Physical-Logical Interoperability: A Solution Framework

Mohammad Soleimani
Chief Technology Officer and EVP, *Kastle Systems*
Chairman, *PSIA Profiles Working Group*
Chairman, *PSIA Physical-Logical Access Interoperability Working Group*
9/23/2013

Establishing the Need

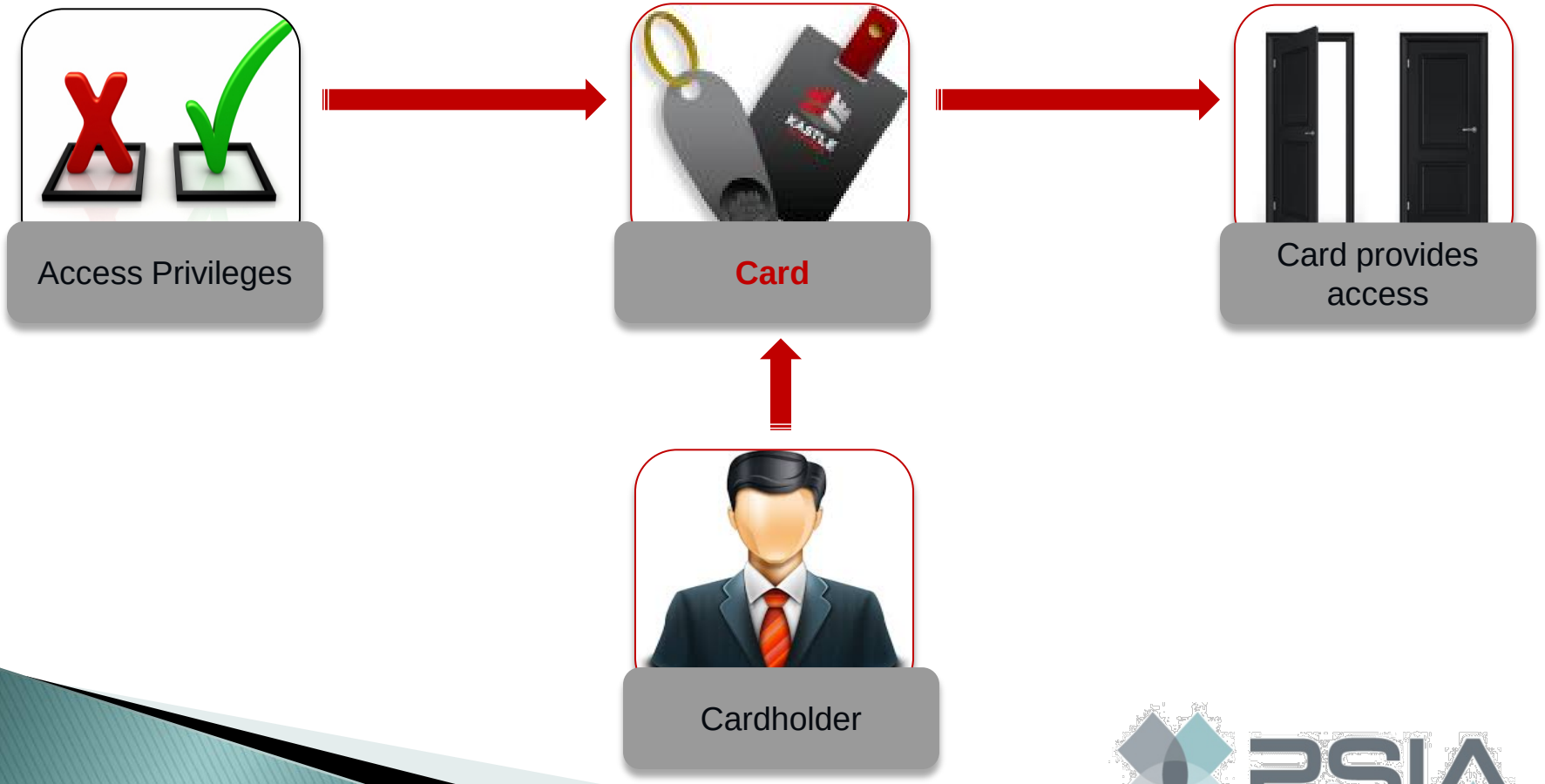
Today there are significant business reasons for enterprises--both large and small--to have system-level interoperability for physical and logical access**:**

- **The convenience, security and efficiency of the one-step employee on-boarding and off-boarding**
- **The ease and security of managing access for visitors and employees, based on their function(s) within the organization**
- **The convenience of using mobile devices to provide physical and logical access**
- **The additional security of restricting access based on location, threat level and other dynamic attributes**

PSIA has established the framework for such a solution and is launching a new working group for Physical-Logical Access Interoperability (PLAI).

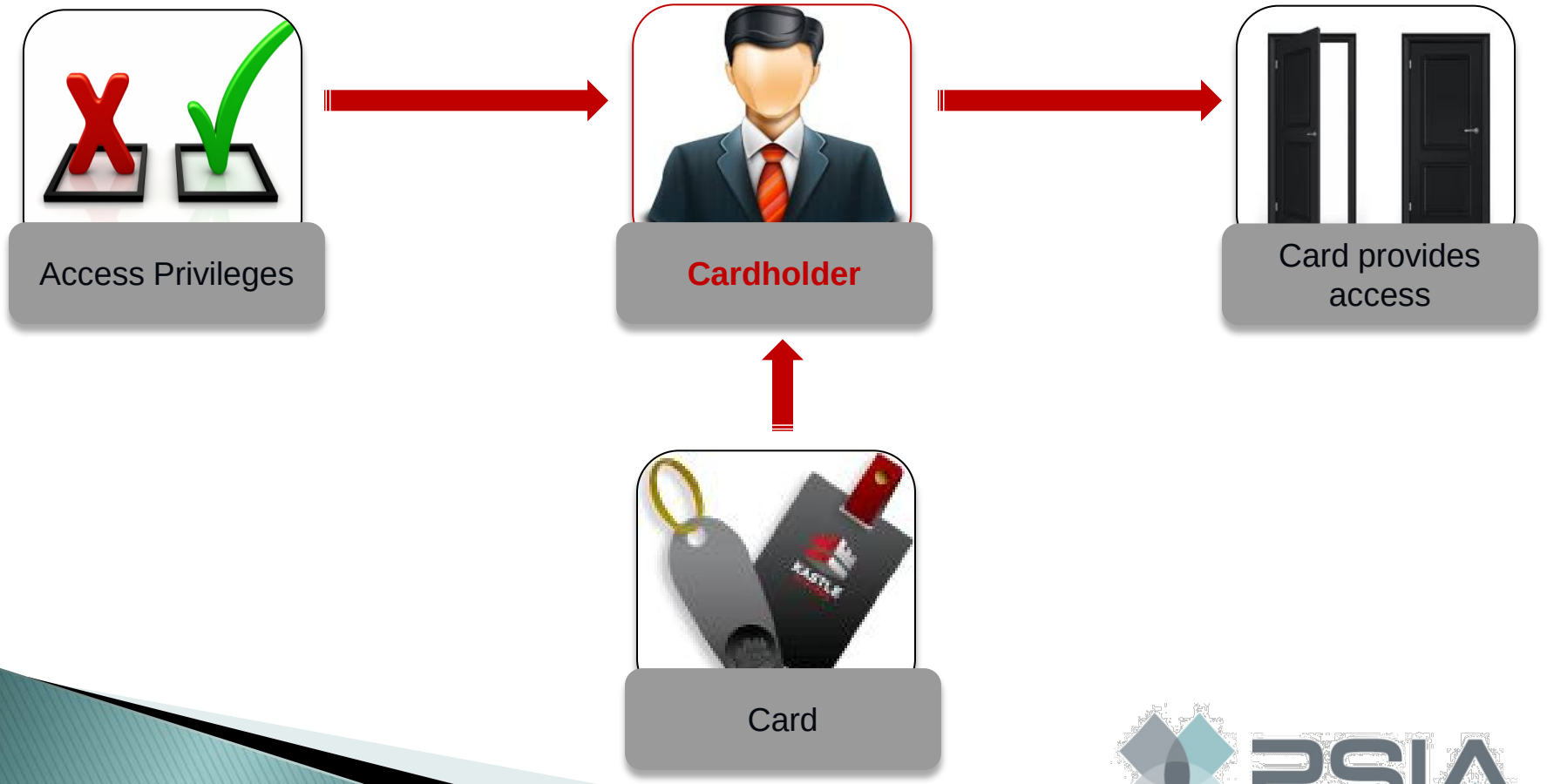
The Evolution of Physical Access: From Card-Centric…

