

UNDERSTANDING BASIC PHYSICAL ACCESS CONTROL



ISSA NATIONAL CAPITAL CHAPTER OCTOBER MEETING

Disclosure of Proprietary Data Notice

SigNet Technologies, Inc. (herein "SigNet") material, which follows, contains information and data which are privileged, confidential, and/or proprietary. This information and data is commercially sensitive and/or financial in nature, is not made available for public review, and is provided to the Potential Customer (herein called "Customer") on a confidential basis for business purposes as it relates to potential services to be performed by SigNet to support business opportunities. The information contained herein is protected, among these things, by the Trade Secrets Act, as codified, and is subject to the disclosure restrictions of 18 U.S.C. Sec. 1905 and international agreements, and any improper use, distribution, or reproduction is specifically prohibited. No license or right of any kind whatsoever is granted to any third party to use the information contained herein unless a written agreement exists between SigNet and the third party who desires access to the information. The information contained herein is provided for purposes of review and collaborative dialogue. No other use of the information and data contained herein is permitted without the express written permission of SigNet. Under no condition should information contained herein be provided in any manner whatsoever to any third party without written permission of SigNet."

Definition of Access Control

Access Control is defined as the protection of Company/Agency resources.

There is no delineation between Logical and Physical Access Control in the definition.

So to take that definition one step further:

Access Control is to protect the Logical and Physical Assets of a Company/Agency.

History of Access Control



Are you Friend or Foe???



History Continued:

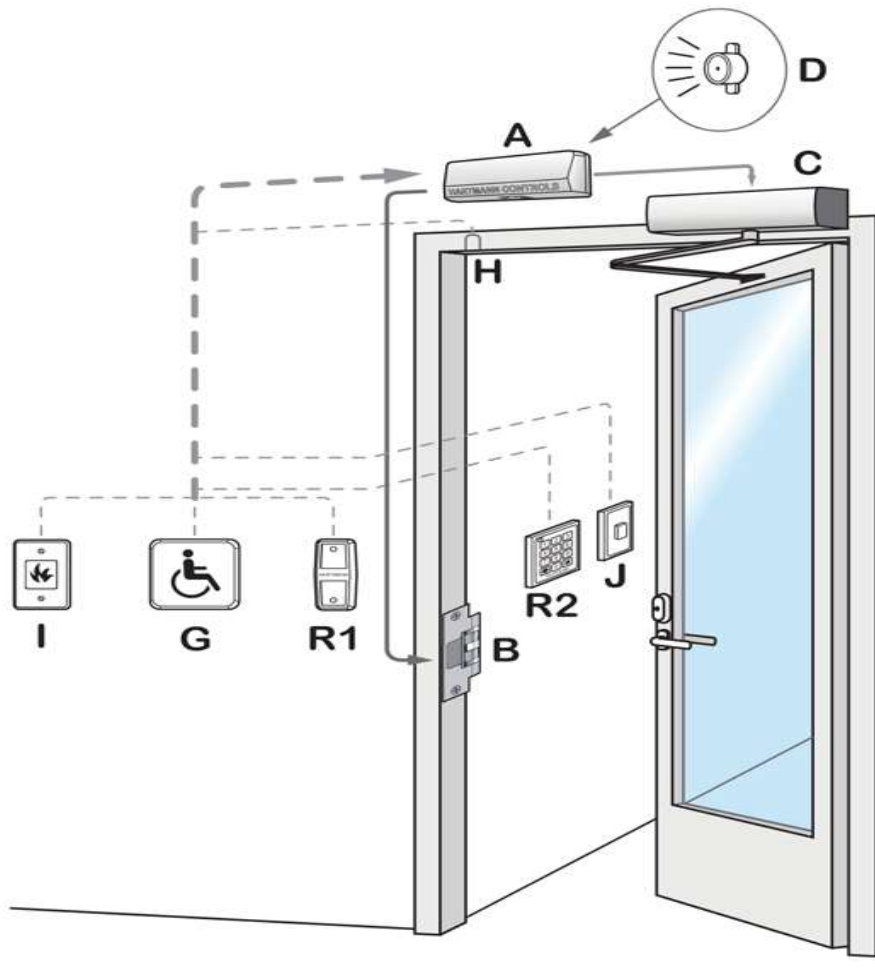
Cardkey was the first electronic PACS.

