



TCG Overview

Briefing to ACSAC

December 7, 2004

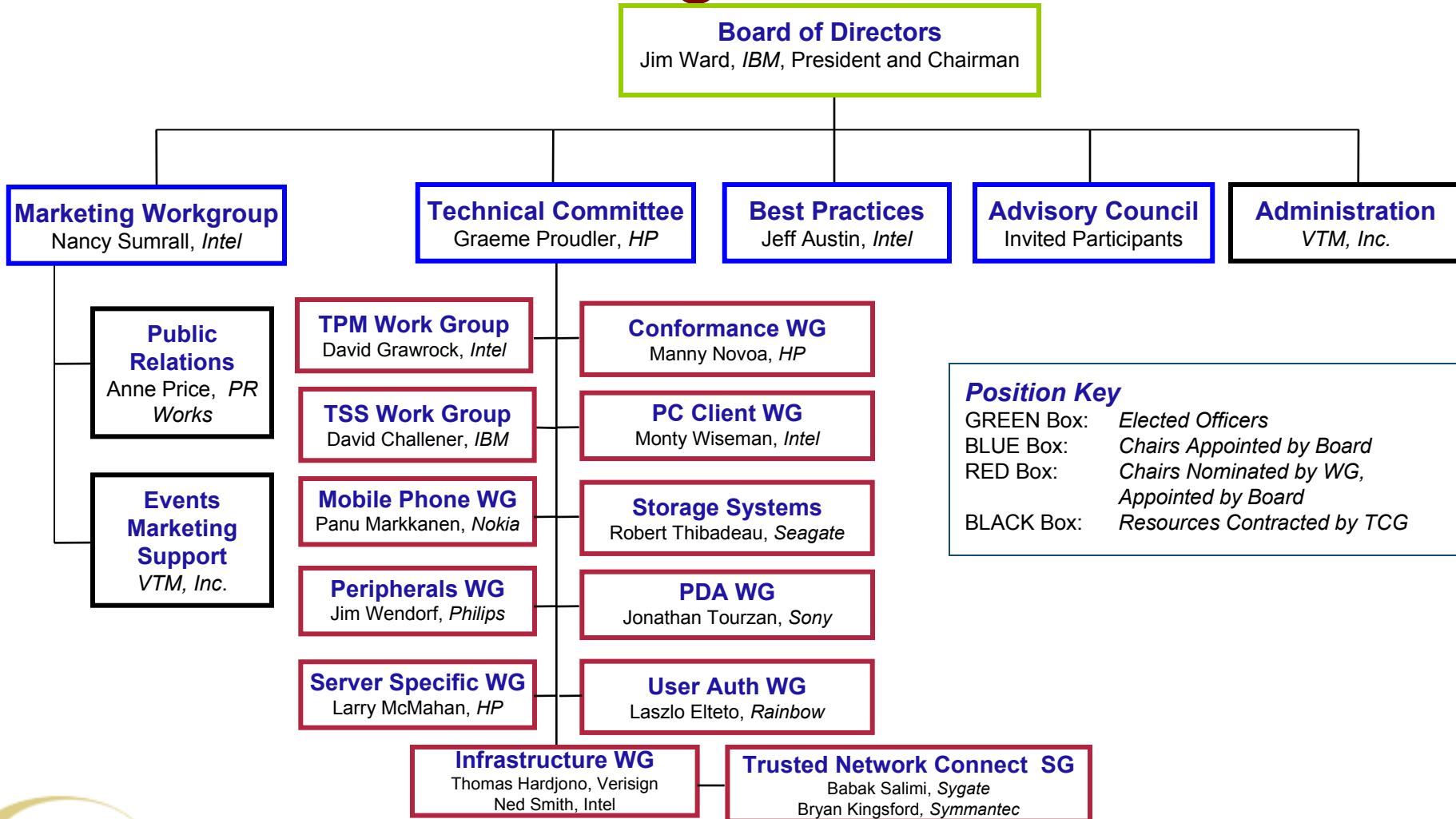
TCG Organization

- **History**
 - Specifications originally developed by TCPA
 - Specifications adopted by TCG
- **URL:**
<http://www.trustedcomputinggroup.org>
- **Membership:**
 - Promoters:
 - AMD, H-P, IBM, Intel, Microsoft, Sony, Sun
 - Contributing members: ~150 companies
 - Adopters: ~25 companies
- **Incorporated**
 - Non-profit corporation
 - Similar to PCI, USB, etc.
 - BOD:
 - Promoters
 - + 2 Elected board members
 - Verisign, Seagate



TCG Confidential

TCG Organization



TCG Confidential

TCG Products Available

- Announced TPM Manufacturers
 - Atmel
 - Broadcom
 - Infineon
 - National Semiconductor
 - ST Microelectronics
- Shipping platforms support TCG
 - HP
 - Thinkpads and desktops
 - IBM
 - Intel
- Software
 - Wave
 - IBM
 - Infineon
 - NTRU
- Compatibility
 - PKCS #11 and CAPI CSPs



TCG Confidential

Fundamental Concepts



TCG Confidential

What is TCG Technology

- Defines a hardware device¹
 - Trusted Platform Module = a TPM
- The TPM cannot be moved
 - Attached to the platform
- The TPM contains
 - cryptographic engine
 - protected storage
- Functions and storage are isolated
 - Provides a “Trust Boundary”

¹ This is a typical implementation but TCG does not specifically mandate a hardware device



TCG Confidential

Scope of TCG Technology

- TCPA is a platform neutral specification
 - IA32
 - IPF
 - PDA
 - Cell phone
- Platform Specific behavior defined by WGs

Trust & Attestation

- Attestation is the basis for Trust
 - Attestation requires a platform identity & quality assertions
 - But not necessarily one that contains PII
- Attestation provided by a trusted components / entities
 - Not software alone
 - Attacks and risks are understood
 - The TPM is the trusted root
- The verifier makes its own decisions
 - The assurance it has in the identity
 - The values of the trust state

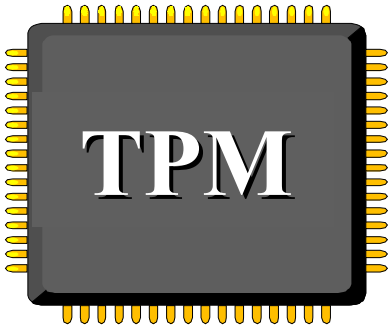


TCG Confidential

Historically TPM has been at the heart of the TCG

In simplest terms:

