Overview of the TPM Key Management Standard

Thomas Hardjono
Greg Kazmierczak
Wave Systems

TRUSTED COMPUTING GROUP™

What is a Trusted Platform Module

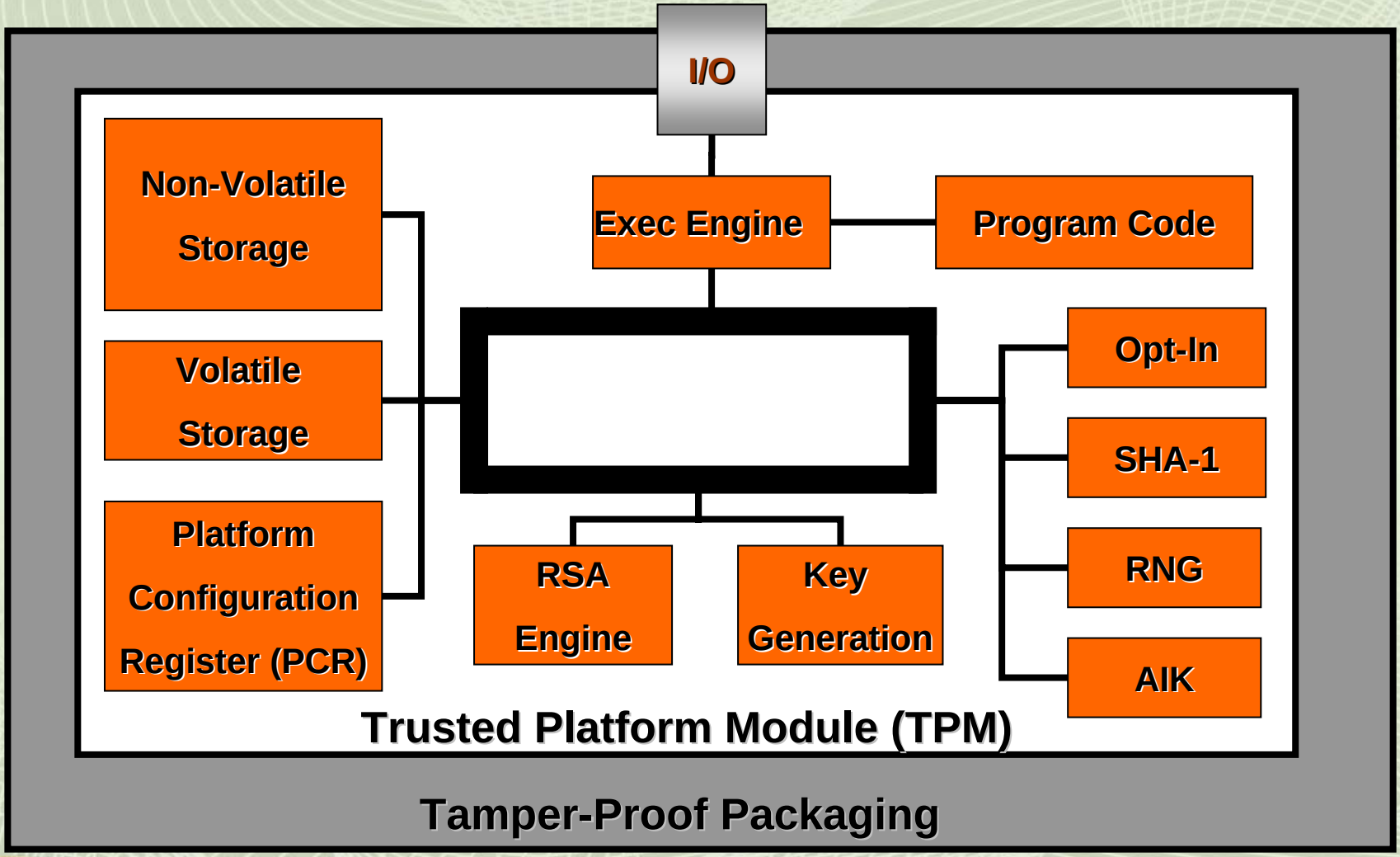
A TPM provides

- protected capabilities to access and process keys, passwords and other data assets stored in shielded locations
- to BIOS, OS, and applications
- optionally provide verifiable proof to a remote challenger

- The TPM contains
  - cryptographic engine
  - protected storage
- The TPM cannot be moved - Attached to the platform
- Functions and storage are isolated
  - Provides a “Trust Boundary”
  - The TPM falls into definition of the *Cryptographic Unit* as defined in IEEE1619.3 Draft D4
- May be used in devices other than PC Platforms
  - Eg. FDE drives, Controllers, Network Access Points, etc.

