Tutorial: TPM for Attestation

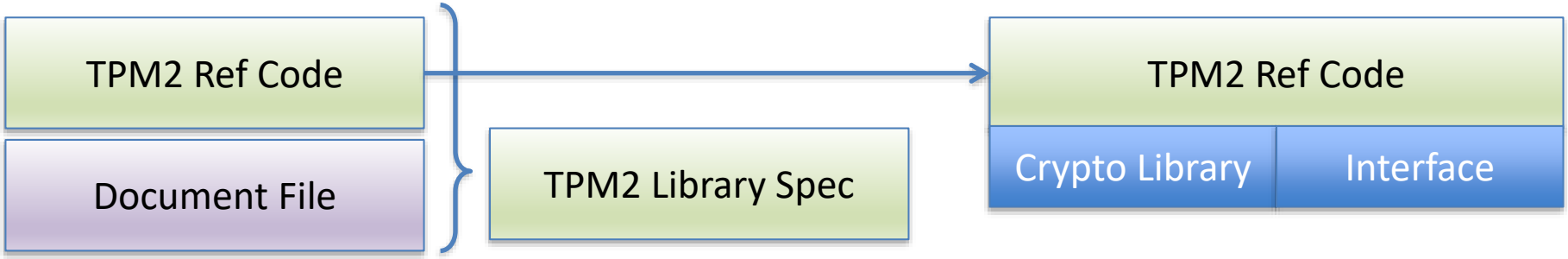
Monty Wiseman
Beyond Identity
Trusted Computing Group, Infrastructure WG Co-Chair
monty.wiseman@beyondidentity.com
mwiseman@computer.org
https://www.linkedin.com/in/monty-wiseman/

Standard Interface

- TPM API standardized and public
  - Independent of the “how” the commands get to there
    - Defined by the Platform
- Generalized Key and Asset Management
- Flexible and Extensible
  - Can be a “big” or “small” as needed
    - Configurable in the reference code in header files.
    - Typically, the largest part is the crypto library!

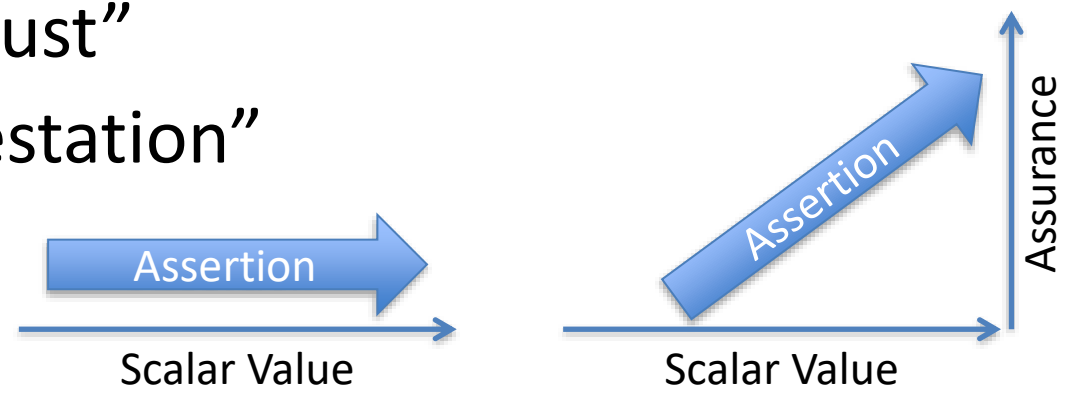
TPM Refence Code is Open

- TPM2 Reference Code
  - https://github.com/TrustedComputingGroup/TPM
  - The TPM2 spec is built from this
  - (There are other derived open source TPM2 Open-Source Project)



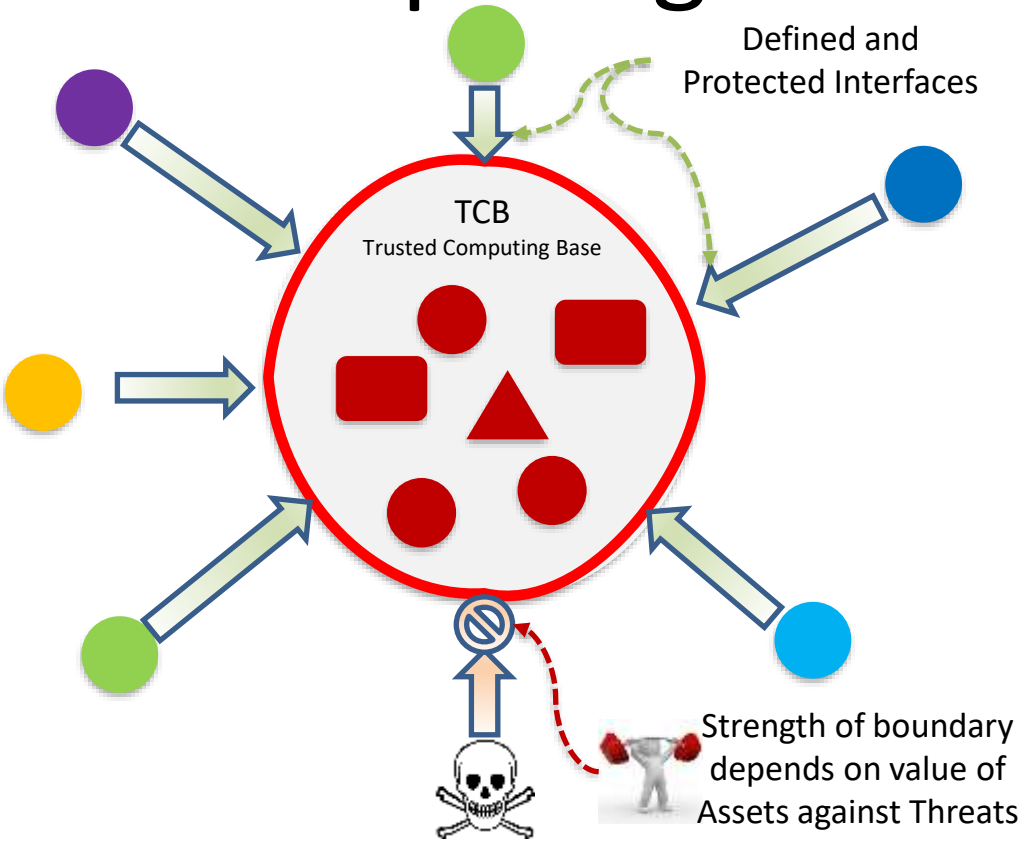
Properties as Vectors

- Concept aligned with RFC8485
- Many signals are simple scalar values
  - Creates assumptions
- Add a “Vector of Trust”
- TPM calls this “Attestation”