– A TPM is like a SmartCard attached to a platform



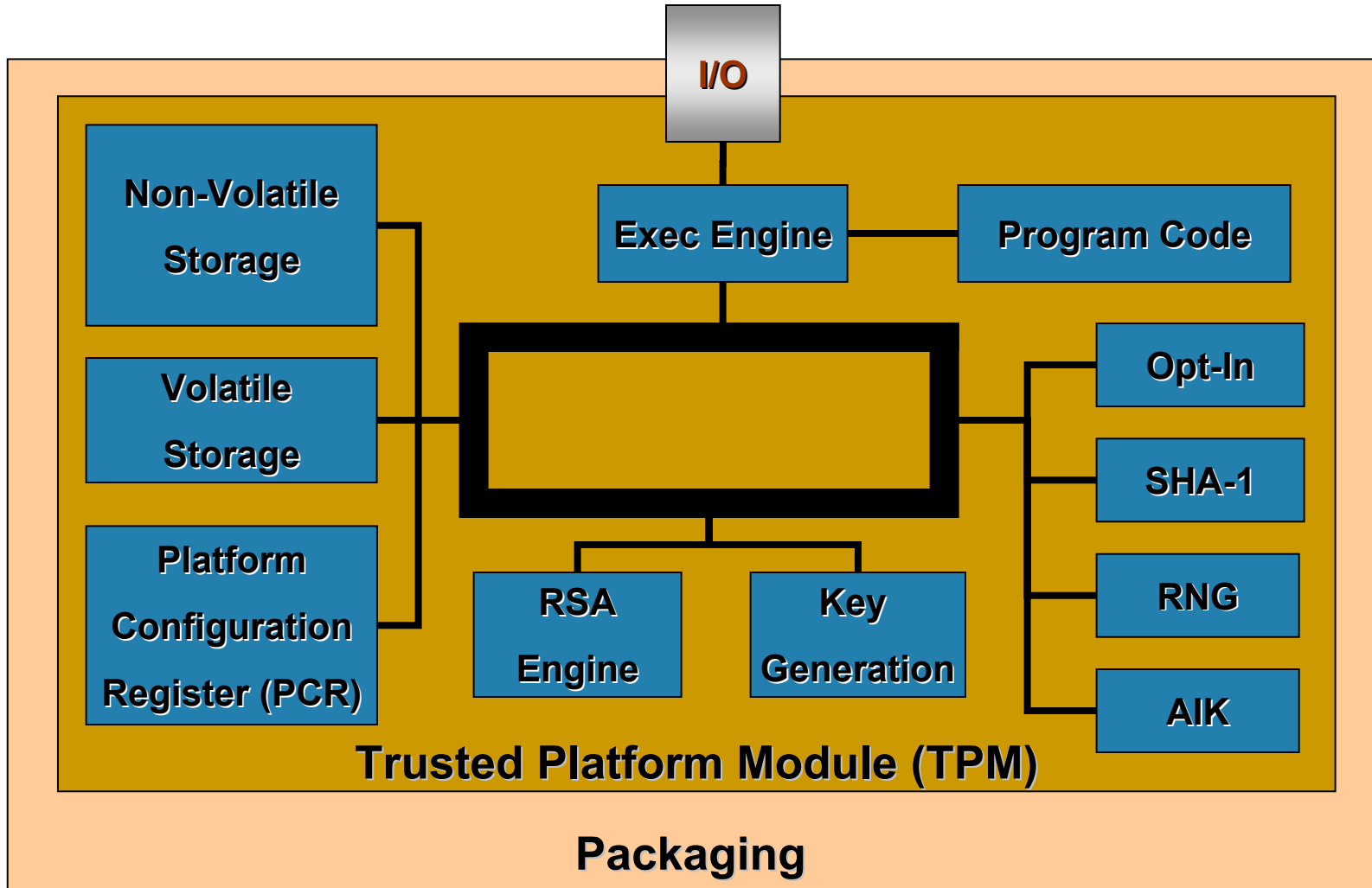
– TCG defines TPM functionality

- Protected operations
- Protected storage
- Privacy features
- Not the implementation

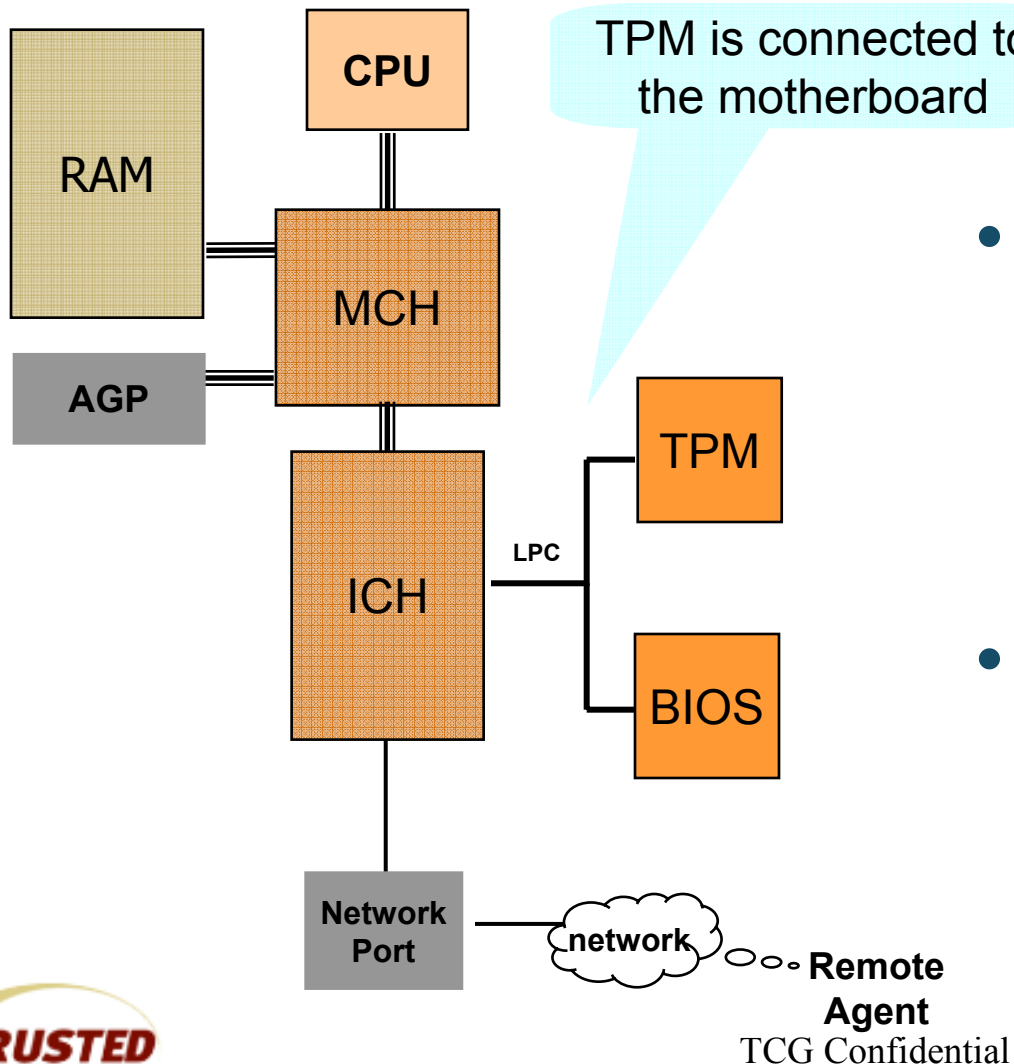
Auxiliary Functions

- Random Number Generator
- Monotonic Counter
- Tick Counter
- Digital Signature
- NV Storage
- Delegation
- Clear Endorsement Key
- Transport Session
- Context Management
- Locality

