

CC-API CCC Proposal TechTalk - Update

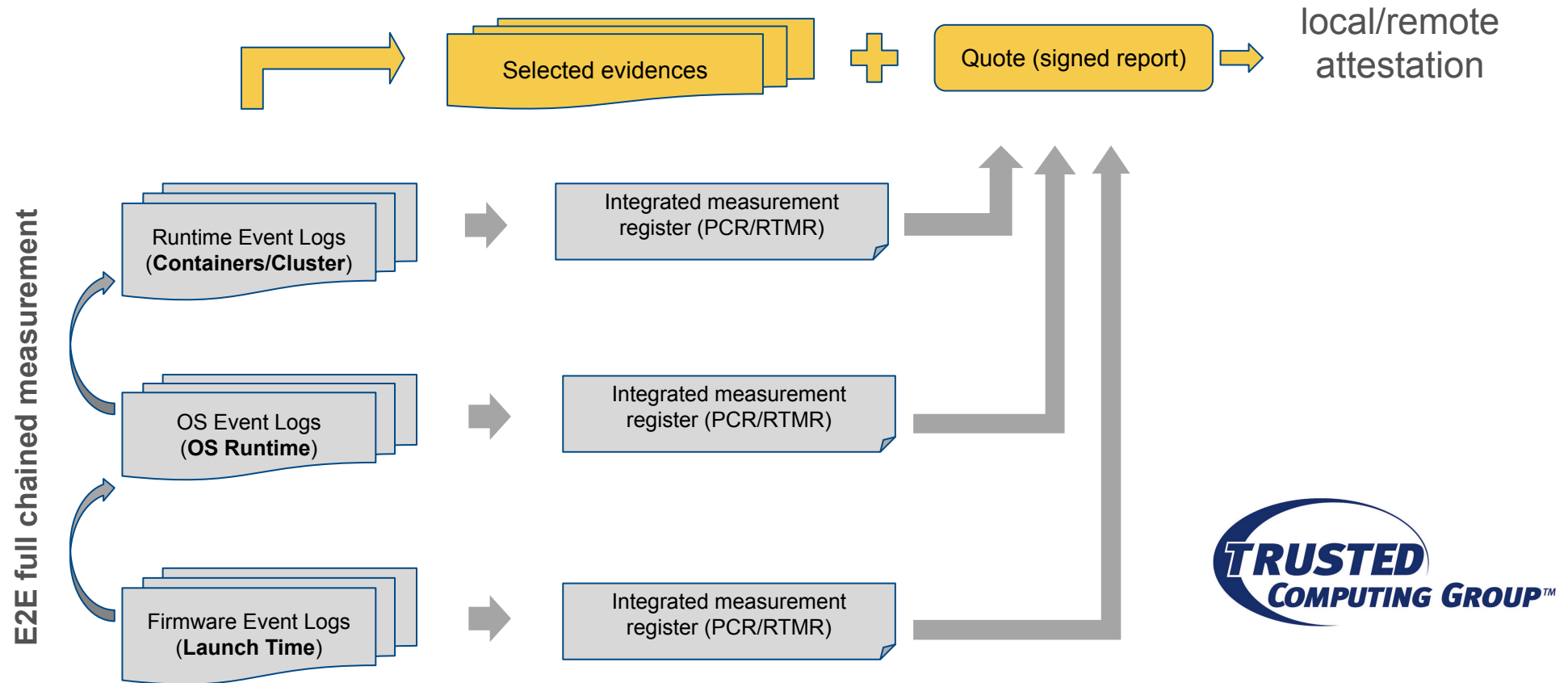
<https://github.com/cc-api>

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

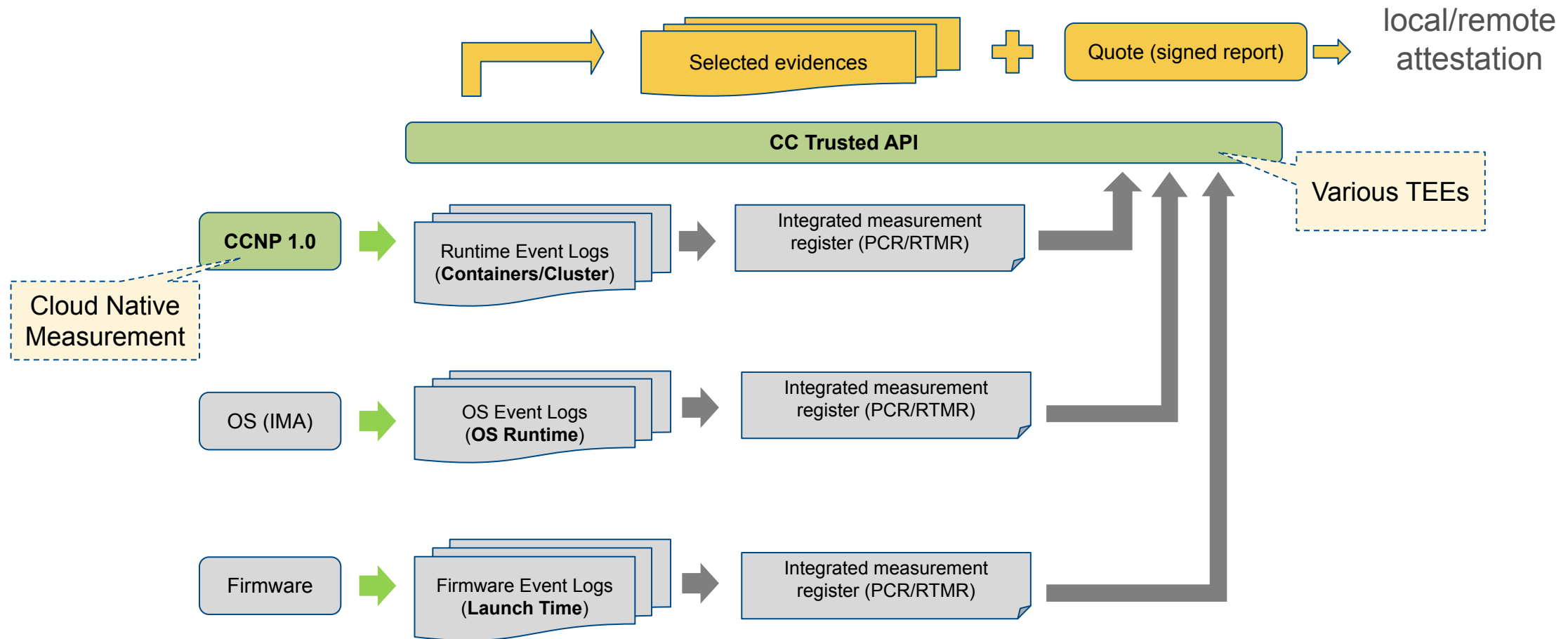
2024/05/07

Background: E2E Full Chained Measurement for Attestation

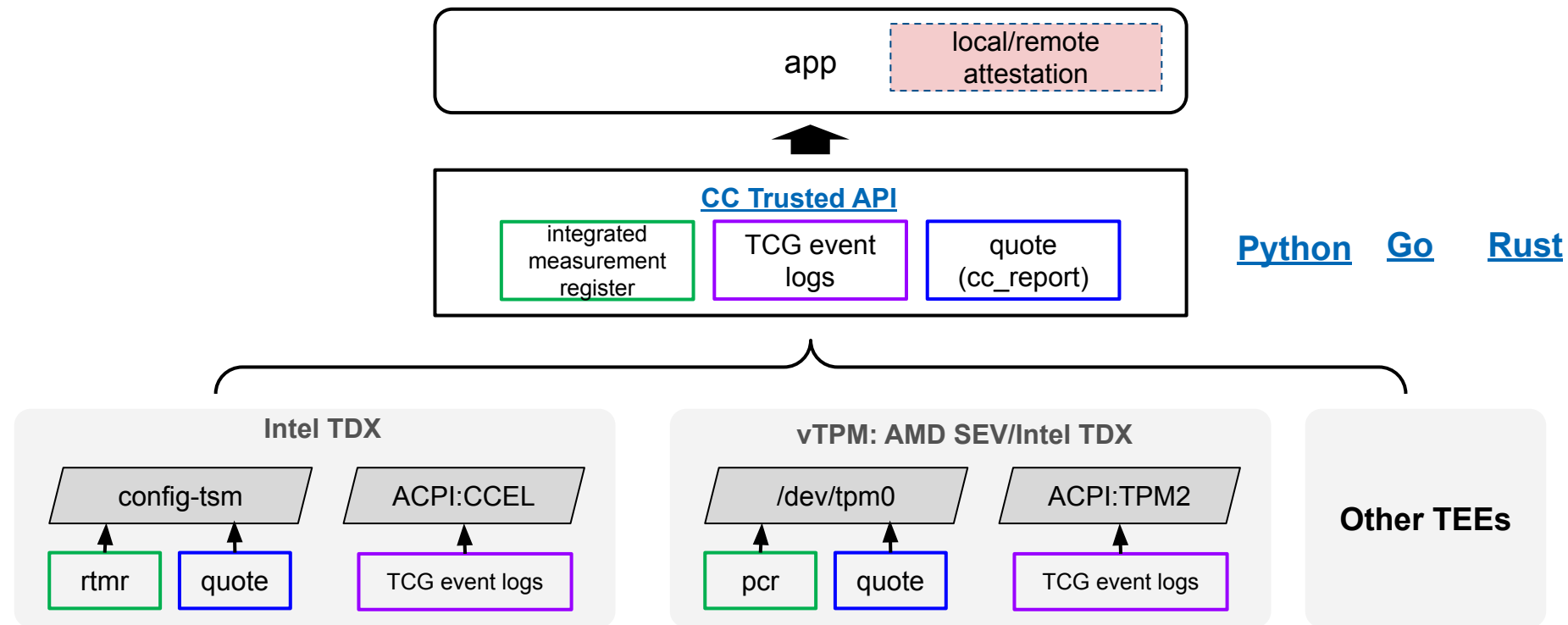


A platform's behavior is determined by both its set of immutable components and its set of mutable components, include boot firmware, pre-OS modules, the OS itself, and loadable drivers and applications. ([TCG Guidance on Integrity Measurements and Event Log Processing](#) page 7)

