SCMS157

TCG Credentials: Their Role in the Trust Infrastructure and Manufacturing

Monty Wiseman

Intel, Corp.

September 18, 2003

Safer Computing Track – Fall IDF

Tuesday

- LT Overview
  SCMS-16
- TCG & TPM v1.2
  SCMS-17
- LT Architecture
  SCMS-18
- Tech Showcase
  Every Day
  Birds of a Feather Lunches
  Tuesday & Wednesday

Wednesday

- Privacy Method for Assuring Trust
  SCMS-19
- [illegible] KB
- [illegible] LT
  [illegible]
- Fundamentals for NGSCB
  SCMS-21
- Migrating Apps to NGSCB
  SCMS-22

You are Here

You're Almost home!

Thursday

- TPM Recovery
  SCMS-25
- TCG Credentials
  SCMS-157
- TPM Mfg & Testing
  SCMS-180

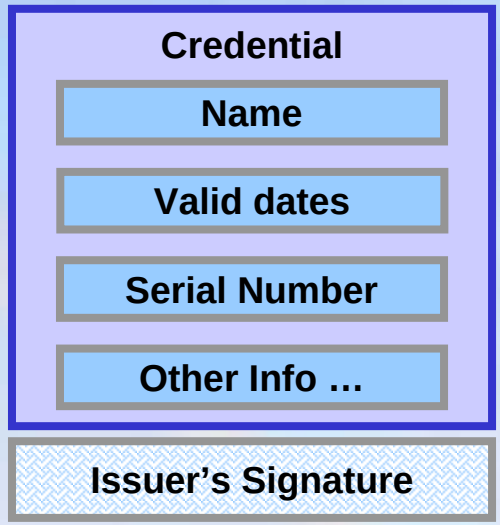
= Overview
= Medium Technical
= Highly Technical

Why do you care about Credentials?

- Credentials are used by an IT infrastructure to maintain policy
  - E.g., User authentication
- TCG introduces the notion of “platform” credentials
  - Typically, most think only of “user” credentials
- Platform manufacturers will care what information the credential contains when issuing Credentials
- Credentials must be signed! What does this mean?
- What impact Credentials have on the manufacturing and distribution process for components and platforms

What is a Credential

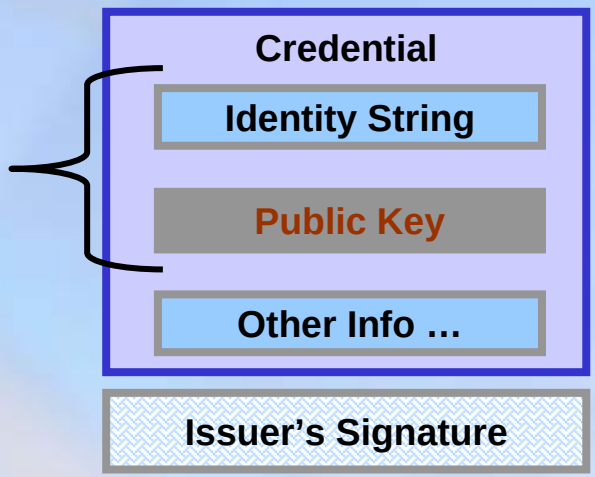
- Contains primary information
  - Identity String (E.g., name), Public Key
  - Attributes
- Auxiliary information
  - Valid dates
  - Serial Number
  - Issuer Name
- Signed by someone verifying that the information is true
  - Without a signature the information cannot be trusted



Types of Credentials

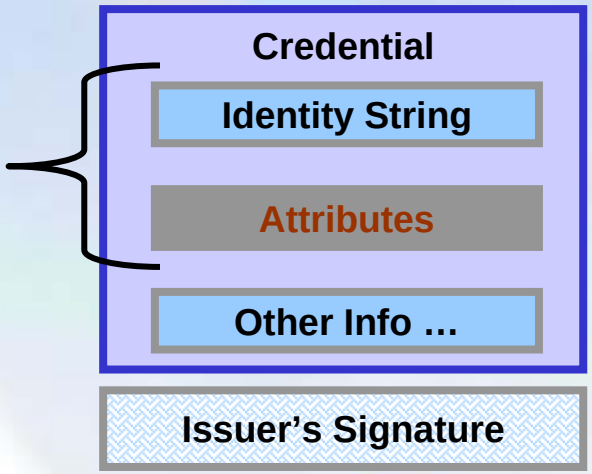
- **Identity Credential**
  - Contains:
    - Identity String
    - Public Key
  - Binds the contents with the public key