TRUSTED COMPUTING GROUP™

The Trusted Platform Module



Ubiquity of The TPM hardware

- Today: over 200 million TPMs in the market
  - Ships on all major OEM platforms
- Market projections:
  - December 2009: 50% penetration
  - December 2010: 75% penetration
  - December 2011: more than 80% penetration

- Sources:
  - User testimonials from key verticals, Fortune 1000, other market leaders
  - Recommended usage by analysts and consultants

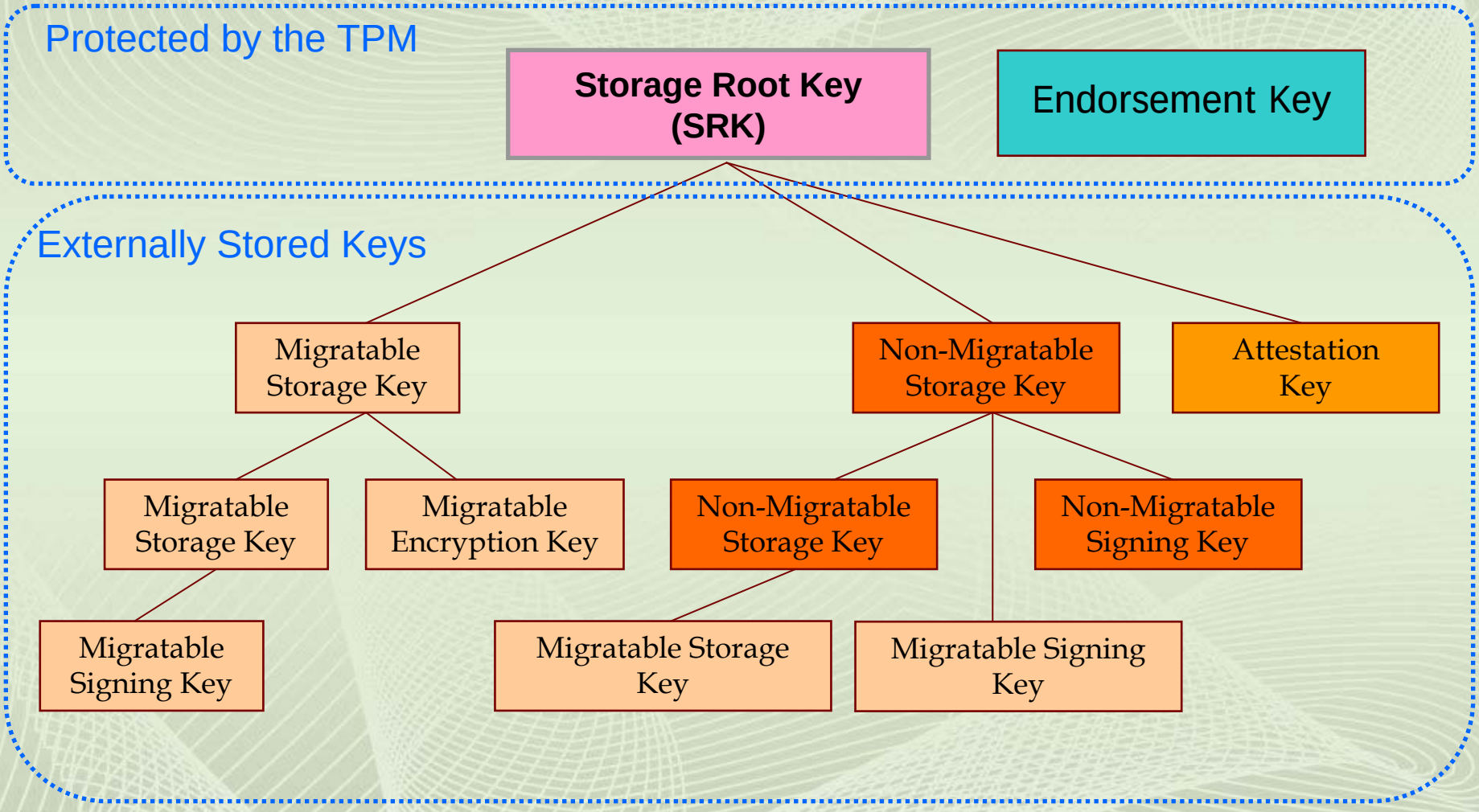
TRUSTED COMPUTING GROUP™

TPM Key Types

- Non-Migratable Key (NMK)
  - A key which is bound to a single TPM. This is a key that is (statistically) unique to a single TPM and can not be migrated or exported from the TPM.
- Migratable Key (MK)
  - A key which is not bound to a specific TPM, and with suitable authorization, can be used outside a TPM or moved to another TPM.