Overview: E2E Full Chained Measurement for CC Cloud

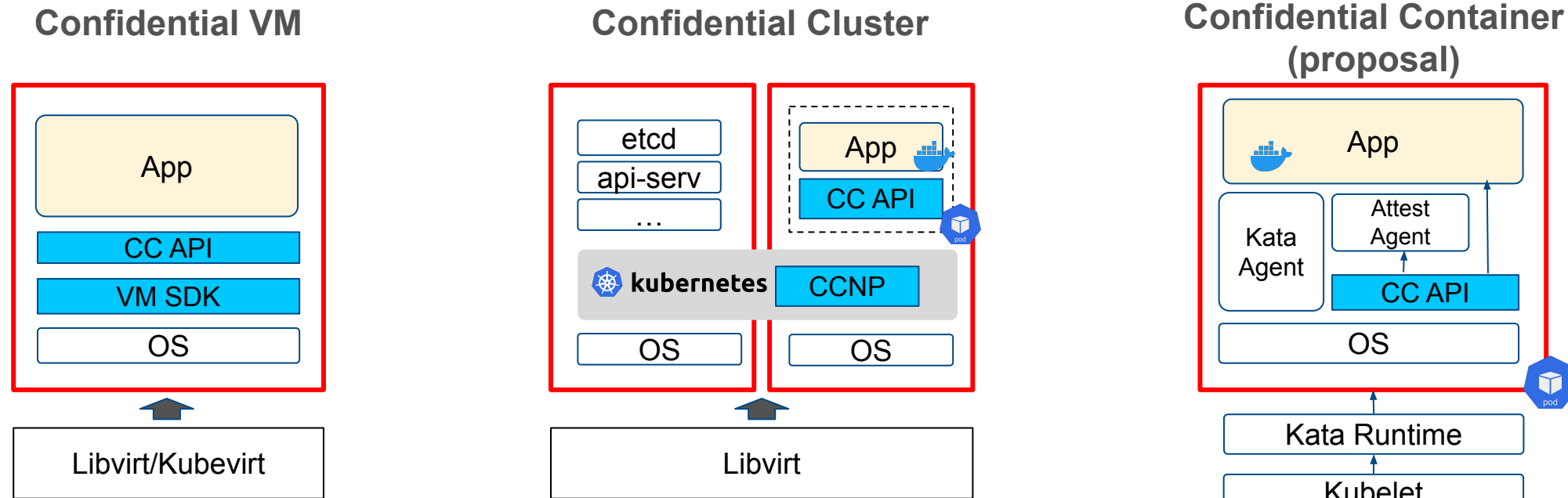


How: Simplify Evidence(Event Logs) Access across TEEs



<https://github.com/cc-api>

How: Simplify the E2E Measurement across Frameworks

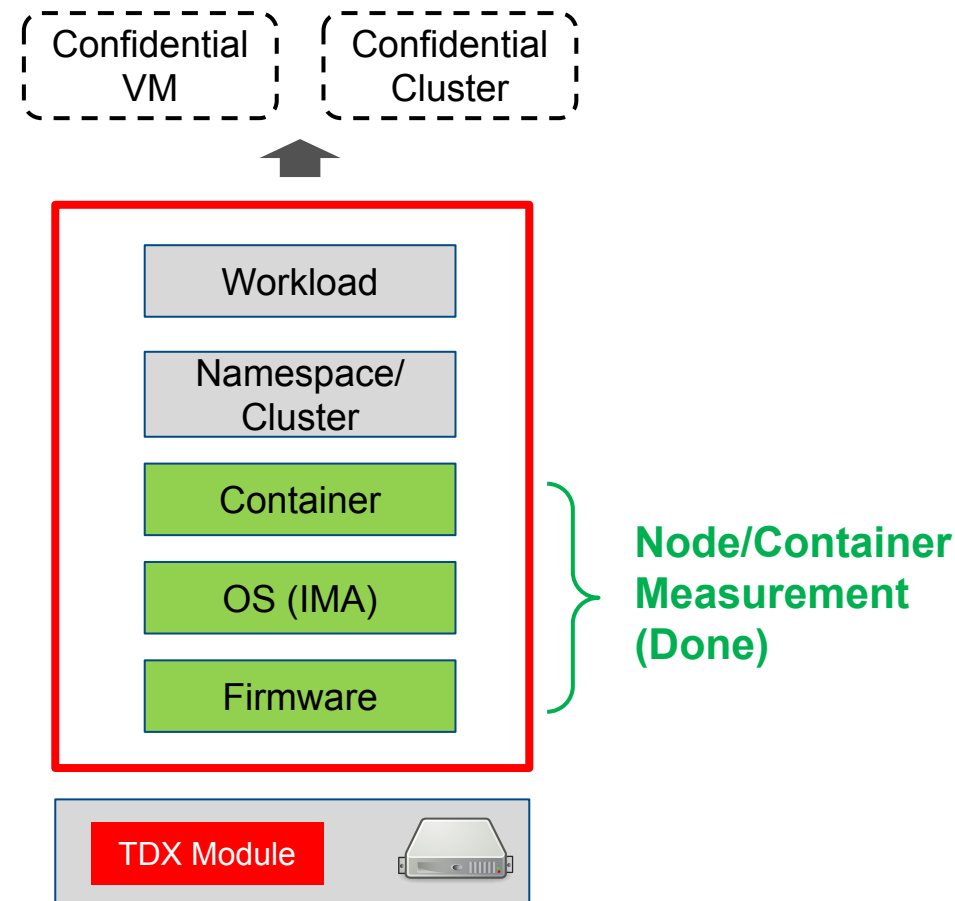
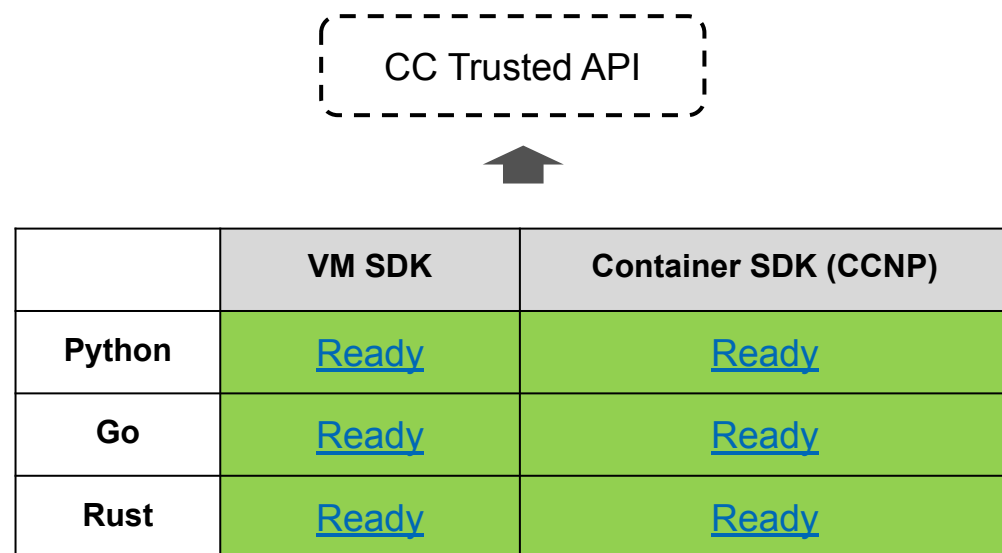