  Statement: Issuer verifies that the Public Key is associated with the Identity String



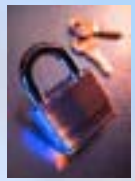
- **Attribute Credential**
  - Contains:
    - Identity String
    - Set of Attributes
  - Binds the attributes

  Statement: Issuer verifies that the Attributes are associated with the Identity String

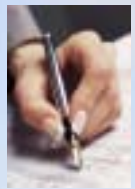


Identity Credential Uses

- Identity Credentials are associated with a key pair
  - Private component is kept secret
  - Public component is “public” and is part of the Credential
- Encryption
  - The public key encrypts data
  - The private key decrypts the above data



- Digital Signature
  - The private key signs a blob of data
  - The public key verifies the above data



- Never mix usage of these keys
  - Never sign with an encryption key
  - Never encrypt with a signature key

Formats

- Definitions
  - X.509 v3
    - Defined by the ITU-T
    - Coding in ASN.1
  - Others:
    - SPKI, XKMS, XML DSIG
- Format for TCG
  - Based on X.509 v3
  - Specific fields defined

Obtaining and using Credentials

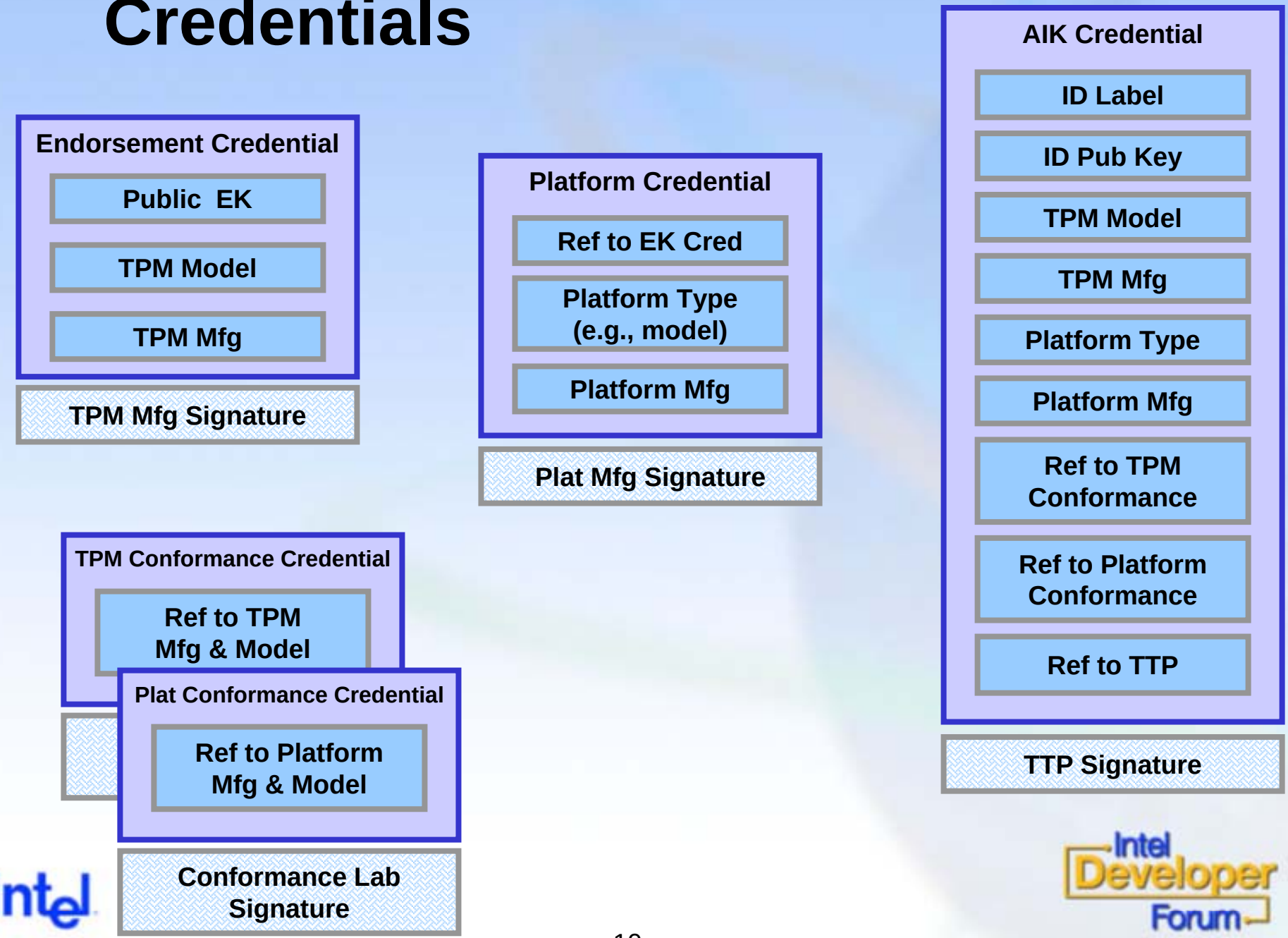
- Certification Authority (CA)
  - Verifies the information
  - Issues the Credentials
    - Compile information into specified format
    - Digitally sign the information
  - Must be trusted by requester and receiver