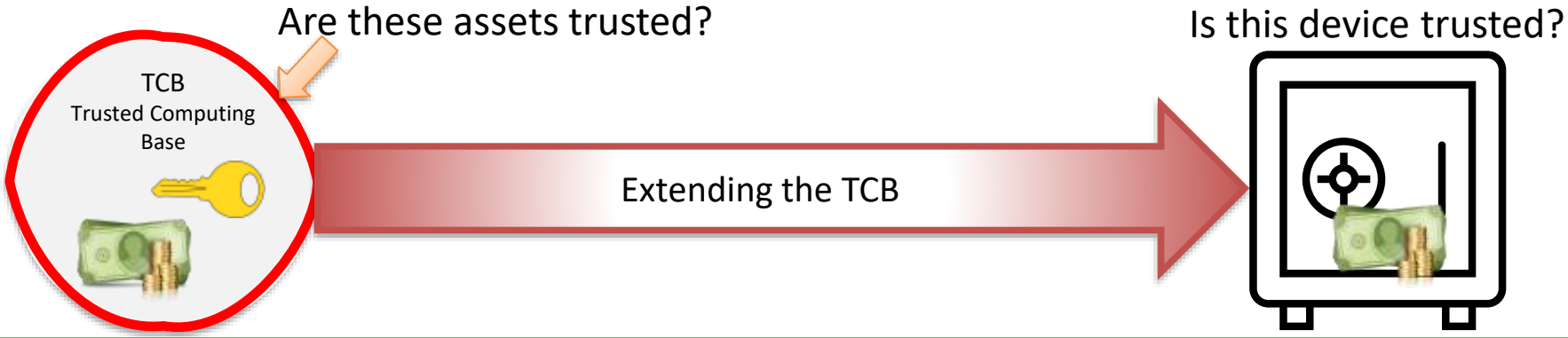
BASIC CONCEPTS-ROOTS

Trusted Computing Base - TCB

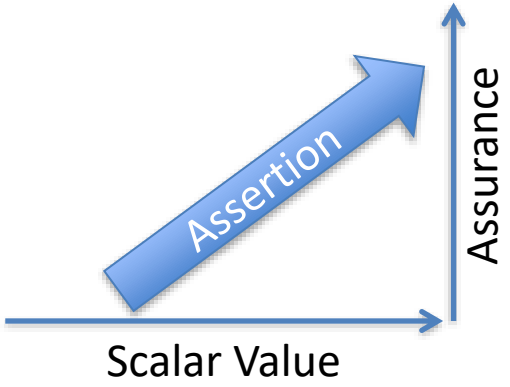


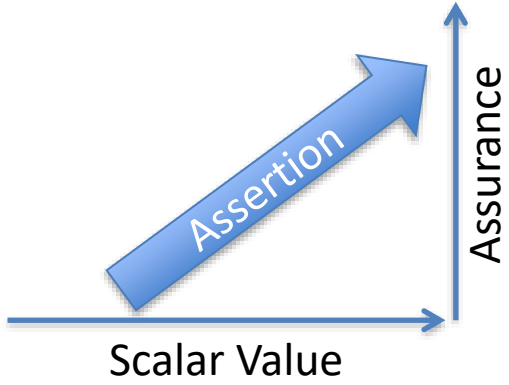
Roots of Trust

- Glossary:
  - It is trusted always to behave in the expected manner, because its misbehavior cannot be detected under normal operation.
  - A component that performs one or more security-specific functions, such as measurement, storage, reporting, verification, and/or update.
- Explanation:
  - Must begin by trusting a set of components to perform necessary functions to support Trusted Computing in the expected manner.
  - Misbehavior of these components is not detectable by the evidence and protocols provided by Trusted Computing.



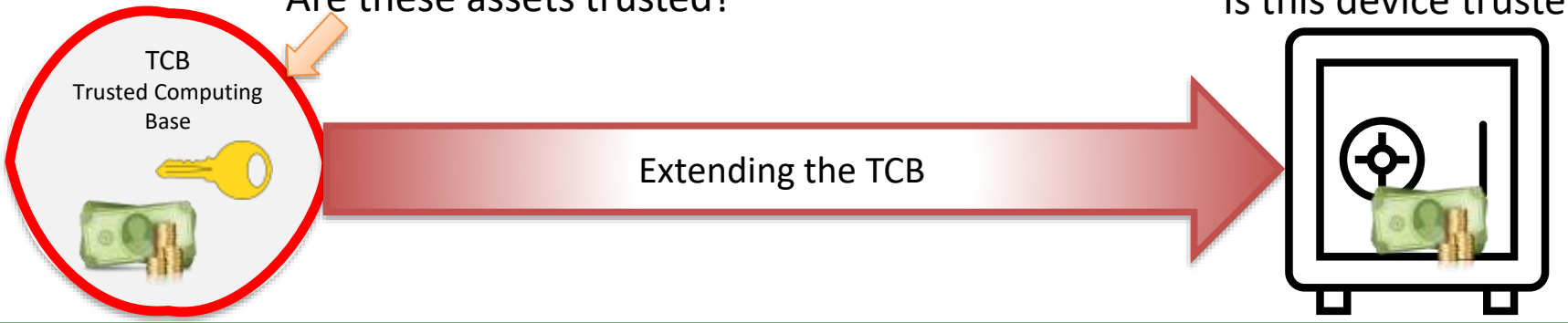
Assurance of TCB and Device Assets



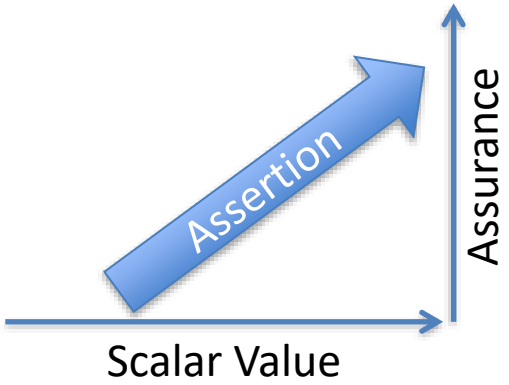


Are these assets trusted?

Is this device trusted?

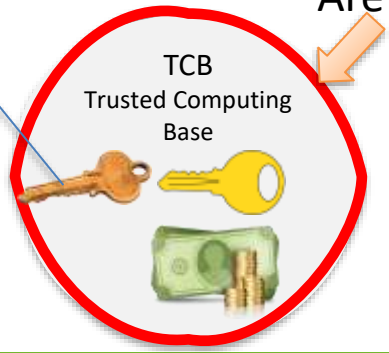


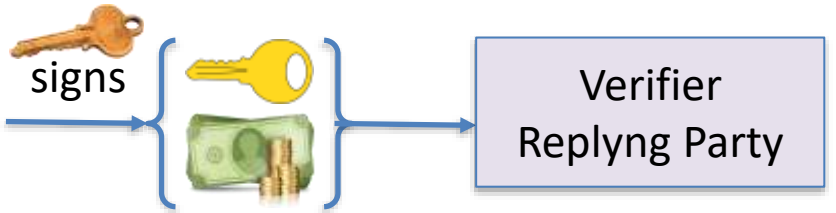
Assurance of TCB Assets



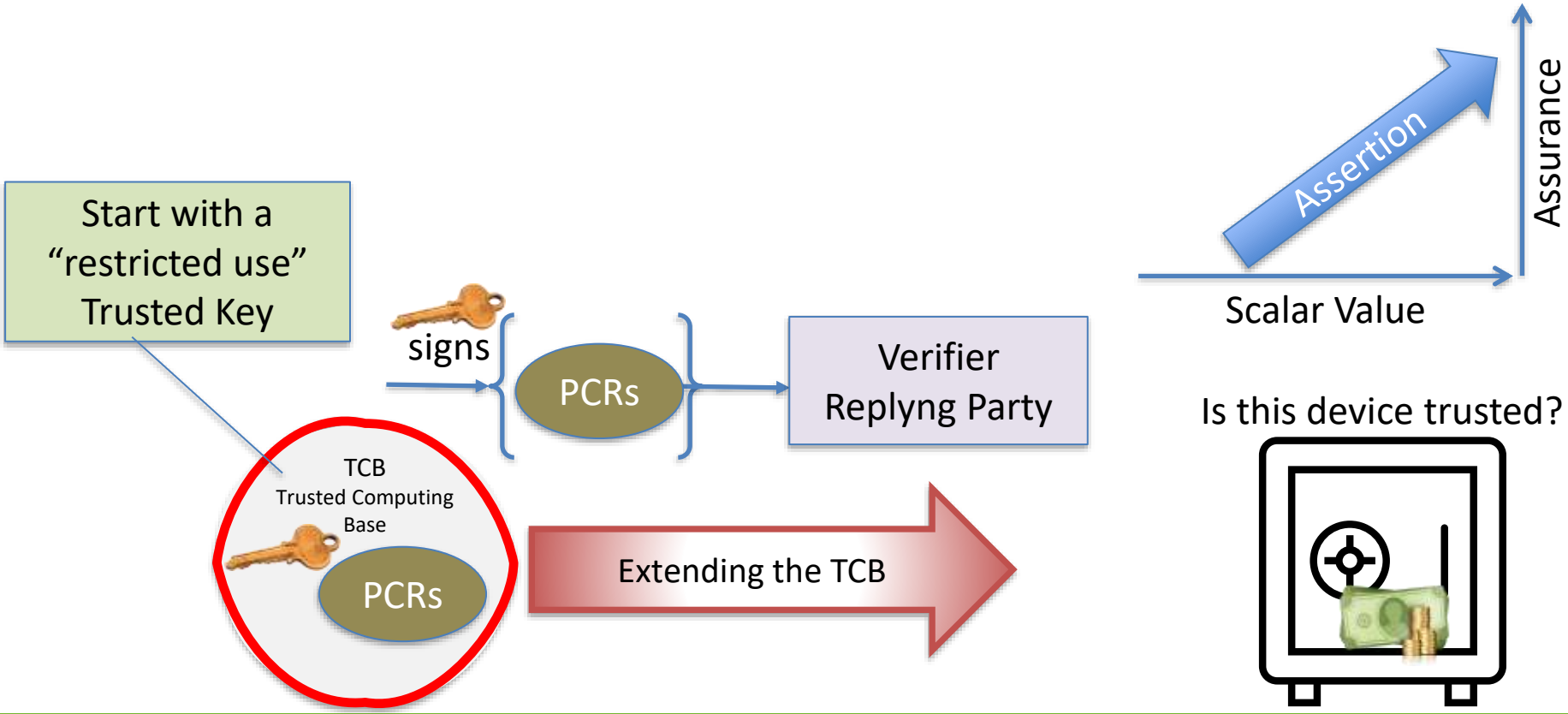
Start with a "restricted use" Trusted Key