Please refer to [Confidential Computing Use case \(Redhat\)](#) for the definitions of confidential VM, confidential cluster, confidential container.

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



Container measurement uses the IMA template for cgroup in [this](#) patch.
[CCC project stage definitions and expectations](#)

Example of Node/Container Measurement

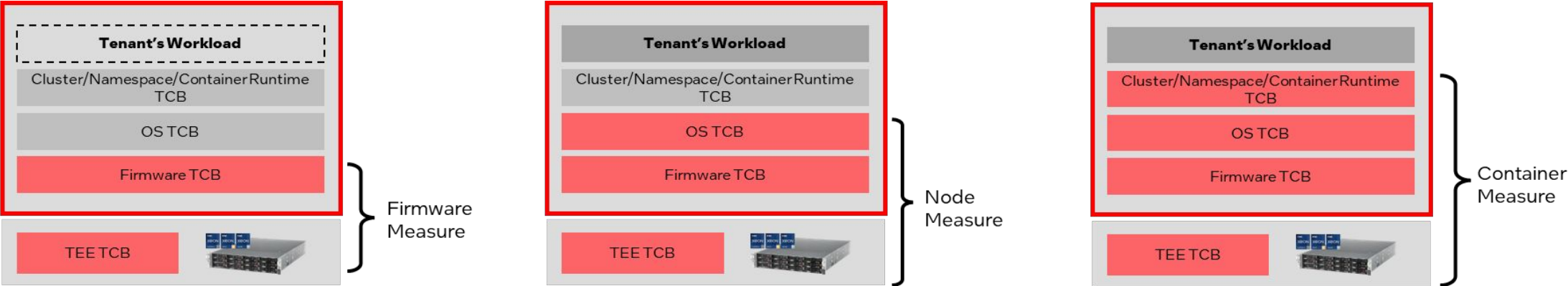
```
root@tdx-guest:/home/tdx/cc-trusted-vmsdk/src/python# python3 cc_event_log_cli.py
cctrusted_vm.cvm DEBUG Successful open device node /dev/tdx_guest
cctrusted_vm.cvm DEBUG Successful read TDREPORT from /dev/tdx_guest.
cctrusted_vm.cvm DEBUG Successful parse TDREPORT.
__main__ INFO Total 6046 of event logs fetched.
-----Header Specification ID Event-----
cctrusted_base.tcg INFO IMR : 0
cctrusted_base.tcg INFO Type : 0x3 (EV_NO_ACTION)
cctrusted_base.tcg INFO Digest:
cctrusted_base.tcg INFO 00000000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
cctrusted_base.tcg INFO 00000010 00 00 00 00 .....
cctrusted_base.tcg INFO Event:
cctrusted_base.tcg INFO 00000000 53 70 65 63 20 49 44 20 45 76 65 6E 74 30 33 00 Spec ID Event03.
cctrusted_base.tcg INFO 00000010 00 00 00 00 00 02 00 02 01 00 00 0C 00 30 00 .....0.
cctrusted_base.tcg INFO 00000020 00 .....
cctrusted_base.tcg INFO -----Event Log Entry-----
cctrusted_base.tcg INFO IMR : 0
cctrusted_base.tcg INFO Type : 0x8000000B (EV_EFI_HANDOFF_TABLES2)
cctrusted_base.tcg INFO Algorithm_id[0] : 12 (TPM_ALG_SHA384)
cctrusted_base.tcg INFO Digest[0]:
cctrusted_base.tcg INFO 00000000 CD 23 12 A0 D8 7E F3 C4 A9 28 DF 87 08 89 69 A8 .#...~...(.i.
cctrusted_base.tcg INFO 00000010 0B 33 D7 BF 3F C5 84 BD DE 63 7B 09 ED 80 8A 8D .3..?...c{....
cctrusted_base.tcg INFO 00000020 82 1A 56 B7 8A 13 A6 EB 50 6D B7 57 84 44 AB BE ..V....Pm.W.D..
cctrusted_base.tcg INFO Event:
cctrusted_base.tcg INFO 00000000 09 54 64 78 54 61 62 6C 65 00 01 00 00 00 00 00 .TdxTable.....
cctrusted_base.tcg INFO 00000010 00 00 AF 96 BB 93 F2 B9 B8 4E 94 62 E0 BA 74 56 .....N.b..tV
cctrusted_base.tcg INFO 00000020 42 36 00 90 80 00 00 00 00 00 00 .....B6.....
cctrusted_base.tcgcel INFO -----Canonical Event Log Entry-----
cctrusted_base.tcgcel INFO Encoding : TLV
cctrusted_base.tcgcel INFO Rec Num : 215
cctrusted_base.tcgcel INFO IMR : 2
cctrusted_base.tcgcel INFO Type : 0x7 (IMA_TEMPLATE)
cctrusted_base.tcgcel INFO Digests:
cctrusted_base.tcgcel INFO Algorithm_id[0] : 12 (TPM_ALG_SHA384)
cctrusted_base.tcgcel INFO Digest[0]:
cctrusted_base.tcgcel INFO 00000000 53 A1 33 D6 C9 6F D6 85 C8 68 17 8D BA 68 4D D4 S.3..o...h...hM.