- Certifiable Migratable Key (CMK)
  - A key whose migration from a TPM is highly controlled and the TPM can attest / certify it properties

The TPM key types are defined at key creation time by the User. Migration destinations are defined and authorized by the TPM Owner.

TPM Key Hierarchy



Key Migration & Backup/Vaulting

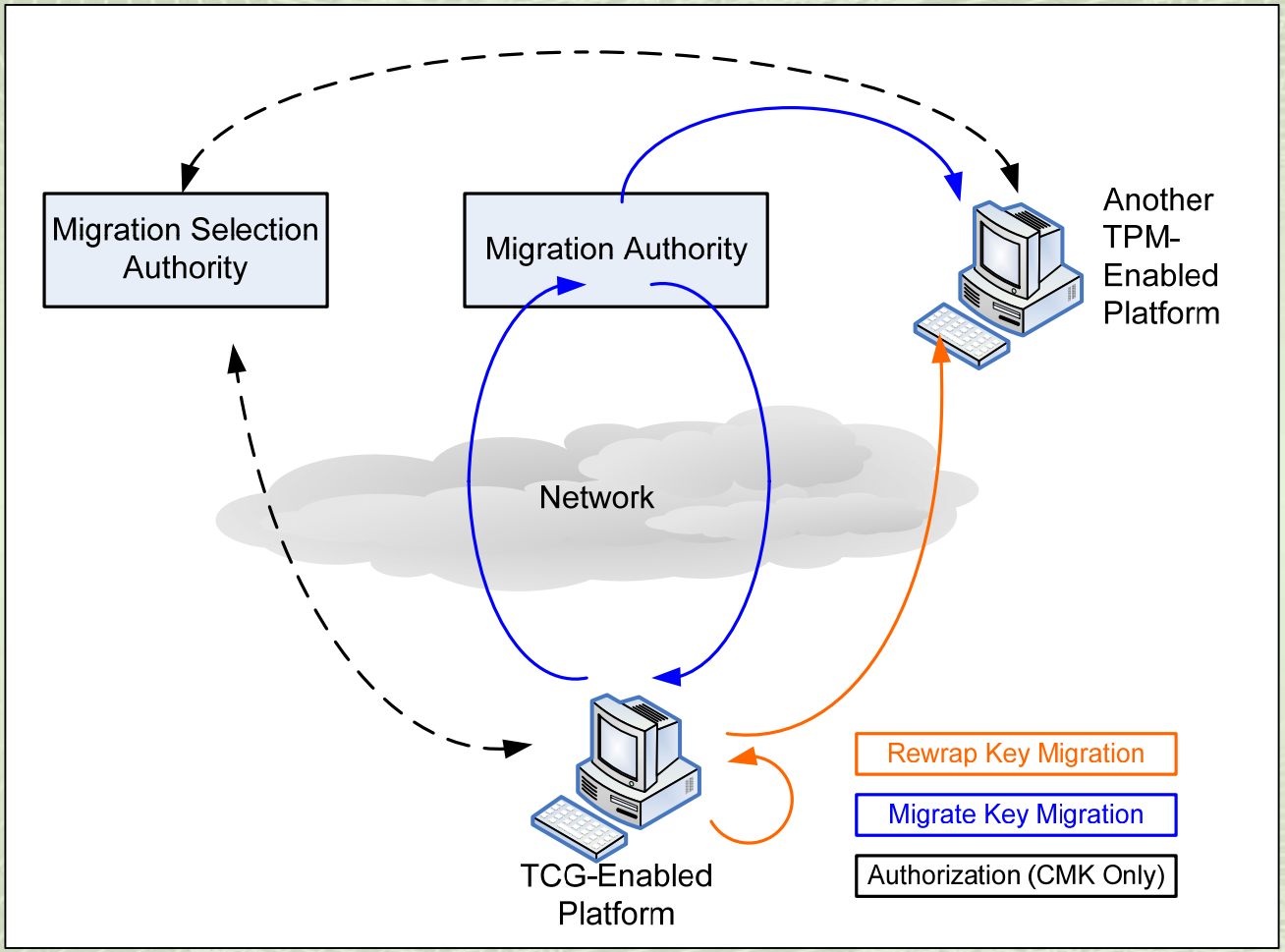
- TPM Key Migration and Vaulting:
  - The ability to migrate a key (and optionally its children keys) from one TCG-compliant platform to another
  - Several flavors:
    - Direct migration
    - *Migration Authority* as intermediary
    - With *Migration Selection Authority* authorization
- The ability to migrate and/or vault key-specific information such as passwords with a key
- The ability to migrate and/or vault application-specific information such as CSP container or certificates with a key