We have moved from a model where access privileges were previously associated with a **CARD...**



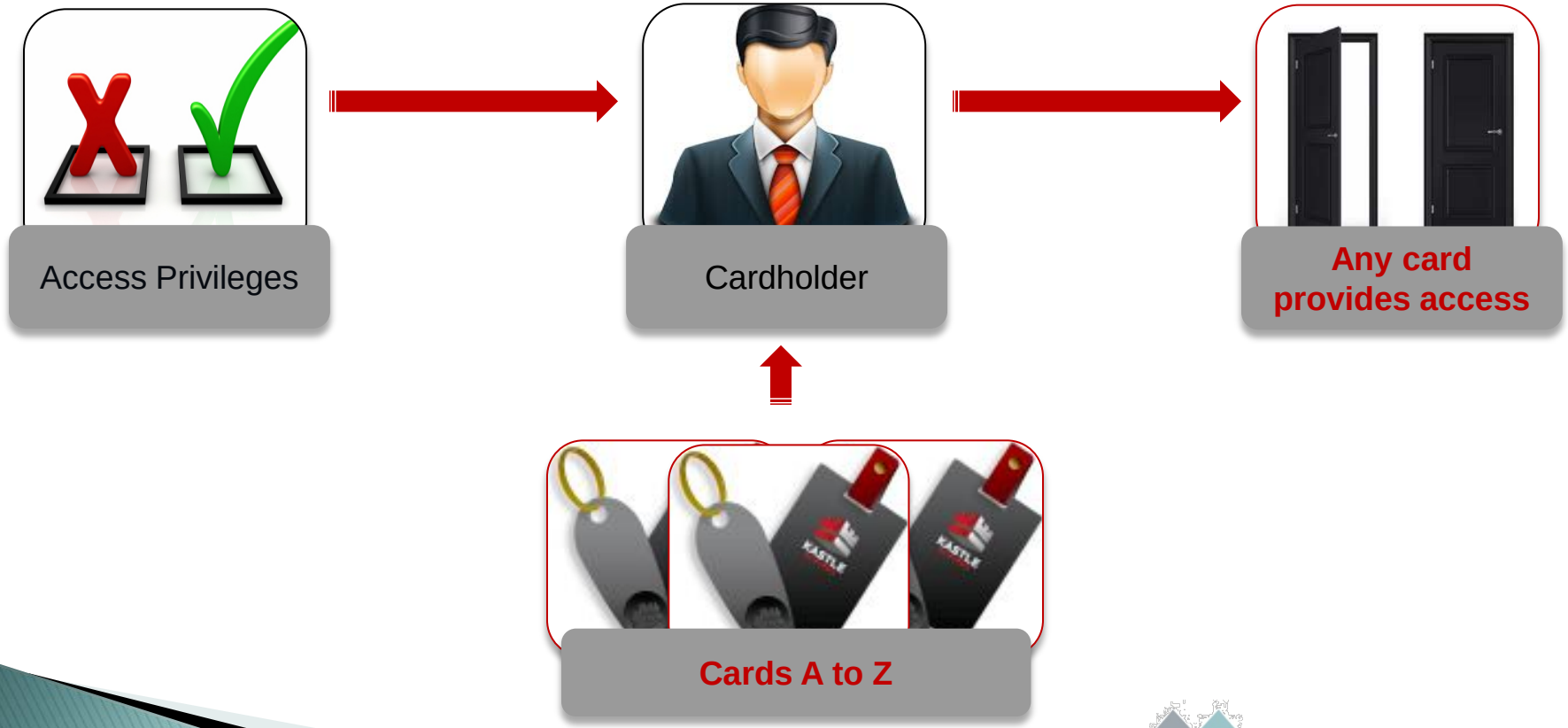
The Evolution of Physical Access: …to Cardholder-Centric

…to access privileges that are now associated with a **CARDHOLDER.**



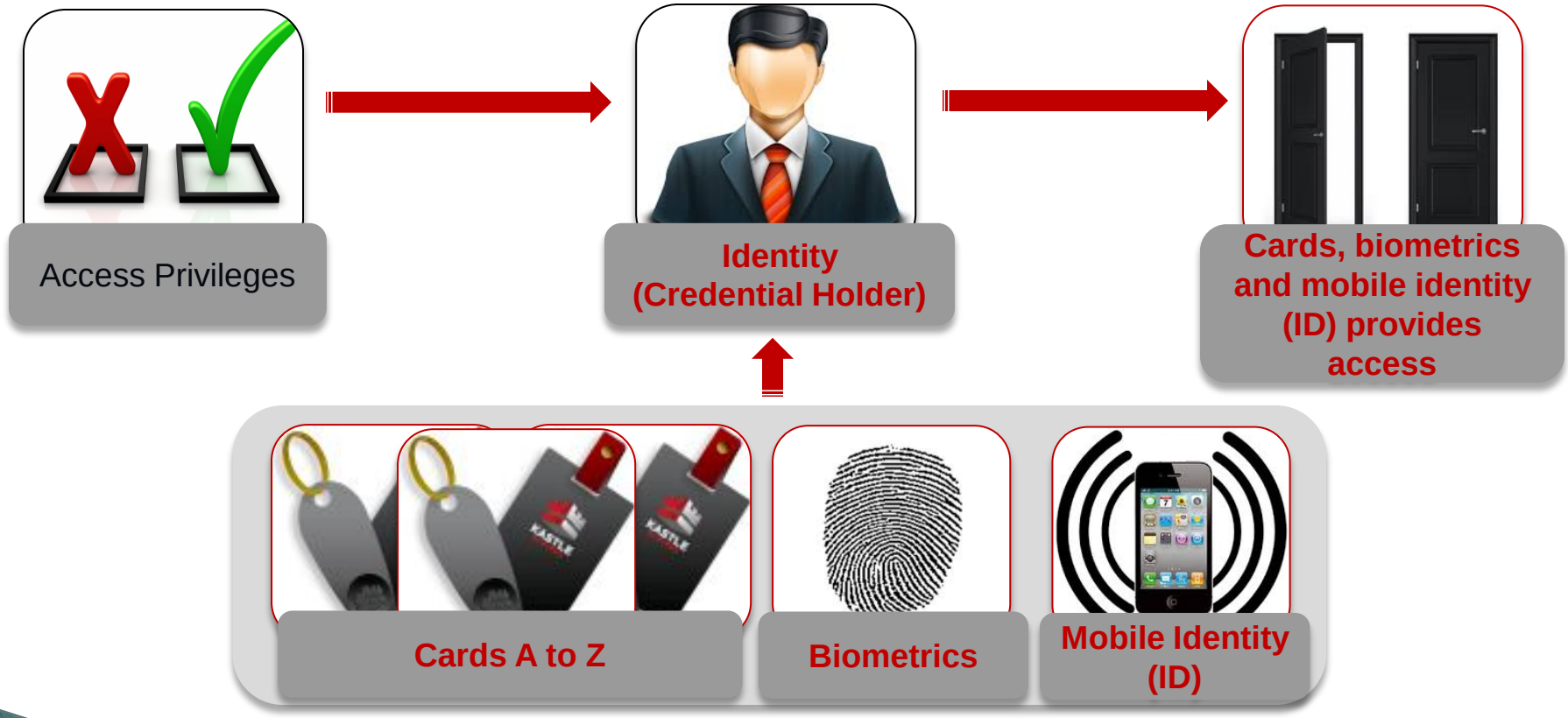
The Evolution of Physical Access: Any-Card Access

