CC-API CCC Proposal TechTalk - Update

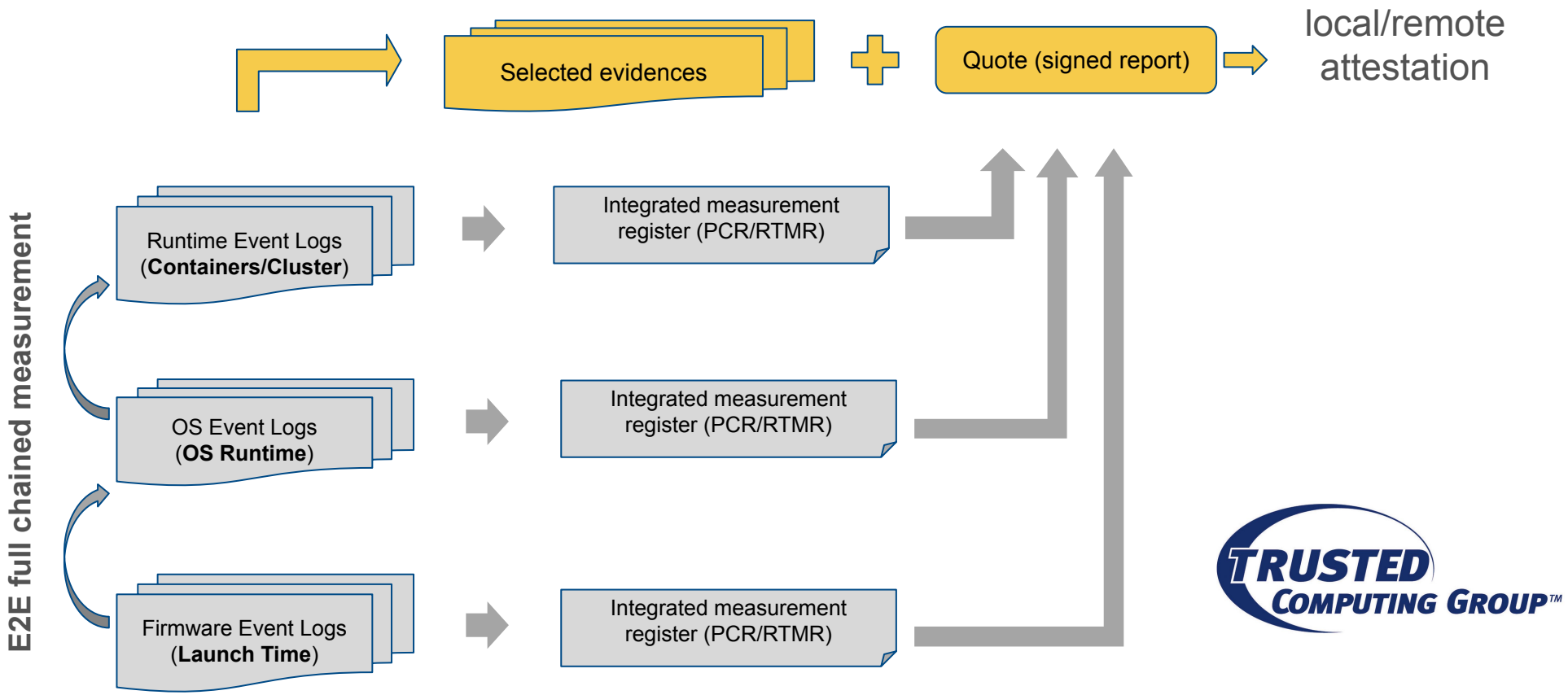
https://github.com/cc-api

Lu Ken, Xia Haidong, Yao Jiewen

Contributor: Bhandaru Malini, Dong Xiaocheng, Hao Ruomeng, Ying Ruoyu, Mingsen Sun, Duan Bing, Ziye Yang, Yao Zhang, Ye Wu, Jianjun Chen, Wenhui Zhang

