Transparent Confidentiality

Henk Birkholz <henk.birkholz@sit.fraunhofer.de>

TTT@CCC, March 10th 2022

Every System Can Do Confidential Computing

- If they are composed and configured appropriately...
- Challenges:
  - Enforcement of technical requirements
- Specific Approaches (building blocks):
  - Encrypted RAM (run-time attacks)
  - Encrypted block-devices (data-addressed attacks)
  - TLS terminated inside a TEE (data leakage attacks)
- The actual challenge is about trustworthy reporting about trustworthiness

Not Every System Can Do Reporting

- Because not every system is composed in a suitable manner...
- Challenge:
  - Believable statements about appropriate technical enforcements
- Specific Approaches (building blocks):
  - Roots of Trusts, such as eSE, SGX/TDX, SME/SVE, TPM...
    (see https://datatracker.ietf.org/doc/draft-ietf-rats-ar4si/)
  - Attesting Environments / Protected Capabilities producing Evidence
    (see https://datatracker.ietf.org/doc/draft-ietf-rats-architecture/)
- The actual challenge is to enforce technology that can report Evidence about the protected capabilities that enable Confidential Computing

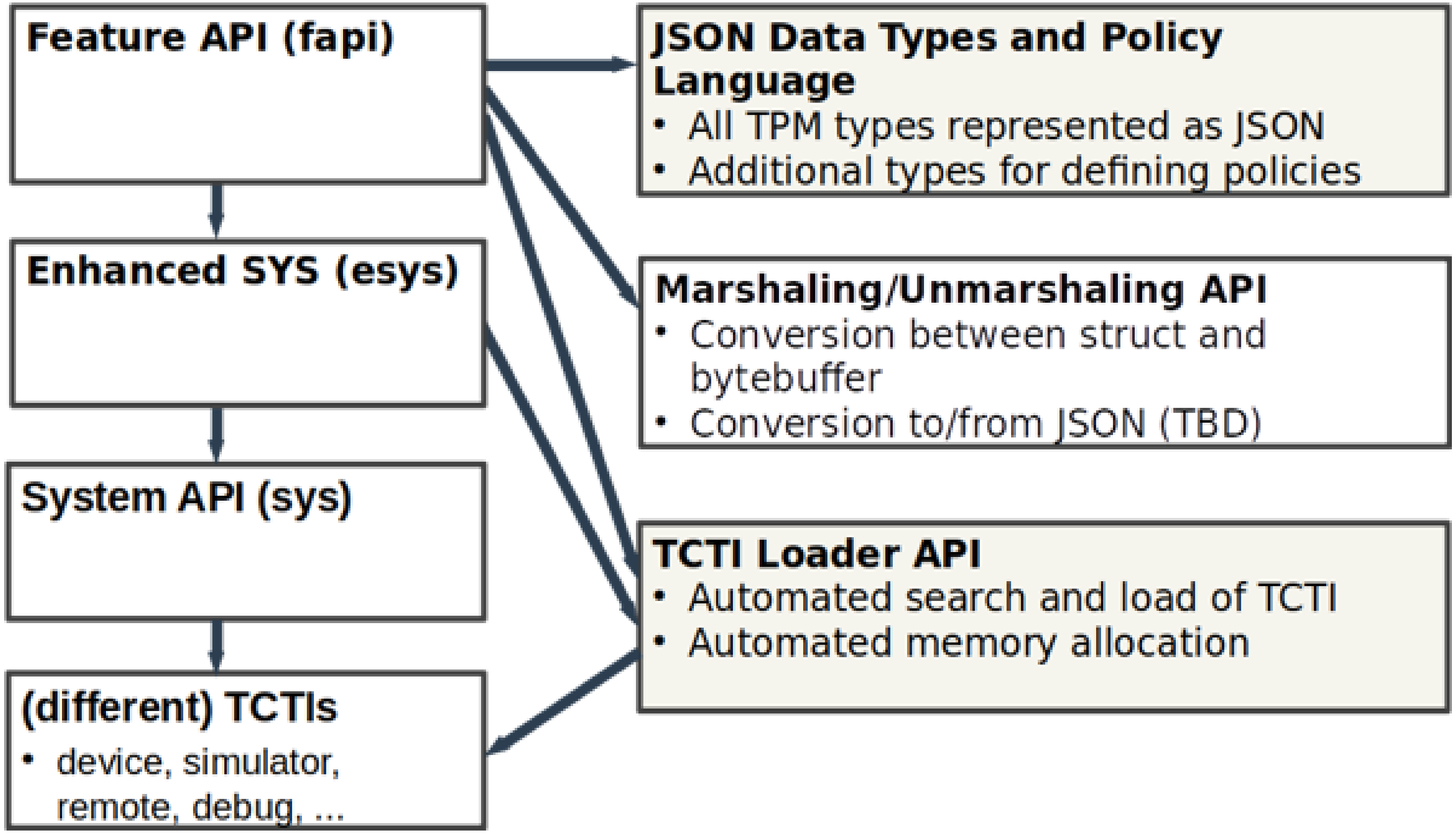
The Trusted Computing Group (TCG)

