Trusted Computing: Introduction & Applications

Lecture 2: TPM Architecture, Base Functionality, and Key Hierarchy

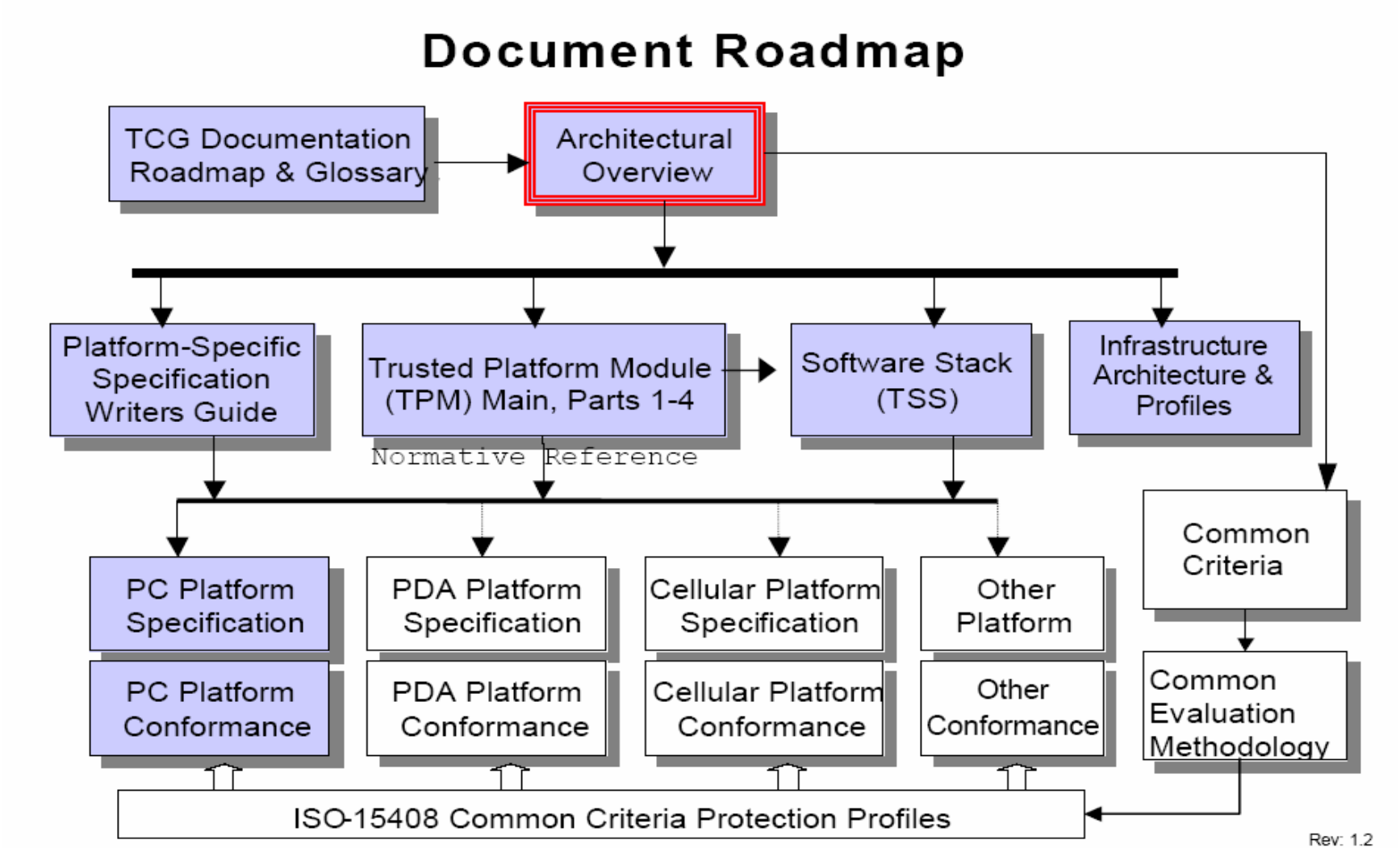
Dr. Andreas U. Schmidt

Fraunhofer Institute for Secure Information Technology SIT,
Darmstadt, Germany

Addendum Lecture 1

- Trusted Computing 2004 - eine unendliche Geschichte Ruediger Weis & Andreas Bogk, cryptolabs Amsterdam & CCC Berlin
- Trusted Computing Group. Design, Implementation, and Usage Principles Version 2.0
- TCG Specification Architecture Overview Specification. Revision 1.3, 28th March 2007

TCG Documents (Copyright TCG)



Literature

1. Trusted Computing Group: TCG Specification – Architecture Overview, Version 1.2, 2006.
2. Trusted Computing Group: TPM Main Part 1 Design Principles, Version 1.2, 2006.
3. C. J. Mitchell (ed.), *Trusted Computing*. IEE Press, 2005.
4. Eckert: IT-Sicherheit (pp. 6xx), Oldenburg
5. D. C. Blight. Trusted Computing. Blackhat Windows 2004. https://www.blackhat.com/presentations/win-usa-04/bh-win-04-blight/bh-win-04-blight.pdf
6. Eimear Gallery, Graeme Proudler Lecture at Royal Holloway: http://www.isg.rhul.ac.uk/files/IY5608_-_Lecture_2_Roots_of_Trust.pdf

Trusted Platform Capabilities

A generic TP must have the following

- Shielded locations: a protected storage area designed for sensitive information (e.g. integrity metrics or cryptographic keys).
- Protected capabilities: *commands* which exclusively manage data in shielded locations
  - integrity reporting,
  - key management,
  - random number generation and
  - Sealing and binding of data
- Integrity measurement, logging and reporting: include the calculation, storage and reporting of metrics over the state or (persistent) characteristics of a certain platform.
- Attestation mechanisms: A TP has to provide different forms of attestation mechanisms that allow an external party to verify the accuracy of a certain piece of information known to the TP.