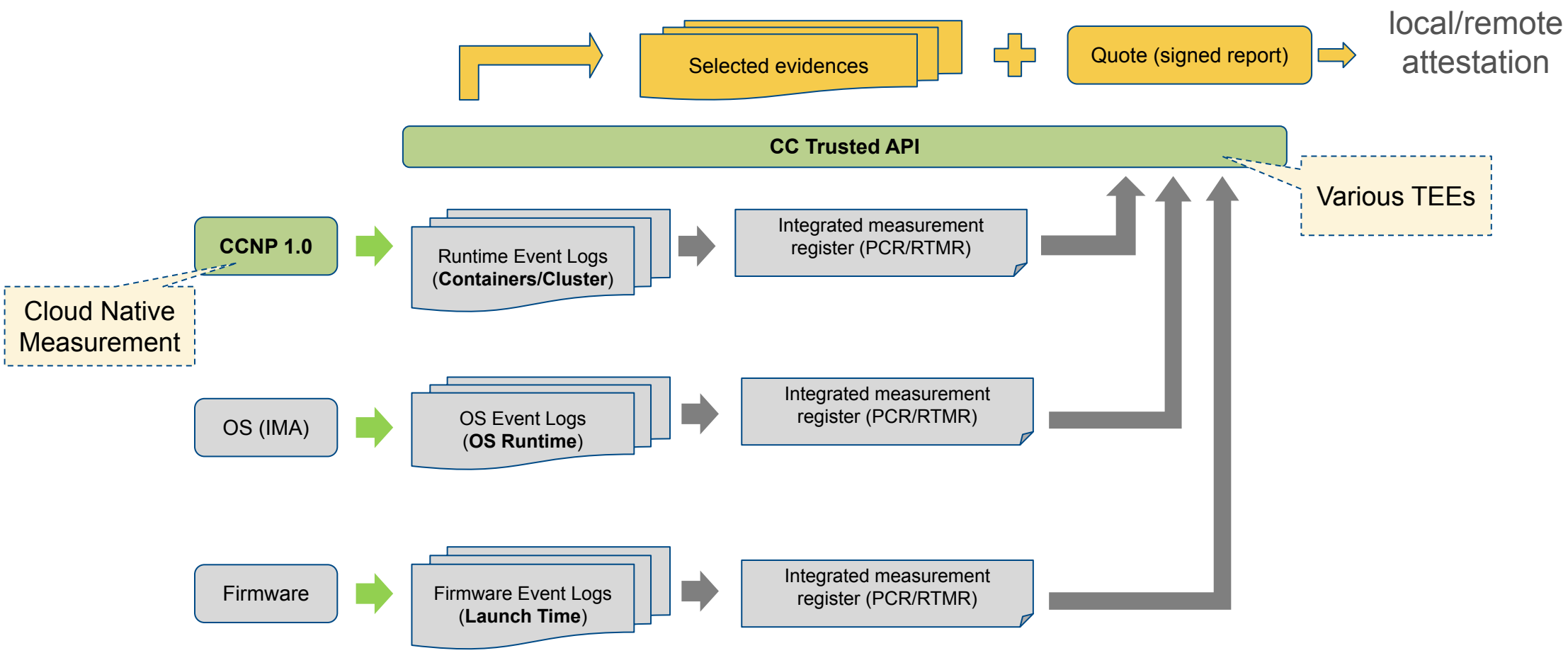
2024/05/07

Background: E2E Full Chained Measurement for Attestation

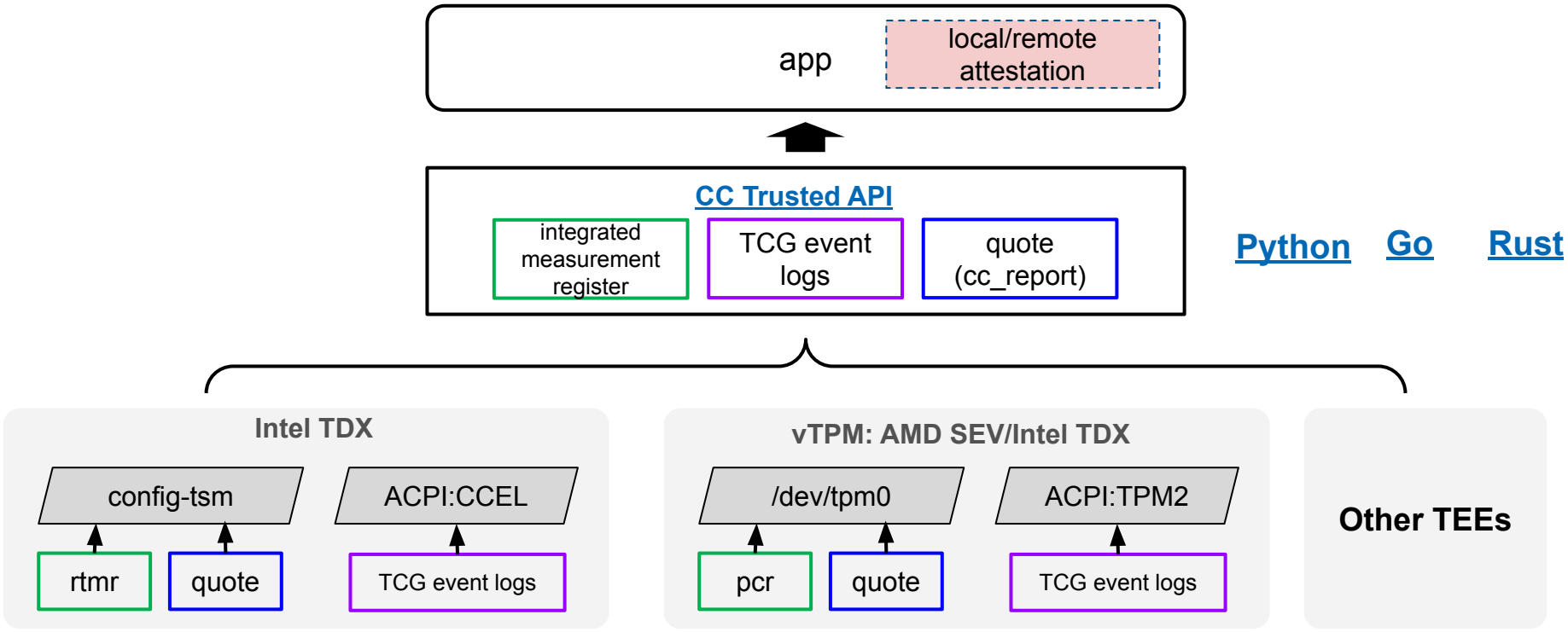


A platform's behavior is determined by both its set of immutable components and its set of mutable components, include boot firmware, pre-OS modules, the OS itself, and loadable drivers and applications. (TCG Guidance on Integrity Measurements and Event Log Processing page 7)

