Project VERAISON (**VER**ific**A**t**I**on of atte**S**tati**ON**)* https://github.com/veraison

What:

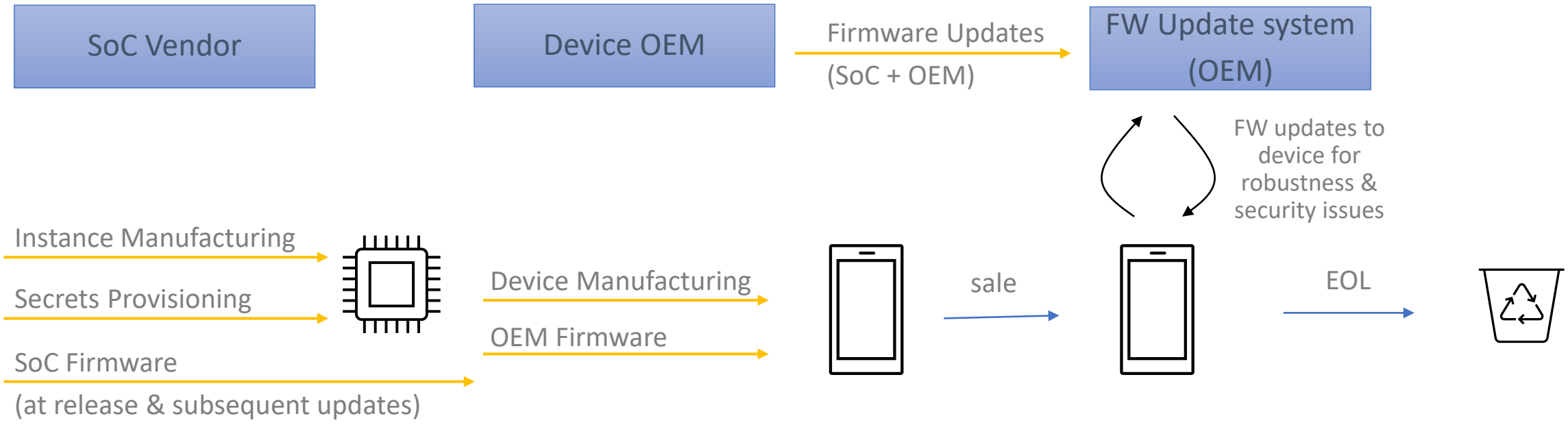
- Author components that can be used to build an Attestation Verification Service

Why:

- Verification of Attestation tokens is a critical part of establishing trust in compute environments
- *However* 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 available which make building Verification Services straightforward