Some of this *may* be provided by a hardware module – the TPM

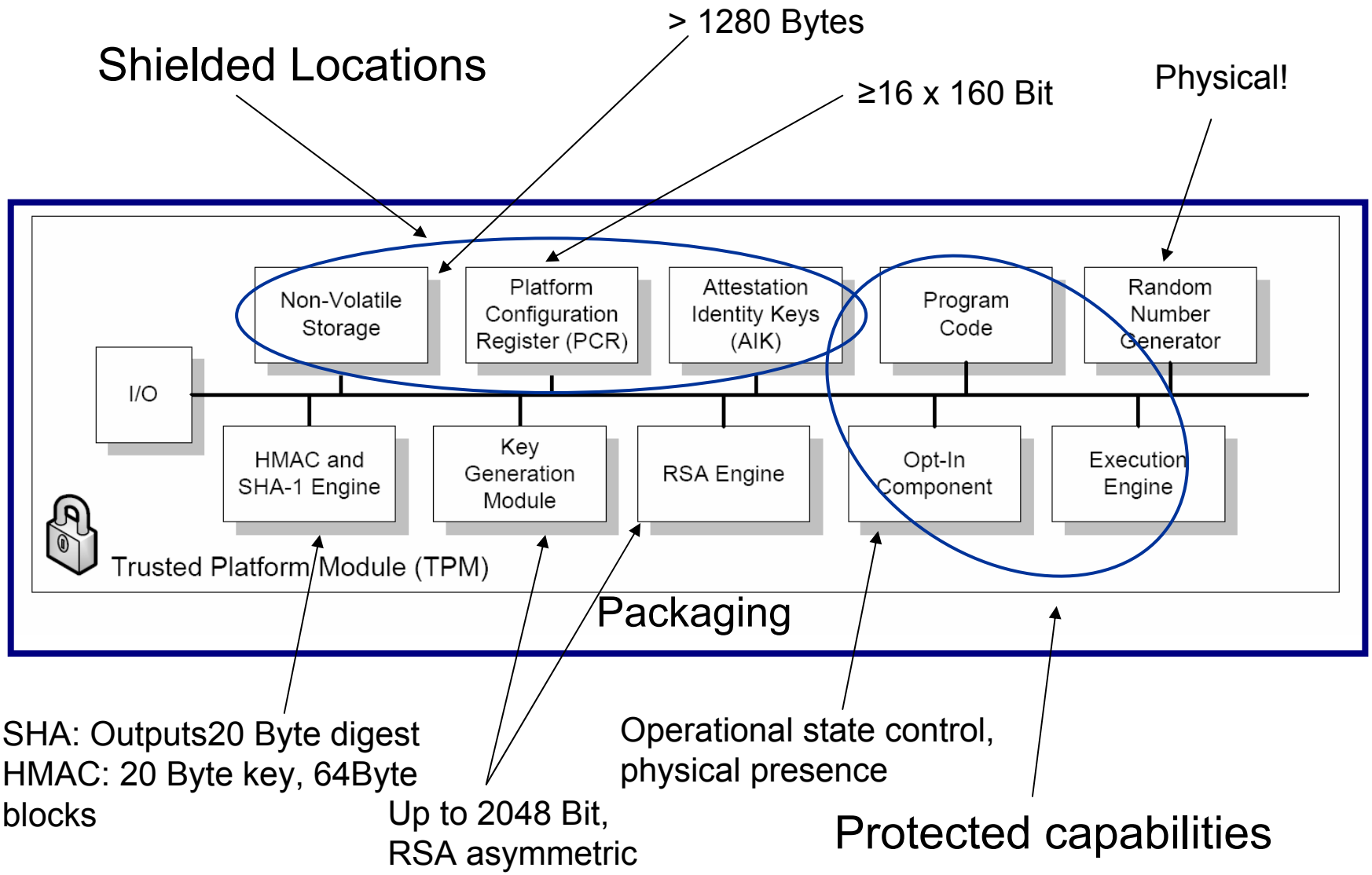
Attestation mechanisms

- Attestation by the TPM: The TPM proves the possession of particular data by applying digital signatures with keys only known to the TPM
  - *Any payload can be signed and attested with AIKs*
- Attestation to the platform: This operation assures that a platform can be trusted for reporting integrity measurements (metrics describing the state or the characteristics of the platform) –
  - Uses platform *credentials,* a concept similar to CA certificates
- Attestation of the platform: The platform proves (possession and veracity) of a set of its current integrity measurements to an (external) verifier
  - *signing of PCRs with AIKs*
- Authentication of the platform: The process of confirming TP's identity.
  - "Platform Authentication is performed using any non-migratable signing key. Certified keys (i.e. signed by an AIK) have the added semantic of being attestable. Since there are an unlimited number of non-migratable keys associated with the TPM, there are an unlimited number of identities that can be authenticated" (TCG Arch Overview)

TPM Characteristics

- 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”
- TCG defines TPM’s functionality
  - Protected capabilities
  - Shielded locations
- Not the implementation
  - Vendors are free to differentiate the TPM implementation
  - Must still meet the protected capabilities and shielded locations requirements