Are these assets trusted?





Assurance of Device Assets



KEY PROPERTIES

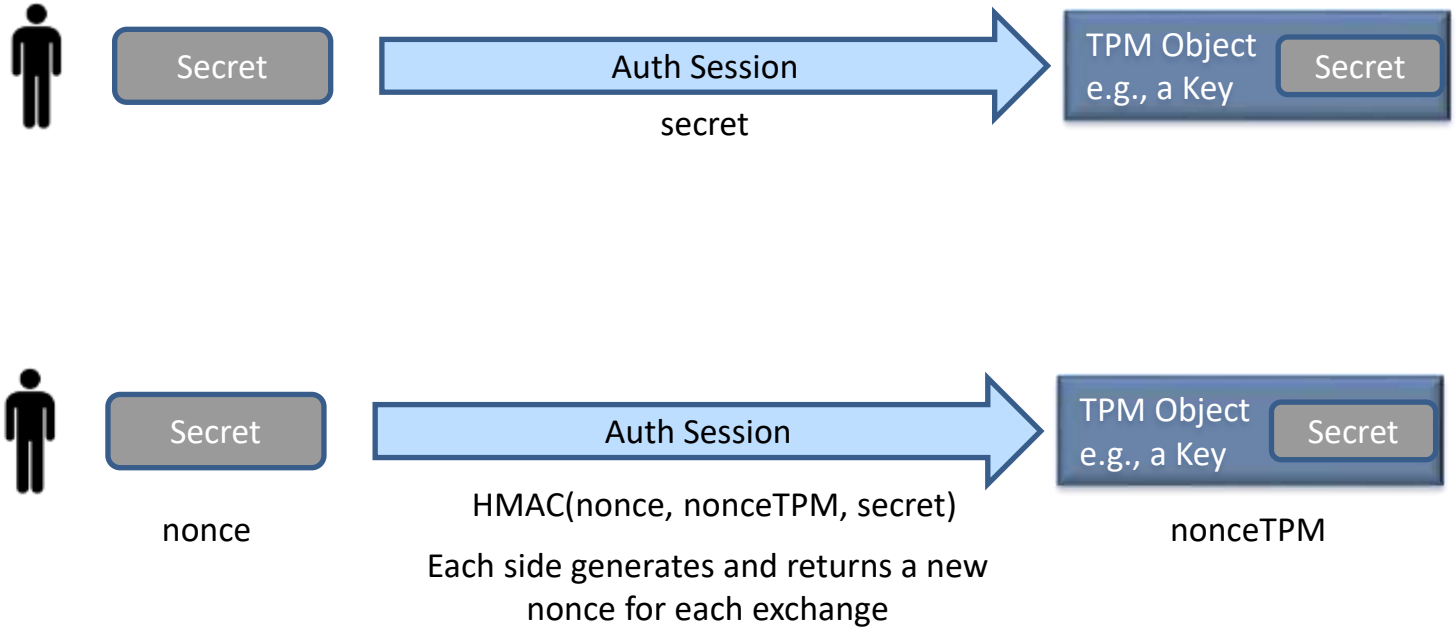
Key (and other objects) Properties

- Attributes
  - fixedTPM, stClear, fixedParent, sensitiveDataOrigin, userWithAuth, adminWithPolicy
- fixedTPM, stClear, fixedParent, sensitiveDataOrigin
  - Properties of the key's generation and management
- UserWithAuth
  - Simple shared secret using HMAC
- Complex Policies

Authorization Basics

- Auth or Policy set During Object creation
  - Applies to all TPM Objects
- Session is established to access (i.e. send a TPM command) to use an object
  - Auth type must match object's policy
- Types:
  - Password
    - In the clear
    - Used for simple environments where entire stack is trusted
  - HMAC
    - Shared secret is protected during transport
  - Policy
    - Provides a flexible set of criteria to use an object

Password and HMAC



HMAC protocol ***very*** simplified

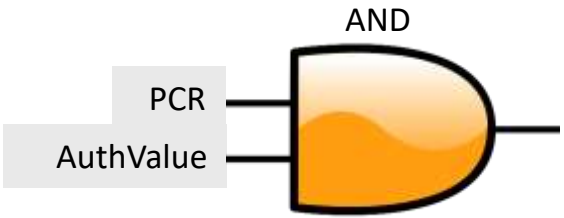
Policies

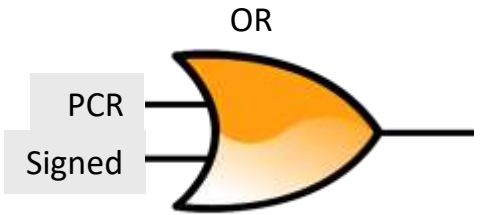
- TPM2_PolicySigned
- TPM2_PolicySecret
- TPM2_PolicyTicket
- TPM2_PolicyPCR
- TPM2_PolicyLocality
- TPM2_PolicyNV
- TPM2_PolicyCounterTimer
- TPM2_PolicyCommandCode
- TPM2_PolicyPhysicalPresence
- TPM2_PolicyCpHash
- TPM2_PolicyNameHash
- TPM2_PolicyDuplicationSelect
- TPM2_PolicyAuthorize
- TPM2_PolicyAuthValue
- TPM2_PolicyPassword
- TPM2_PolicyNvWritten
- TPM2_PolicyTemplate
- TPM2_PolicyAuthorizeNV

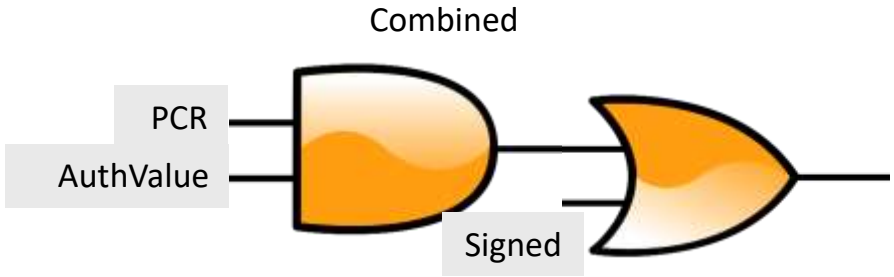
Simple Policy Example

- When creating a key restrict to a PCR[0] value:
  - Determine policyHash for a particular PCR and its value
  - Create Key (e.g., a signing key)
    - Set attributes to indicate use of key must meet a policy
    - Pass in policyHash determined above
    - TPM stores policyHash with the other key attributes
  - Using the key
    - Establish a Policy Session
    - Execute TPM2_PolicyPCR indicating PCR[0]
    - TPM updates session's policyDigest
    - TPM2_Sign
      - If session's policyDigest == object's policyHash then allow command