Since access privileges are given to a cardholder, **ANY CARDS** associated with that cardholder get all of the access privileges that they have.



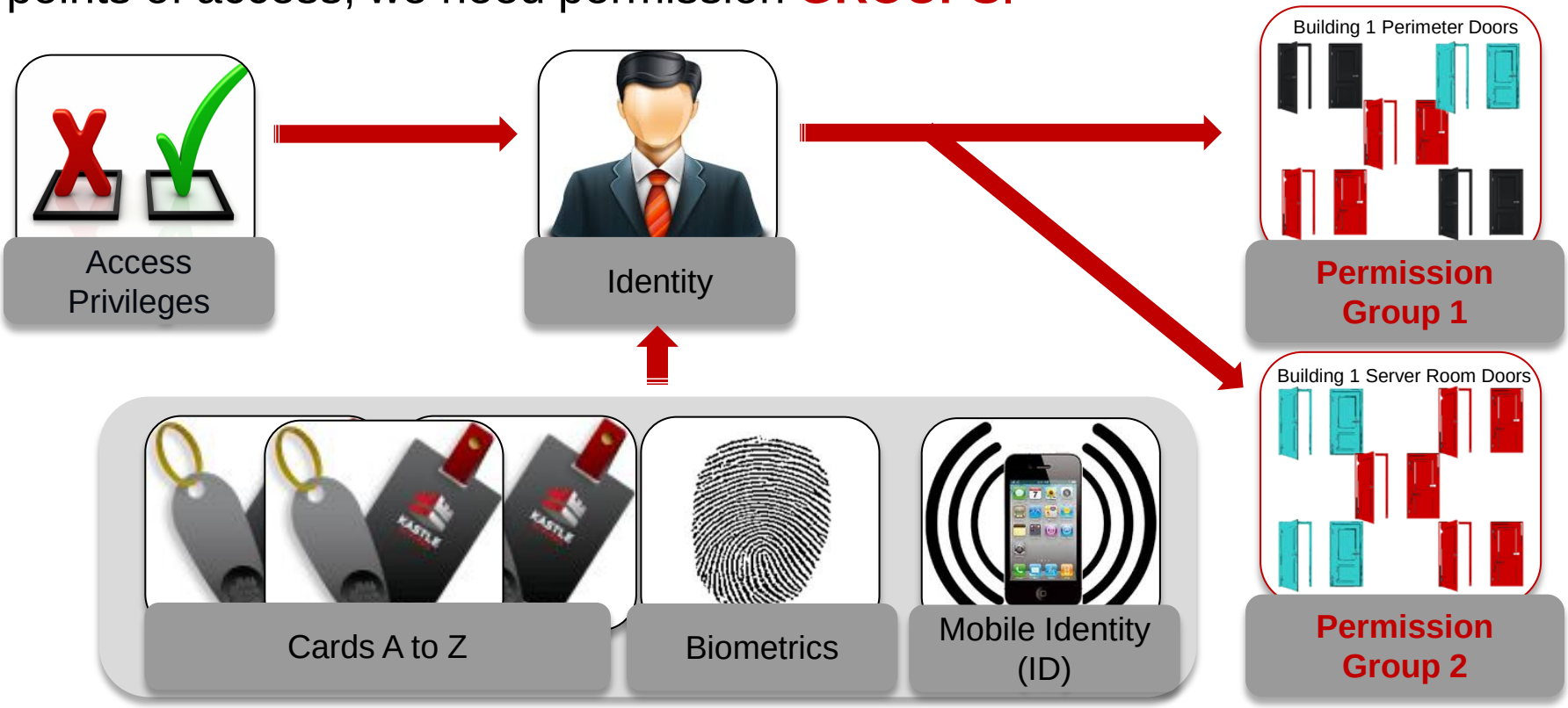
The Evolution of Physical Access: Any-Credential Access

In this next case, **ANY CARDS, BIOMETRICS AND MOBILE ID** associated with *(what is now)* an identity get all of the access privileges that they have.