Overview: E2E Full Chained Measurement for CC Cloud

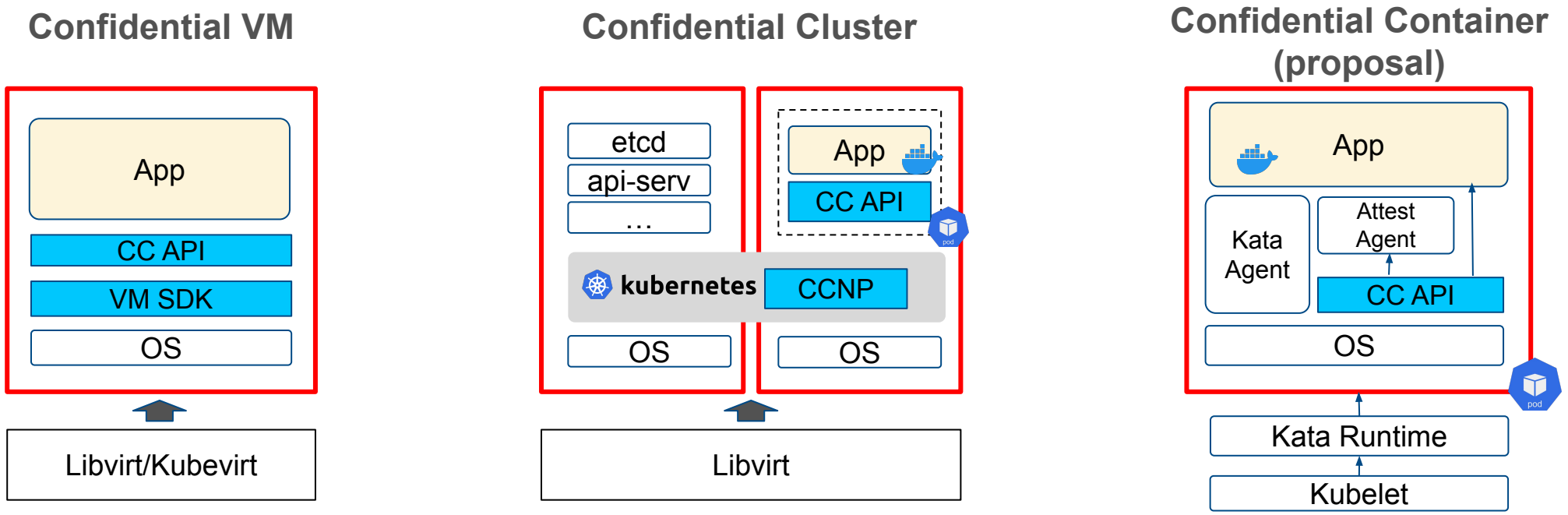


How: Simplify Evidence(Event Logs) Access across TEEs



https://github.com/cc-api

How: Simplify the E2E Measurement across Frameworks



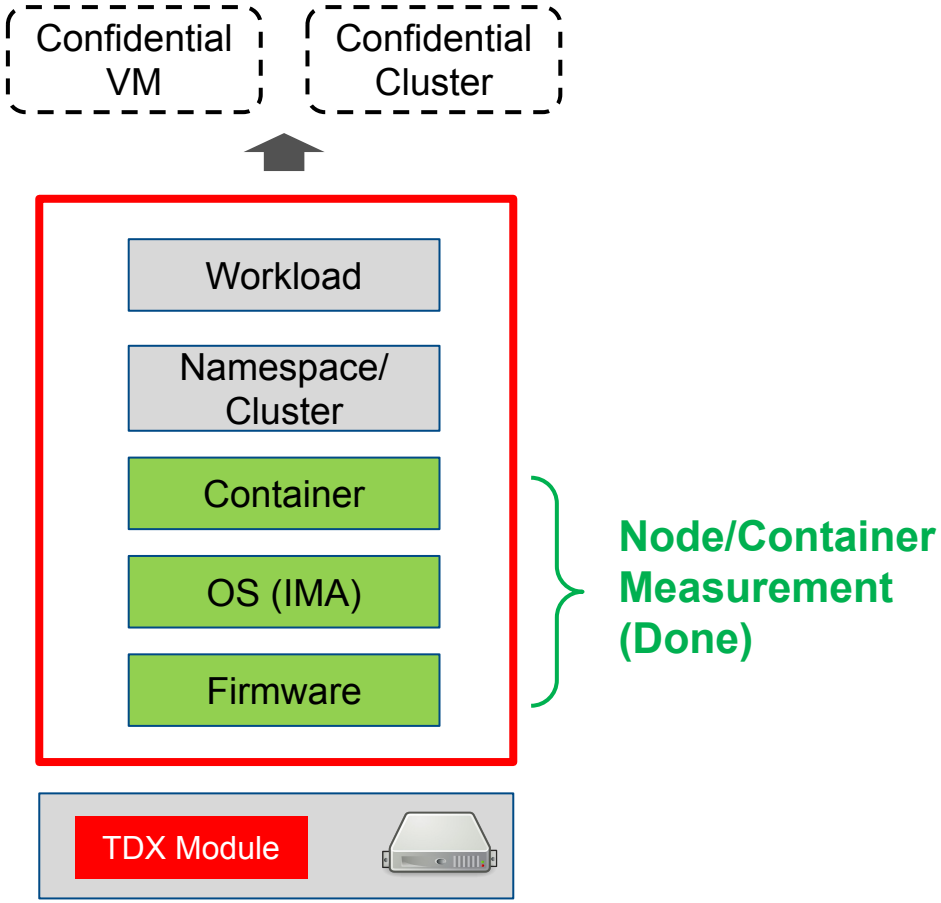
Please refer to [Confidential Computing Use case (Redhat)] for the definitions of confidential VM, confidential cluster, confidential container.

APIs

API	Description	Parameters	Response
get_default_algorithms	Get the default Digest algorithms supported by trusted foundation.	N/A	A TcgAlgorithmRegistry object telling the default algorithms
get_measurement_count	Get the count of measurement register.	N/A	An integer telling the count of measurement registers
get_cc_measurement	Get measurement register according to given selected index and algorithms.	- **imr_select ([int, int])**: The first is index of measurement register, the second is the algorithms ID	An integer telling the count of measurement registers
get_cc_report	Get the quote for given nonce and data.	- **nonce**: a number used to protect private communications by preventing replay attacks - **data**: the data specified by user - **extraArgs**: the placeholder for extra arguments required in vTPM or other TEE cases	A Quote object
get_cc_eventlog	Get eventlog for given index and count.	- **start**: the index of the event log to start fetching - **count**: the number of event logs to fetch	A TcgEventLog object
replay_cc_eventlog	Replay event logs based on data provided.	- **event_logs**: the list of parsed event logs to replay	A dictionary containing the replay result displayed by IMR index and hash algorithm.