Policies can be Combined



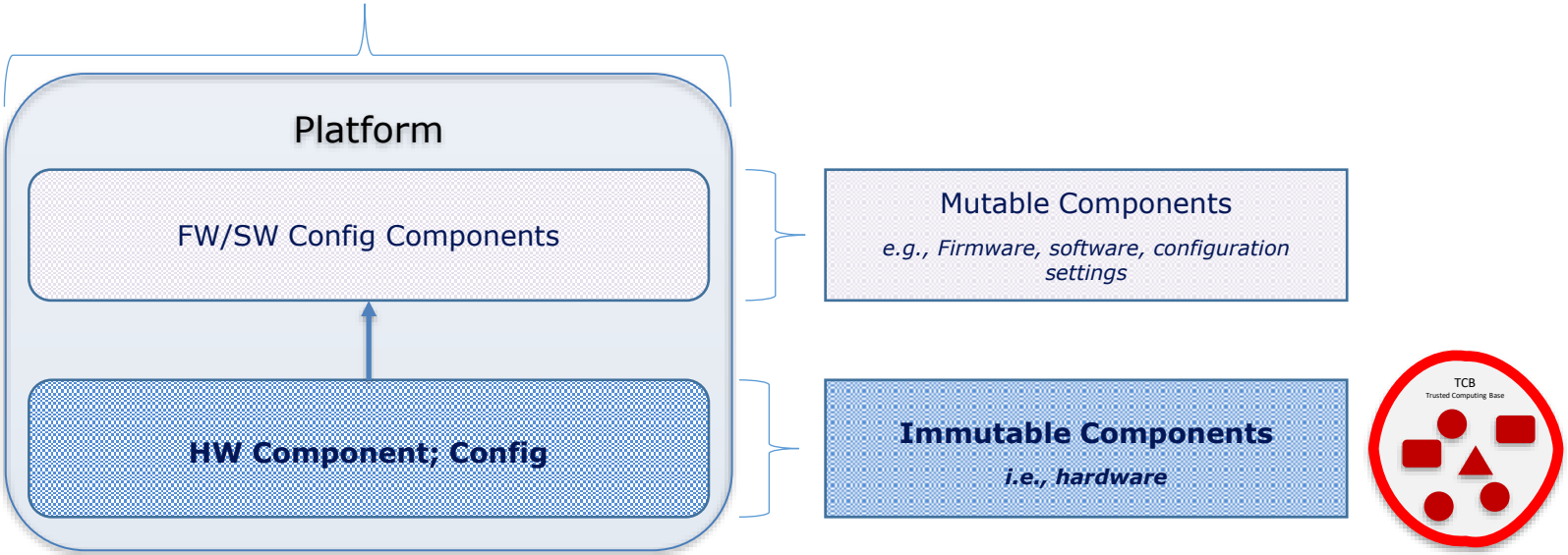




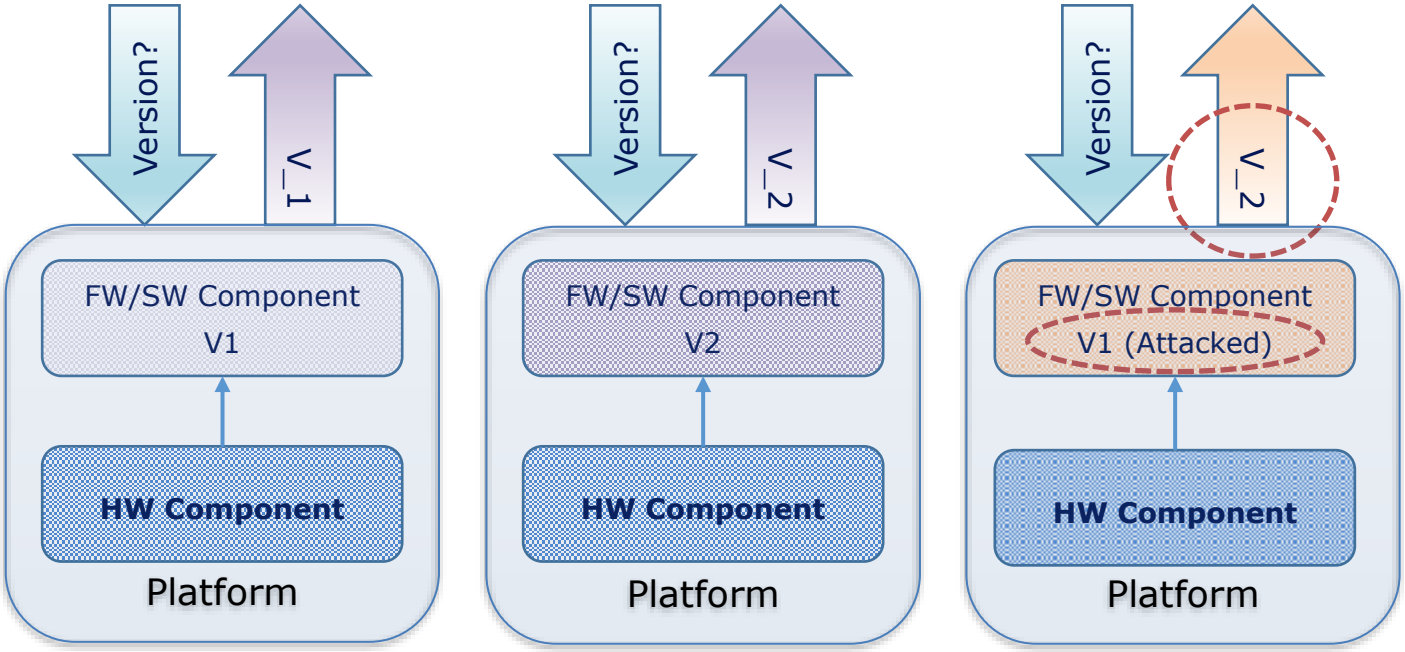
DEVICE PROPERTIES

Platform Identity = Hardware + Firmware

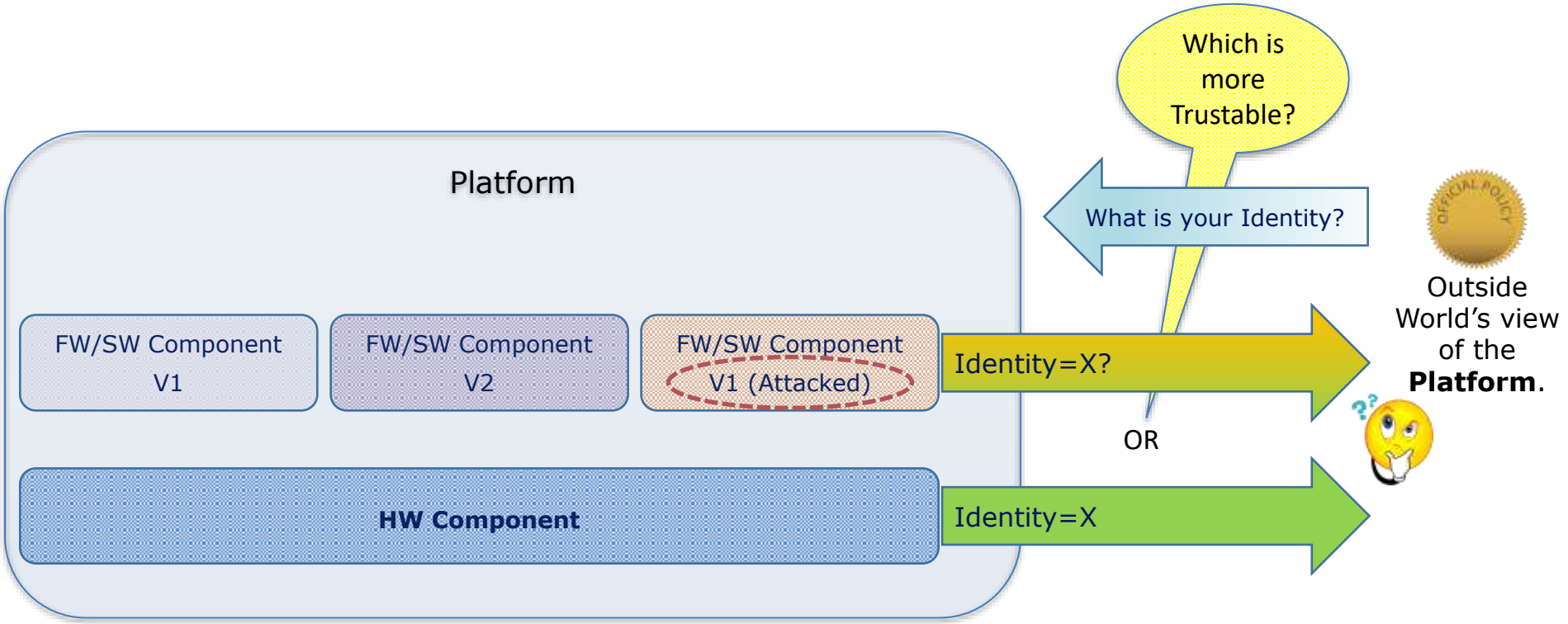
Outside World's view of the **Platform**.