Basic TPM Layout



TCG PC Client H/W Design



- In 1.1b all designs used the LPC bus
 - LPC bus was not required
- In 1.2 all designs **MUST** use the LPC bus

TPM Feature and Function

Base Features

TPM Storage

- Key operations protected by TPM's hardware
- No access to private key data

TPM Authentication

- Provides authentication of platform
- Pseudonymous identity
- No universal identification of platform

Integrity Features

Integrity Storage (Seal/Unseal)

- Protected Storage
 - Platform Integrity

Platform Attestation

- Platform Authentication
 - Platform Integrity

Platform Integrity (PCRs)

Stores the platform integrity in a protected location

Other cryptographic functions

- H/W Random Number Generator
- Hash functions

Trust



TCG Confidential

Roots of Trust

- Roots of Trust form the foundation for platform trust
- Roots of Trust are explicitly trusted by verifiers through policy

TPM

Root of Trust for Storage (RTS)

- Protects TPM data in external storage devices
- Provides confidentiality and integrity for the external blobs
- Ensures the release of information occurs only in named environments
- RTS protected data can migrate to other TPMs

Root of Trust for Reporting (RTR)

- Establishes platform identities
- Reports platform configurations
- Protects reported values
- Establishes a context for attesting

The RTR shares responsibility of protecting measurement digests with the RTS
The TPM package protects RTS ↔ RTR interaction

Root of Trust for Measurement (RTM)

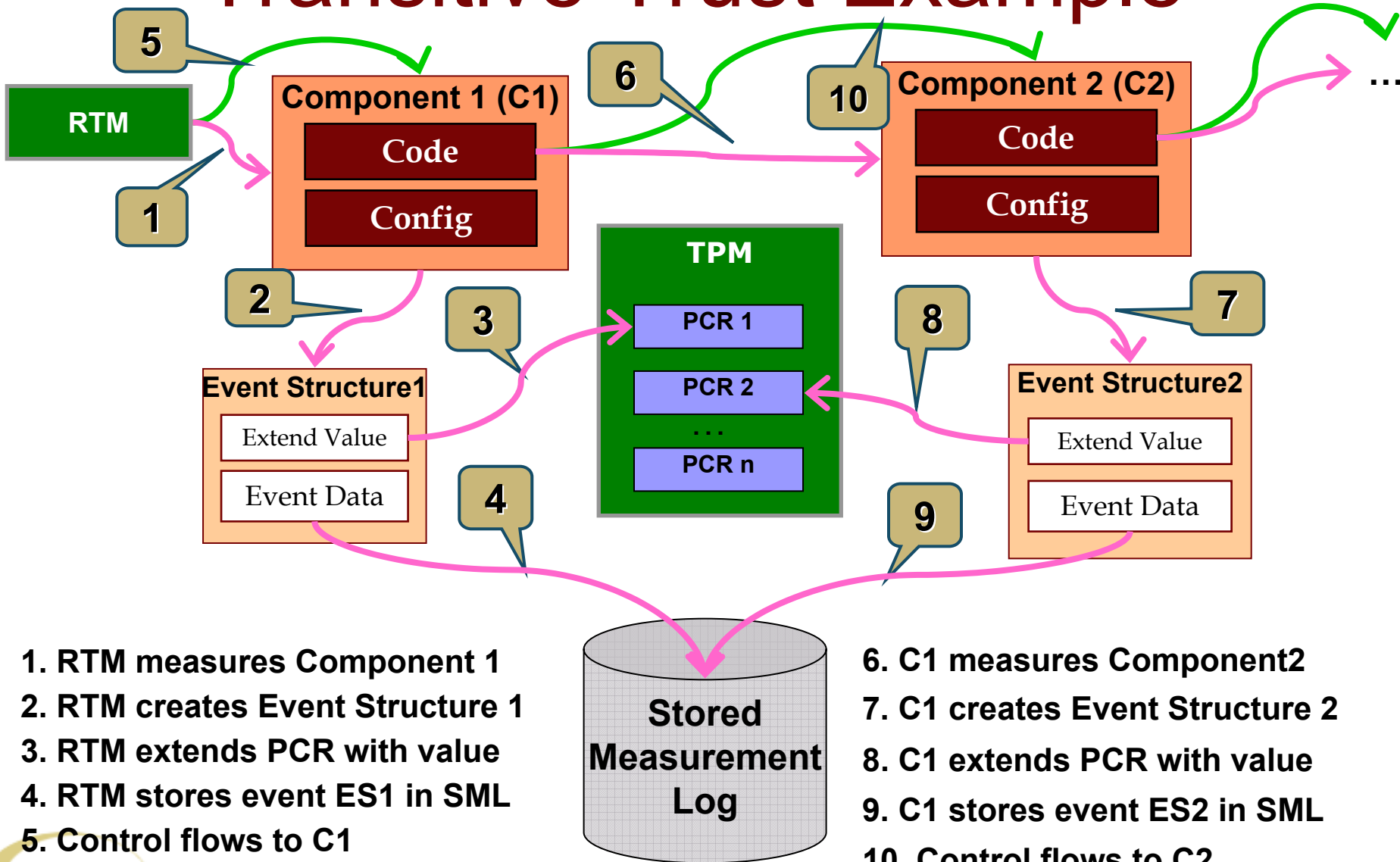
- Measures the platform's trust state
- Is considered immutable
- CRTM
 - The component that contains the RTM code

Platform

Transitive Trust

- Expands trust beyond the RTM
- Steps:
 - First: Record the state of a block of code
 - Then: Transfer control to code block
- Subsequent blocks of code repeat the steps

Transitive Trust Example



1. RTM measures Component 1
2. RTM creates Event Structure 1
3. RTM extends PCR with value
4. RTM stores event ES1 in SML
5. Control flows to C1