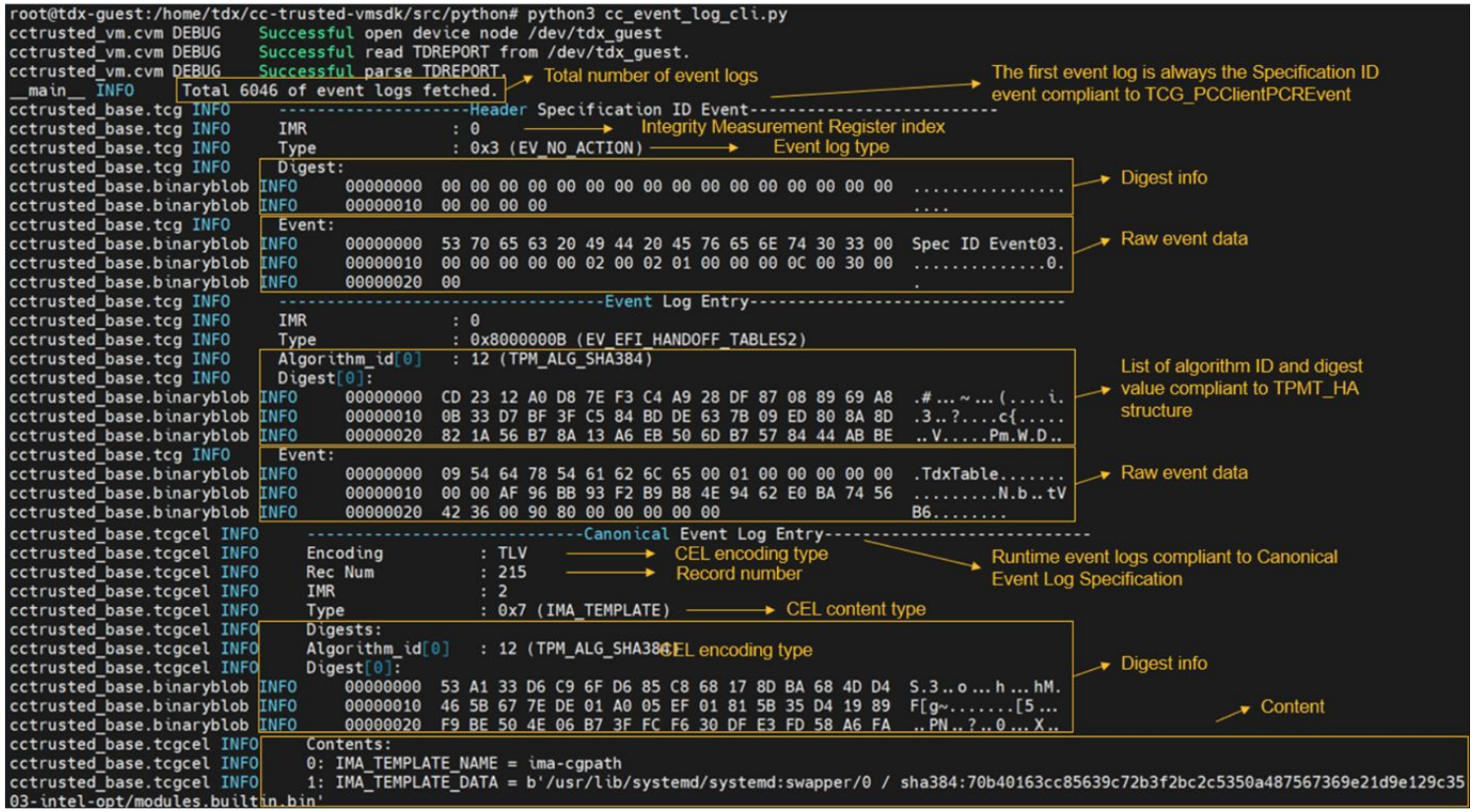
Current Status

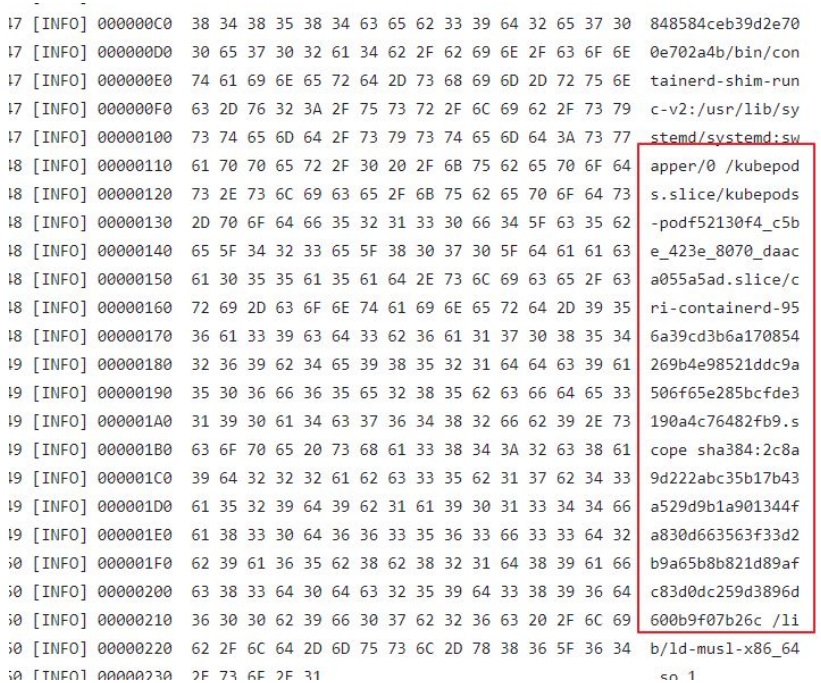
	VM SDK	Container SDK (CCNP)
Python	Ready	Ready
Go	Ready	Ready
Rust	Ready	Ready



Container measurement uses the IMA template for cgroup in this patch.
CCC project stage definitions and expectations