- Used in:
  - S/MIME
    - Sign and encrypt messages
  - SmartCard transactions
    - Sign and encrypt documents
  - SSL
    - Verifies the server
      - (could also verify the user but that is not widely used)

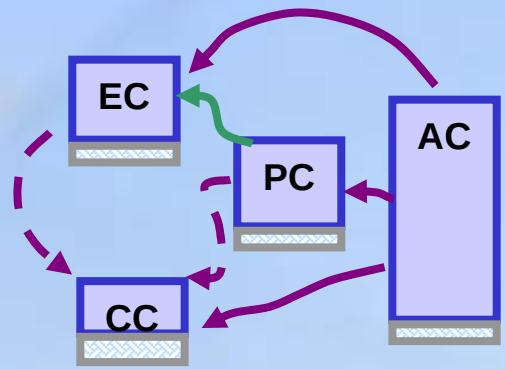
Types of TCG Credentials

- **What is the use/purpose of each Credential:**
  - **What statement is made by each**
  - **What claim is made by each issuer**

Credentials

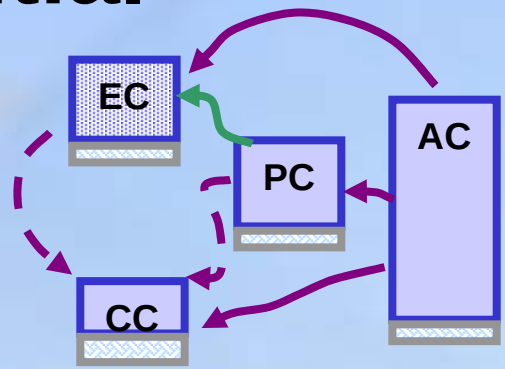


TPM Credentials



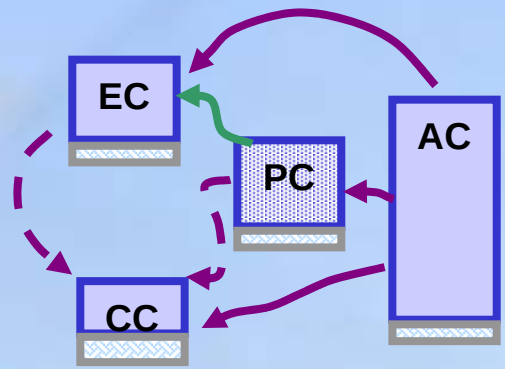
- Types:
  - Endorsement Credential
    - One per platform
  - Platform Credential
    - One per platform
  - TPM Conformance Credential
    - One per “model” of platform
  - Platform Conformance Credential
    - One per “model” of platform
  - Validation Credentials
    - One per component (Optional for a TCG-platform)
  - AIK (Attestation Identity Key) Credential
    - Any number per platform
- Signers
  - The “issuer” signs the Credentials
- Creation and distribution mechanism is not specified by TCG