- TCG delivers specification for system components that produce believable reports (Evidence) for over 20 years.
- Specific Approaches (building blocks):
  - Trusted Platform Module (TPM)
    - https://www.iso.org/standard/66510.html
    - https://trustedcomputinggroup.org/wp-content/uploads/2019_TCG_TPM2_BriefOverview_DR02web.pdf (overview)
  - Device Identifier Composition Engine (DICE)
    - https://trustedcomputinggroup.org/wp-content/uploads/DICE-Certificate-Profiles-r01_pub.pdf (guidance)
  - Measurement and Attestation RootS (MARS)
    - https://trustedcomputinggroup.org/wp-content/uploads/TCG_MARSLibrarySpecification_v1_r4_6march2022.pdf (public review)

Exhibit A: The TPM Software Stack

- Exhibit A can be found at: https://trustedcomputinggroup.org/wp-content/uploads/TSS_Overview_Common_v1_r10_pub09232021.pdf
- Corresponding OSS can be found at: https://tpm2-software.github.io/
- Section 1.3 in the TSS Overview includes references for implementers, such as:
  - https://trustedcomputinggroup.org/wp-content/uploads/TCG_TPM2_r1p59_Part2_Structures_pub.pdf
  - https://trustedcomputinggroup.org/wp-content/uploads/TCG_TPM2_r1p59_Part3_Commands_pub.pdf

Exhibit A: The TPM Software Stack (TSS) (in a nutshell)



Feature API (fapi)

Enhanced SYS (esys)

System API (sys)

(different) TCTIs

- device, simulator, remote, debug, ...

JSON Data Types and Policy Language

- All TPM types represented as JSON
- Additional types for defining policies

Marshaling/Unmarshaling API

- Conversion between struct and bytebuffer
- Conversion to/from JSON (TBD)

TCTI Loader API

- Automated search and load of TCTI
- Automated memory allocation

Exhibit B: Canonical Event Log (CEL)

- Exhibit B can be found at: https://trustedcomputinggroup.org/wp-content/uploads/TCG_IWG_CEL_v1_r0p41_pub.pdf
- An abstraction layer on top of (Evidence) Event Logs (e.g., IMA)
- CEL in a nutshell (RFC 8610 CDDL in support of TSS included):