cctrusted_base.tcgcel INFO 00000010 46 5B 67 7E DE 01 A0 05 EF 01 81 5B 35 D4 19 89 F[g~.....[5...
cctrusted_base.tcgcel INFO 00000020 F9 BE 50 4E 06 B7 3F FC F6 30 DF E3 FD 58 A6 FA ..PN...?...X..
cctrusted_base.tcgcel INFO Contents:
cctrusted_base.tcgcel INFO 0: IMA_TEMPLATE_NAME = ima-cgpath
cctrusted_base.tcgcel INFO 1: IMA_TEMPLATE_DATA = b'/usr/lib/systemd/systemd:swapper/0 / sha384:70b40163cc85639c72b3f2bc2c5350a487567369e21d9e129c35
03-intel-opt/modules.builtin.bin'
```

```
17 [INFO] 000000C0 38 34 38 35 38 34 63 65 62 33 39 64 32 65 37 30 848584ceb39d2e70
17 [INFO] 000000D0 30 65 37 30 32 61 34 62 2F 62 69 6E 2F 63 6F 6E 0e702a4b/bin/con
17 [INFO] 000000E0 74 61 69 6E 65 72 64 2D 73 68 69 6D 2D 72 75 6E tainerd-shim-run
17 [INFO] 000000F0 63 2D 76 32 3A 2F 75 73 72 2F 6C 69 62 2F 73 79 c-v2:/usr/lib/sy
17 [INFO] 00000100 73 74 65 6D 64 2F 73 79 73 74 65 6D 64 3A 73 77 stemd/systemd:sw
18 [INFO] 00000110 61 70 70 65 72 2F 30 20 2F 68 75 62 65 70 6F 64 apper/0 /kubepod
18 [INFO] 00000120 73 2E 73 6C 69 63 65 2F 68 75 62 65 70 6F 64 73 s.slice/kubepods
18 [INFO] 00000130 2D 70 6F 64 66 35 32 31 33 30 66 34 5F 63 35 62 -podf52130f4_c5b
18 [INFO] 00000140 65 5F 34 32 33 65 5F 38 30 37 30 5F 64 61 61 63 e_423e_8070_daac
18 [INFO] 00000150 61 30 35 35 61 35 61 64 2E 73 6C 69 63 65 2F 63 a055a5ad.slice/c
18 [INFO] 00000160 72 69 2D 63 6F 6E 74 61 69 6E 65 72 64 2D 39 35 ri-containerd-95
18 [INFO] 00000170 36 61 33 39 63 64 33 62 36 61 31 37 30 38 35 34 6a39cd3b6a170854
19 [INFO] 00000180 32 36 39 62 34 65 39 38 35 32 31 64 64 63 39 61 269b4e98521ddc9a
19 [INFO] 00000190 35 30 36 66 36 35 65 32 38 35 62 63 66 64 65 33 506f65e285bcfde3
19 [INFO] 000001A0 31 39 30 61 34 63 37 36 34 38 32 66 62 39 2E 73 190a4c76482fb9.s
19 [INFO] 000001B0 63 6F 70 65 20 73 68 61 33 38 34 3A 32 63 38 61 cope sha384:2c8a
19 [INFO] 000001C0 39 64 32 32 32 61 62 63 33 35 62 31 37 62 34 33 9d222abc35b17b43
19 [INFO] 000001D0 61 35 32 39 64 39 62 31 61 39 30 31 33 34 34 66 a529d9b1a901344f
19 [INFO] 000001E0 61 38 33 30 64 36 36 33 35 36 33 66 33 33 64 32 a830d663563f33d2
19 [INFO] 000001F0 62 39 61 36 35 62 38 62 38 32 31 64 38 39 61 66 b9a65b8b821d89af
19 [INFO] 00000200 63 38 33 64 30 64 63 32 35 39 64 33 38 39 36 64 c83d0dc259d3896d
19 [INFO] 00000210 36 30 30 62 39 66 30 37 62 32 36 63 20 2F 6C 69 600b9f07b26c /11
19 [INFO] 00000220 62 2F 6C 64 2D 6D 75 73 6C 2D 78 38 36 5F 36 34 b/ld-musl-x86_64
19 [INFO] 00000230 2F 73 6F 2F 31 <n 1
```

Refer: [Full Event Log Collected within VM](#)

Refer: [Full Event Log Collected within Container](#)