TPM component architecture



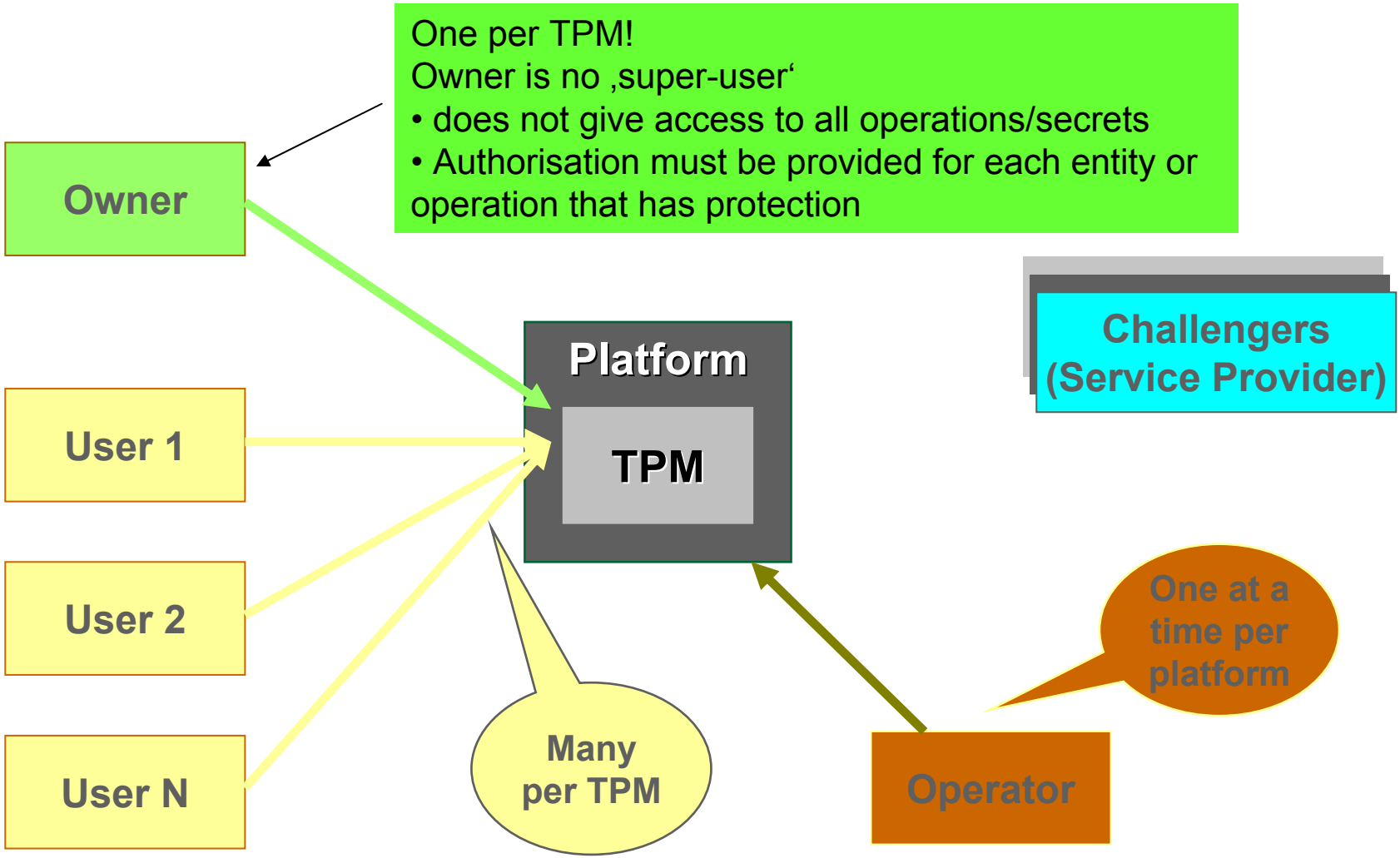
What can it do?

- generation of asymmetric and symmetric keys,
- calculation of signatures and hash values,
- asymmetric and symmetric encryption,
- encryption of cryptographic keys (binding),
- secure storage (shielded locations) and processing (protected capabilities) of small objects and hash values (of measurement values from the platform configuration),
- creation of signed reports on the measurement values,
- key management (endorsement and attestation identity keys),
- functions to let the owner of the platform take possession of the platform and (de)activate the TPM,
- a trustworthy timer.
  - Minimum requirement: monotonic increment every 5 secs for at least 7 years. No reset – useful against roll-back attacks

TPM – RNG (from 6.)

- Comprised of three components:
  - Entropy source and collector;
  - State register; and
  - A mixing function.
- Entropy source and collector
  - Entropy source: is the process or processes which provide entropy.
  - Sources include noise, clock variations, for example.
  - The collector: is the process that collects the entropy, removes the bias and smoothes the output. For example, if the raw entropy data has a bias of 60% 1s and 40% 0s then the collector takes this information into account before sending data to the state register.
- State register
  - Where the output from the entropy collector is stored.
  - The implementation may use 2 registers –a non-volatile and a volatile:
    - The state of non-volatile register is stored to the volatile register on start-up.
    - Changes to the state of the state register from either the entropy source or mixing function affect the volatile register.
    - The state of the volatile register is stored to the non-volatile register at power down.
- Mixing function
  - Takes the state register and produces the RNG output.

Players according to TCG



TPM operational states

- Enabled / disabled
  - TPM may be enabled/disabled multiple times within a boot period. Disabled, the TPM restricts all operations except the ability to report TPM capabilities and to update PCRs. When enabled, all features of the TPM are available.
    - SHA still available
    - Ownership can be disabled
    - Persistence flag
- Activated / deactivated
  - Deactivation is similar to disabled, but operational state changes are possible. (i.e. change owner or activation with physical presence). When activated all features of the TPM are available.
    - Persistent
    - Does not take effect until next re-intialisation
- Owned / unowned
  - A platform is owned when an EK exists and the true owner knows owner authorization data. The owner of a platform may perform all operations including operational state changes.