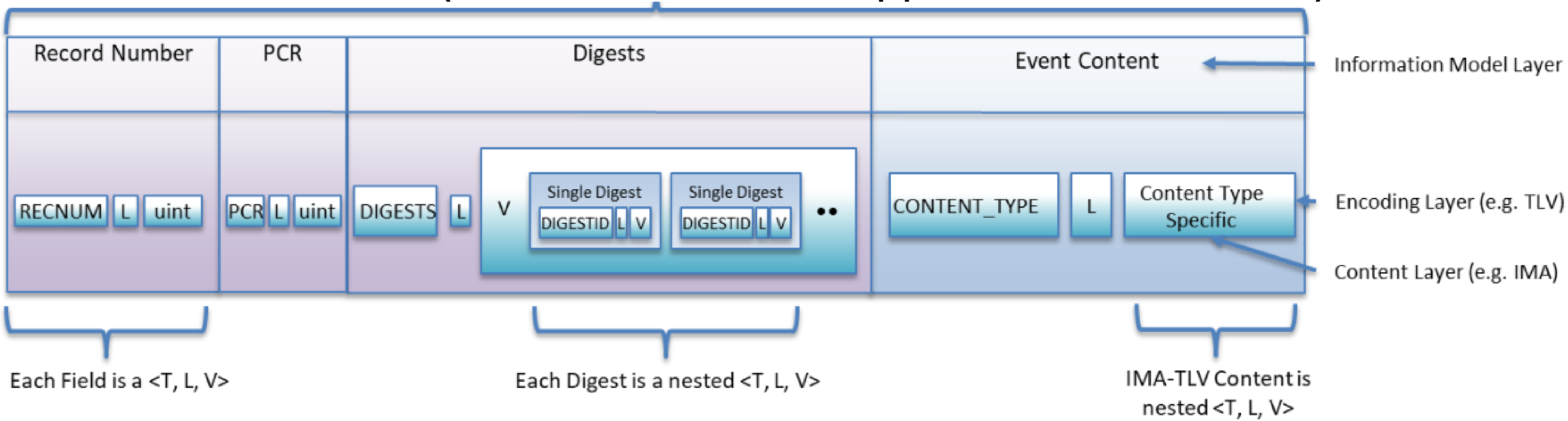
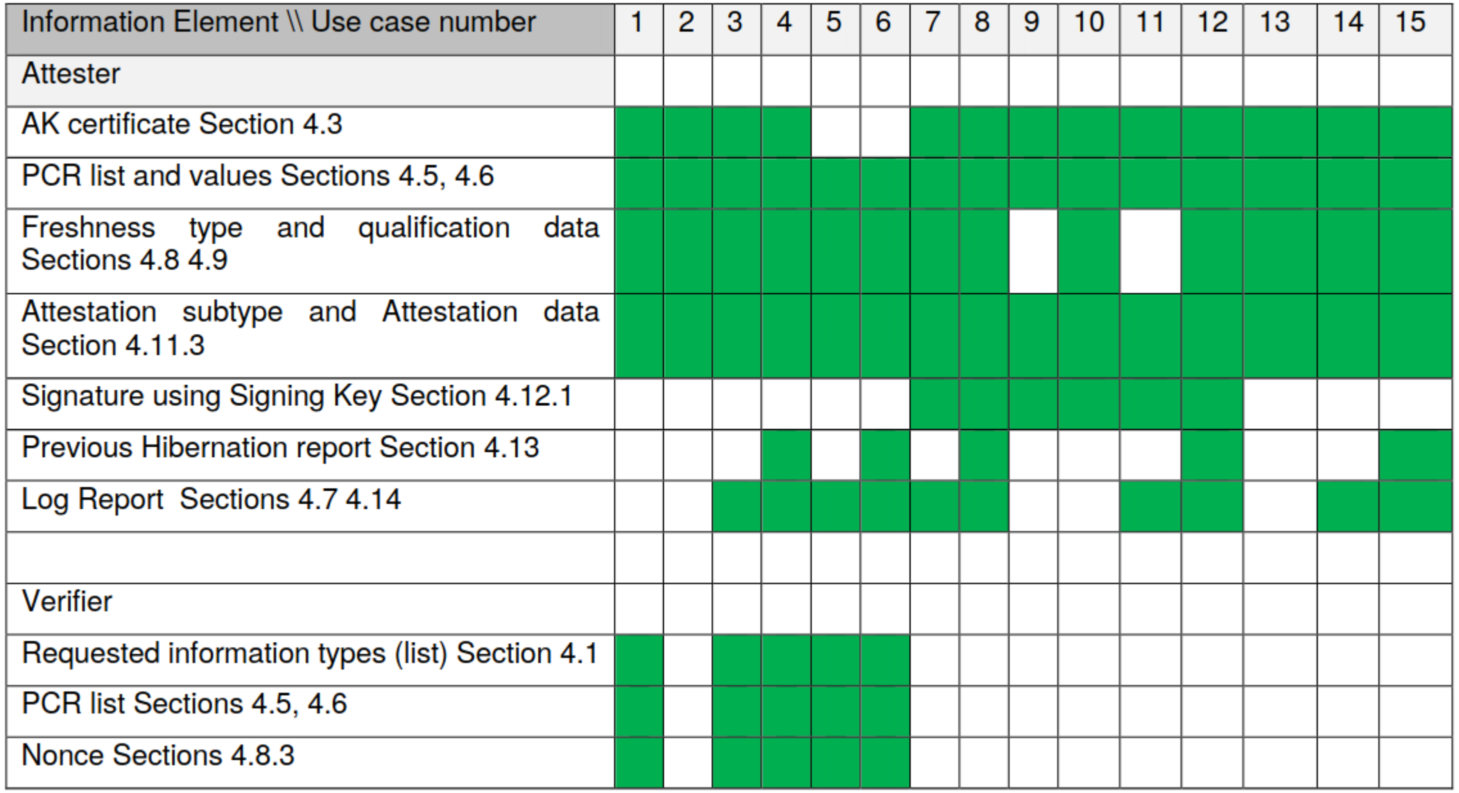