If you had a card and where given privilege's then the door would unlock and you would gain entry.

- No CRT*
- All alerts/events were printed on a dot matrix printer*
- All changes were verified through a dot matrix printer*
- Reports were very limited*

This was a Card centric PACS – Obsoleted due to the fact that the Weigand format card is easily cloned.

Basic Door Configuration



Controller

A	POE-ODM
----------	---------

Outputs

B	Electric Strike
C	Auto Door Opener
D	Extra Loud Buzzer*

Inputs

G	Handicap Open
H	Door Contact
I	Emergency Alarm
J	Doorbell
R1	Inside Reader
R2	Outside Reader

*Optional Internal Extra Loud Buzzer

History Continued:

Today's PACS is now an information gathering tool that is **“Identity Centric”**

With a Card Centric PACS we are validating the Identity of the individual that is caring the credential.

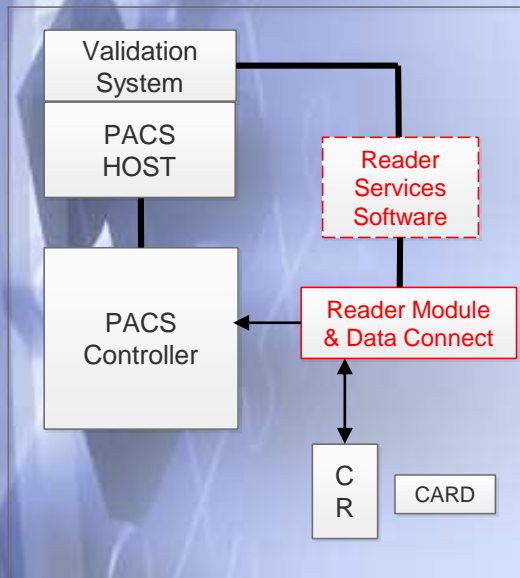
Certificates are placed on the credential to Authenticate that it is a valid credential and then a PIN and BIO-Metrics are used to further identify the individual.

Now we are more interested in the person than the card so our definition of Access Control has changed.

“Access Control is the protection of Company/Agency resources from unauthorized use.”