Problem with Trusting Firmware/Software for Platform Identity

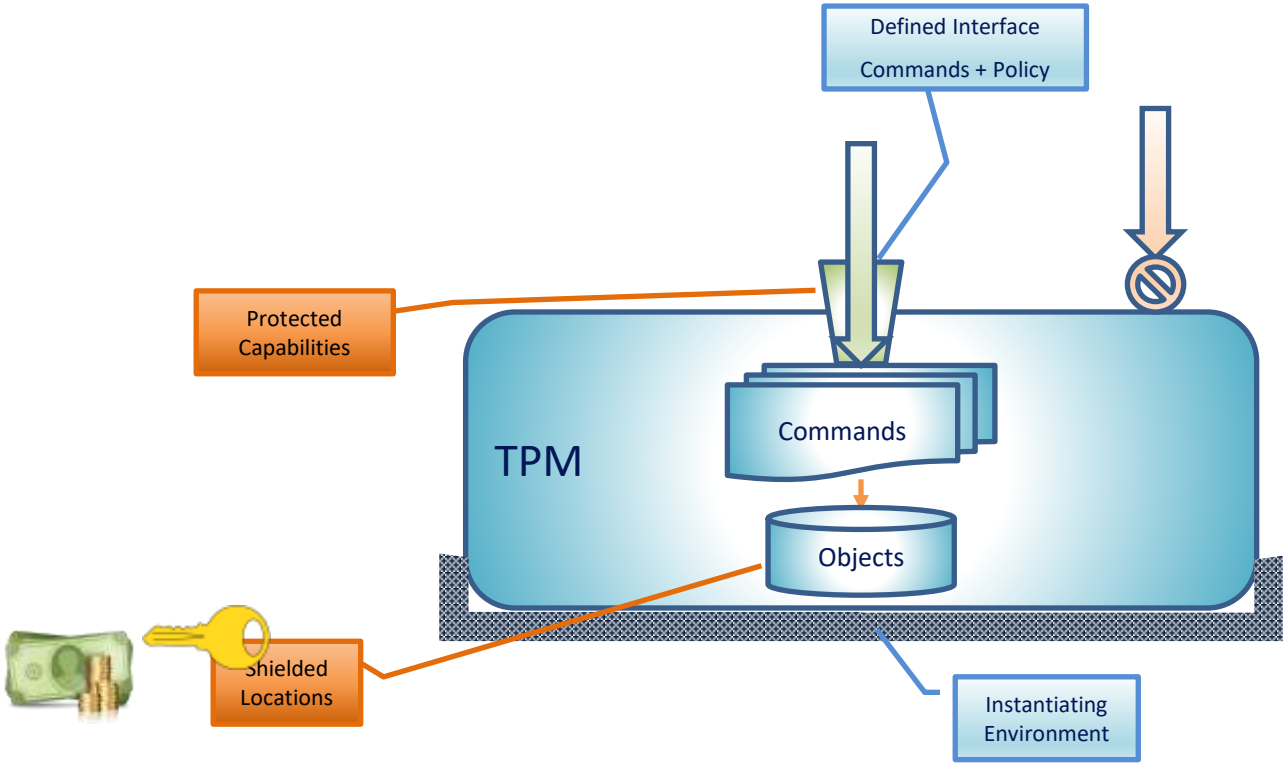


Source of Platform's [Actual] Identity



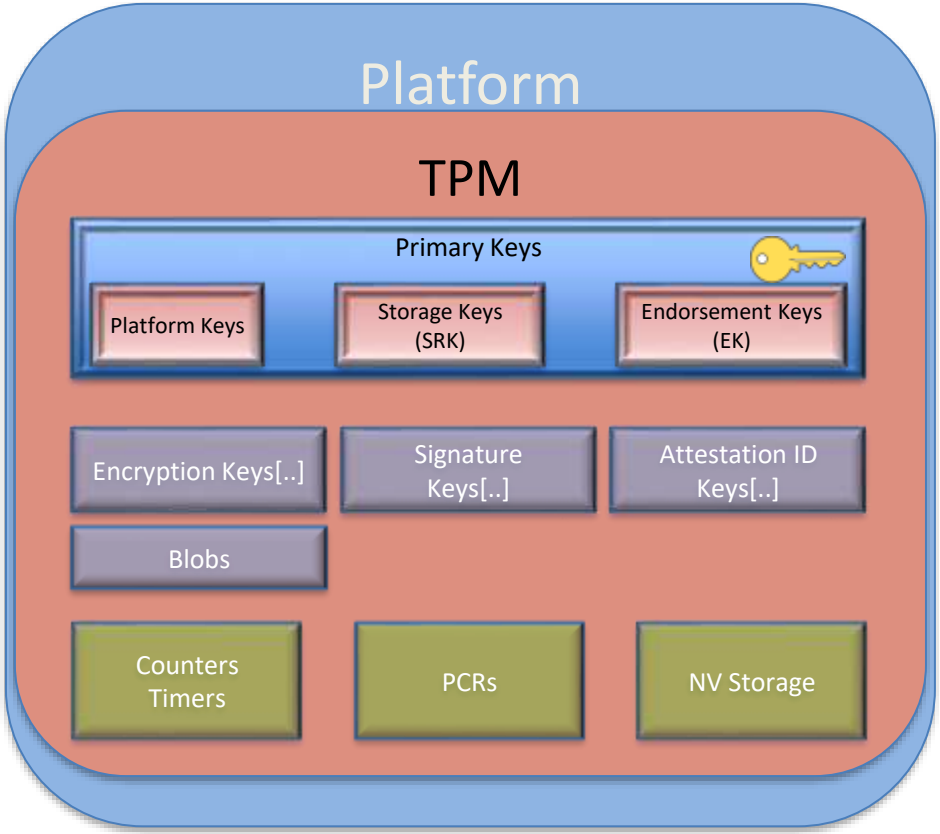
Where Identity = h/w model + h/w identity + f/w identity