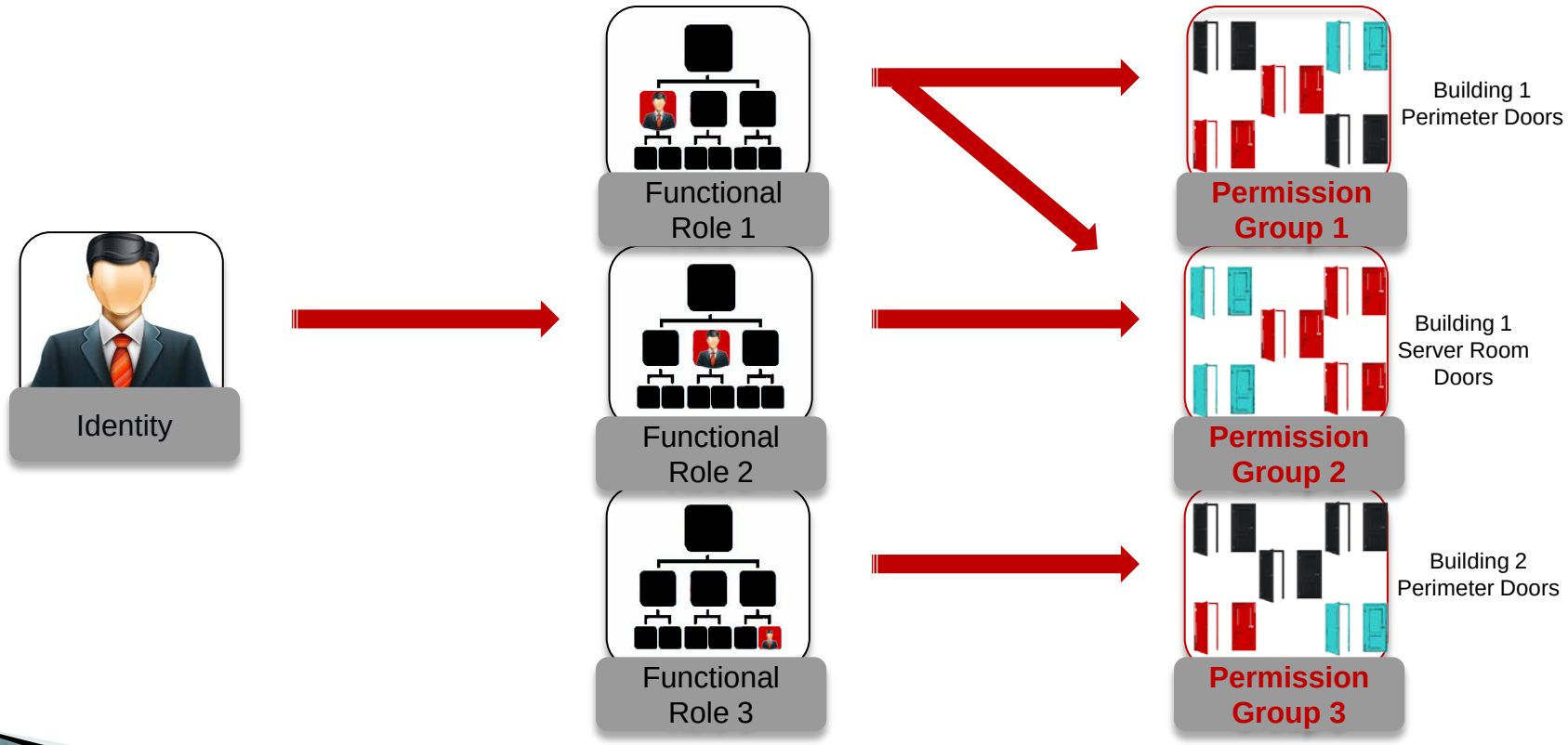
Permission Groups for Easier Assignments

The previous model works for small offices. But for enterprises with many points of access, we need permission **GROUPS**.

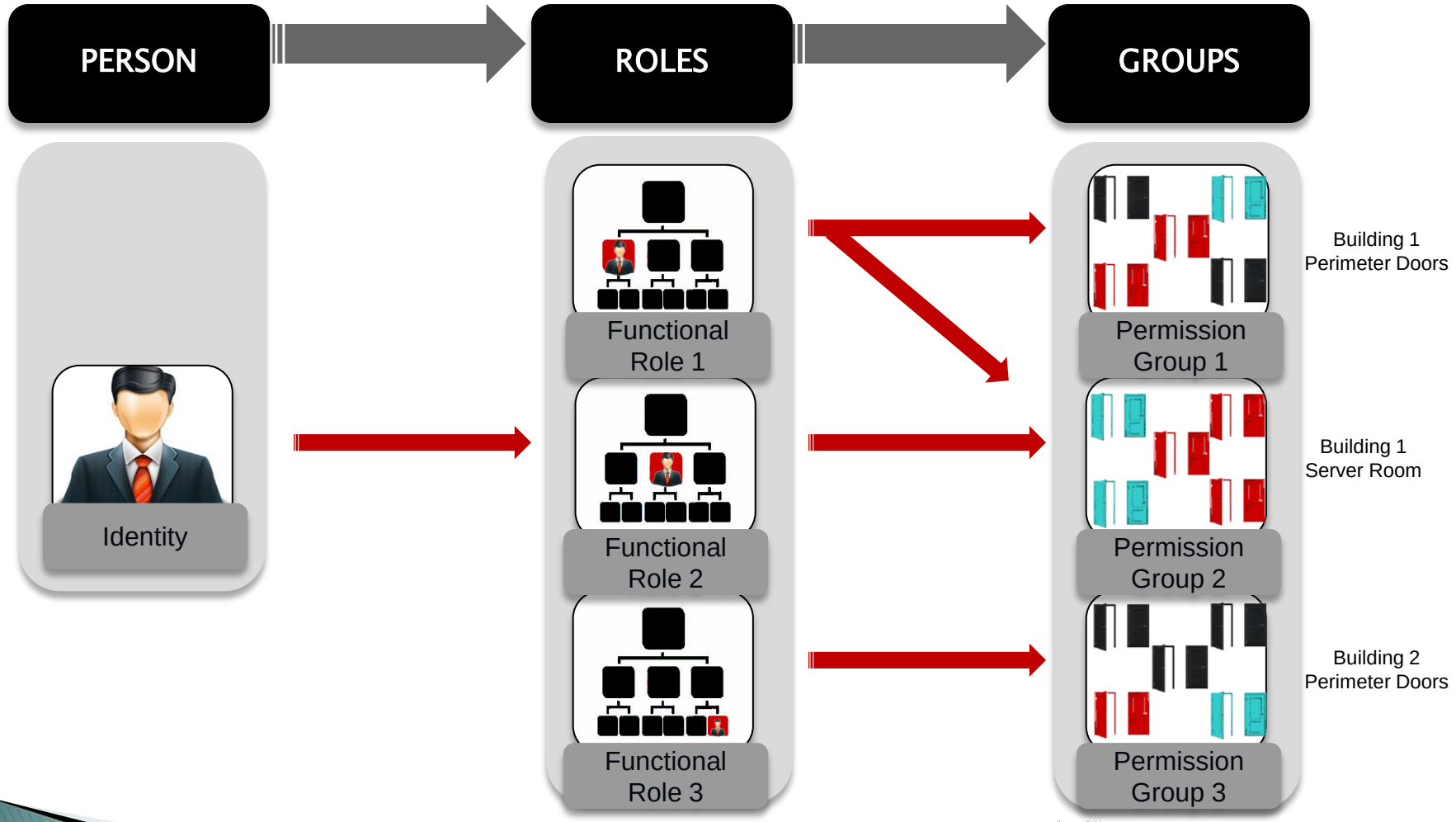


Management Through Functional Roles

For multi-location enterprises with a sizeable number of employees, we need to group personnel into functional **ROLES** and have permission groups associated with those roles.