Example of Node/Container Measurement

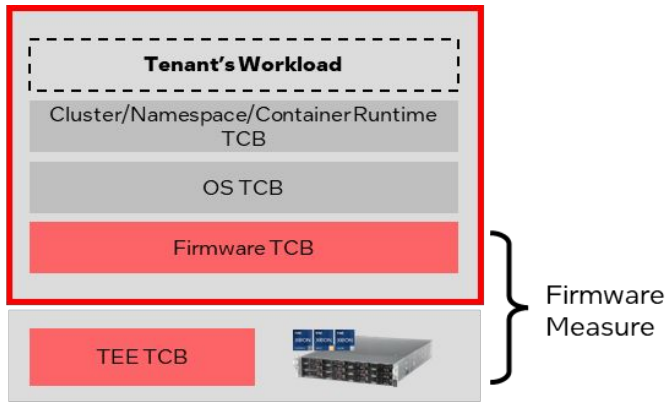


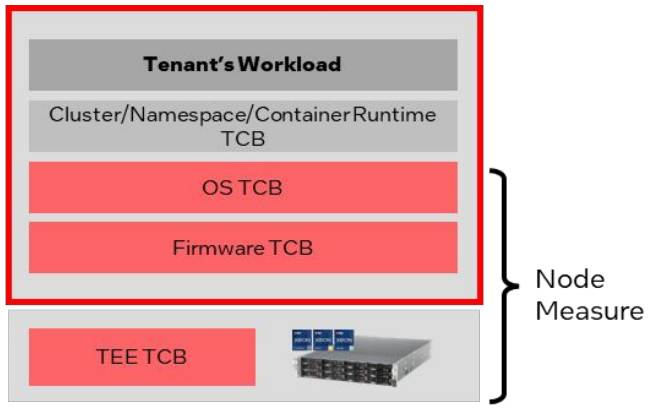


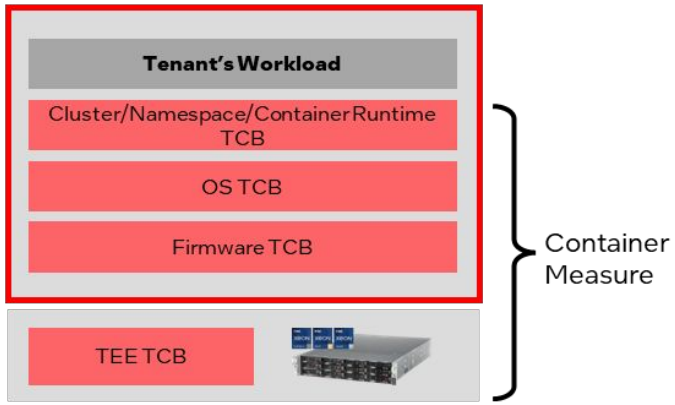
Refer: [Full Event Log Collected within VM]

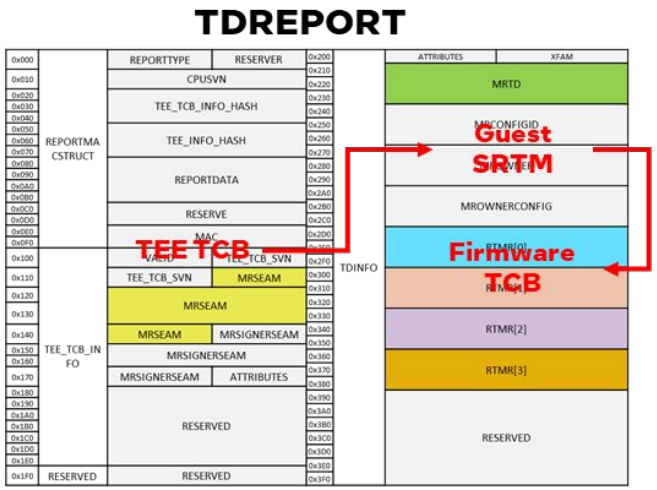
Refer: [Full Event Log Collected within Container]