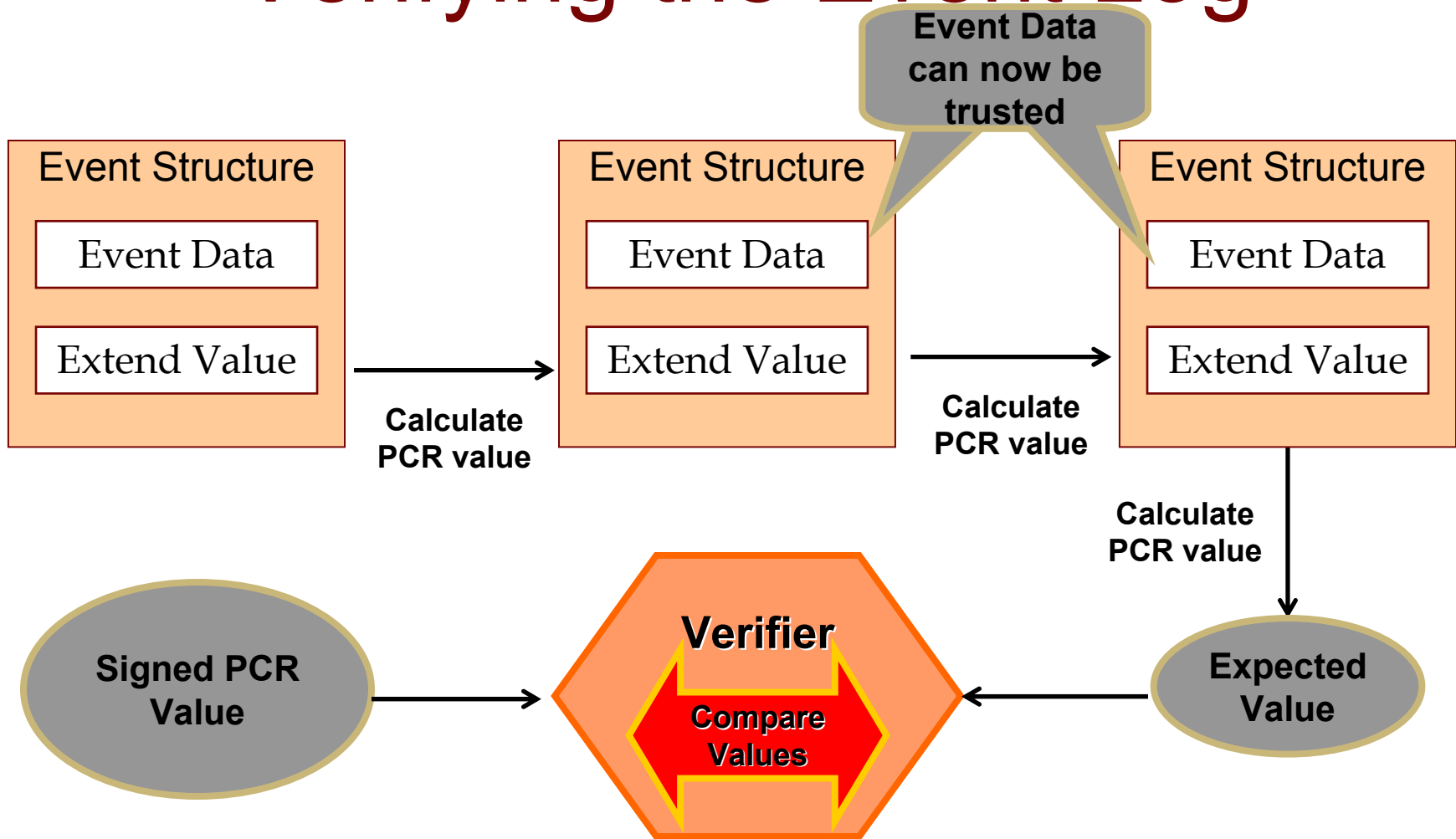
6. C1 measures Component 2
7. C1 creates Event Structure 2
8. C1 extends PCR with value
9. C1 stores event ES2 in SML
10. Control flows to C2

TCG Confidential

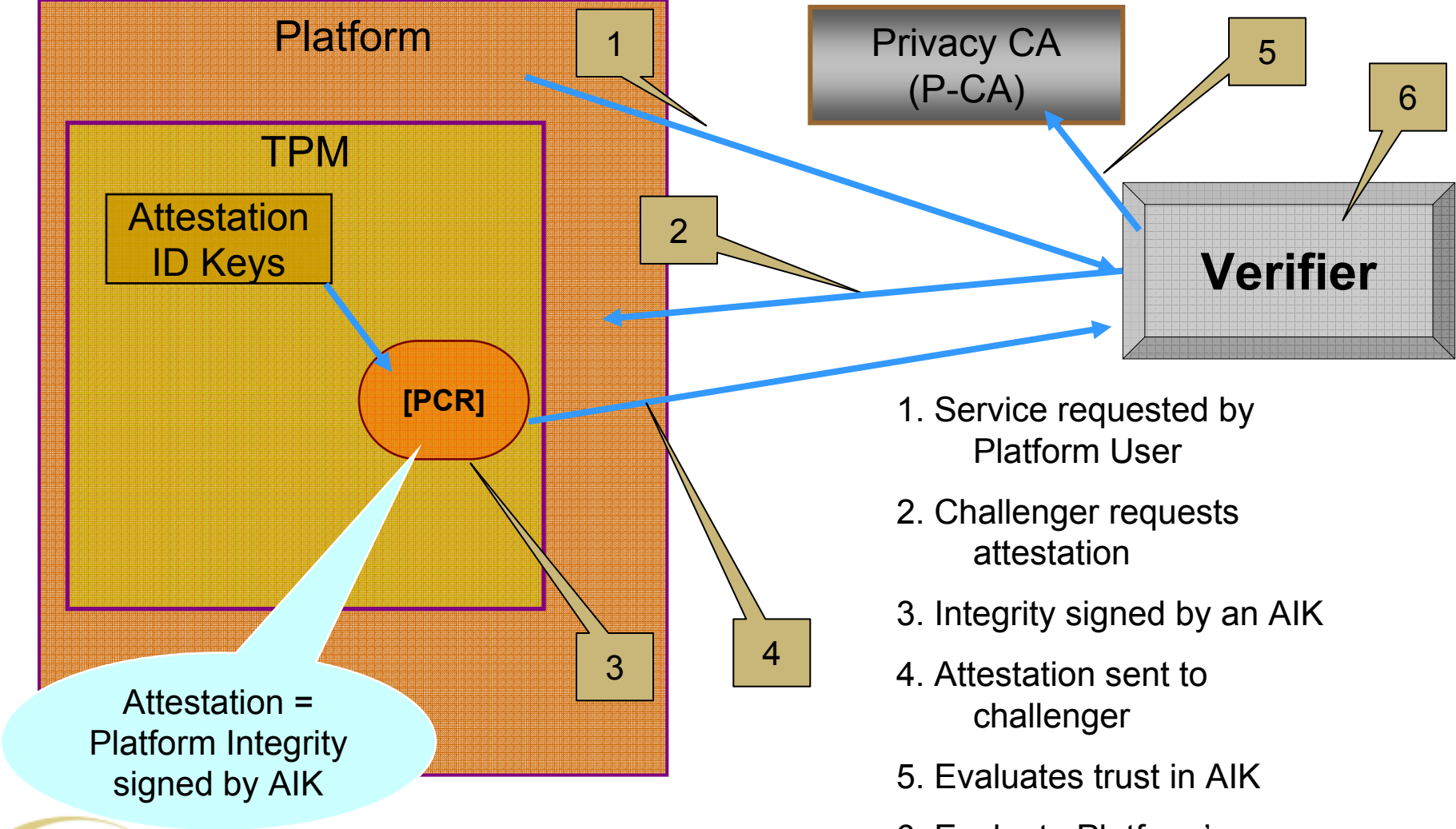
Platform Configuration Registers (PCRs)

- Stores cumulative configuration
- Update is an Extend operation:
 - $[PCR] = \text{SHA-1} \{ [PCR] + \text{Extend value} \}$
 - Value:
 - It is infeasible to calculate the value A such that:
 - $\text{PCRdesiredValue} = \text{Extend} (A)$
- Initialized to zero at TPM_Init or TPM_HASH_START
- Parsing of PCRs via Platform Specific Specifications
 - Achieve standard expected behavior