Migration Entities

- Migration Authorities (MA)
  - The MA participates in the migration of a migratory key. Migration of a MK or CMK is coordinated by an MA, and the key may be vaulted in the MA or temporally transit through the MA.
- Migration Selection Authorities (MSA)
  - The Migration Selection Authority (MSA) authenticates and authorizes a CMK migration destination without handling the key itself.

The TPM Owner authorizes the migration destination and the key owner authorizes the migration transformation. The MSA can also authorize the migration destination as a proxy for the owner.

Key Migration Flow



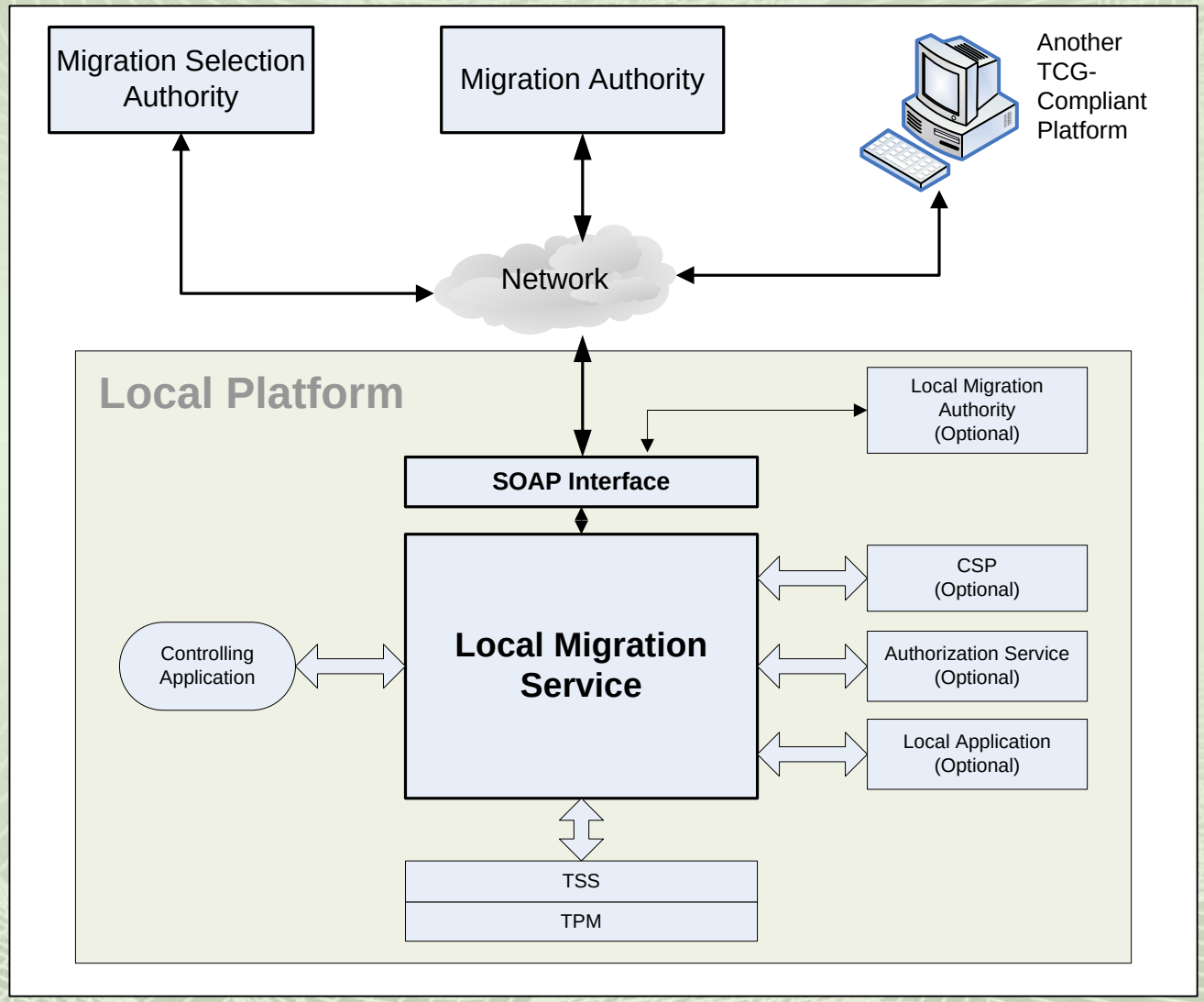
The TCG Migration Specification addresses the interoperability requirements for key and key associated information to be securely transferred from a TCG-compliant source platform to a TCG-compliant destination platform, with or without the assistance of a Migration Authority.