Basic TPM Description



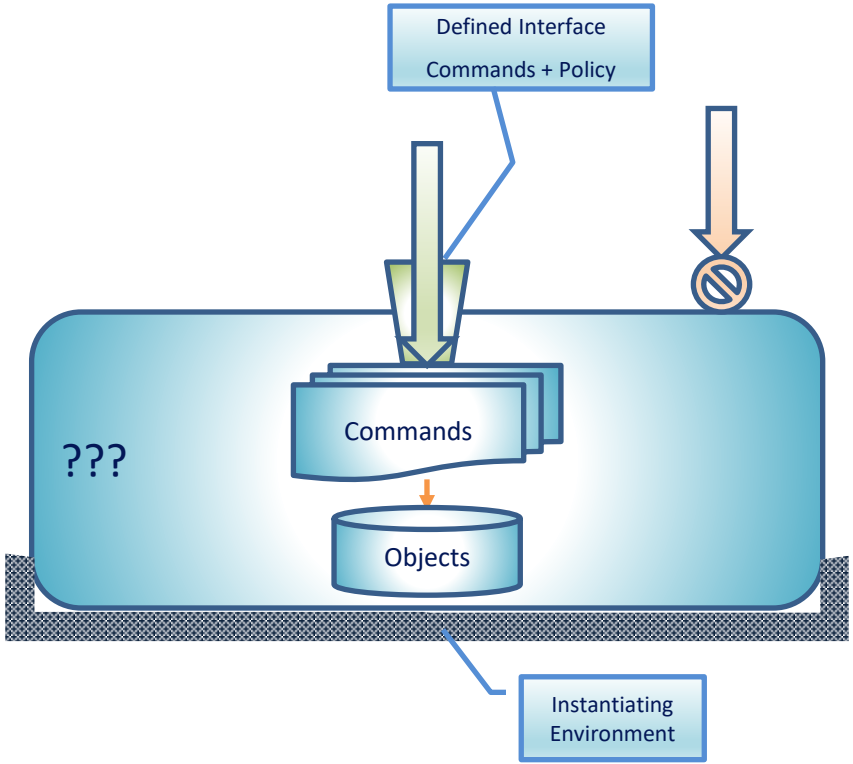
BASIC CONCEPTS - TPM

TPM General Architecture



- TPM Attached to the Platform
  - Provides Platform with Identity and Key Management
- Keys and other Assets Protected TPM
  - Endorsement Key (EK) provides proof of TPM's source.
- TPM Uses a Key Hierarchy
  - Allows multiple stakeholders
  - TPM can load and use a virtually unlimited number of AIKs, signature and encryption keys
- TPM Contains typically 24 PCRs
  - These are populated by the platform's components, OS, etc.
  - Starting with the RTM
- NV Storage
  - Policy Enable General Storage
- Counters and Timers
  - General purpose or can be used in policies

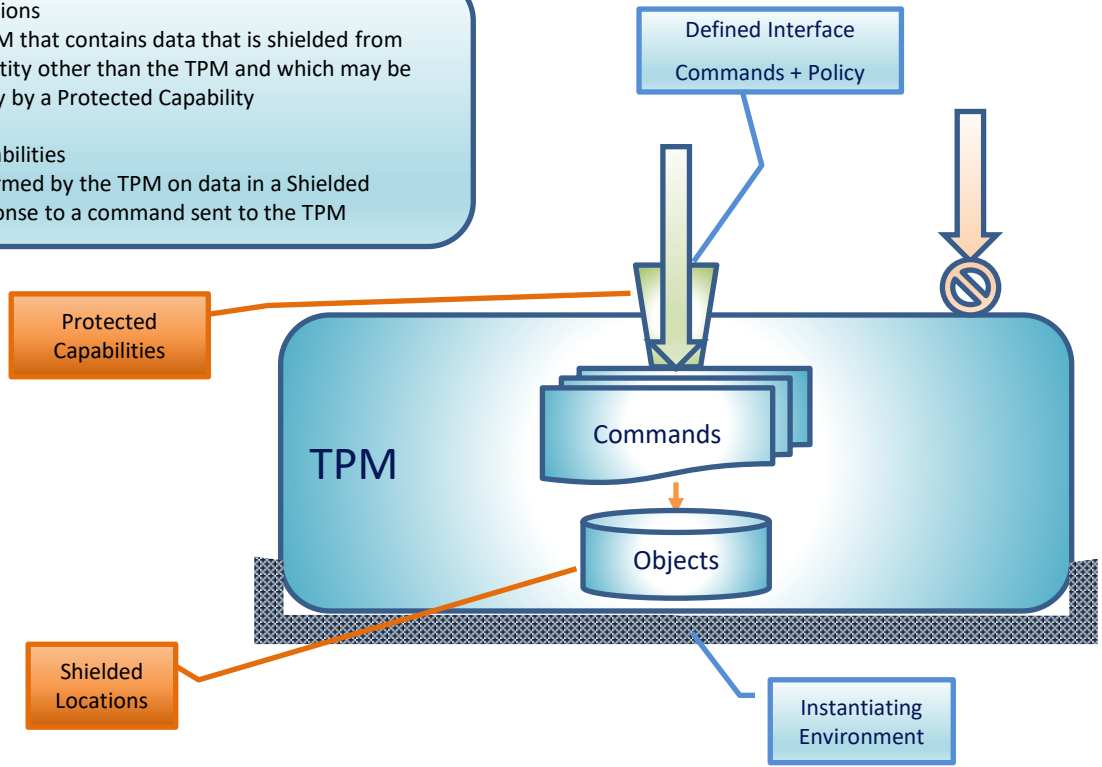
General Trusted Execution Environment (TEE)



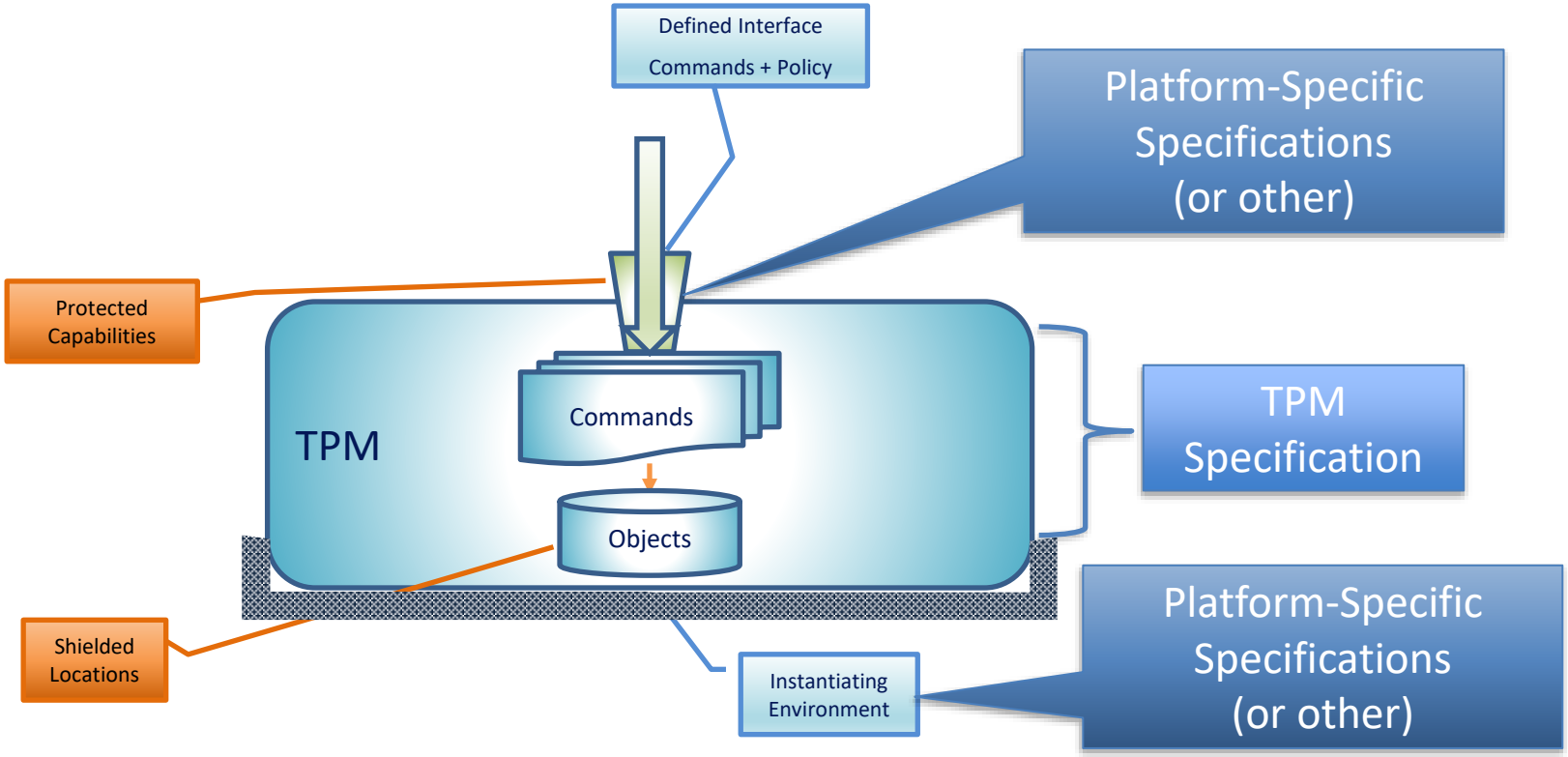
Basic TPM Description

TPM Shielded Locations
location on a TPM that contains data that is shielded from access by any entity other than the TPM and which may be operated on only by a Protected Capability

