Securing Information Transfer in Distributed Computing Environments

AbdulRahman A. Namankani

Out Line

- What does it mean?
- Identity Information
- Identity Trust Domain
- Security Analysis
- Security Requirement
- A suggestive solution
- Conclusion

What does it mean?

Securing Information Transfer in Distributed Computing Environment …

A collection of loosely coupled processors interconnected by a communication network

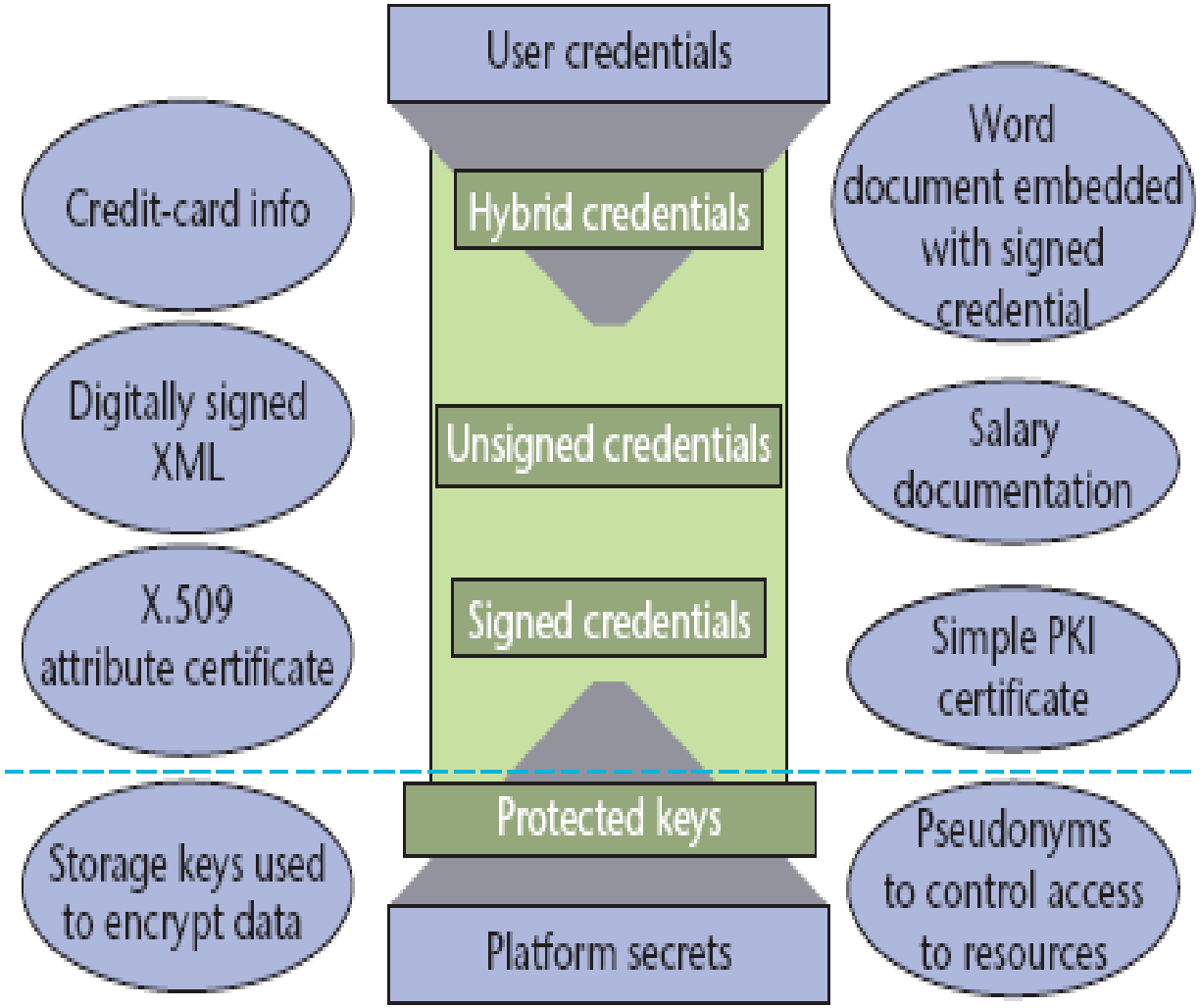
Identity Information

- Cryptographic key
- Unsigned credentials
- Signed credentials
- Hypride credentials