Verifying the Event Log



Using an AIK

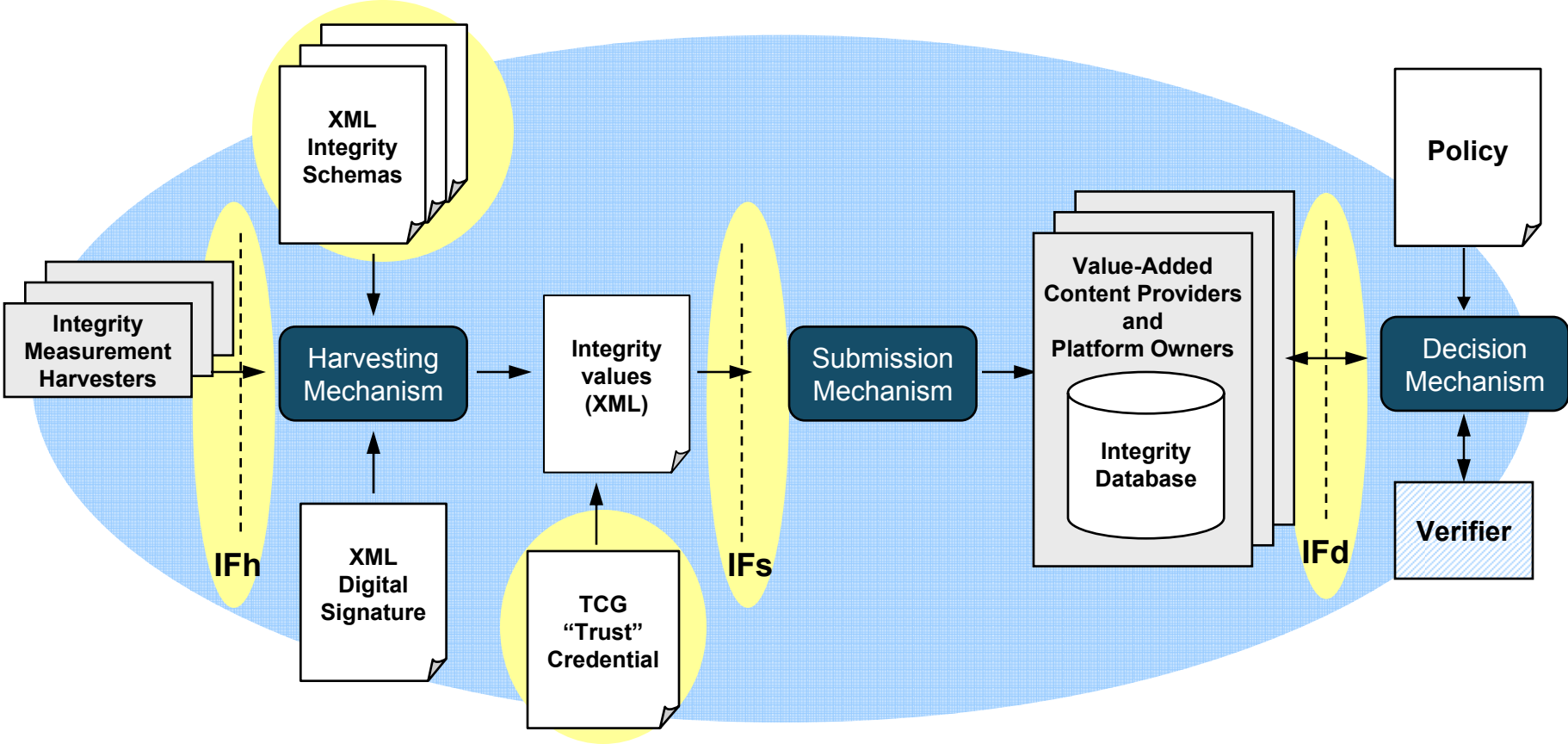


Identity Management and Integrity Management Infrastructure (for platforms)



TCG Confidential

Integrity Management Model



Out-of-Band Integrity Information Collection
 "Harvesting"
 TCG Confidential

 = TCG specification

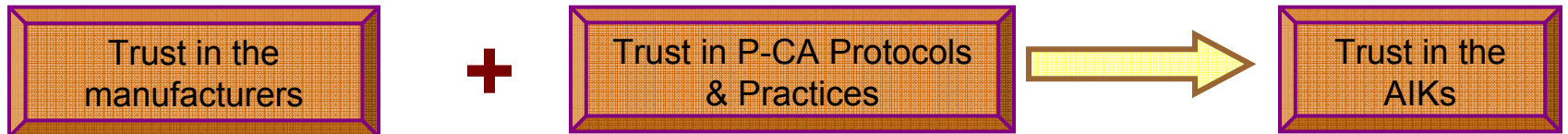


TCG Credentials

- **Endorsement Credential**
 - Certificate containing a public EK
- **Attestation Identity Credential**
 - Certificate containing a public AIK
- **Platform Credential**
 - Signed document containing assertions about a platform
- **Conformance Credential**
 - Signed Document containing assertions about a platform or its components
- **Validation Data / Integrity Values**
 - Document containing assertions about a component

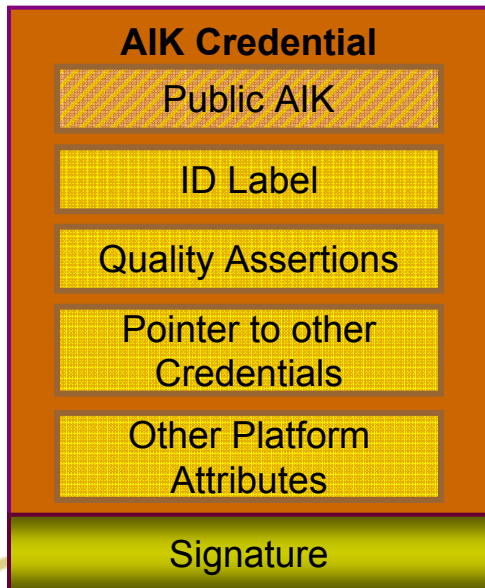
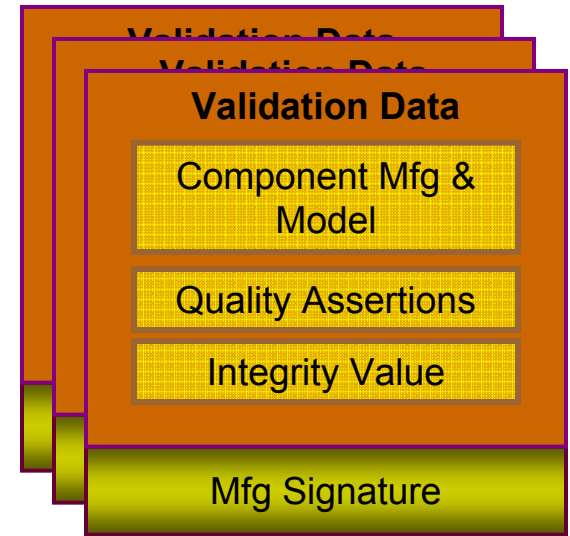
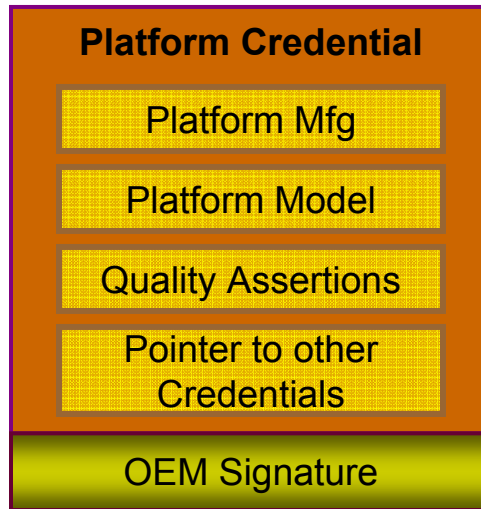
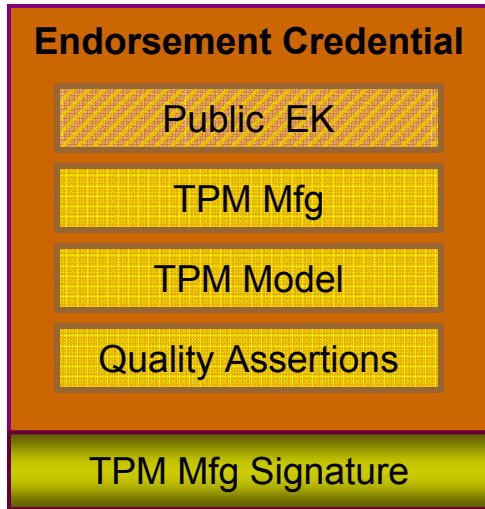
TCG Credential Concepts