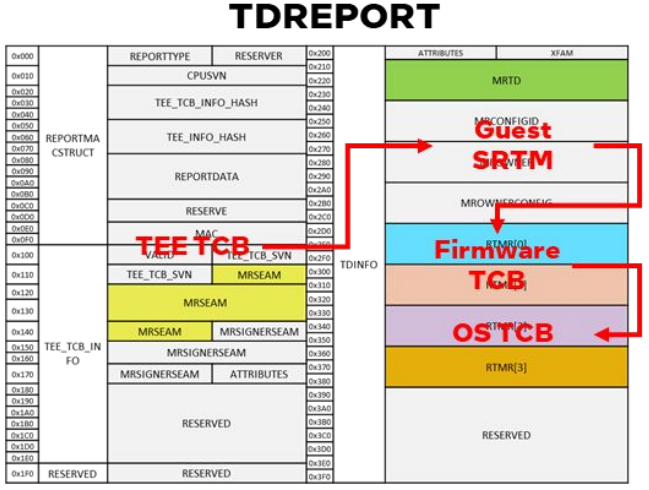
Measurement in CC(TDX) Report

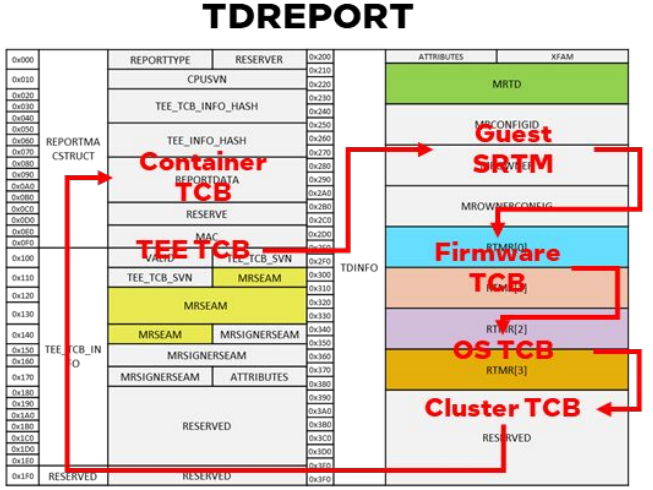












Demo

How to use Evidence

Use Case 1: Google's go-tpm-tool

MachineState = Firmware + OS + Container

Use Case 2: Model As-a Service

Measure = Firmware + VM + PaaS (k8s) + Container