Migration Structures

- Migration Blob
  - TPM-generated BLOB which holds the encrypted key exported from a TPM.

- Migration Package (MP)
  - An XML document used for the purposes of archiving or migrating one or more keys to another platform.
  - Contains identifiers for the package, the migrating key, and an optional number of children keys of the subject migrating key.
  - For each key which is being migrated, the MP may optionally contain:
    a. password values
    b. application data

Migration Model



Local Migration Service

- LMS is a client service which is responsible for
  - Creation of a Migration Package (MP), or
  - Parsing of a MP, retrieved either from a remote or local MA or other valid source, which is to be imported.
- LMS has the architectural responsibility to identify valid MAs and MSAs, and implement confidentiality and integrity services for MPs.
  - LMS may optionally interact with other local services or applications in order to ensure that archived or recovered keys may be successfully restored and used by the intended application(s).
  - LMS interaction with local services and applications may be initiated by the local services and applications or it may be initiated by the LMS – both models are supported.

The Migration WSDL

- Describes the set of commands related to TPM key migration and backup/vaulting.
- Commands/actions:
  - **Authenticate** – prove valid possession of enabled and activated TPM
  - **Upload** - Sends an MP to MA
  - **Download** – Retrieves an MP from MA for client
  - **Query** – interrogate the MA as to what valid MPs exist for this client
  - **Delete** – client requests deletion of MP by MA
  - **Get MA Service Information** – client requests service information
  - **Get MA Key** – client requests MA certificate

Conclusions & Summary

- The TPM arguably one of the most ubiquitous security hardware in the PC industry today:
  - Adoption signs also in the IP network industry
  - Core part of the TCG's Network Admission Control (TNC) value-prop
- Enterprise key management systems/solutions will need to:
  - Support key management lifecycle for TPMs
  - Support the TPM as a platform identity token
  - Support TPM-enabled (TPM-aware) applications
  - Manage the TPM as a generic secure key store and trust-anchor store

TRUSTED COMPUTING GROUP™

END + QUESTIONS

TCG Infrastructure Work Group specifications:

- https://www.trustedcomputinggroup.org/specs/IWG

Migration Package Schema:

- https://www.trustedcomputinggroup.org/XML/SCHEMA

Migration Service WSDL:

- https://www.trustedcomputinggroup.org/XML/WSDL

TRUSTED COMPUTING GROUP™