Measurement in CC(TDX) Report

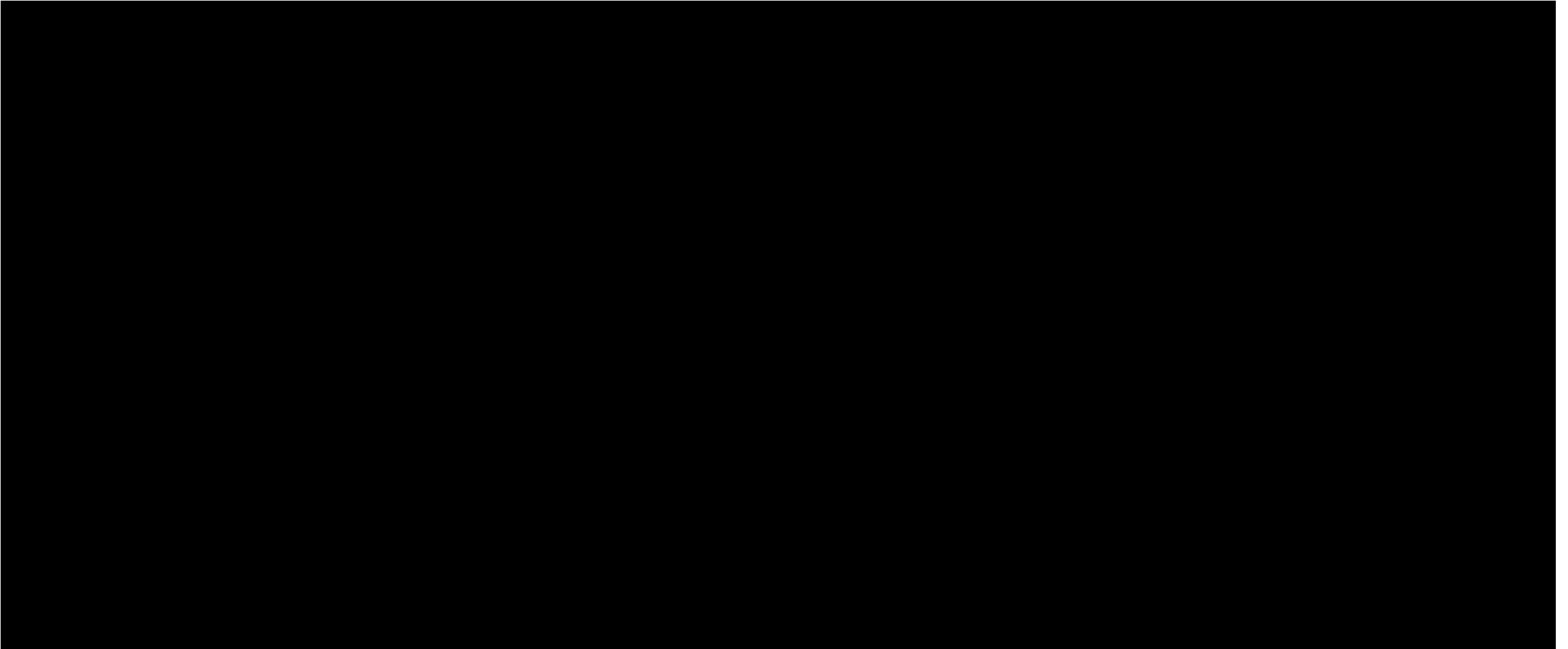


TDREPORT				
ADDRESS	REPORTMA CSTRUCT	REPORTTYPE	RESERVER	ATTRIBUTES
		REPORTTYPE	RESERVER	ATTRIBUTES
0x000	REPORTMA CSTRUCT	CPUSVN	0x200	MRTO
0x010		TEE_TCB_INFO_HASH	0x210	
0x020		TEE_TCB_INFO_HASH	0x220	
0x030		TEE_TCB_INFO_HASH	0x230	
0x040		TEE_TCB_INFO_HASH	0x240	
0x050		TEE_TCB_INFO_HASH	0x250	
0x060		TEE_TCB_INFO_HASH	0x260	
0x070		TEE_TCB_INFO_HASH	0x270	
0x080		TEE_TCB_INFO_HASH	0x280	
0x090		TEE_TCB_INFO_HASH	0x290	
0x0A0	REPORTDATA	REPORTDATA	0x2A0	MROWNERCONFIG
0x0B0		REPORTDATA	0x2B0	
0x0C0		REPORTDATA	0x2C0	
0x0D0		REPORTDATA	0x2D0	
0x0E0		REPORTDATA	0x2E0	
0x0F0		REPORTDATA	0x2F0	
0x100		REPORTDATA	0x300	
0x110		REPORTDATA	0x310	
0x120		REPORTDATA	0x320	
0x130		REPORTDATA	0x330	
0x140	RESERVE	RESERVE	0x340	RTMR[0]
0x150		RESERVE	0x350	
0x160		RESERVE	0x360	
0x170		RESERVE	0x370	
0x180		RESERVE	0x380	
0x190		RESERVE	0x390	
0x1A0		RESERVE	0x3A0	
0x1B0		RESERVE	0x3B0	
0x1C0		RESERVE	0x3C0	
0x1D0		RESERVE	0x3D0	
0x1E0	TEE_TCB_IN FO	TEE_TCB_IN FO	0x3E0	RTMR[1]
0x1F0		TEE_TCB_IN FO	0x3F0	
0x200		TEE_TCB_IN FO	0x400	
0x210		TEE_TCB_IN FO	0x410	
0x220		TEE_TCB_IN FO	0x420	
0x230		TEE_TCB_IN FO	0x430	
0x240		TEE_TCB_IN FO	0x440	
0x250		TEE_TCB_IN FO	0x450	
0x260		TEE_TCB_IN FO	0x460	
0x270		TEE_TCB_IN FO	0x470	
0x280	RESERVED	RESERVED	0x480	RESERVED
0x290		RESERVED	0x490	
0x2A0		RESERVED	0x4A0	
0x2B0		RESERVED	0x4B0	
0x2C0		RESERVED	0x4C0	
0x2D0		RESERVED	0x4D0	
0x2E0		RESERVED	0x4E0	
0x2F0		RESERVED	0x4F0	
0x300		RESERVED	0x500	
0x310		RESERVED	0x510	