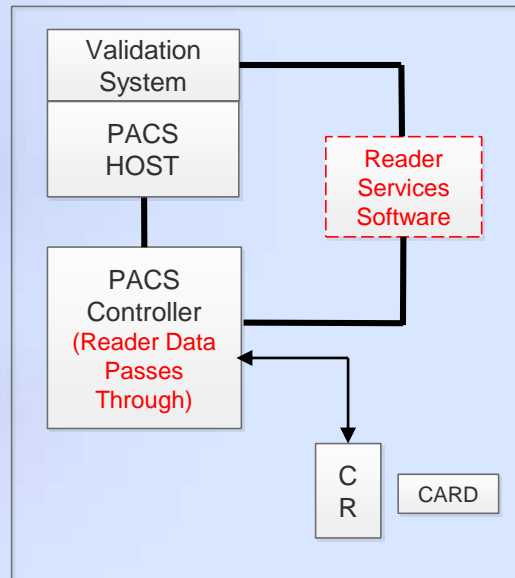
PACS Authentication Solutions

SigNet Type 1



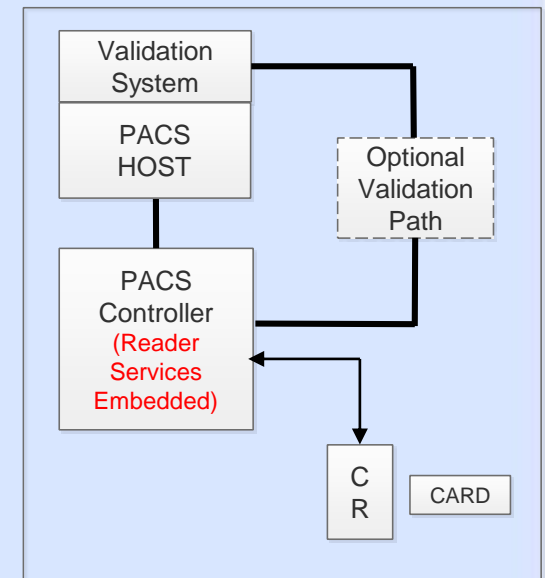
OUTBOARD
AUTHENTICATION
WIEGAND TO PACS

SigNet Type 2



PASS-THROUGH
AUTHENTICATION
RESULTS TO PACS

SigNet Type 3

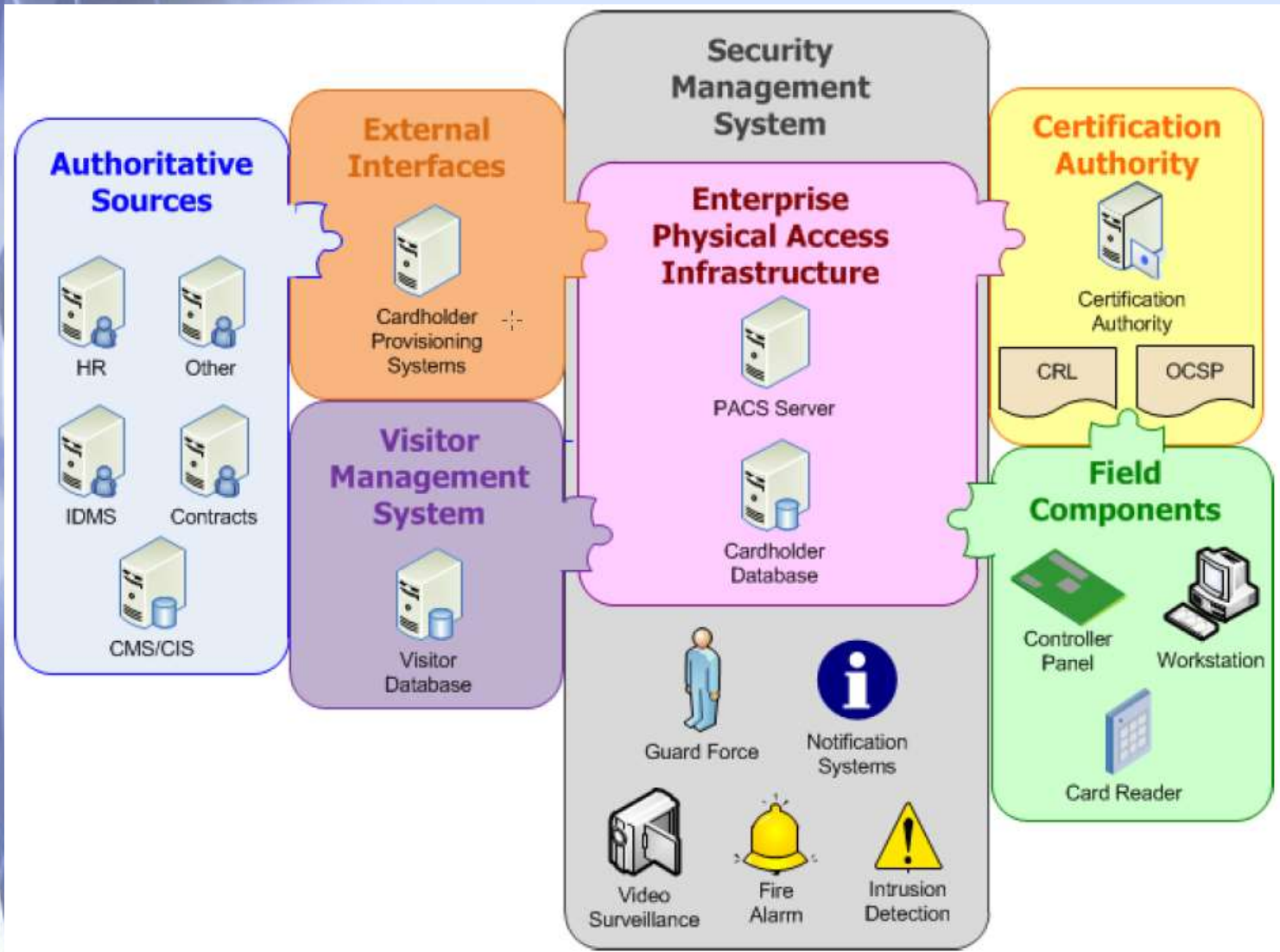


EMBEDDED
AUTHENTICATION
INTERNAL TO PACS

← One Way Communications (Wiegand)

↔ Two Way Communications (RS-485)