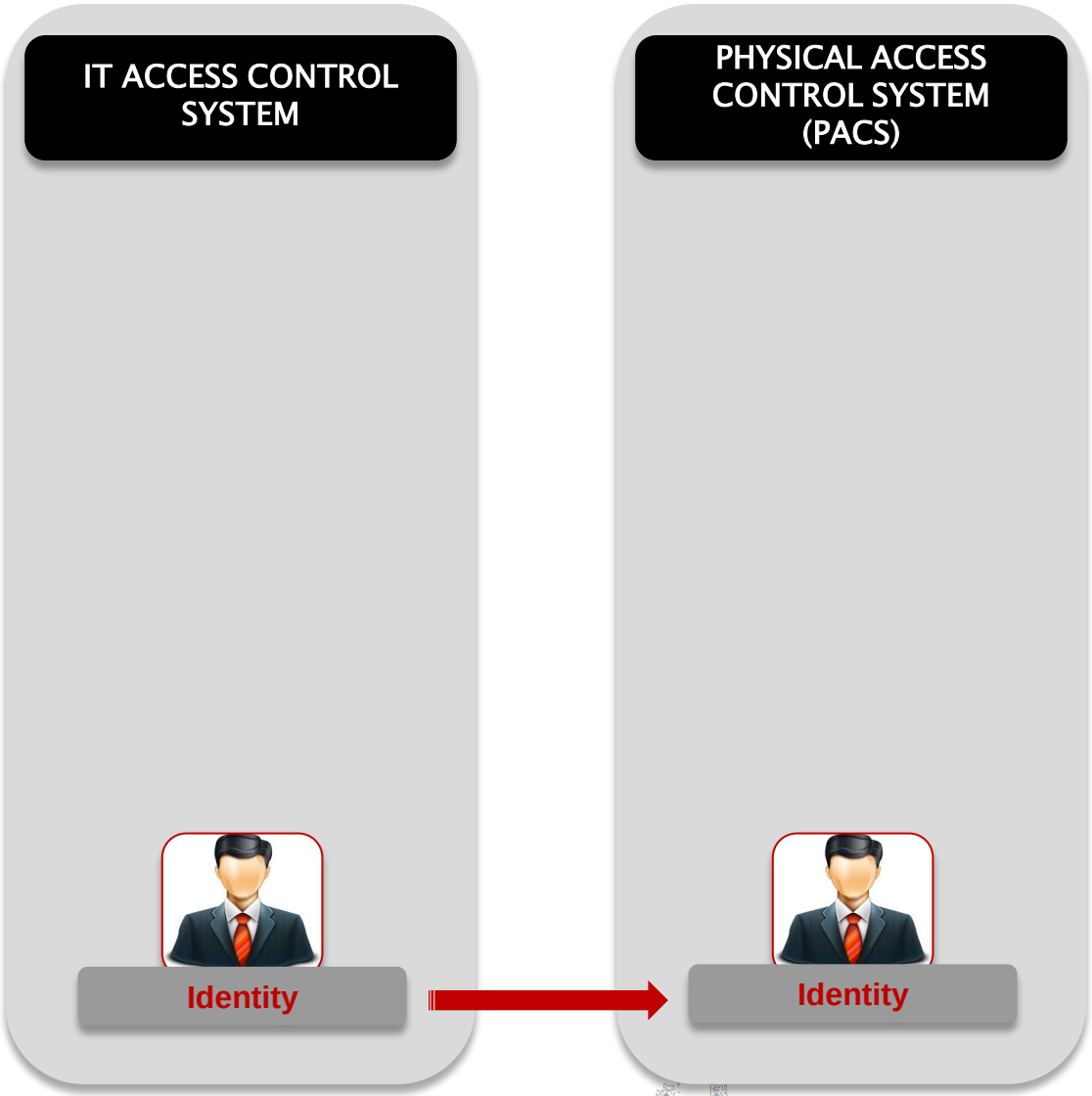


Person, Roles & Groups



PLAI Will Define Specifications for Four Levels of Integration: First-Level Integration

This is suitable for almost all organizations that have an IT staff and is based on Lightweight Directory Access Protocol (LDAP).



First-Level Integration: Single PACS

This is a single-step process:

1. Authoritative source for Identity (AS for short, typically IT) assigns the identity and passes it to a single PACS through PLAI agent.

First-Level Integration: Multiple PACSs

This is a multi-step process:

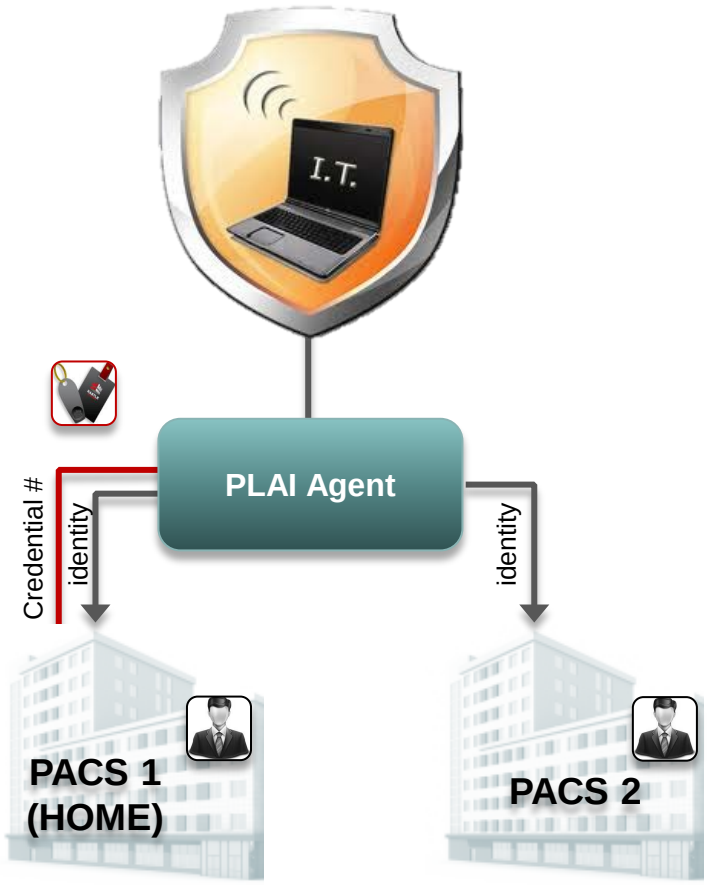
1. AS assigns the identity and passes it to both PACSs through PLAI agent.

First-Level Integration: Multiple PACSs

This is a multi-step process:

1. IT assigns the identity and passes it to both PACSs through PLAI agent.

2. PACS 1, which is the Home PACS for the credential holder, assigns a credential number to that identity and sends that information to PLAI Agent



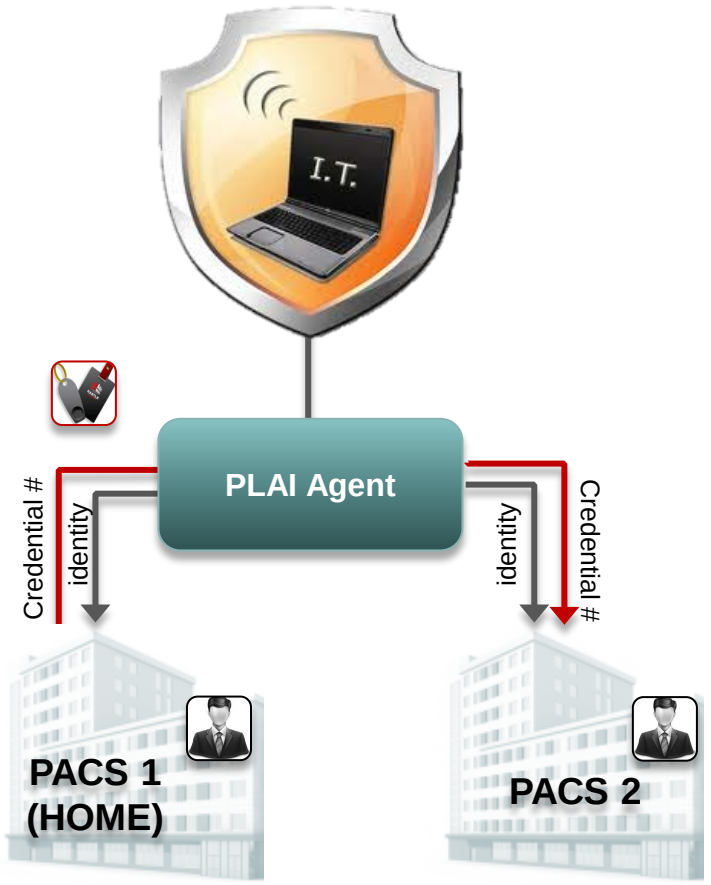
First-Level Integration: Multiple PACSs

This is a multi-step process:

1. IT assigns the identity and passes it to both PACSs through the PLAI agent.

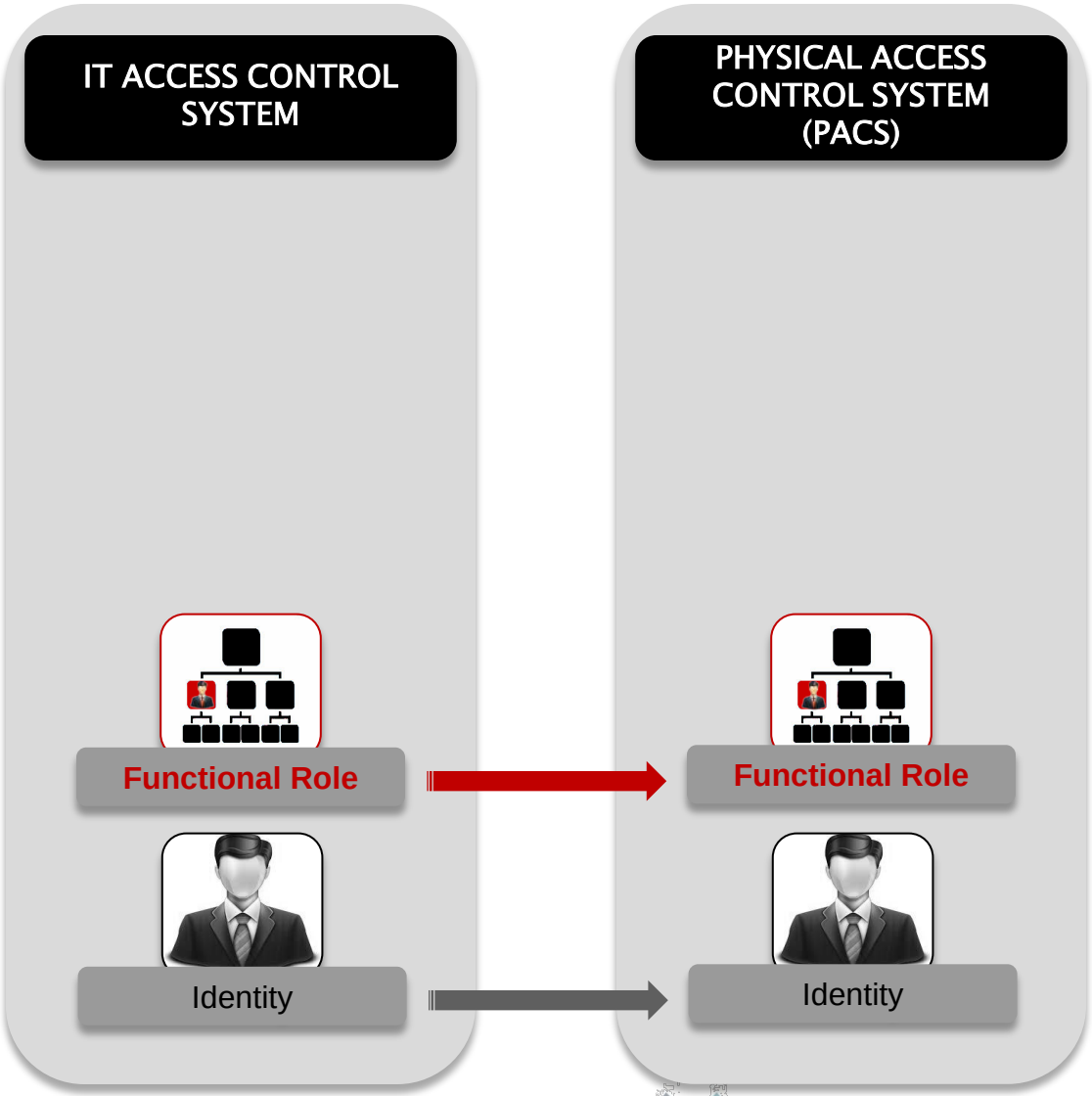
2. PACS 1, which is the Home PACS for the credential holder, assigns a credential number to that identity and sends to PLAI Agent.

3. The credential number is then pushed to PACS 2 through the PLAI Agent.



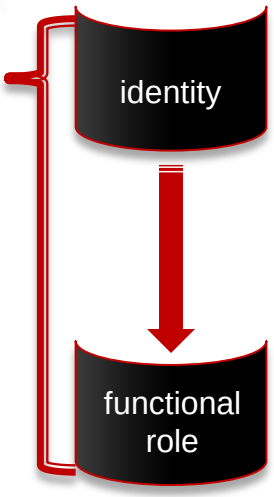
Second-Level Integration

This is used by enterprises that have embraced a role-based access control model for IT infrastructure.



Second-Level Integration: Single PACS

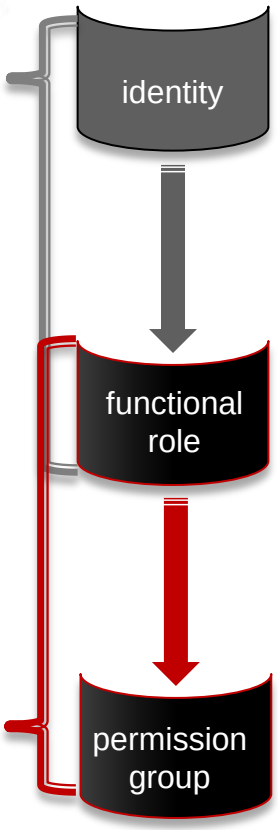
1. IT manages identity to functional-role mapping.