- TCG Credentials provide evidence useful during the issuance of an AIK credential
- TCG Credentials provide evidence of a valid:
 - TPM
 - Platform
 - Other components



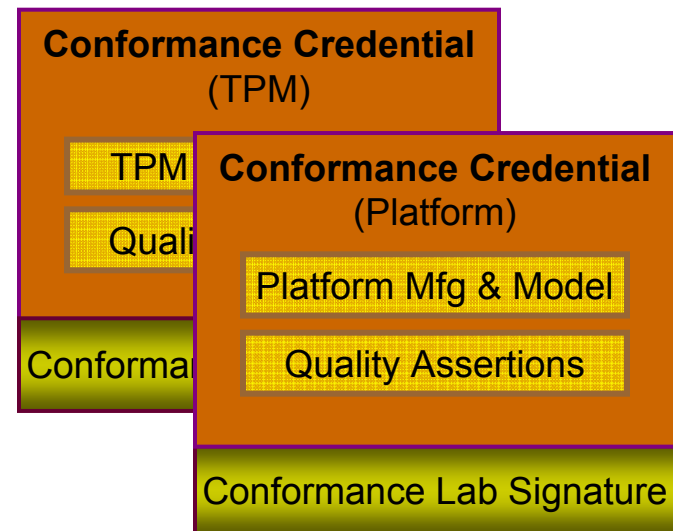
- Credentials impact manufacturing and distribution of
 - Components
 - “Finished Platforms”

Example Credential Contents



Two Credential Types

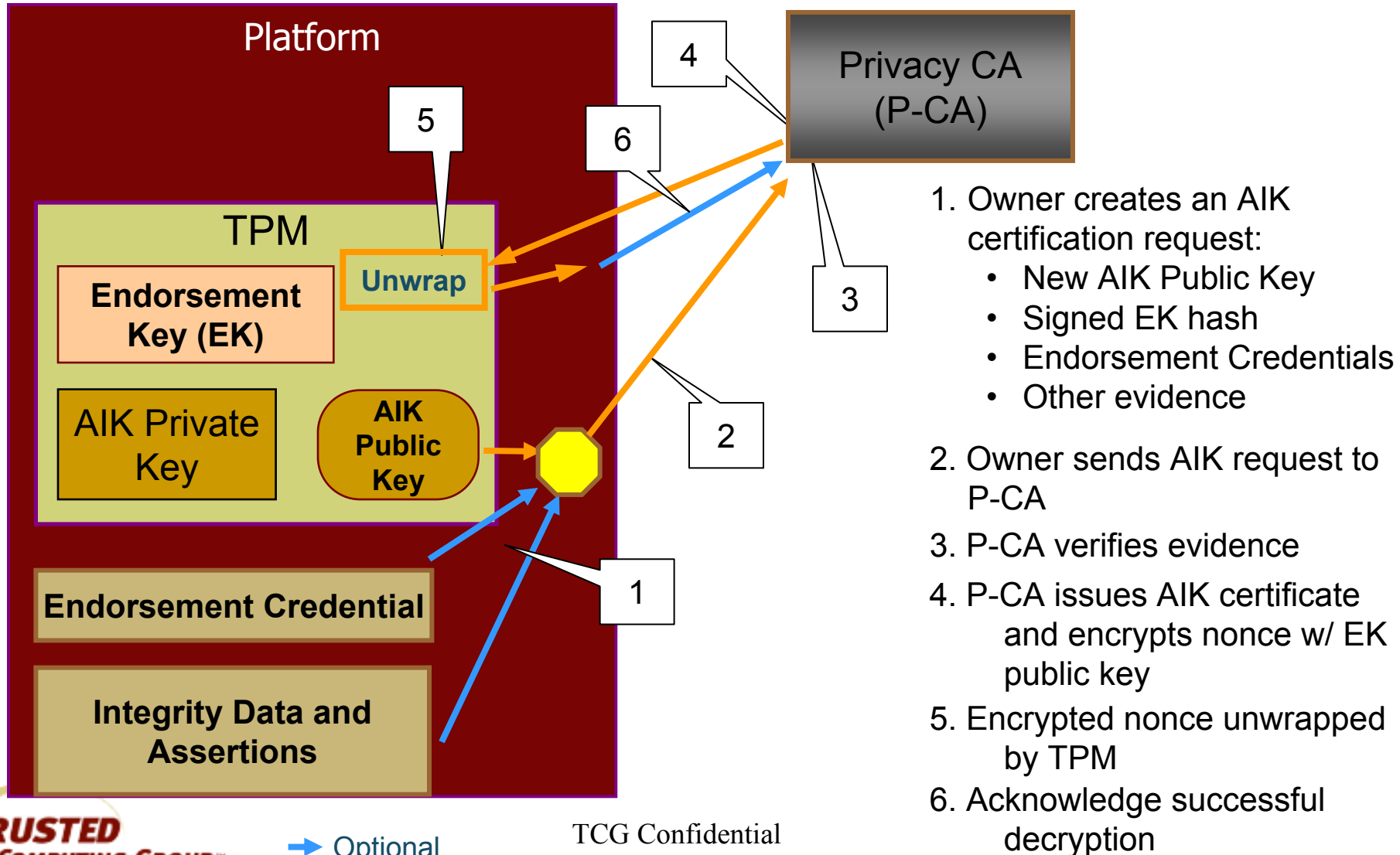
- 1) Certificates – containing public keys
- 2) Signed Documents – containing integrity and attribute data



Platform Identity Management Model

- Register an AIK with a trusted entity
 - AIKs are pseudonymous identifiers
 - Use EK to establish uniqueness and trust of AIK
- Authenticate using AIK