Endorsement Key Credential



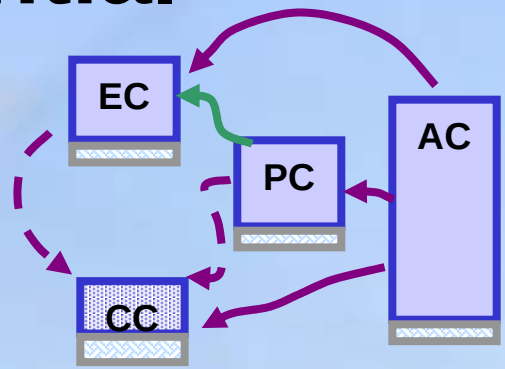
- Issuer: Entity claiming the security properties of the TPM
  - This could be the TPM Manufacturer
- Identifies: The specific TPM
- Contains the Public Key component of the Endorsement Key
- Purpose:
  - Provides attestation that this is a “genuine” TPM
  - Identifies the specific TPM
  - Provides the Public Key used to encrypt the AIKs

Platform Credential



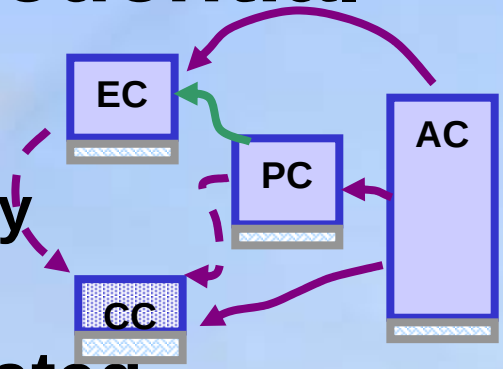
- **Issuer: Entity claiming the security properties of the Platform**
  - **This could be the Platform Manufacturer**
- **Identifies: The specific platform**
- **Contains:**
  - **Pointer to the Endorsement Credential**
  - **May contain other information about the platform**
- **Purpose:**
  - **Provides attestation of the platform's security components by the platform manufacturer**
  - **Add examples of security components:**
    - **How the TPM Is bound to the platform**
    - **etc.**

TPM Conformance Credential



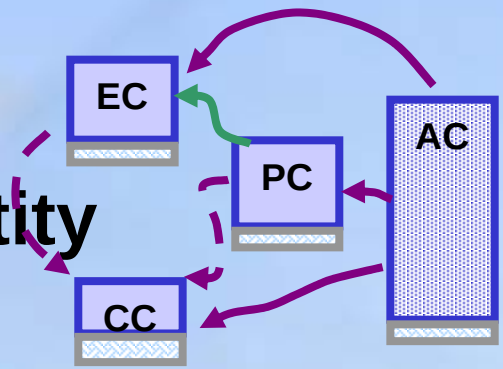
- **Issuer:**
  - **Same as Endorsement Credential entity**
  - **Or, Evaluation Lab**
- **Identifies: The entity that evaluated the TPM**
- **Contains: A reference to the TPM "manufacturer" and model number**
- **Purpose:**
  - **Provides attestation of the TPM's security properties by an accredited party**