Use Case 3: General Attestation Client like ITA

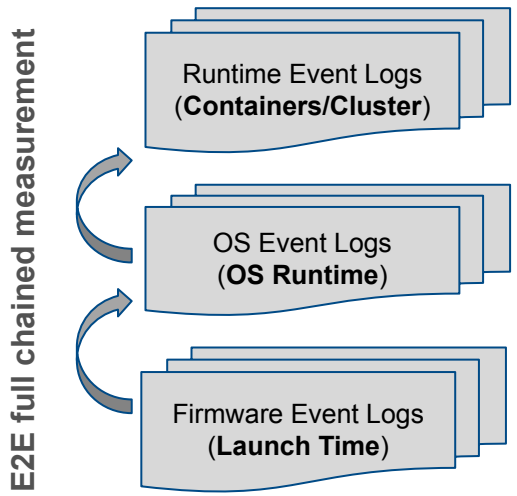
Launch Time Measurement Only = Firmware

Use Case 4: Server Component Attestation in OCP

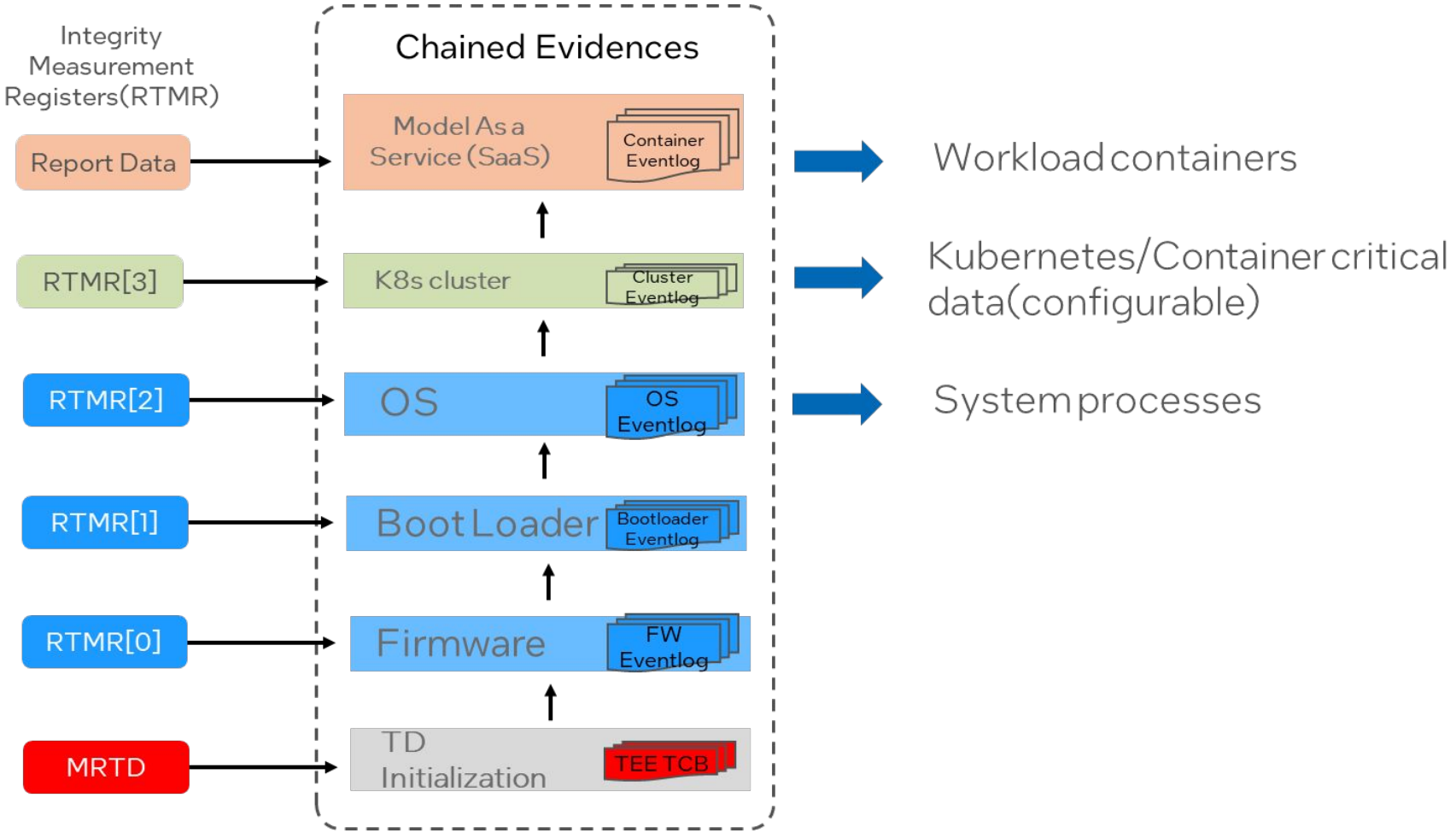
Firmware Measurement

More use cased defined from IETF like workload identity, supply chain etc.