AIK Credential Issuance



1. Owner creates an AIK certification request:
 - New AIK Public Key
 - Signed EK hash
 - Endorsement Credentials
 - Other evidence
2. Owner sends AIK request to P-CA
3. P-CA verifies evidence
4. P-CA issues AIK certificate and encrypts nonce w/ EK public key
5. Encrypted nonce unwrapped by TPM
6. Acknowledge successful decryption

Keys



TCG Confidential

Persistent Keys

- Endorsement Key (EK)
 - Provide controllable uniqueness
 - Permanent
 - Not part of the key hierarchy
- Storage Root Key (SRK)
 - All keys are protected by this key
 - Root of Key Hierarchy
 - Changed on new owner

Key Types and Classes

- **Storage Keys**
 - Protects keys or external data
- **Signing Keys**
 - Digital signatures
- **Attestation Identity Keys (AIKs)**
 - Special Signing keys
 - Provides attestation
- **Non-Migratable Keys**
 - Permanently bound specific TPM, i.e., platform
- **Migratable Keys**
 - Can be migrated to other platforms
- **Certified Migratable Keys**
 - Can be migrated to only “certified” authorities

Key Hierarchy

Protected by the TPM

Storage Root Key (SRK)

Endorsement Key

Protected by the RTS

Migratable Storage Key

Non-Migratable Storage Key

Attestation ID Keys (signing)

Migratable Storage Key

Migratable Signing Key

Non-Migratable Storage Key

Non-Migratable Signing Key

Migratable Signing Key

Migratable Signing or Storage Key

Migratable Signing or Storage Key

Protected Storage

Seal / Unseal

- Purpose:
 - Seals data on the platform, to the platform
- Data Seals to the specific platform (by a TPM key)
- Data *may* be sealed to a platform's configuration (specified by PCRs)
- Key is authorized for use

Bind / Unbind

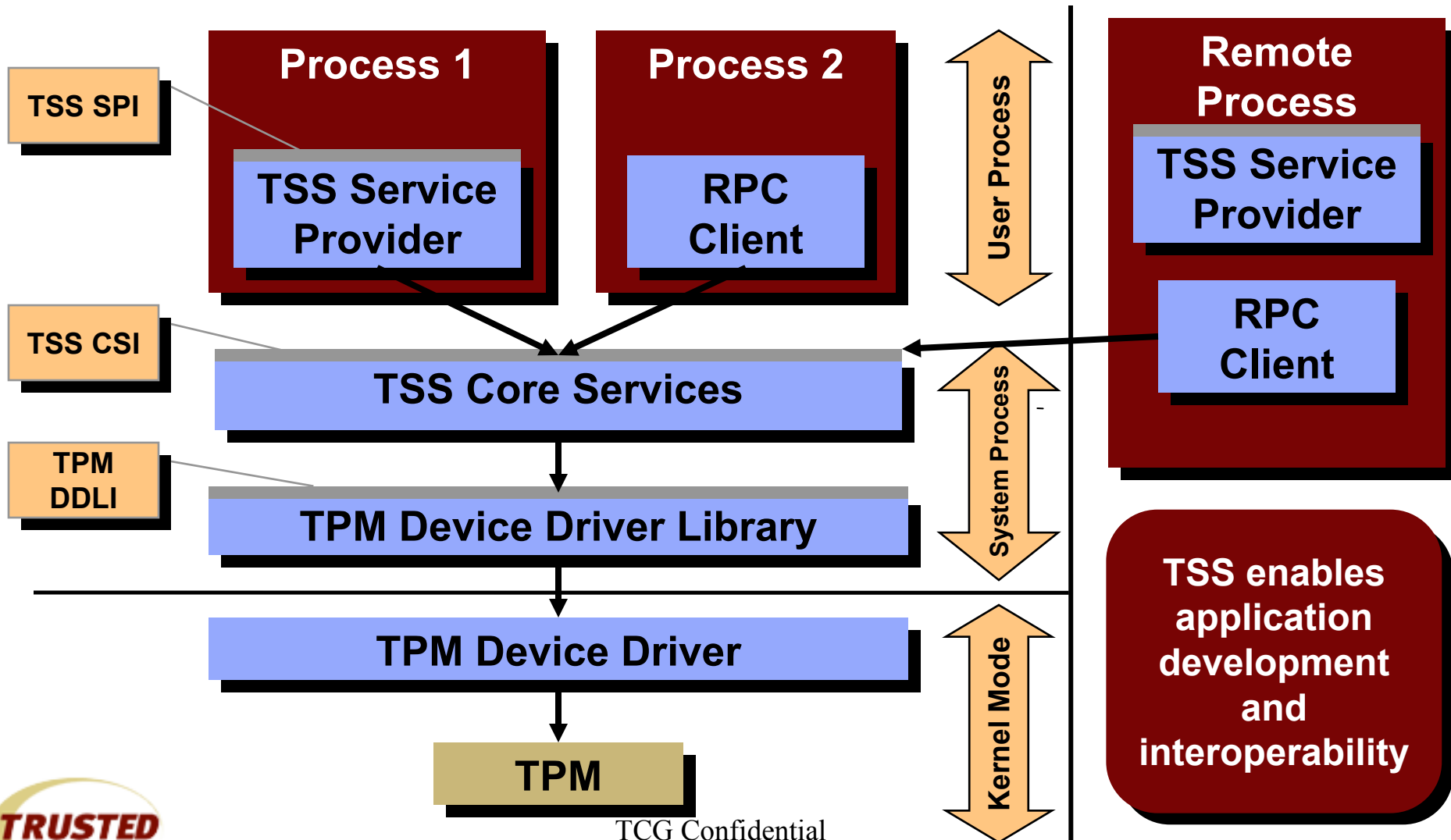
- Purpose:
 - Allows external app to send encrypted data to a specific platform or set of platforms
- Bind is an external operation
 - Asymmetric encryption
- Unbind is a TPM operation
- Unbind key may be:
 - Tied to a specific platform
 - Tied to a configuration (1.2)
 - Tied to a non-migratable key