Platform Conformance Credential



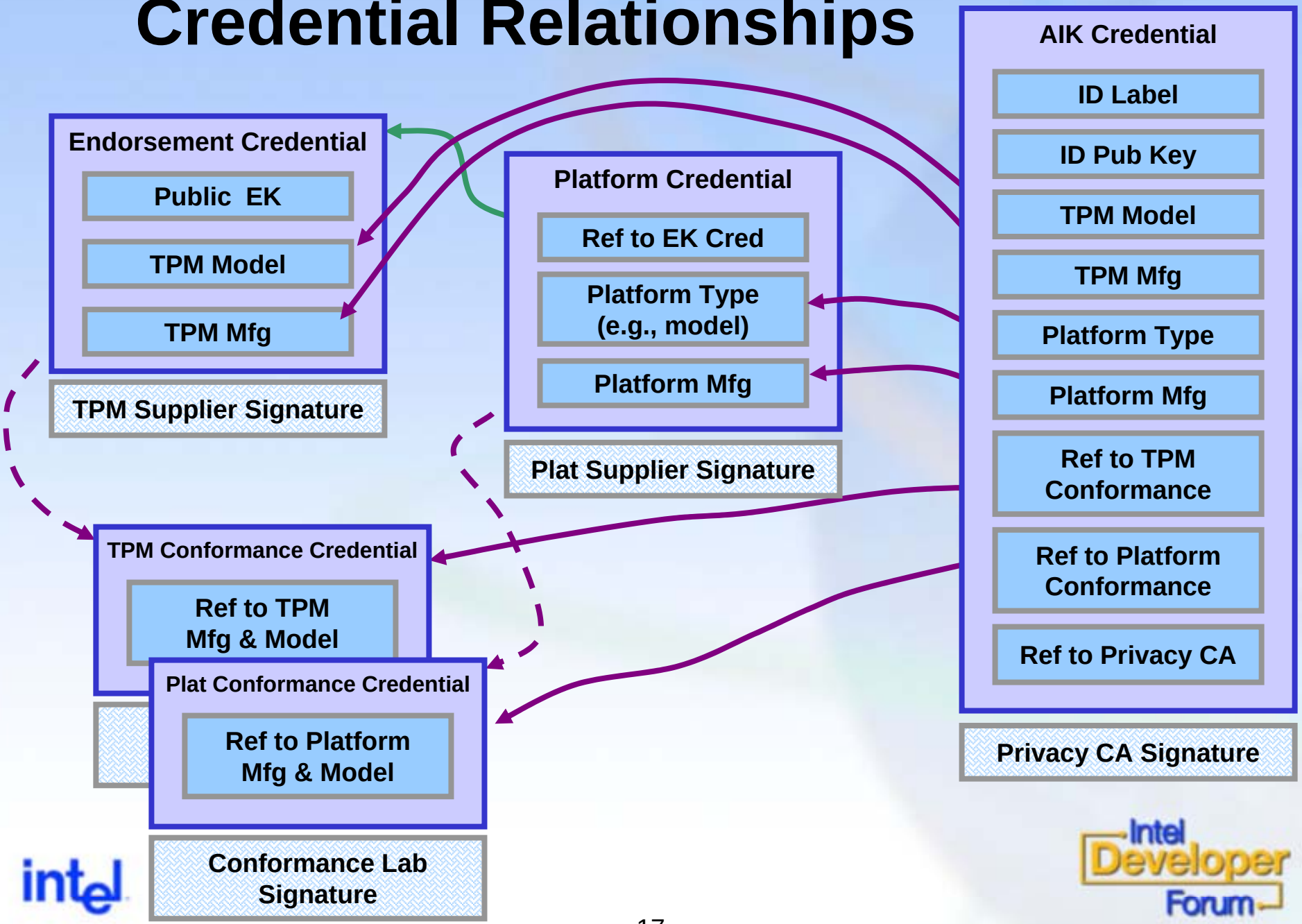
- **Issuer:**
  - **Same as Platform Credential entity**
  - **Or, Evaluation Lab**
- **Identifies: The entity that evaluated the platform**
- **Contains: A reference to the platform “manufacturer” and model number**
- **Purpose:**
  - **Provides attestation of the platform’s security properties by an accredited party**

AIK Credential



- Issuer: Privacy CA
- Identifies: The Attestation Identity Key (i.e., the AIK)
- Contains: As much or little information as dictated by requester and issuer policy
- Purpose:
  - Signs operations that provide platform authentication or platform attestation
  - Unlimited number can be created per platform
  - Provides aliasing of the platform