select evidences according to use case

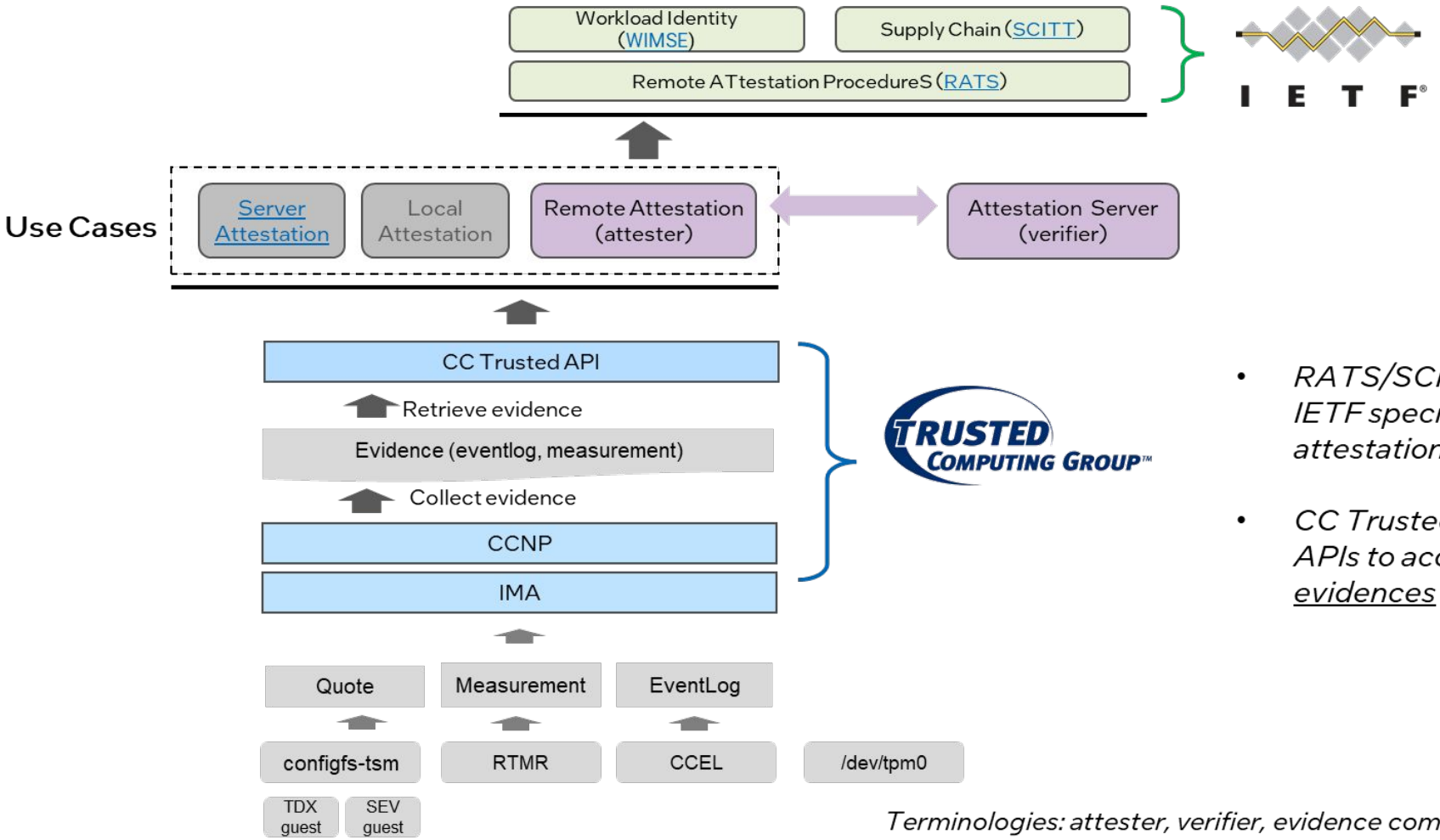


How to use Evidence



Backup

Measurement(Evidence) and Attestation



- *RATS/SCITT/WIMSE are aligning with IETF specification for tenant's remote attestation use case*
- *CC Trusted API provides vendor agnostic APIs to access and TCG compliant evidences (i.e., measurement, event log)*

Terminologies: attester, verifier, evidence comes from rfc9334; while trusted state comes from TCG Guidance on Integrity Measurements and Event Log Processing.