Combinations of operational states

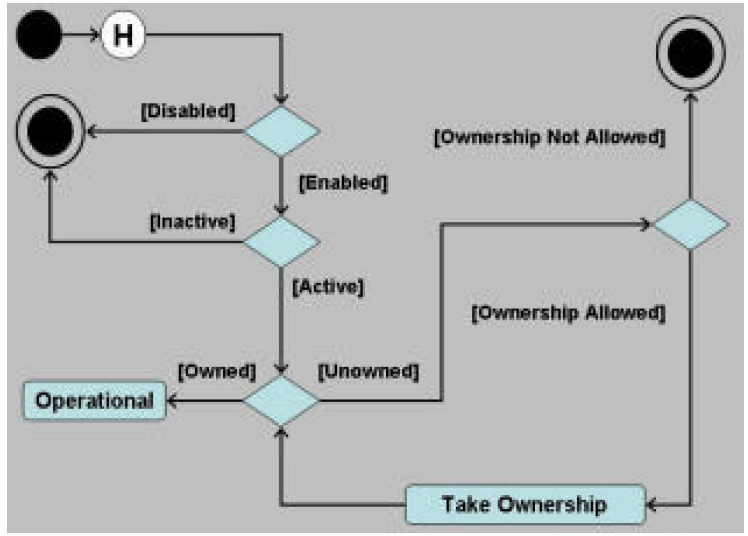
State #	E	A	O	Explanation
1	X	X	X	Fully operational state
2		X	X	Ownership is set and can be changed to new owner
3	X		X	nonsensical
4			X	Ownership is locked, cannot be changed
5	X	X		Local and remote ownership possible
6		X		Ownership can be set
7	X			nonsensical
8				TPM off, default shpping setting

- A ‚normal‘ TPM deployment procedure at the end-user as owner
  - S8 – S6 – S5 – take ownership – S2 – enable – S1

Take ownership 1/2

- TPM has no owner when shipped (to system integrator or user)
- Taking ownership normally requires *physical presence*
  - A user action that can't be performed by software (yet possibly remote)
  - Required in part. To enable TPM and establish initial ownership
  - Implementation examples
    - Button directly wired to TPM (some IBM Laptops)
    - BIOS setup…
    - Future: Biometry?
- TPM ownership can always be reset via physical presence – old secrets are discarded
- TPM ownership can be asserted via physical presence – no secrets are exposed

Take ownership 2/2



- Uses the Endorsement Key
  - Nonmigratable 2048 RSA pair (PUBEK, PRIVEK)
  - Created by TPM manufacturer, unique per TPM
  - PRIVEK never leaves TPM
- Control state to be active, enabled
- Optionally control physical presence
- TPM_TakeOwnership(OwnerAuth, …)
  - Creates 160-bit authentication value, encrypts with PUBEK and stores it in non-volatile memory
  - Creates 2048-bit RSA Storage Root Key (SRK) on TPM
  - Cannot run TPM_TakeOwnership again: Ownership Enabled flag ← False
  - Done once by IT department or laptop owner.

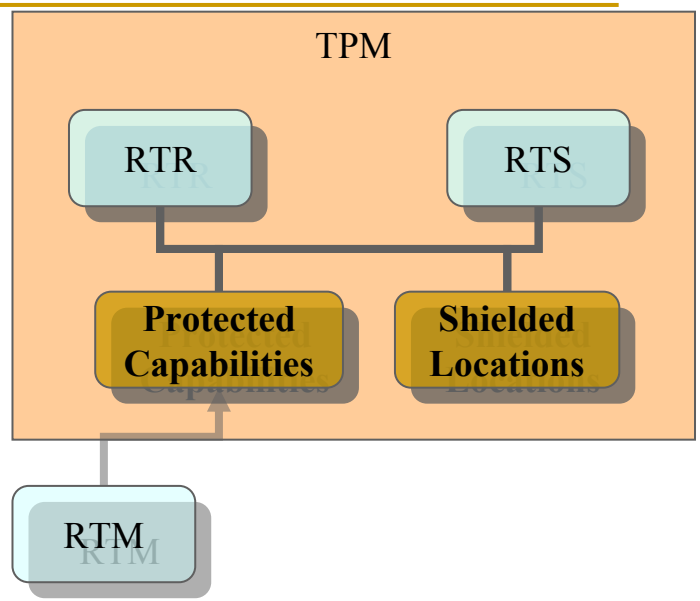
Key types and classes

- EK
- Storage Keys
  - Protects keys or external data
  - Storage Root Key SRK
  - Subordinate storage keys, generated by TPM and protected by SRK
- Signing Keys
  - Digital signatures
- Attestation Identity Keys (AIKs)
  - Special Signing keys
  - Provide pseudonymous attestation
  - Can be produced in unlimited number
  - Non-migratable
- Non-Migratable Keys
  - Permanently bound specific TPM, i.e., platform
- Migratable Keys
  - Can be migrated to other platforms
- Certified Migration Keys
  - Can be migrated only to “certified” authorities
- Bind keys
  - To encrypt small data packages (e.g. symmetric keys)
- Legacy keys
  - Created outside a TPM and imported
- Authentication keys
  - Symmetric keys to protect transport sessions