TDREPORT				
ADDRESS	REPORTMA CSTRUCT	REPORTTYPE	RESERVER	ATTRIBUTES
		REPORTTYPE	RESERVER	ATTRIBUTES
0x000	REPORTMA CSTRUCT	CPUSVN	0x200	MRTO
0x010		TEE_TCB_INFO_HASH	0x210	
0x020		TEE_TCB_INFO_HASH	0x220	
0x030		TEE_TCB_INFO_HASH	0x230	
0x040		TEE_TCB_INFO_HASH	0x240	
0x050		TEE_TCB_INFO_HASH	0x250	
0x060		TEE_TCB_INFO_HASH	0x260	
0x070		TEE_TCB_INFO_HASH	0x270	
0x080		TEE_TCB_INFO_HASH	0x280	
0x090		TEE_TCB_INFO_HASH	0x290	
0x0A0	REPORTDATA	REPORTDATA	0x2A0	MROWNERCONFIG
0x0B0		REPORTDATA	0x2B0	
0x0C0		REPORTDATA	0x2C0	
0x0D0		REPORTDATA	0x2D0	
0x0E0		REPORTDATA	0x2E0	
0x0F0		REPORTDATA	0x2F0	
0x100		REPORTDATA	0x300	
0x110		REPORTDATA	0x310	
0x120		REPORTDATA	0x320	
0x130		REPORTDATA	0x330	
0x140	RESERVE	RESERVE	0x340	RTMR[0]
0x150		RESERVE	0x350	
0x160		RESERVE	0x360	
0x170		RESERVE	0x370	
0x180		RESERVE	0x380	
0x190		RESERVE	0x390	
0x1A0		RESERVE	0x3A0	
0x1B0		RESERVE	0x3B0	
0x1C0		RESERVE	0x3C0	
0x1D0		RESERVE	0x3D0	
0x1E0	TEE_TCB_IN FO	TEE_TCB_IN FO	0x3E0	RTMR[1]
0x1F0		TEE_TCB_IN FO	0x3F0	
0x200		TEE_TCB_IN FO	0x400	
0x210		TEE_TCB_IN FO	0x410	
0x220		TEE_TCB_IN FO	0x420	
0x230		TEE_TCB_IN FO	0x430	
0x240		TEE_TCB_IN FO	0x440	
0x250		TEE_TCB_IN FO	0x450	
0x260		TEE_TCB_IN FO	0x460	
0x270		TEE_TCB_IN FO	0x470	
0x280	RESERVED	RESERVED	0x480	RESERVED
0x290		RESERVED	0x490	
0x2A0		RESERVED	0x4A0	
0x2B0		RESERVED	0x4B0	
0x2C0		RESERVED	0x4C0	
0x2D0		RESERVED	0x4D0	
0x2E0		RESERVED	0x4E0	
0x2F0		RESERVED	0x4F0	
0x300		RESERVED	0x500	
0x310		RESERVED	0x510	

TDREPORT				
ADDRESS	REPORTMA CSTRUCT	REPORTTYPE	RESERVER	ATTRIBUTES
		REPORTTYPE	RESERVER	ATTRIBUTES
0x000	REPORTMA CSTRUCT	CPUSVN	0x200	MRTO
0x010		TEE_TCB_INFO_HASH	0x210	
0x020		TEE_TCB_INFO_HASH	0x220	
0x030		TEE_TCB_INFO_HASH	0x230	
0x040		TEE_TCB_INFO_HASH	0x240	
0x050		TEE_TCB_INFO_HASH	0x250	
0x060		TEE_TCB_INFO_HASH	0x260	
0x070		TEE_TCB_INFO_HASH	0x270	
0x080		TEE_TCB_INFO_HASH	0x280	
0x090		TEE_TCB_INFO_HASH	0x290	
0x0A0	REPORTDATA	REPORTDATA	0x2A0	MROWNERCONFIG
0x0B0		REPORTDATA	0x2B0	
0x0C0		REPORTDATA	0x2C0	
0x0D0		REPORTDATA	0x2D0	
0x0E0		REPORTDATA	0x2E0	
0x0F0		REPORTDATA	0x2F0	
0x100		REPORTDATA	0x300	
0x110		REPORTDATA	0x310	
0x120		REPORTDATA	0x320	
0x130		REPORTDATA	0x330	
0x140	RESERVE	RESERVE	0x340	RTMR[0]
0x150		RESERVE	0x350	
0x160		RESERVE	0x360	
0x170		RESERVE	0x370	
0x180		RESERVE	0x380	
0x190		RESERVE	0x390	
0x1A0		RESERVE	0x3A0	
0x1B0		RESERVE	0x3B0	
0x1C0		RESERVE	0x3C0	
0x1D0		RESERVE	0x3D0	
0x1E0	TEE_TCB_IN FO	TEE_TCB_IN FO	0x3E0	RTMR[1]
0x1F0		TEE_TCB_IN FO	0x3F0	
0x200		TEE_TCB_IN FO	0x400	
0x210		TEE_TCB_IN FO	0x410	
0x220		TEE_TCB_IN FO	0x420	
0x230		TEE_TCB_IN FO	0x430	
0x240		TEE_TCB_IN FO	0x440	
0x250		TEE_TCB_IN FO	0x450	
0x260		TEE_TCB_IN FO	0x460	
0x270		TEE_TCB_IN FO	0x470	
0x280	RESERVED	RESERVED	0x480	RESERVED
0x290		RESERVED	0x490	
0x2A0		RESERVED	0x4A0	
0x2B0		RESERVED	0x4B0	
0x2C0		RESERVED	0x4C0	
0x2D0		RESERVED	0x4D0	
0x2E0		RESERVED	0x4E0	
0x2F0		RESERVED	0x4F0	
0x300		RESERVED	0x500	
0x310		RESERVED	0x510	