User credentials

High-Level

Low-Level

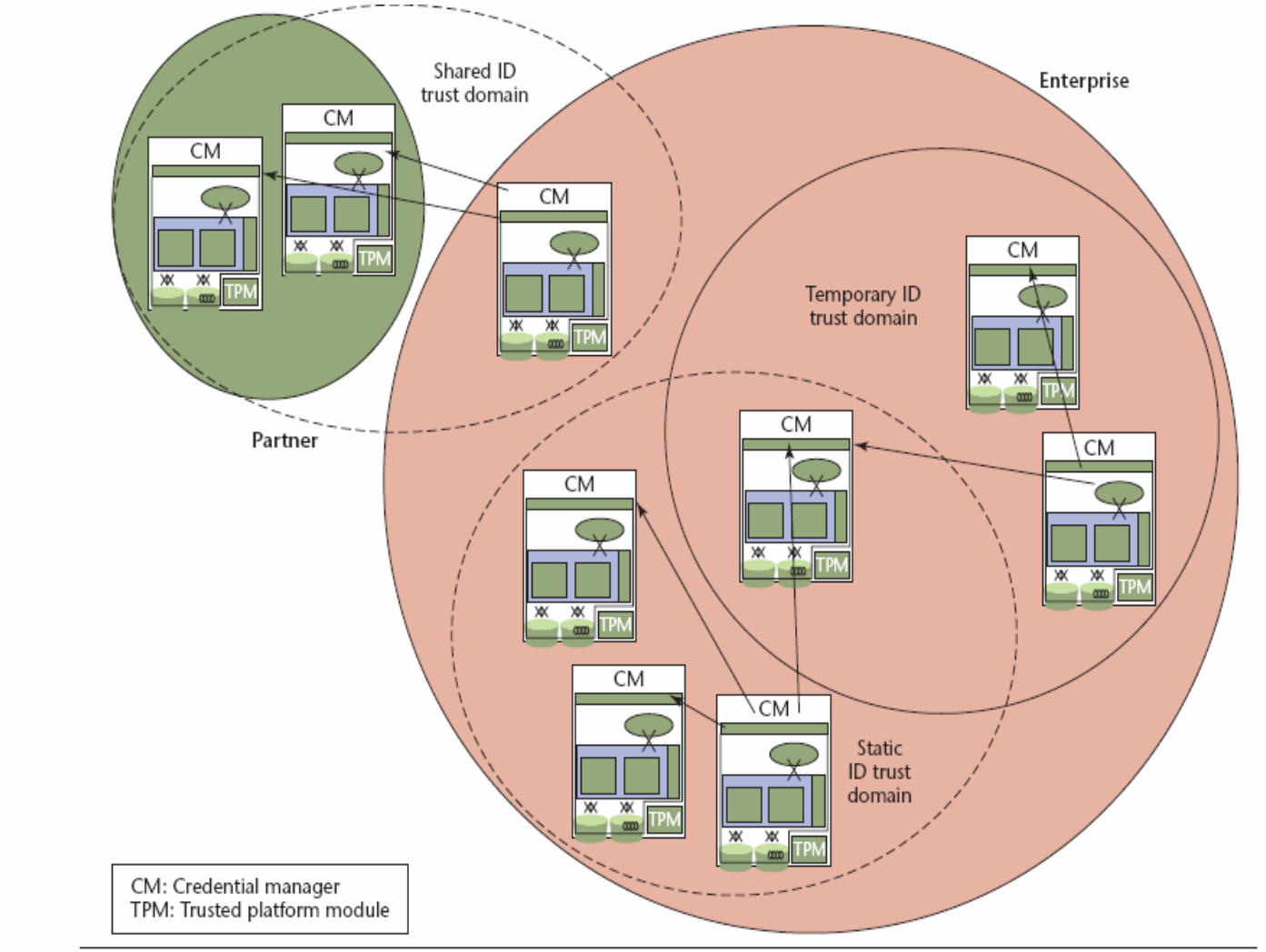


Presistent

Mobile

Shared

Identity Trust Domain



Do we need to transfer Identity informations?