Roots of Trust

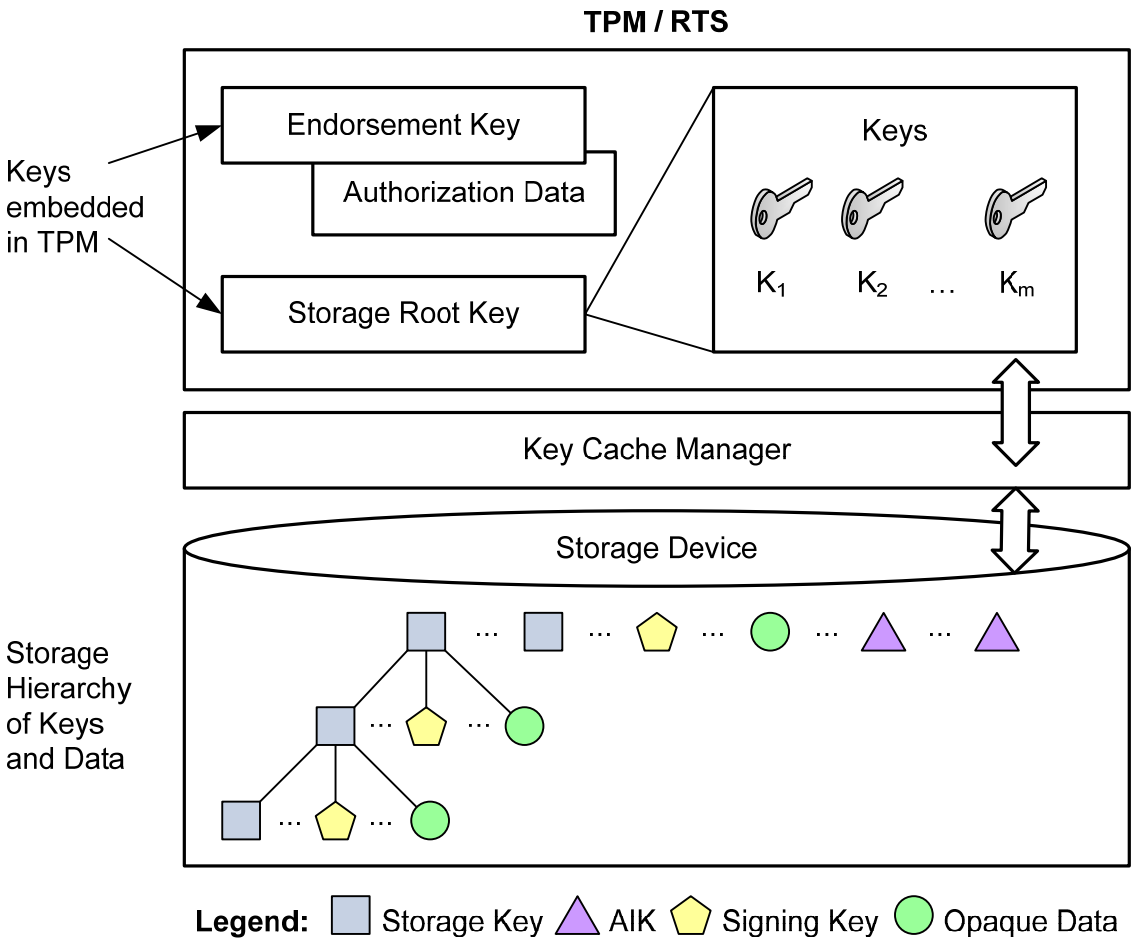
- A **Root-of-trust** is a component that must behave as expected, because its misbehaviour cannot be detected.
- Roots of trust enable the gathering, storage and reporting of evidence/references about the trustworthiness of software environment running on the platform.
- They represent the components of a TP which must be implicitly trusted if the evidence/references are to be trusted.