TCG Software Stack

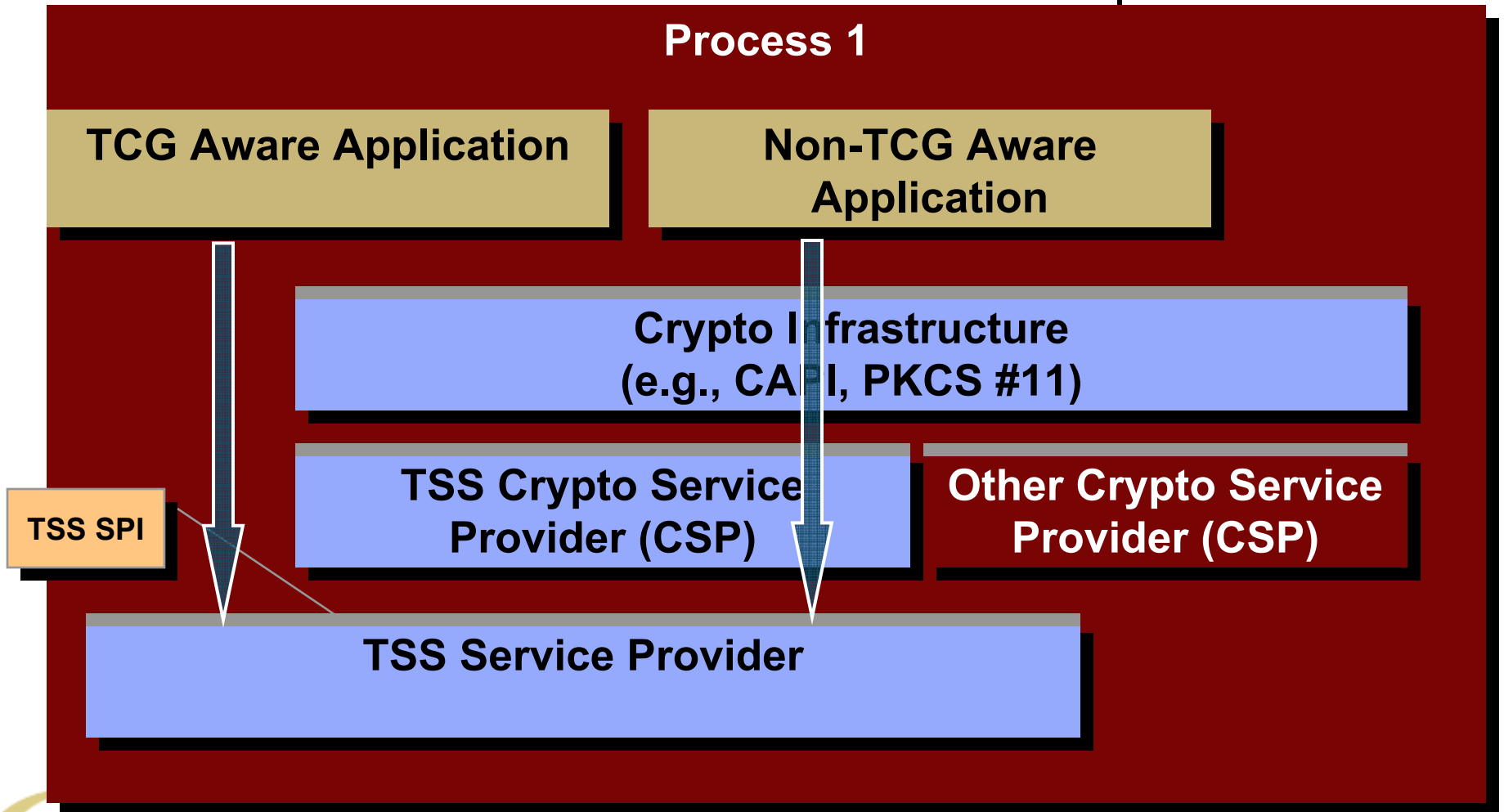


TCG Confidential

TSS Block Architecture



Using Crypto Infrastructures



Applications & Summary

- Client measurement agents
- Network access control using metrics provided by client agents
- Repositories of platform integrity data
- Infrastructure and interoperability
- Supporting services
 - Platform CAs
 - Value-added content providers
 - Network access control policies
 - Remediation

TCG is maturing

Products are available ... Base technology defined

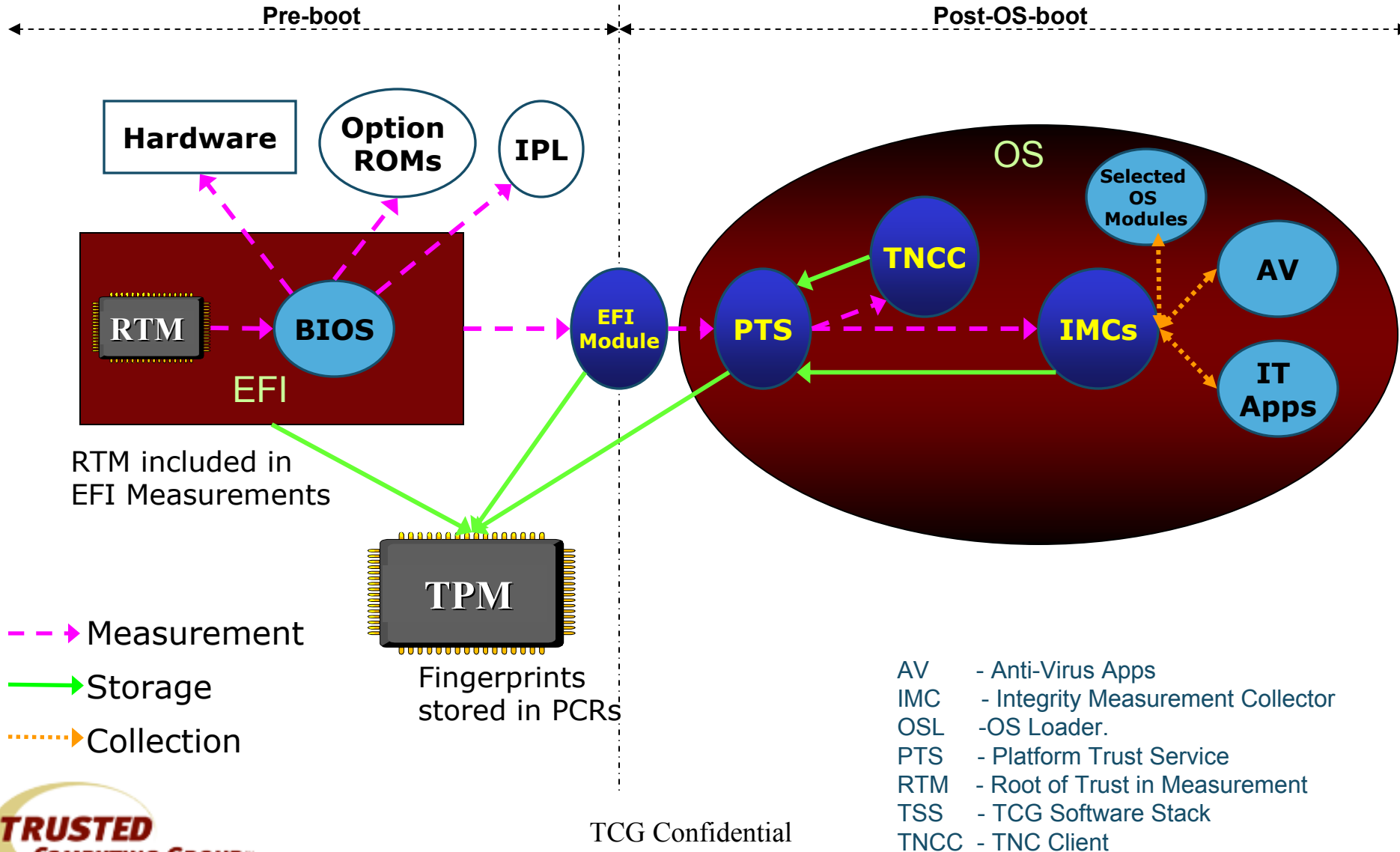
... but, still time to affect changes

Backup



TCG Confidential

Integrity Measurement (EFI)



TCG Confidential