Call For a Solution

1. Maintain data conf.
2. Maintain data intg.
3. Perform in a controlled manner
4. Prevent the policies corruption
5. Ensure the solution’s accountability and compliance with policy

Key Approches

- Policy-based encryptions
- Tamper-resistant hardware during the migration
- Use a third parties to provide a basis for trust, accountability and policy checking
- Audited access to data, based on stated policy

Terms

- Security Policy
  - A statement of what is ,and what is not, allowed
- Security Michanism
  - Methodes used to enforce the policy
- Threat
  - A potential violation of security
- Confidentiality: Keeping data and resources hidden
- Integrity: Preventing unauthorized modification

Encryptions

- Most computer encryption systems belong in one of two categories:
  - Symmetric-key encryption
  - Public-key encryption

Control Access

	file1	file2	file3
Andy	rx	r	rwo
Betty	rwxo	r	
Charlie	rx	rwo	w

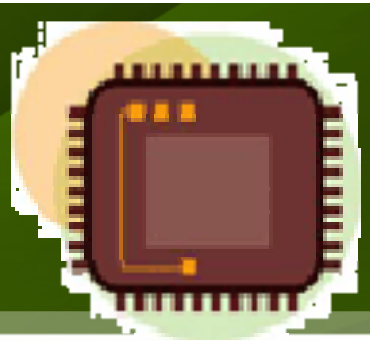
Back to the
main topic …

TCG

- Not-for-profit organization formed to
  - Develop
  - Define
  - and promote open standards

  for hardware-enabled trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals, and devices.

TPM



- Trusted Platform Module
- Low-Cost TPMs are becoming commodities in business computing devices, laptops and desktops
- Act as a root of trust
- Used mainly to protect keys and other platform secrets and to exe cryptography operations

But …

- TCG specifications are based on a monolithic platform
- TPM is bounded to that platform
- Requires the platform owner to explicitly authorize credential migration to specific destination platform

Additional requirement is needed !!

A Policy-Driven Migration

- Providing a mechanism to migrated user-credentials associated with policy that govern there use, security, accountability and privicy during the migration
- Adding a Trusted Third Party (TTP)
  - Address the problem of not knowing the dest. in advance