TCG-specified Roots of Trust



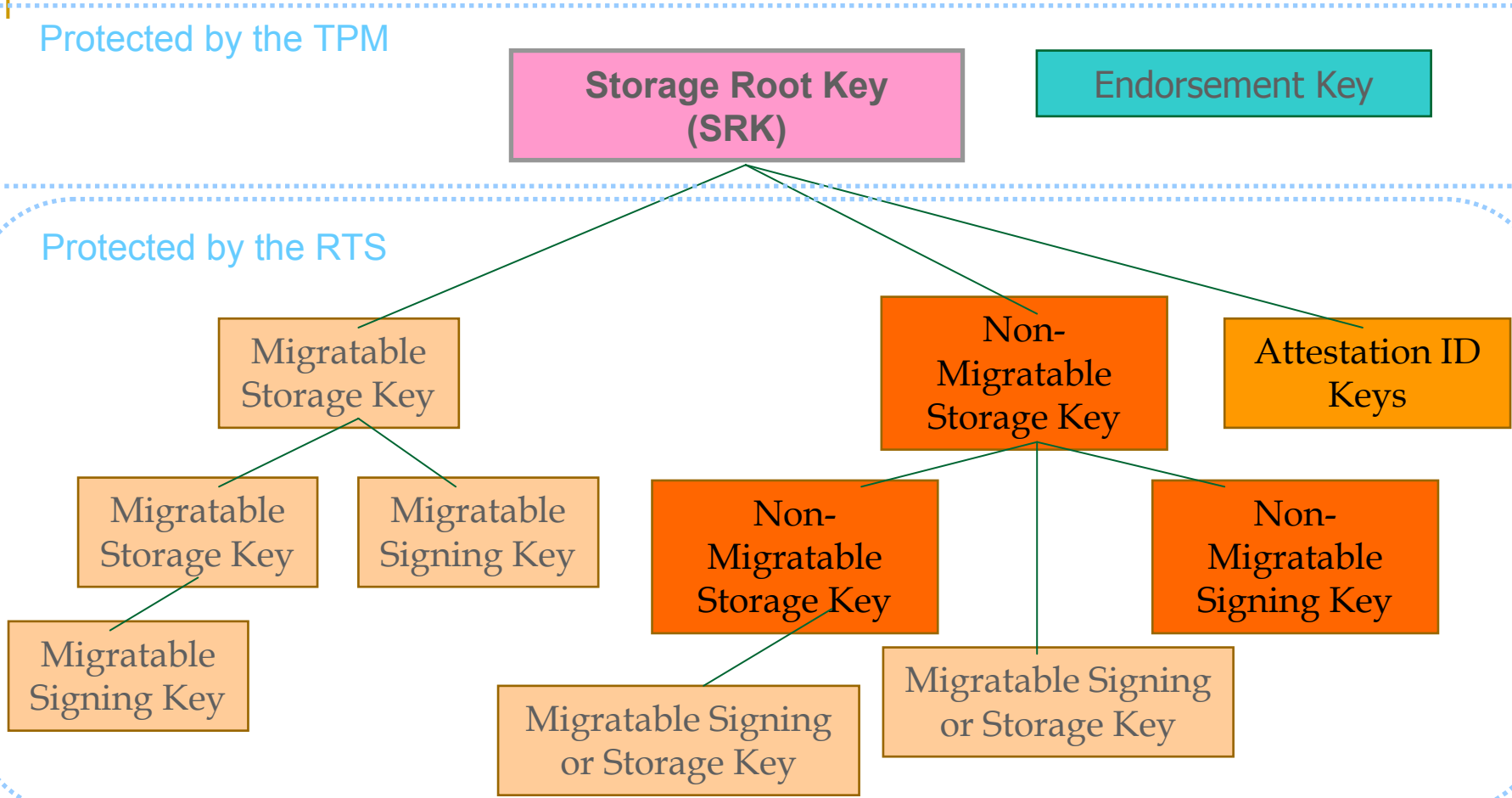
- A **Root of Trust for Measurement (RTM)** – The component that can be trusted to reliably measure the software/firmware which executes after some sort of reset (e.g. BIOS ext)
  - Provides cryptographic mechanism to digitally sign TPM state and information
- A **Root of Trust for Reporting (RTR)** and a **Root of Trust for Storage (RTS)** – The components that can be trusted to store and report reliable information in and about the platform.
  - The RTS Provides cryptographic mechanism to protect information held outside of the TPM, can be as simple as a key
- The Core Root of Trust for Measurement (**CRTM**) and the Dynamic Root of Trust for Measurement (**DRTM**) are the roots of trust for measurement.
  - For the foreseeable future, it is envisaged that the static-RTM will be integrated into the normal computing engine of the platform, where the provision of additional BIOS boot block or BIOS instructions (the CRTM) cause the main platform processor to function as the RTM.
  - Static RTM is CPU after platform reset.
- The TPM is the root of trust for reporting and the root of trust for storage.

Key protection by the RTS



- RTS manages a small amount of volatile memory where keys are held while performing signing and decryption operation
- SRK protects first level keys within TPM
- Inactive keys may be encrypted and moved off-chip to make room for other more active keys.
- Management of the key slot cache is performed external to the TPM by a Key Cache Manager (KCM).
- RTS is optimized to store small objects roughly the size of an asymmetric key (e.g. ~210 byte payload). A variety of object types can be stored, such as symmetric and asymmetric keys, pass-phrases, cookies, authentication results and opaque data.

Key Hierarchy – upper level encrypt lower levels

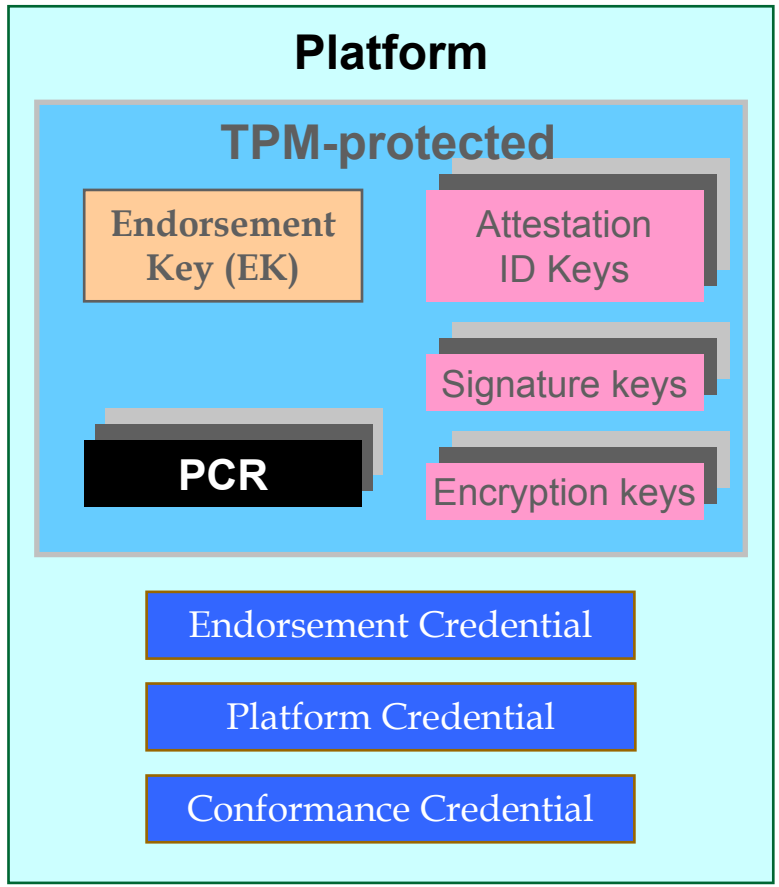


Storage Root Key (SRK) All keys are protected by this key, the root of the key hierarchy

SRK is changed on new owner – beware!