Second-Level Integration: Single PACS

1. IT manages identity to functional-role mapping.

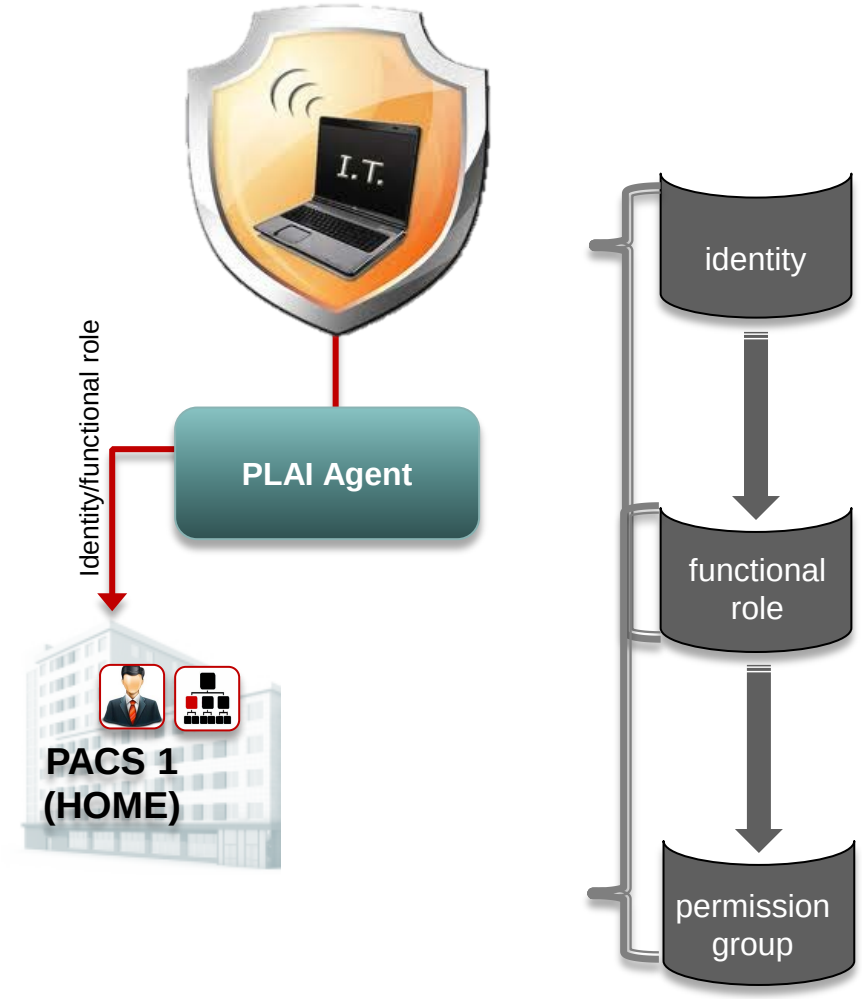
2. PACS 1 manages functional-role to permission-group mapping.



PSIA

Second-Level Integration: Single PACS

1. IT manages identity to functional-role mapping.
2. PACS 1 manages functional-role to permission-group mapping.
3. IT pushes the identity and functional role to PACS 1 through PLAI agent.



Second-Level Integration: Multiple PACSs

1. IT pushes the identity and functional role to PACS 1 and PACS 2 through PLAI agent.

Second-Level Integration: Multiple PACSs

1. IT pushes the identity and functional role to PACS 1 through PLAI agent.

2. PACS 1 provides the credential number to PACS 2 through PLAI agent.

Second-Level Integration: RESULT

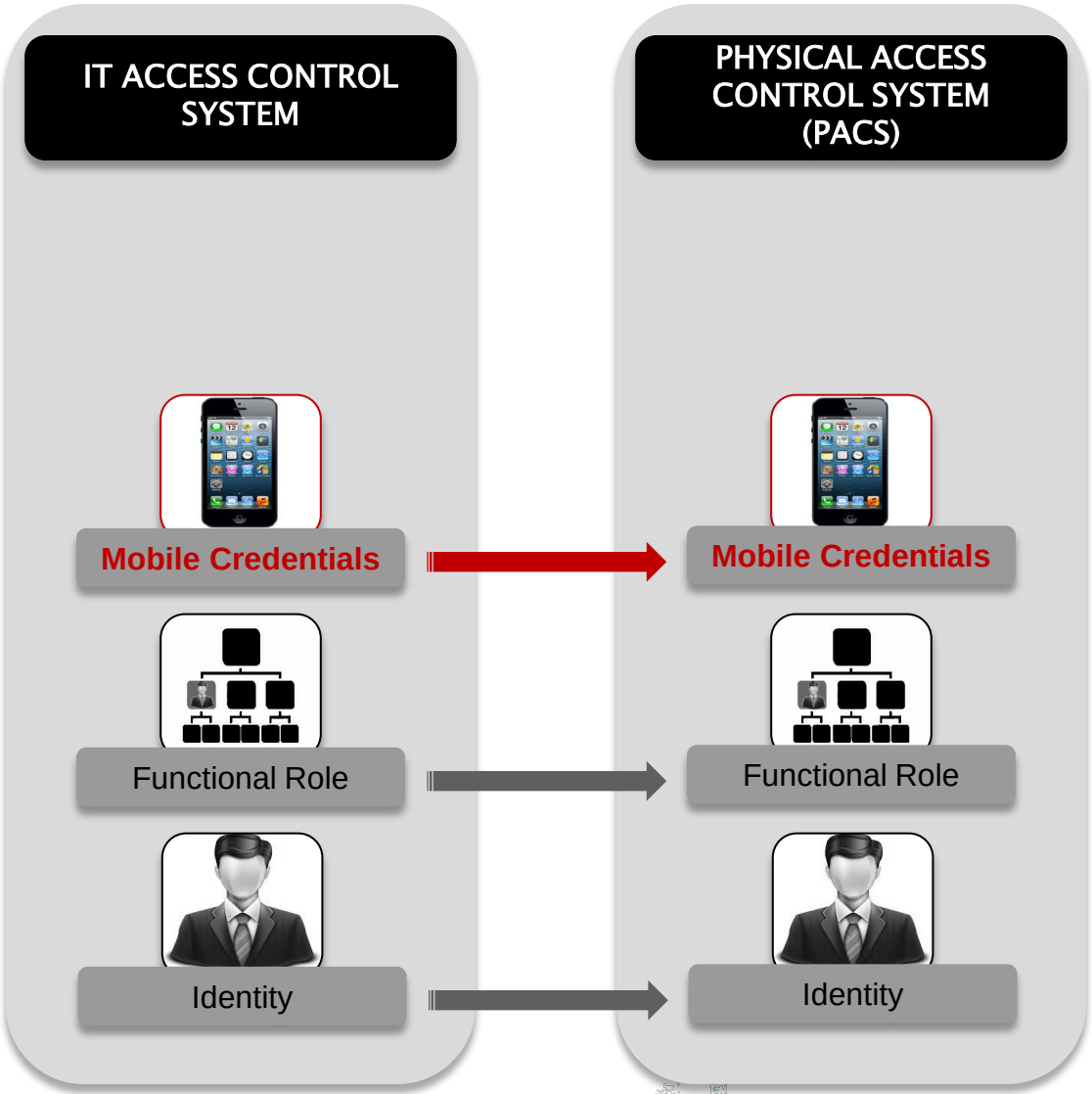
The result is the automatic provisioning and de-provisioning of physical access across multiple PACSs.

Note: The simplest case of role definition is defining a role for the visitor where pre-defined access is granted.

PSIA

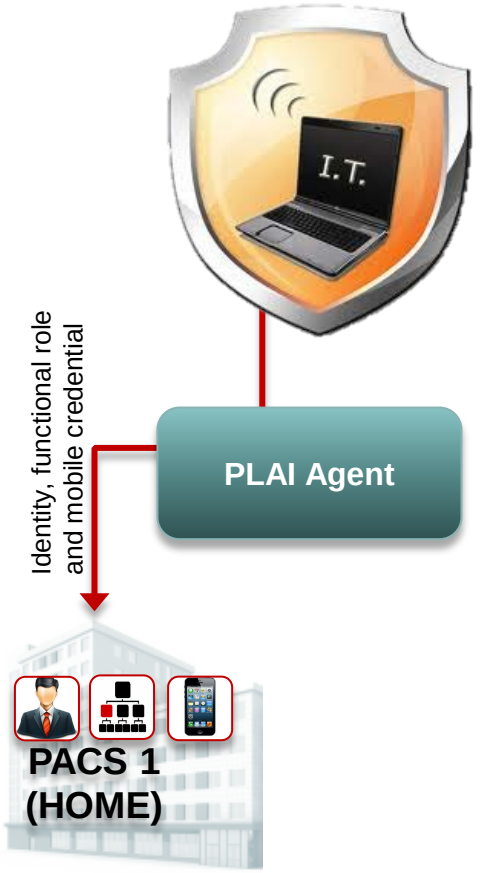
Third-Level Integration

- Mobile credentials are quickly capturing the interest of the general public.
- A variety of new locks are readily-available:
  - Bluetooth 2.0
  - Bluetooth 4.0
  - NFC
- Central management of these credentials is essential for any enterprise deployment.