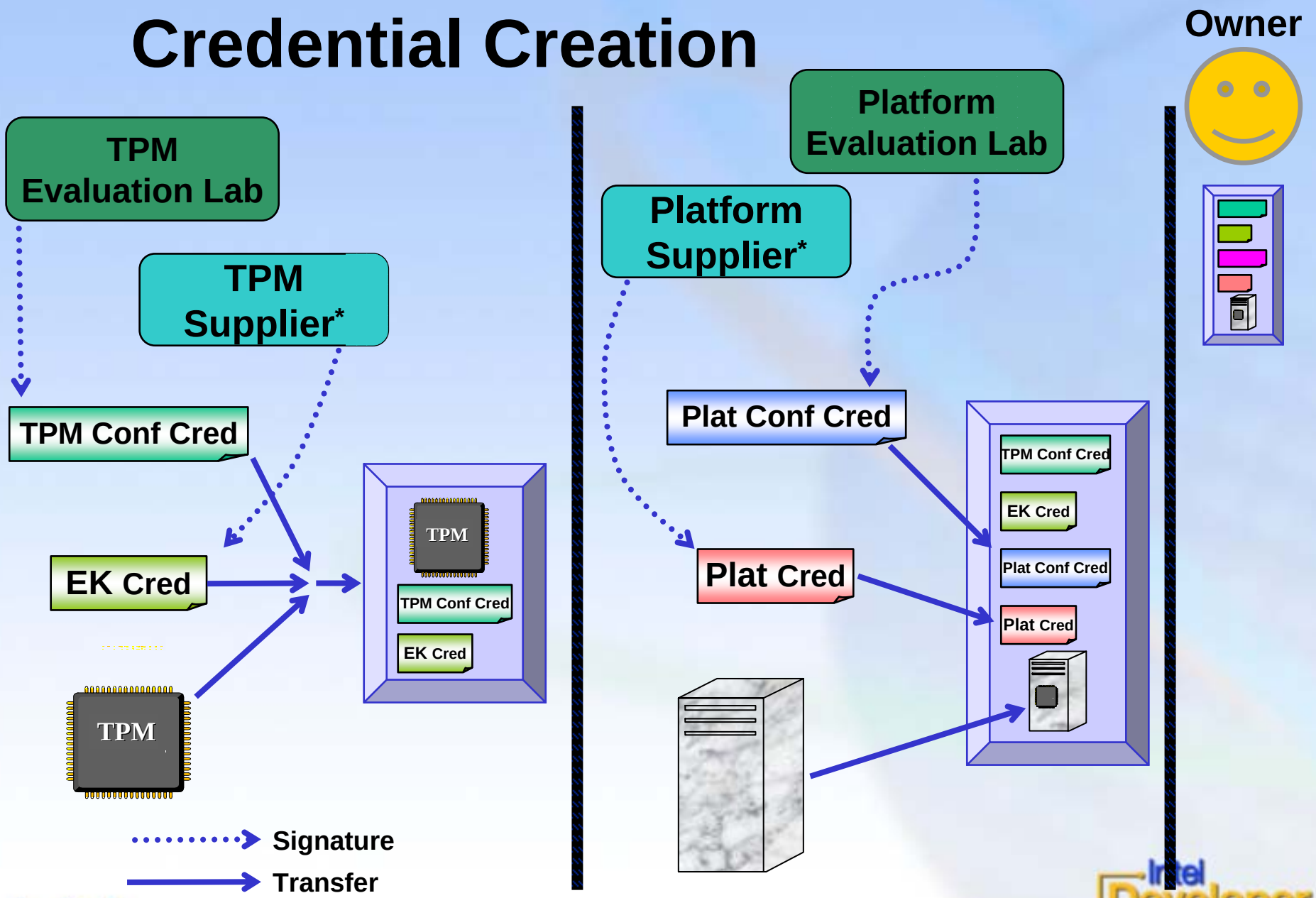
Credential Relationships



Putting it all together

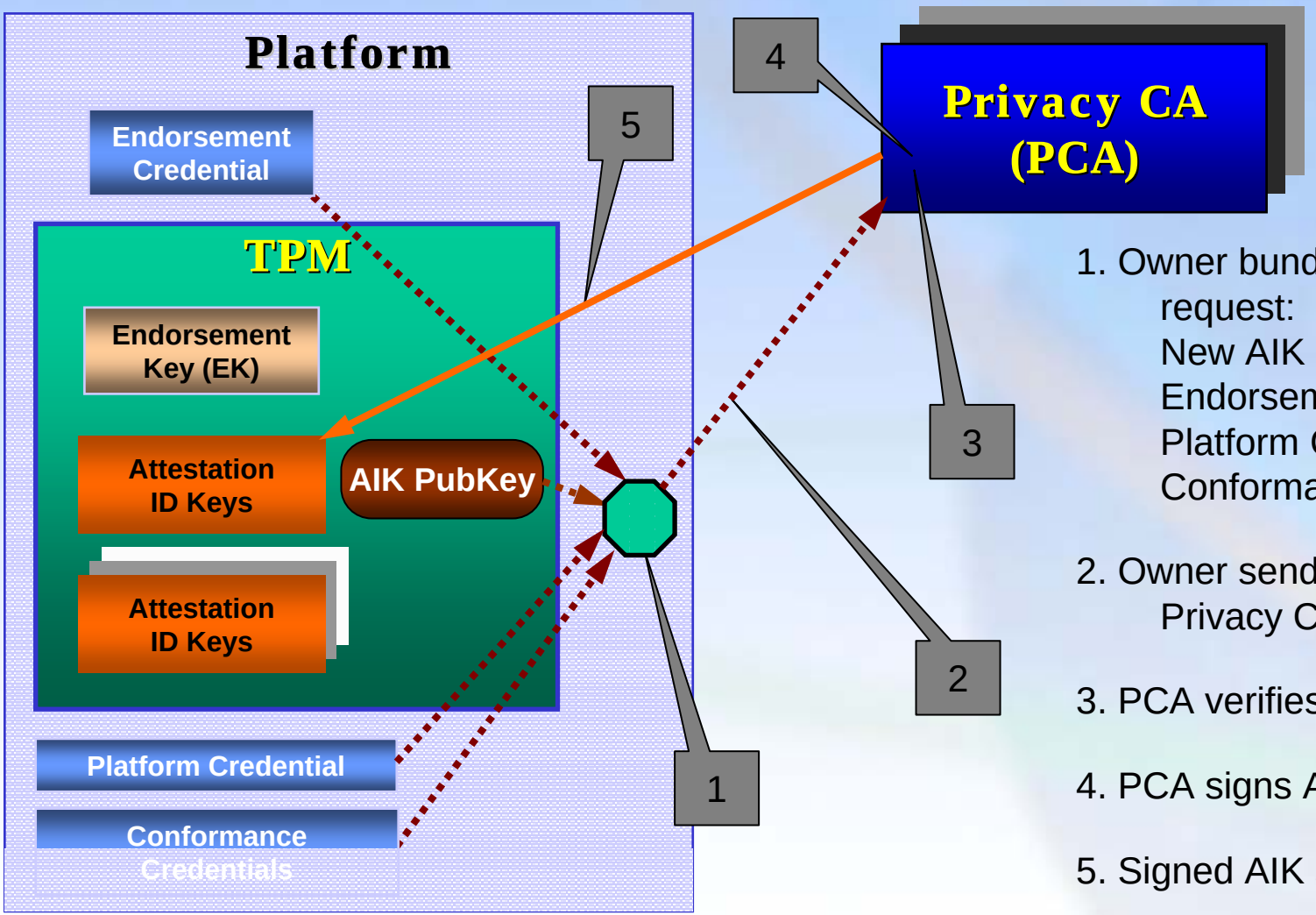
- Credential creation
- How Credentials provide trust while providing aliasing / anonymity
- Credentials and their role within the ecosystem

Credential Creation



* This is the entity claiming the security properties of the TPM or the Platform. This may be the manufactures but that is not a requirement