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

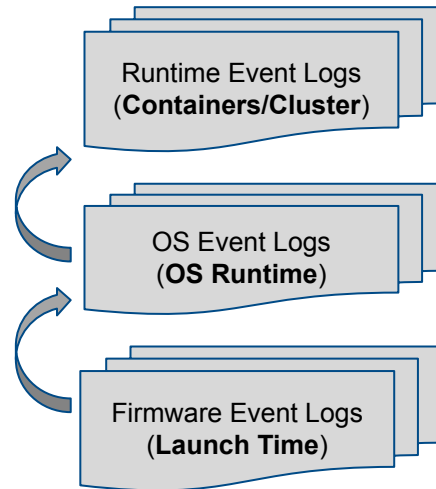
Firmware Measurement

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

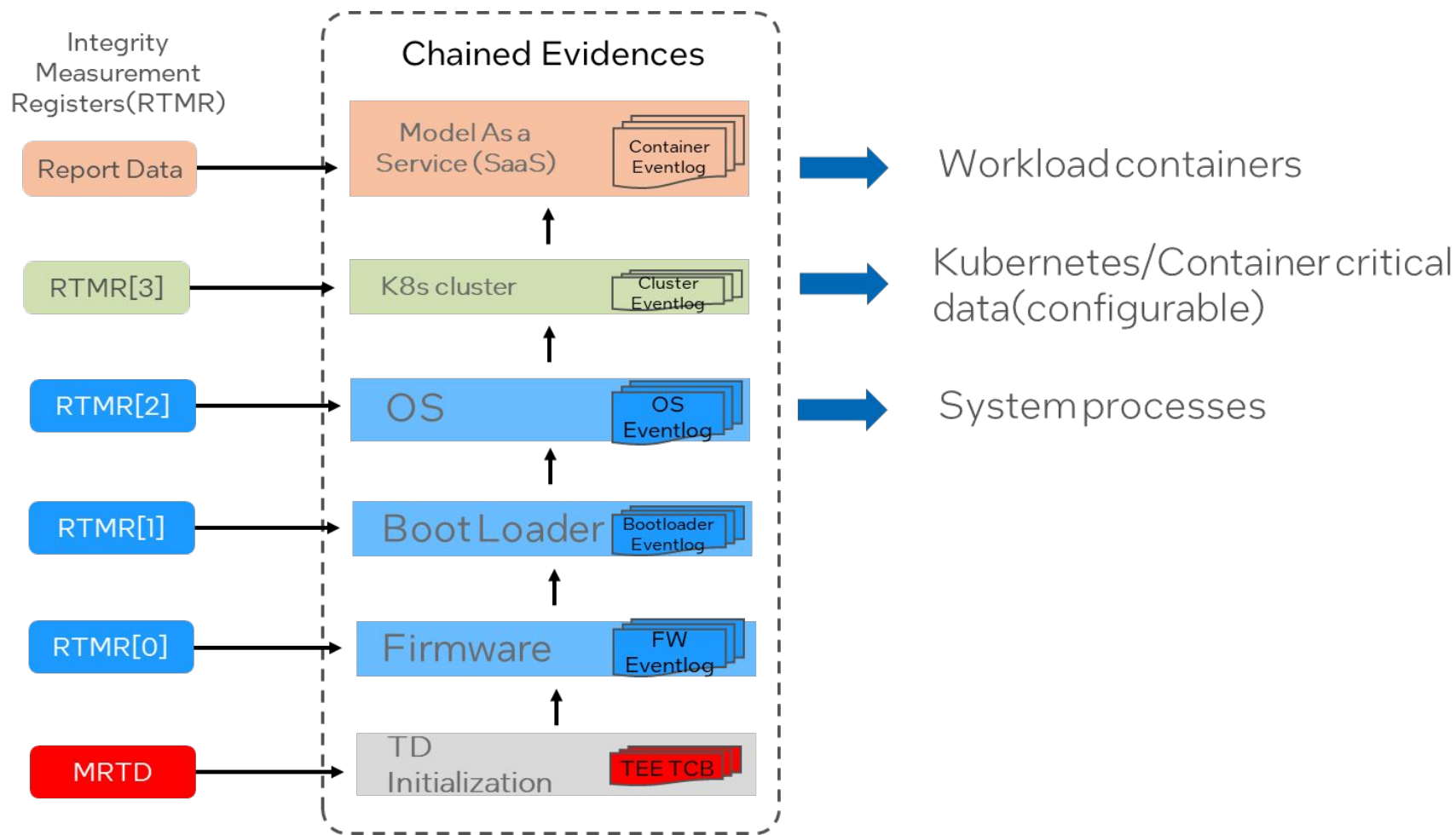


select evidences according to use case

E2E full chained measurement



How to use Evidence



Backup

Measurement(Evidence) and Attestation