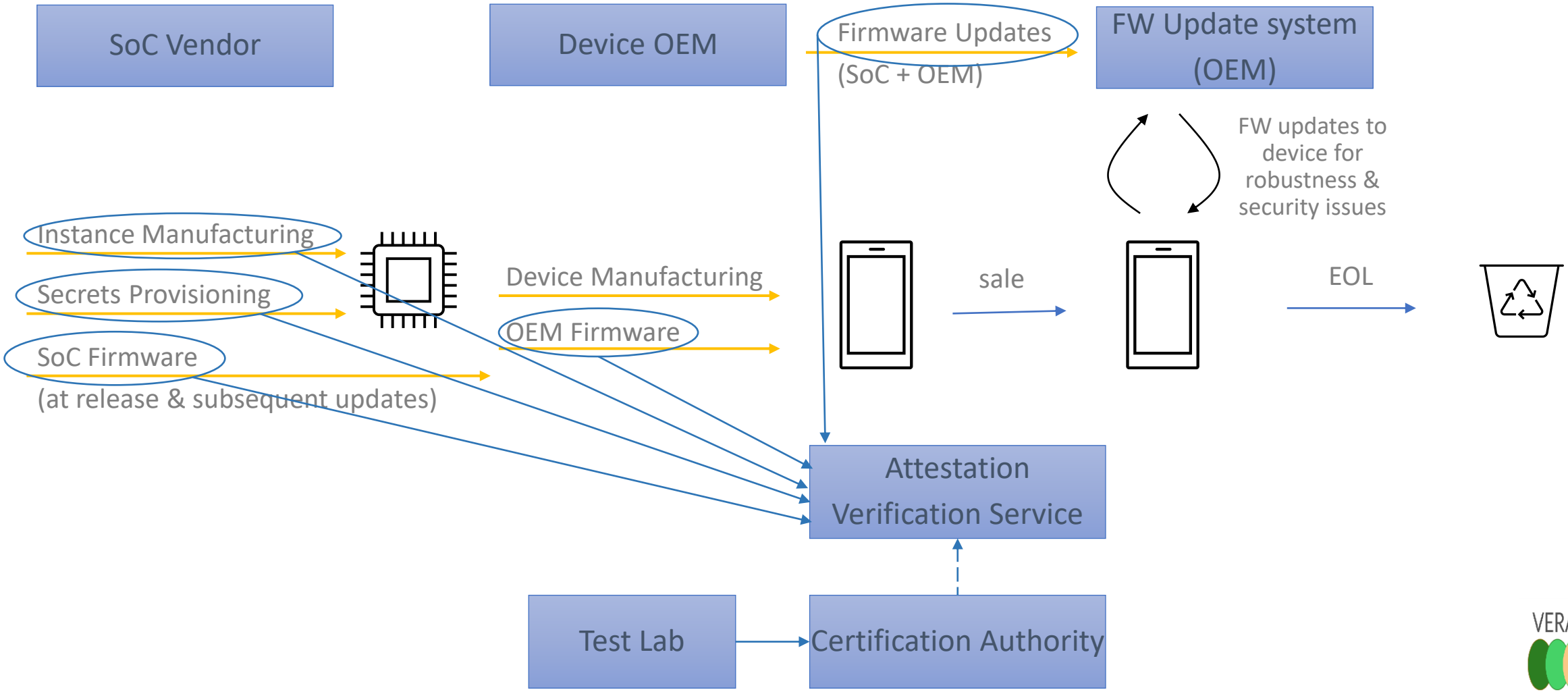
VERAISON

Supply Chain & Lifecycle (somewhat idealised)



VERAISON

Information Flow for Verification



VERAISON

Project Veraison

- Veraison is an Open Source project, operating with fully Open Governance
- Arm is making contributions to the core team but the intent is to have an industry wide scope
  - Use cases are several but applicability to the Confidential Compute community is of particular interest
- Reference implementations: EAT – PSA Token, Arm CCA, DICE
- Token verification is flexible - policy driven or extensible via plugins
- The project will also build some reference deployments to prove the components
- Industry standards used where possible
  - IETF RATS Architecture & Information model
  - TCG DICE Endorsement data format working group

VERAISON

Generalised Model for Verification

- Cryptographic integrity of a Token needs to be proven by:
  - Root of Trust identity
- Attestee evidence verified by reference values for:
  - Hardware identities
  - Firmware Component Identity Measurements
  - Configuration measurements
- Verified evidence can correlate to Derived Claims from other endorsements
  - e.g. Certification Schemes