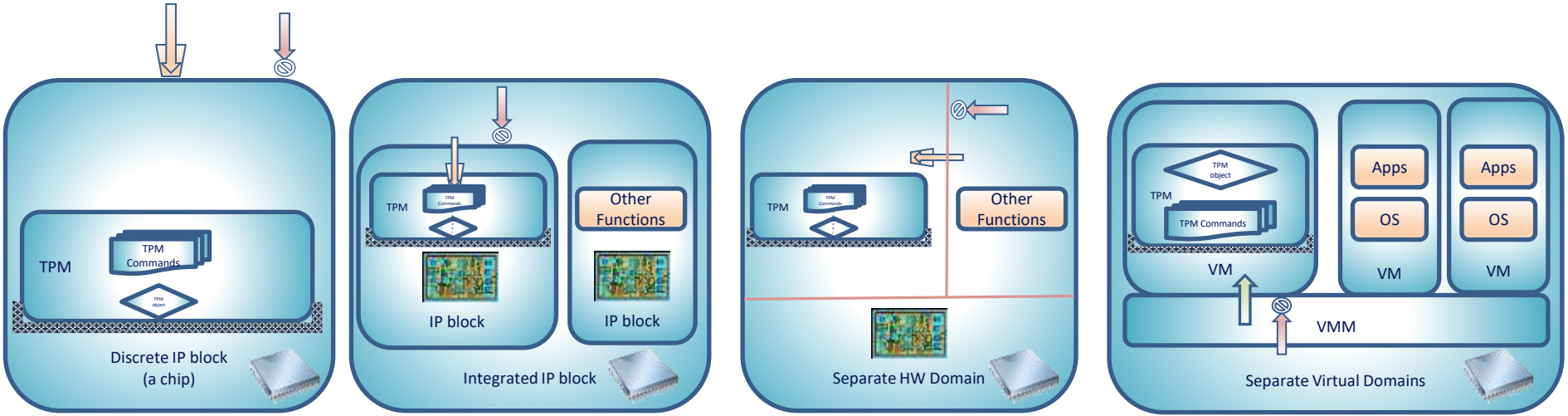
TPM Protected Capabilities
operation performed by the TPM on data in a Shielded Location in response to a command sent to the TPM



Scope of TCG Specifications



Implementation Options



Protection against physical attacks left to:

- Use Cases
- Platform Design

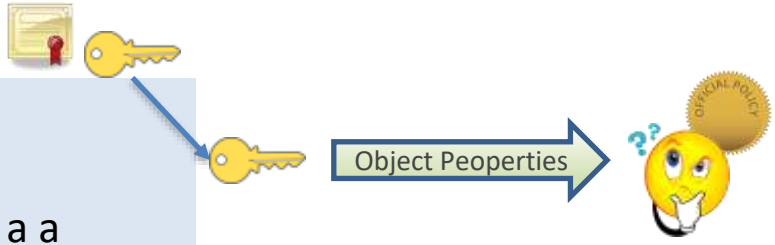
ATTESTATION

Attestation Key

- Term is left over from TPM 1.2
  - TPM 1.2 keys had limited properties
  - But we still use it as a “term of art”
- “Technically” an Attestation Key is a TPM 2.0 “Restricted Signing Key”
  - Necessary properties:
    - Fixed (may not be duplicatable)
    - May only sign internally generated data
      - There is a process to sign external data but the hash must be generated by the TPM.

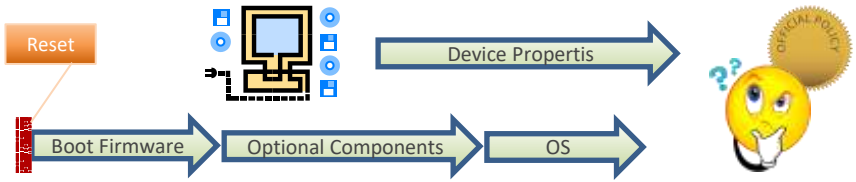
Attestation

- Proof of a Object's Properties
  - Proof of a key or device's Properties
    - Cryptographic binding between an object and a a trusted key



Proof of a Device's [boot-time] Integrity

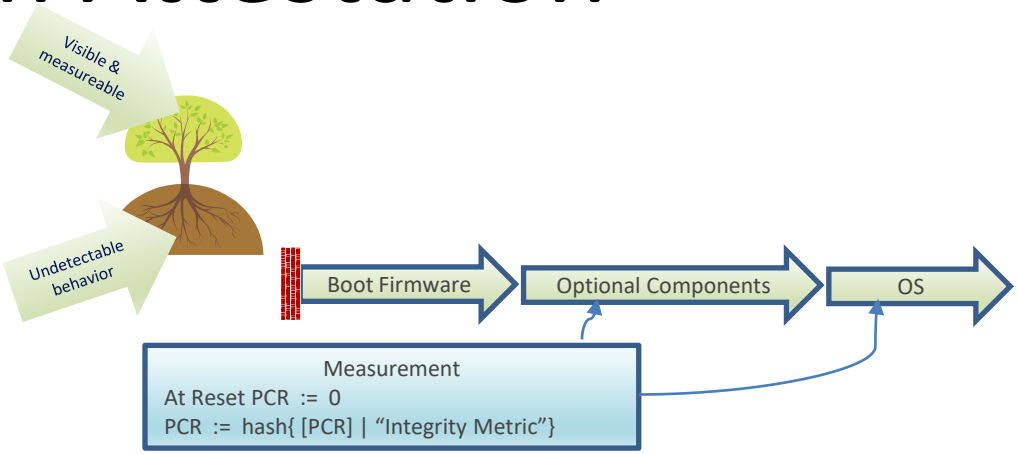
- Proof of the identity of the platform's firmware, software components and configuration



Platform Attestation

Roots

- Elements which must be trusted
- Misbehavior is not detectable
- Objective: Keep these small

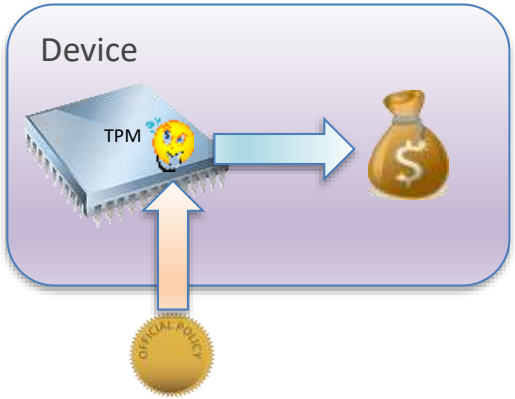


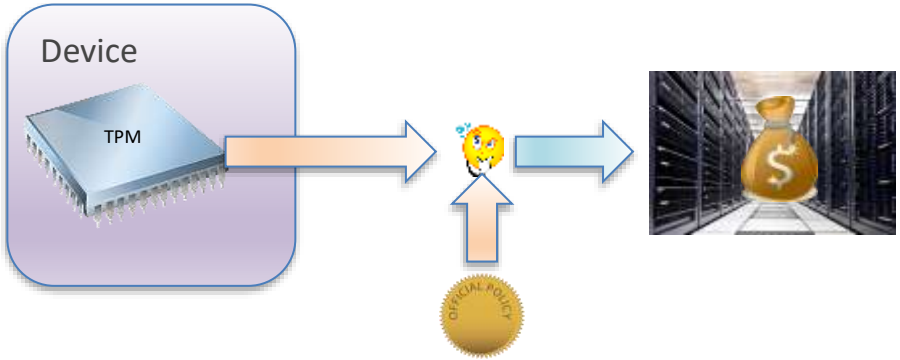
Integrity Measurement

- Recorded metrics of the platform’s characteristics
- Typically done using a series of cryptographic recordings
  - At Reset PCR[X] := 0 then
  - PCR[X] = hash{PCR[X] | Integrity Metric of component 1} then
  - PCR[X] = hash{PCR[X] | Integrity Metric of next component}, etc.