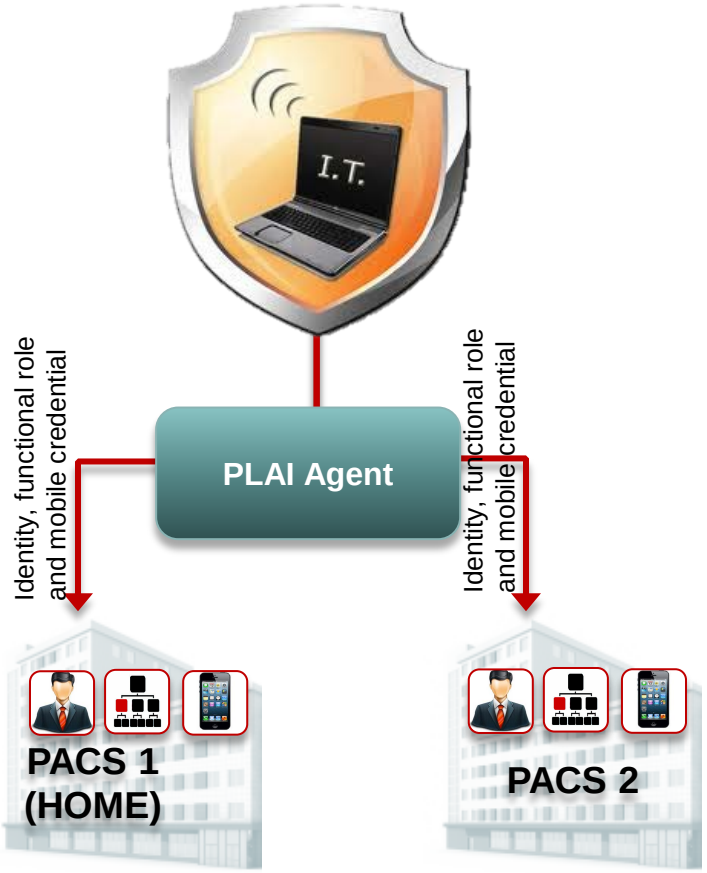
Third-Level Integration: Single PACS

- IT pushes the identity, functional role and mobile credential to PACS 1 through PLAI agent.



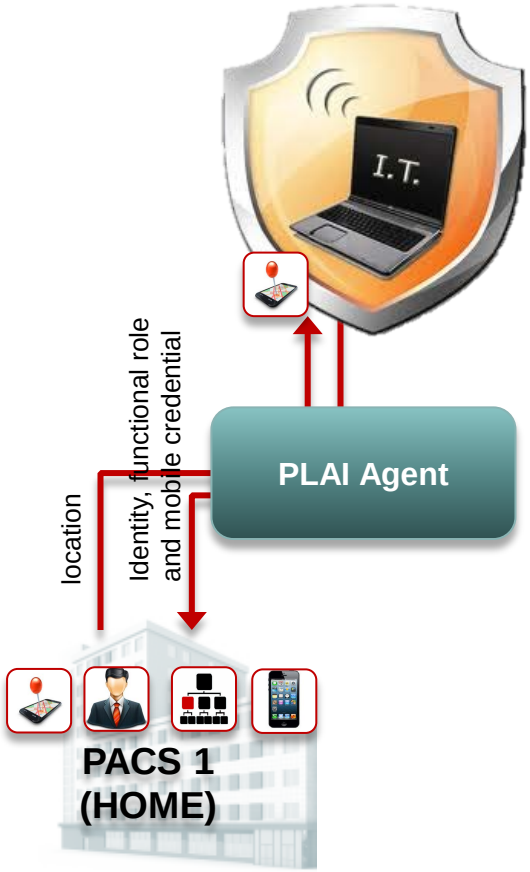
Third-Level Integration: Multiple PACSs

- IT pushes the identity, functional role and mobile credential to both PACSs through PLAI agent.



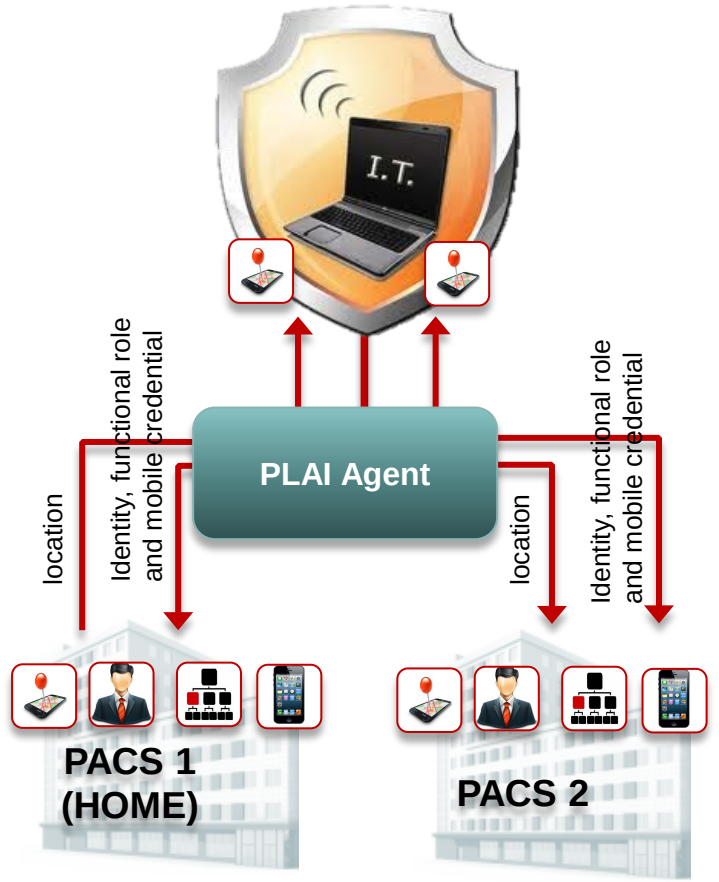
Fourth-Level Integration: Single PACS

IT pushes the identity, functional role and mobile credential to PACS 1, as PACS 1 provides the dynamic attribute *(location, in this case)* back to IT through PLAI agent.



Fourth-Level Integration: Multiple PACSs

IT pushes the identity and functional role to both PACSs, as both PACSs provide the dynamic attribute *(location, in this case)* back to IT through PLAI agent.



The industry needs the harmonized management of physical and logical integration, for better security and a more efficient workflow.

It is ESSENTIAL to have a set of detailed, well-defined and well-tested specifications in order to have plug-and-play COMPATIBILITY among different vendors.

LDAP-based interfaces will ease the adoption with IT.

For more information contact:
PSIA

info@psialliance.org