Project Veraison

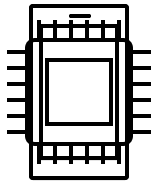
Attestation Verification Components

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

Setting the scene:

- *“Confidential Computing protects data in use by performing computation in a hardware-based Trusted Execution Environment”*
  - *Confidential Computing: Hardware-Based Trusted Execution for Applications and Data*
- CC service users *must* be able to establish that a TEE is trustworthy
  - Hardware & Software aspects are "correct"
- The means to establish trustworthiness is Attestation
- Being able to produce an Attestation report alone is not sufficient
- The report must be Verified to prove the constituent claims

VERAISON



Supply Chain & Lifecycle (somewhat idealised)

SoC Vendor

Device OEM

Firmware Updates
(SoC + OEM)

FW Update system

FW updates to device for robustness & security issues

Instance Manufacturing

Secrets Provisioning

Soc Firmware
(at release & subsequent updates

Device Manufacturing

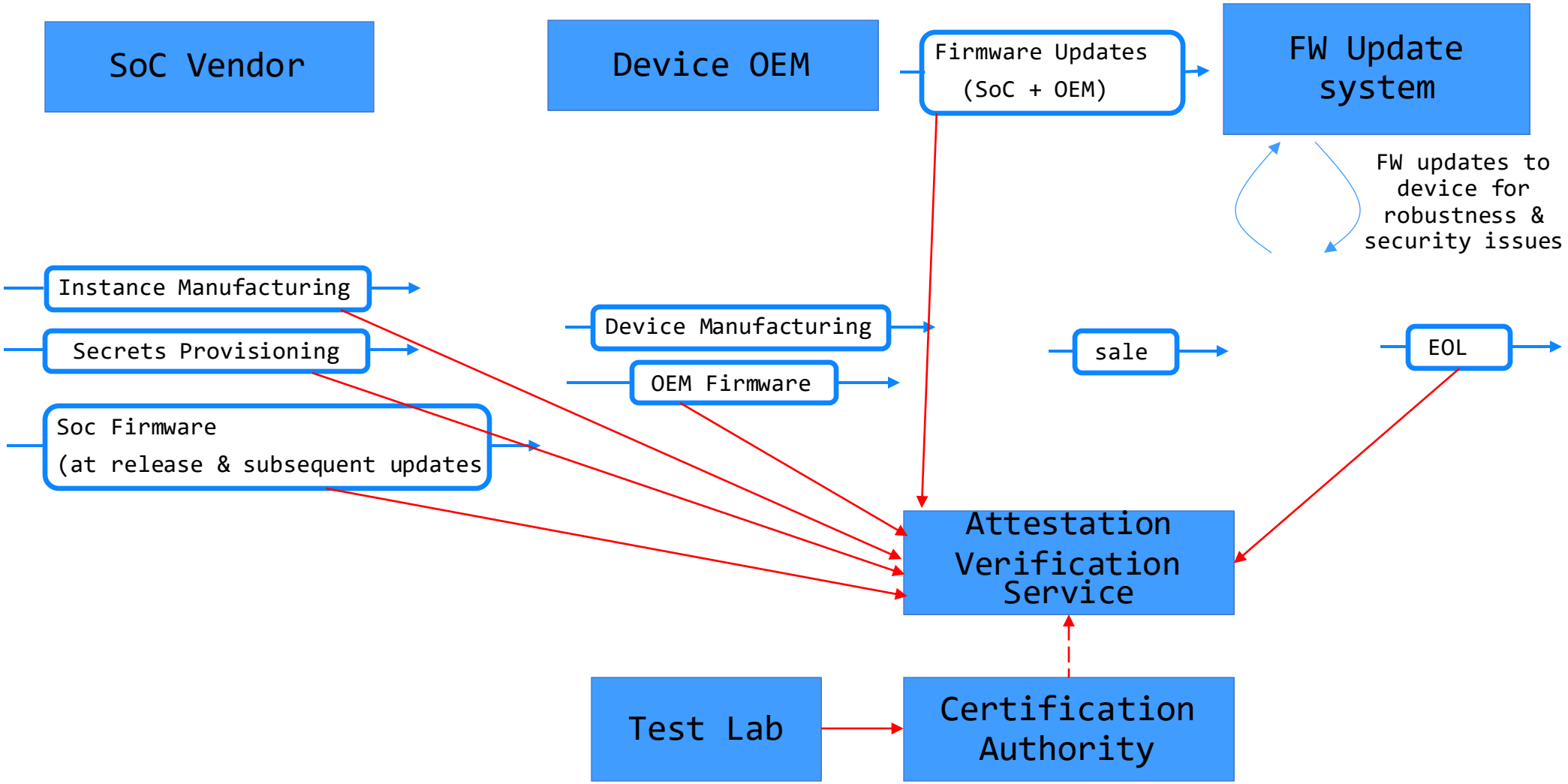
OEM Firmware

sale

EOL

VERAISON

Information Flow for Verification



VERAISON

Process of Verification

- Verification operations must:
  - Deserialise & syntax check attestation report data models
  - Check Cryptographic Signing
    - which requires knowledge of relevant trust anchor(s)
  - Confirm measurements within claims match Reference Values
    - Ref values need to be drawn from supply chain
    - and be up to date
    - Multiple actors, business and trust relationships
  - Apply any semantic relationships between claims
    - e.g., certain hardware & firmware combinations
- Perform all operations while being trustworthy itself