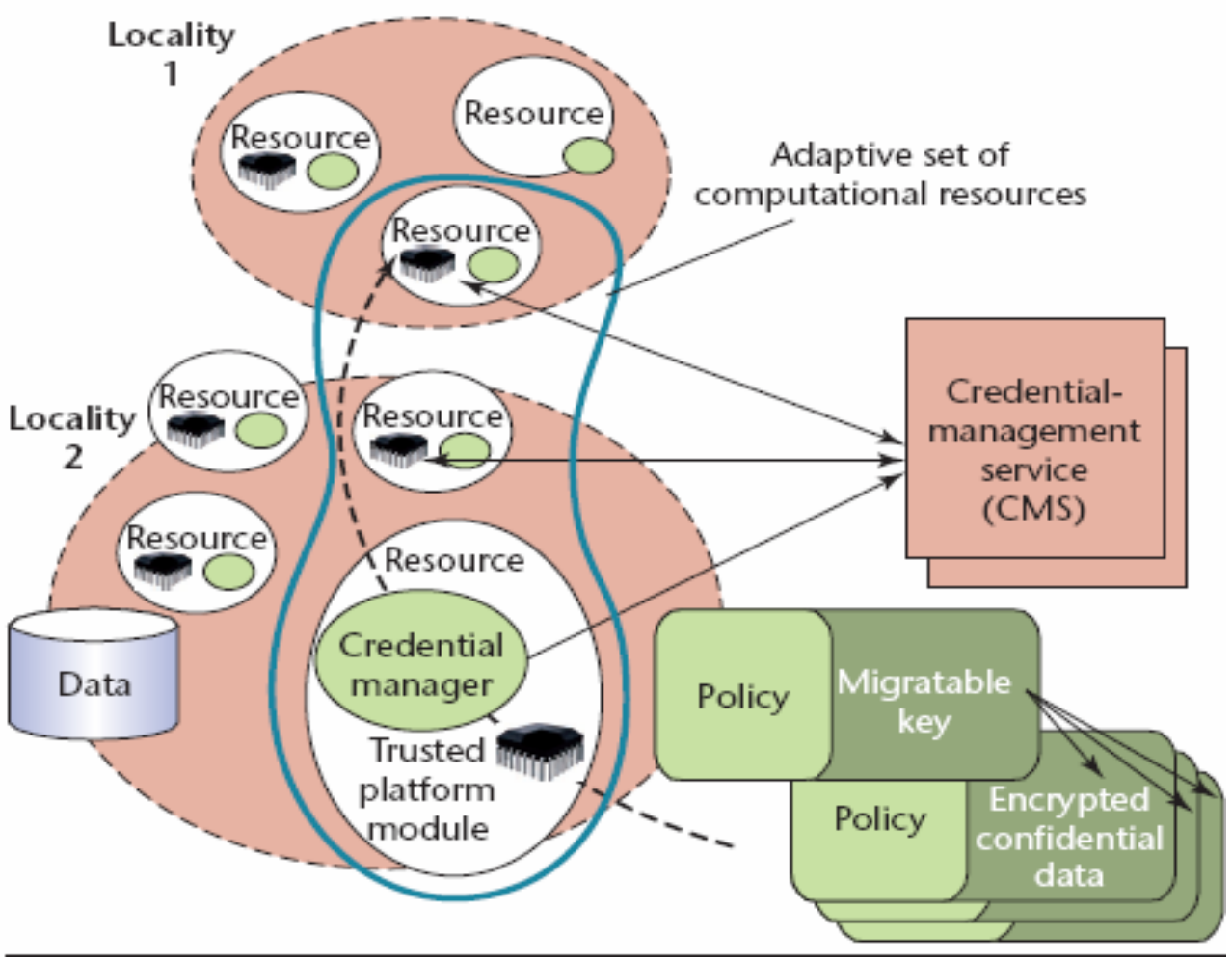
Credential-Managment System (CMS)

- Security mechanism
- Running in local platform to protect credential
- Define how to migtrate data
- Also, adding a trusted HW for encryption
- And adding the policy mech. to ensure that the target meet the required policy to receive data and key