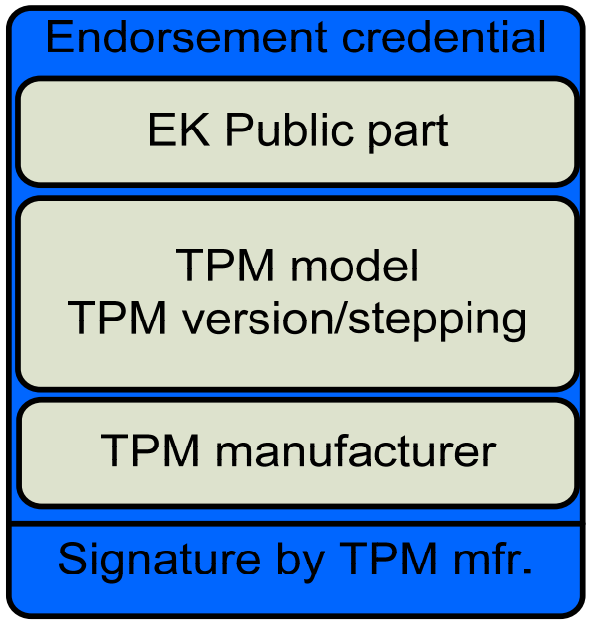
Credentials

- TCG Credentials are certificates by which a TP can show certain attributes to a verifier
  - Based on X.509 certificates and expressed in ASN.1 syntax
  - Used e.g. in attestation
  - Carry a lot of attributes
  - 5 types of credentials with involved interrelations
  - 3 come with the shipped TP



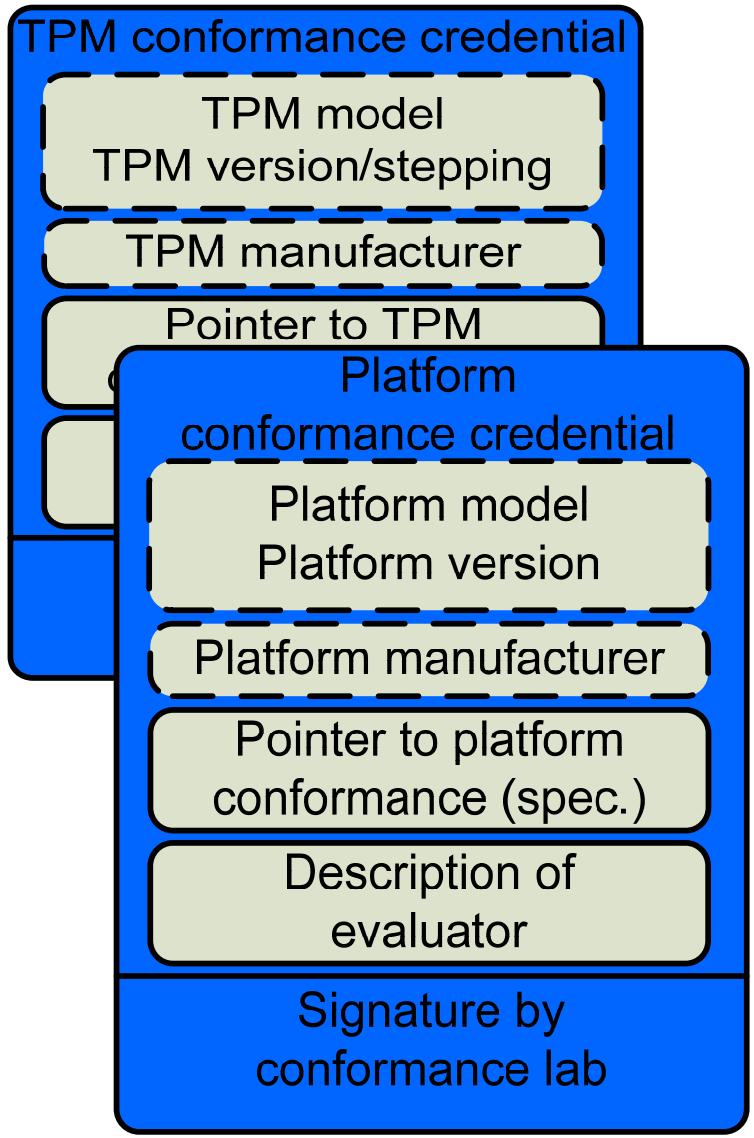
Endorsement credential

- Issued by „whoever generates the EK“
- Usually during manufacturing process, i.e. by the TPM manufacturer (mfr.) or vendor
- Claims that
  - This is a TPM
  - EK was properly generated and embedded
- One per TPM instance
- EKPUB is privacy-sensitive