Exhibit C: Trusted Attestation Protocol (TAP)

- Exhibit C can be found at: https://trustedcomputinggroup.org/wp-content/uploads/TNC_TAP_Information_Model_v1.00_r0.36-FINAL.pdf
- Definition of common/generic information elements and their application in interaction models and typical use-cases.
- Conveyance of information elements between: Attester <-> Verifier



Information Element \\ Use case number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Attester															
AK certificate Section 4.3	🟩	🟩	🟩	🟩			🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
PCR list and values Sections 4.5, 4.6	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Freshness type and qualification data Sections 4.8 4.9	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩		🟩		🟩	🟩	🟩	🟩
Attestation subtype and Attestation data Section 4.11.3	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Signature using Signing Key Section 4.12.1							🟩	🟩	🟩	🟩	🟩	🟩			
Previous Hibernation report Section 4.13				🟩		🟩		🟩				🟩			🟩
Log Report Sections 4.7 4.14			🟩	🟩	🟩	🟩	🟩	🟩			🟩	🟩		🟩	🟩
Verifier															
Requested information types (list) Section 4.1	🟩		🟩	🟩	🟩	🟩									
PCR list Sections 4.5, 4.6	🟩		🟩	🟩	🟩	🟩									
Nonce Sections 4.8.3	🟩		🟩	🟩	🟩	🟩									

Exhibit D: Attestation WG output

- Exhibit D's charter can be found at: https://trustedcomputinggroup.org/work-groups/attestation/
- ATWG ensures that:
  - attestation related specifications
  - references, and
  - guidance from TCG

  are consistent across work groups
- ATWG's goal is compatibility and interoperability with other industry efforts focused on attestation, e.g.:
  - https://datatracker.ietf.org/wg/rats/documents/
  - https://globalplatform.org/technical-committees/trusted-platform-services-tps-committee/

Summary

- Reporting of system trustworthiness can be facilitated via TCG-based technology; enabling believable transparency in confidentiality guarantees
- TCG offers generic building blocks in support of remote attestation
    - TPM, DICE, MARS, etc.
- TCG provides various specifications and guidelines on how to implement the message flows for remote attestation
    - TSS, CEL, TAP, etc.
- TCG creates new concepts and illustrates landscapes of current ecosystems taking into account the work of various SDOs:
    - CyberResilence WG, Attestation WG, Infrastructure WG, NetworkEquipment WG, etc.