VERAISON

Verification software components

- If every deployment prepares custom logic for the verification process
  - Quality, and hence trustworthiness, may vary
  - Building a verifier is a barrier to entry
- Project Veraison (**VER**ific**A**t**I**on of atte**S**tati**ON**) will build software components that can be used for attestation verification services
- 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

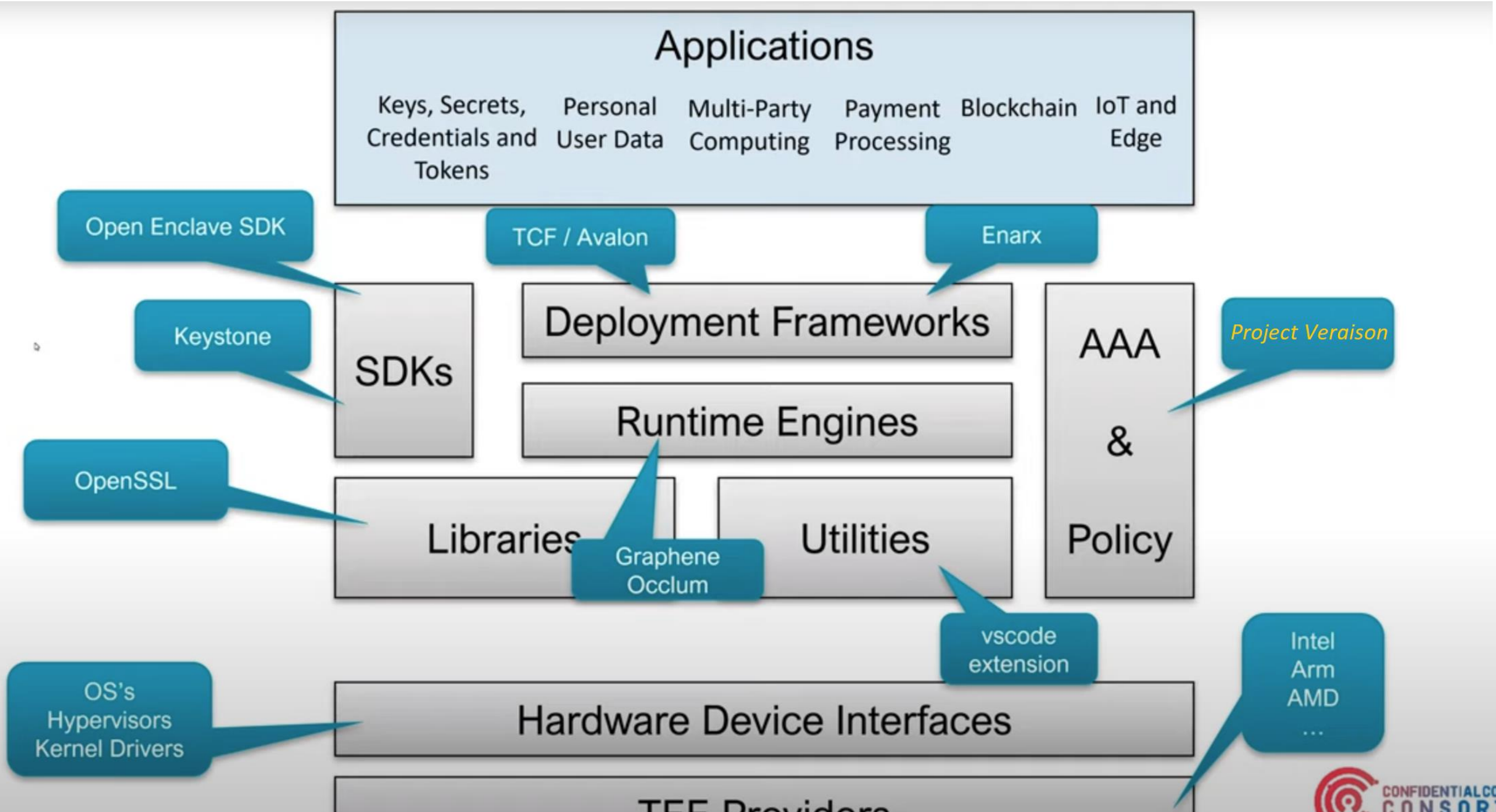
VERAISON

Status

- Project is active on github (https://github.com/veraison)
- Open Governance / weekly public meetings
- Active collaboration with standards bodies (IETF RATS, TCG)
- Initial Design work complete
- Core functionality demostones (PSA-EAT, DICE)
  - Demo integration for Enterprise TPM use case with EnactTrust
- Long list of potential features / capabilities
- Contributions most welcome

VERAISON

CCC ‘fit’


Applications
Keys, Secrets, Credentials and Tokens
Personal User Data
Multi-Party Computing
Payment Processing
Blockchain
IoT and Edge
Open Enclave SDK
TCF / Avalon
Enarx
Keystone
SDKs
Deployment Frameworks
Runtime Engines
AAA & Policy
Project Veraison
OpenSSL
Libraries
Graphene Occlum
Utilities
vscode extension
OS's Hypervisors Kernel Drivers
Hardware Device Interfaces
Intel Arm AMD …
TEE Providers

https://github.com/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