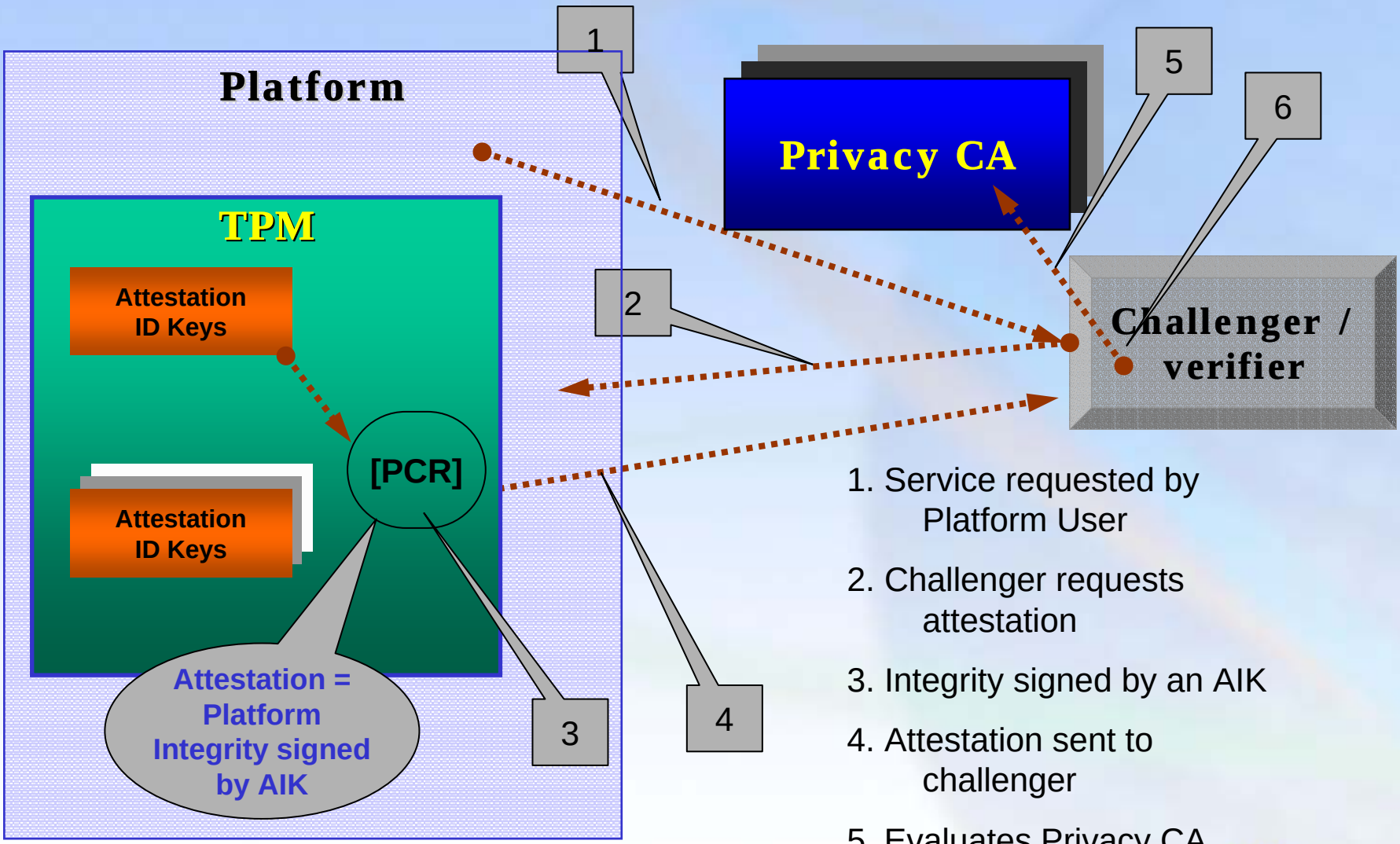
Role of Credentials in Attestation



1. Owner bundles into an AIK request:
   New AIK PubKey
   Endorsement Cred,
   Platform Cred,
   Conformance Creds
2. Owner sends AIK request to Privacy CA (PCA)
3. PCA verifies Credentials
4. PCA signs AIK
5. Signed AIK sent to TPM

For an alternate method review:
"Privacy Method for Assuring Trust SCMS-19"
presentation

Role of Credentials in Attestation



1. Service requested by Platform User
2. Challenger requests attestation
3. Integrity signed by an AIK
4. Attestation sent to challenger
5. Evaluates Privacy CA
6. Evaluate Platform's Integrity

Storage of Keys and Credentials

- **Keys and Credentials are not intended to be "stored" on the TPM**
  - **TPM has limited resources**
- **During Platform Use**
  - **AIKs**
    - **User may need ready access to these**
    - **Likely to be stored by the application**
  - **EK, Platform, and Conformance Credentials**
    - **Only used to get AIKs**
      - No need for ready access
    - **Need to be protected**
      - Privacy Sensitive
- **See course "Recovering from Computer Failures, if TPMs Go Bad" SCMS-25**

Distribution of Keys and Credentials

- Platform does not ship with any AIKs
- EK, Platform, and Conformance Credential are OS independent
- Can be supplied:
  - On distribution CD
  - On hard drive partition
  - Downloaded via the Web
  - etc.
- Must be made available to platform owner if original distribution copy is not available

Revocation

- An compromised TPM or Platform can no longer be trusted
- Trust is revoked by notification to those interested:
  - Privacy CAs
  - Challengers / verifiers

Credentials: Their role within the ecosystem

- IT infrastructures have policies e.g.,:
  - Only platforms owned by the company can access the network
  - Only Trusted platforms can sign documents
  - Only Trusted platform can receive confidential data
- Attestation using an AIK provides the IT infrastructure with the necessary trust statements

Summary / Next Steps

- Credentials allows automated trust policies to be enabled
- Start design process for manufacturing line to provide credentials
- Start designing your IT infrastructure to issue and use credentials

Thank you for attending.

Please fill out the Session Evaluation Form.