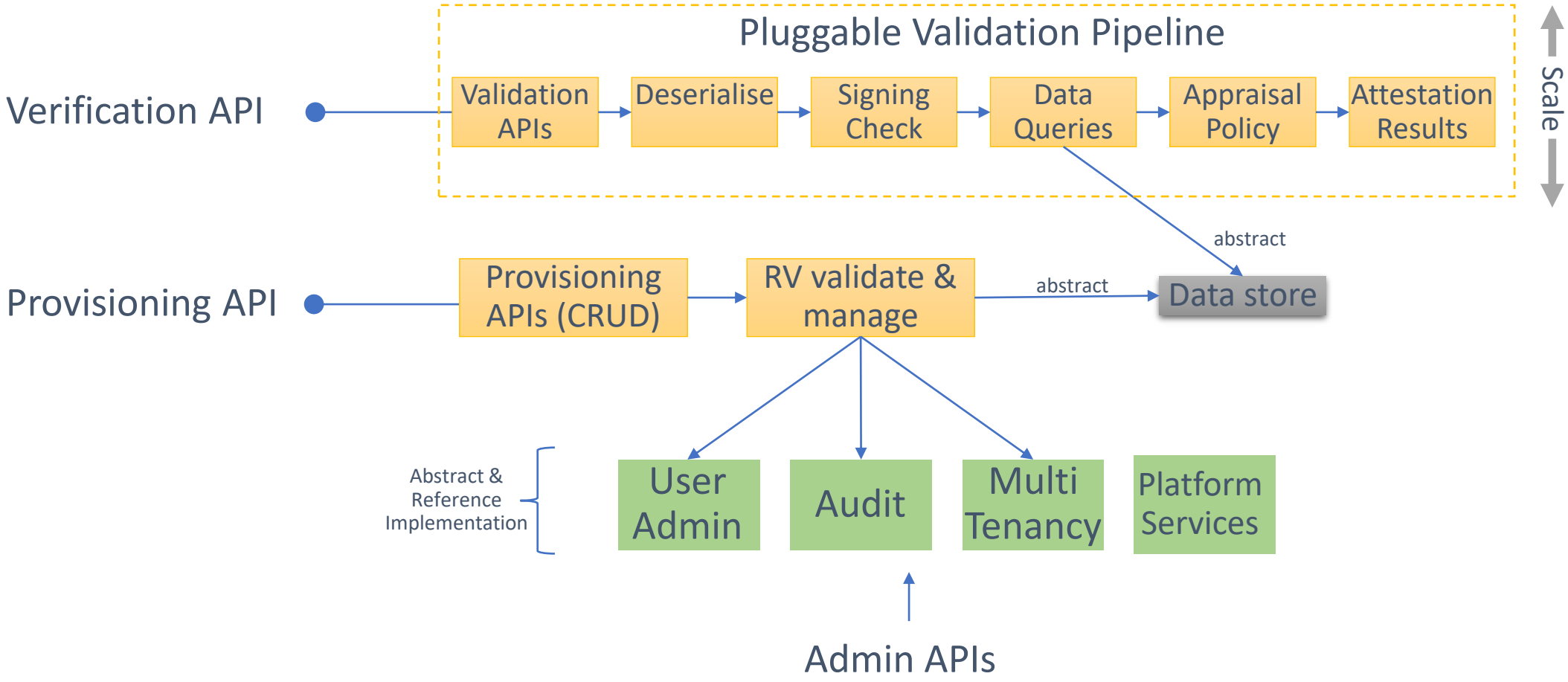
VERAISON

Design Overview

- API driven
- Extensible Verification Pipeline
  - Supports Plugins to encompass multiple token formats
  - Post Evidence checking Appraisal Policy using OPA or Plugin
    - Support for Derived Results
  - Attestation Results
    - Simple Boolean
    - Verified set of Evidence
    - Evidence normalised – per proposed standardisation work
  - Metrics
    - Recorded API usage
  - Consumable as component or as compute unit
- Access to Provisioned Reference Values (endorsements)
  - Also potentially by reference to external sources e.g. Firmware Transparency logs (Trillian)
  - Provisioning APIs & data model for queries
- APIs consumable as libraries or ‘compute units’

VERAISON

Veraison componentry



VERAISON

Out of Scope

- It is not intended to look at other aspects of verification e.g.
  - Unification of Attestation Token formats
  - Normalising the means by which a Relying Party requests Attestation
  - Common Attestation protocol

VERAISON

Project Status

- Project active as an OSS project (https://github.com/veraison)
- Weekly public meetings
- Working with TCG on standard Endorsement data format
  - Publication pending
- Early stage implementation repos for:
  - Validation pipeline & plugin mechanism
  - Provisioning APIs & endorsement storage data
  - EAT, PSA, DICE implementations
- End to End demo for PSA token shown at last IETF Hackathon (RATS WG)

Project Veraison community: https://veraison.zulipchat.com

VERAISON

Get Involved

- We would be very interested in collaboration from this skilled & knowledgeable community

  - Principles / Assumptions
  - Realities of horrible provisioning flows
  - Design Aspects
  - Consumption / Reference deployments

VERAISON


VERAISON