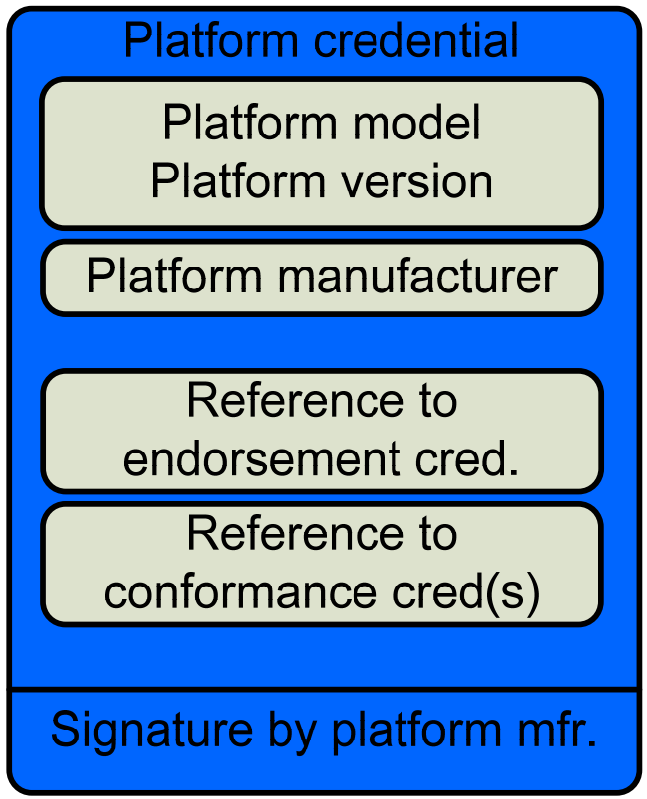
Conformance credentials

- Means for attesting a platform‘s/TPM‘s conformance to a spec., e.g. TCG
- indicates the evaluator accepts that the TBB design and implementation in accordance with established evaluation guidelines.
- Multiple conformance credentials may reside in one TP
- Conformance credntials do not identify platform



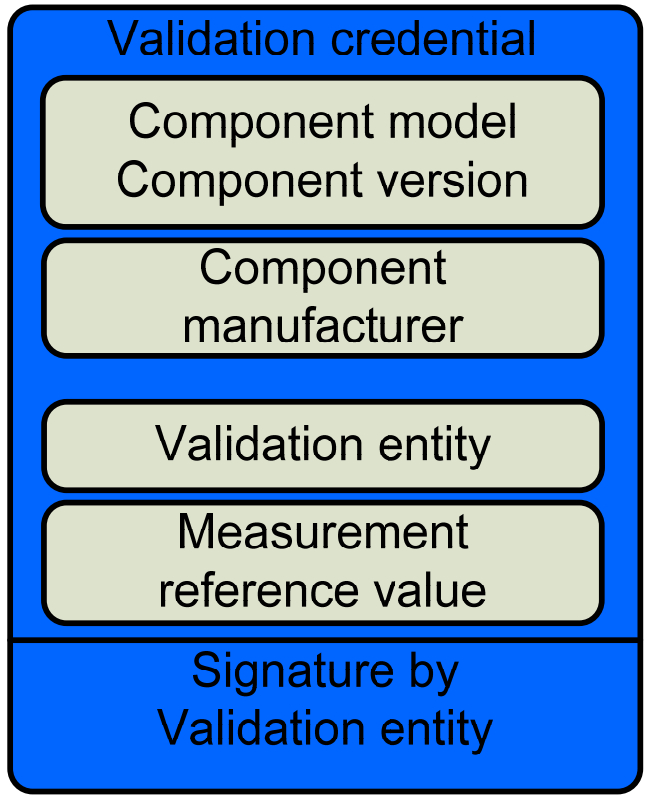
Platform credential

- Isued by TP mfr. or vendor
- Identifies TP mfr. and properties
- Provides evidence that
  - TP contains TPM as described by endorsement cred.
  - Conformance according to conf. cred(s)
- Credential references consist of a message digest of the referred credential.
- Privacy-sensitive: may hint to a TP‘s identity



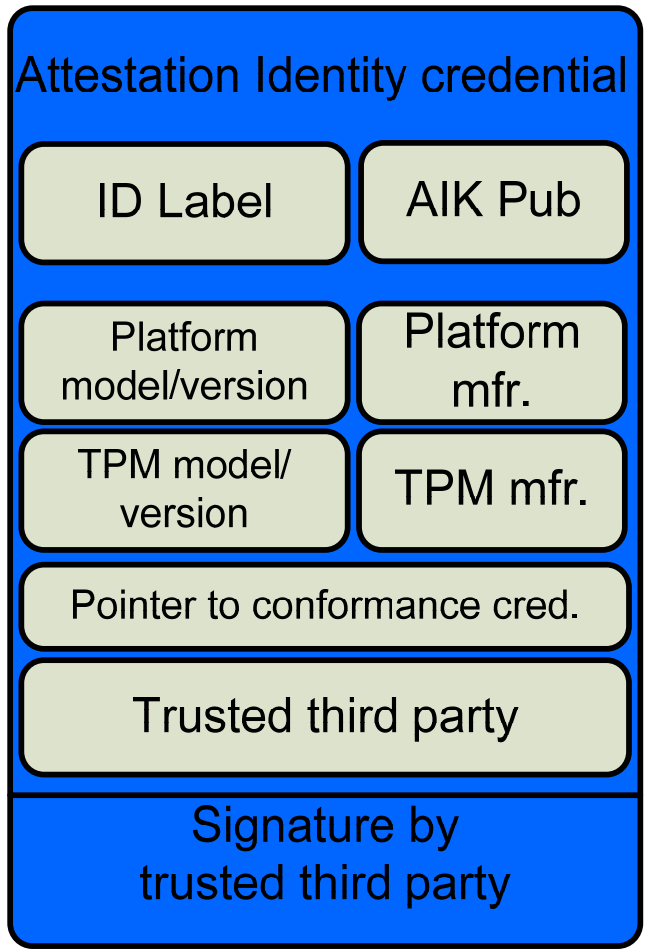
Validation credentials

- To validate components such as
  - Video adaptors
  - Storage adaptors
  - Keyboard/mouse
  - Network adaptors
  - …
- Isuued by a validation entity, e.g. the component mfr. or a lab
- Provides measurement reference values (digests) taken in a clean-room situation



AIK credentials

- Certifactes for AIKs in attestation process
- Issued by trusted third party (privacy CA – PCA)
- Attests:
  - The platform contains a TPM of the named type
  - TPM owns the AIK
  - Is tied to valid endorsement, platform and conformance credentials
- Does not reveal a platform‘s identity



AIK credential usage in Remote Attestation