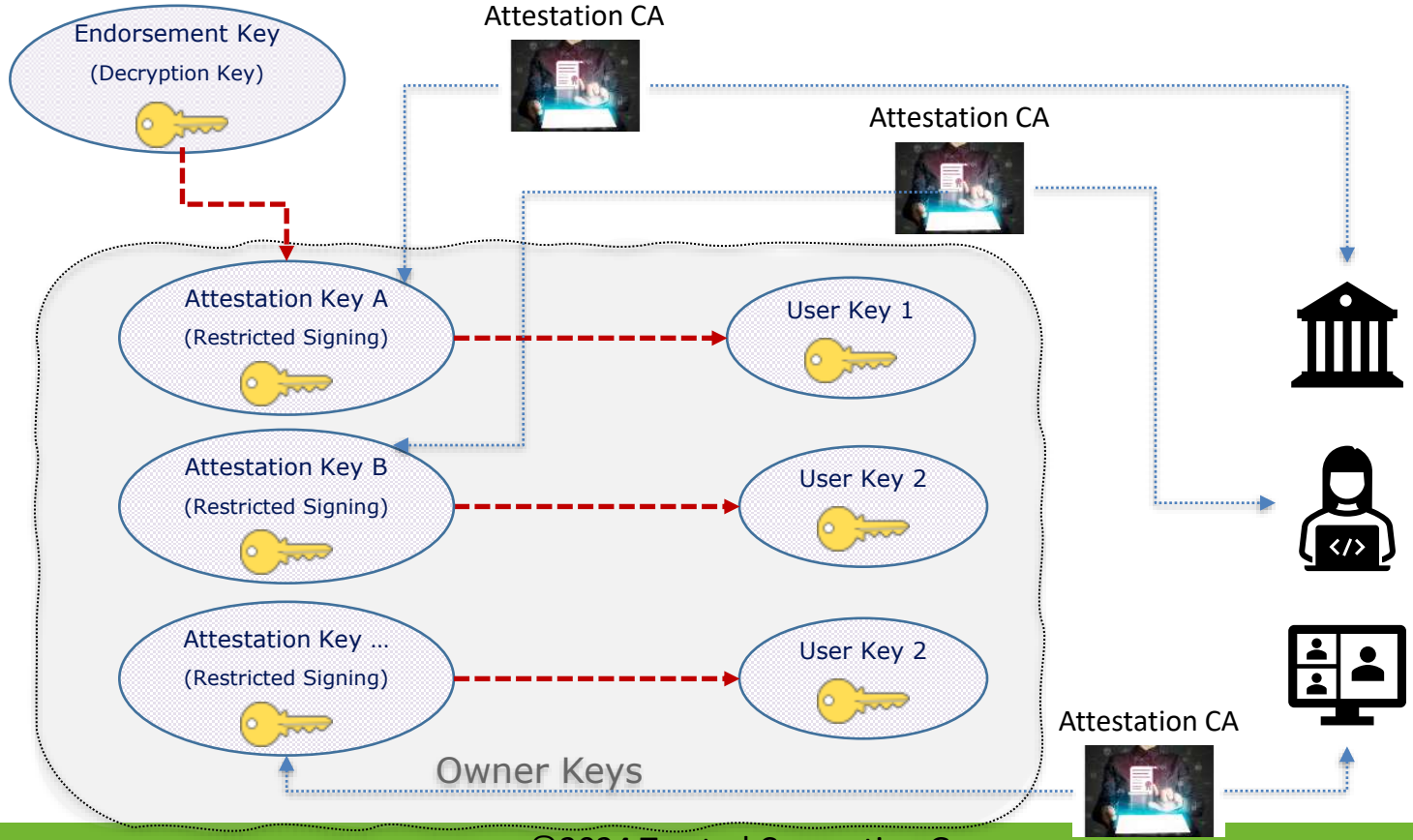
Attestation Types

- Local
  - TPM enforces Policy
    - Seal / Unseal
    - Protect use of Local keys
    - Protect local NV storage
- Remote
  - RP Enforces Policy
    - Quote
    - Protect a key used for network traffic
    - Object Properties





Attestation Domains



Flow is Generalized

EK to Attestation Key

Attestation CA

Generate Att Key

Attestation Key A
(Restricted Signing)

Send:
1. "Name of Key"
2. TPMT_Public
3. EK Cert

Verify EK Cert

Check TPMT_Public

Check "Name" matches TPMT_Public

Generate Nonce (or sym key).

Encrypt with EK Public key

Send: Encrypted "Nonce"

ActivateCredentil

- Unique Key
- For privacy reasons, the EK on clients is a decryption key – it cannot sign

Decrypt Nonce IFF Name == Att Key

Issue Cert

AK Certificate

TPM Manufacturer

TPM Manu Cert

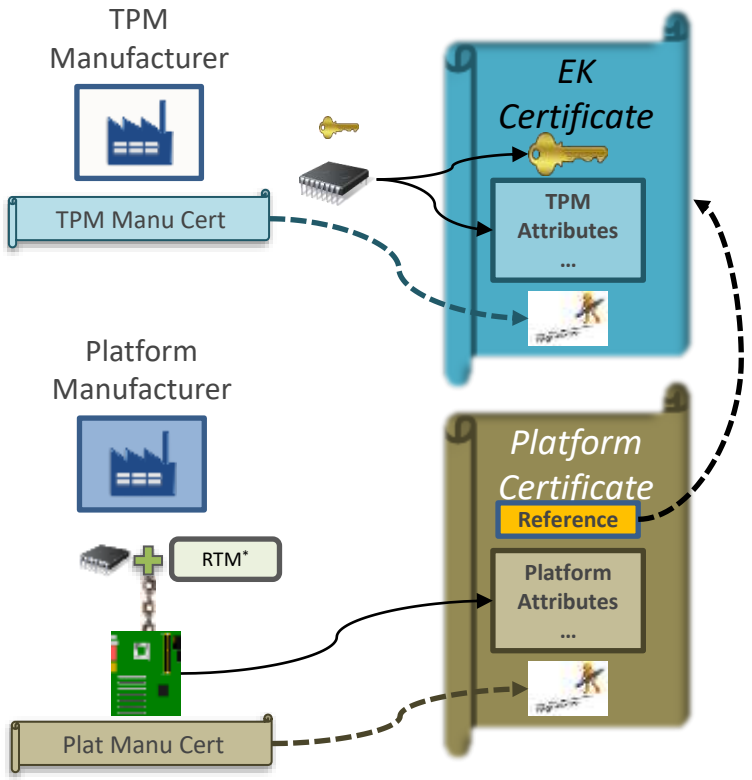
EK Certificate

iDevID (802.1ar)

- In “Clients” the Endorsement Key (EK) is a decryption key for privacy.
- ICT doesn’t generally need privacy
  - Likely, actually not!
- In TPM 2.0 can have multiple Primary Endorsement key (formal term for the EK)
- There is a specification for implementing iDevID/lDevID (802.1ar) using a TPM
  - https://trustedcomputinggroup.org/resource/tpm-2-0-keys-for-device-identity-and-attestation

EK to Platform Certificate Binding

- TPM
  - EK Cert signed by TPM Vendor
- Platform Manufacturer (PM) attaches TPM to platform
  - EK is bound to the Platform
  - Provides a platform-specific key
- Platform Certificate
  - Attributes assert information about the platform
    - As built data (components)
    - RTM binding to TPM
- Supply chain obtains proof of assertions
  - Verify Platform and EK Certificate signatures
  - Verify EK Certificate bound to that platform



* RTM: Root of Trust for Measurement

END OF IETF-120 TUTORIAL