CMS

TPM

The Root of Trust



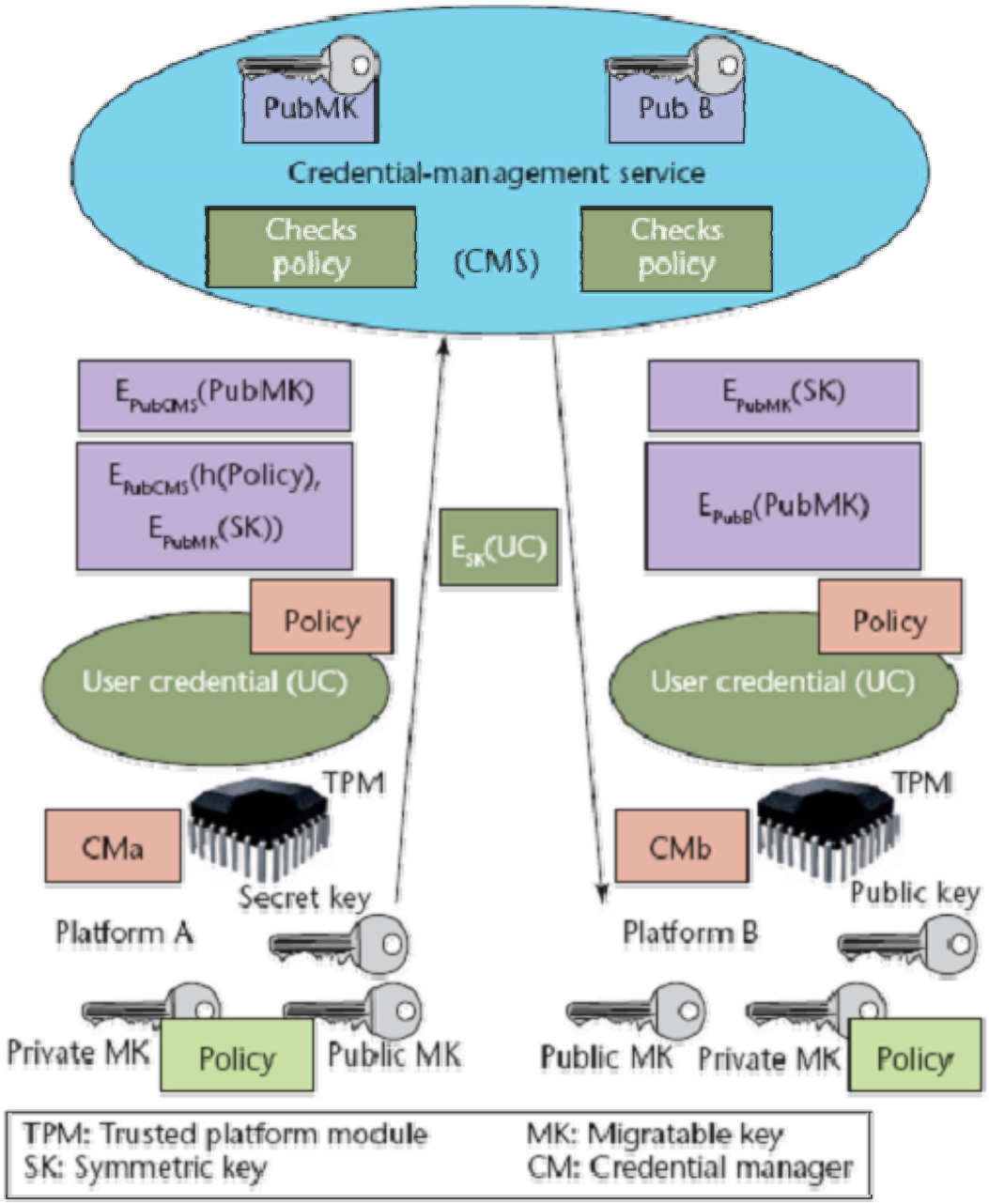
Policy

- Remotely verify the software state and identify the target platform as belonging to a known partner
- Migrate only within a given set of platforms
- Check for stated purposes for which data will be used in the new system
- TTP will be used as an interpreter for the policy

Putting things together ..

- We can relay on TCG protocols to migrate low-level user-credentials
- TPM act as a local credential and as a source for used authenticate
- TTP will be working as trusted authority and used to generate IBE decryption keys, the same entity as CMS

Example …


PubMK
Pub B
Credential-management service
Checks policy
(CMS)
Checks policy
E_{PubCMS}(PubMK)
E_{PubCMS}(h(Policy), E_{PubMK}(SK))
E_{SK}(UC)
E_{PubMK}(SK)
E_{PubB}(PubMK)
Policy
User credential (UC)
Policy
User credential (UC)
TPM
CMa
Secret key
Platform A
TPM
CMb
Public key
Platform B
Private MK
Policy
Public MK
Public MK
Private MK
Policy
TPM: Trusted platform module
SK: Symmetric key
MK: Migratable key
CM: Credential manager

Summary

- What does it mean?
- Identity Information
- Identity Trust Domain
- Security Analysis
- Security Requirement
- A suggestive solution

In Conclusion