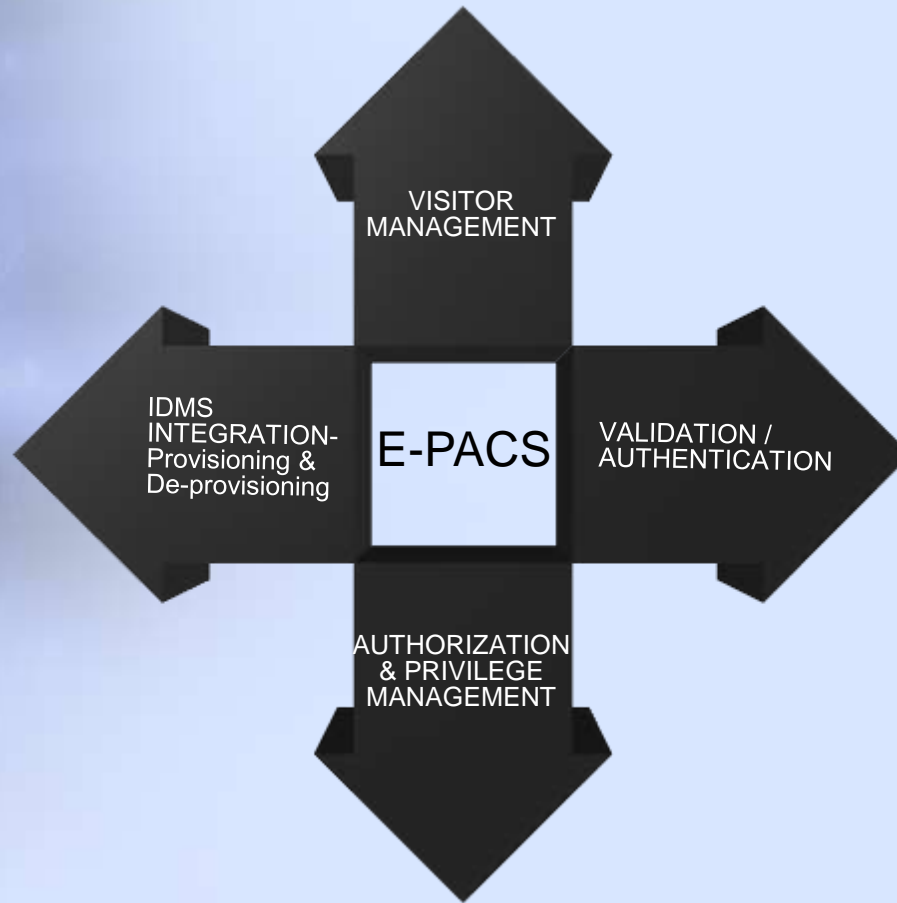
E-PACS with FICAM Layer



INTEGRATION WITH AGENCY'S ICAM PLATFORM

- ❑ External Interfaces for PACS – Safety, Security, Command & Control
 - PSIM – Physical Security Information Management
 - PIAM – Physical Identity & Access Management
 - PDR - PACS Data Repositories (for multiple PACS, PACS IDMS)
 - VSS – Video Surveillance Systems
 - VMS – Visitor Management Systems
 - Duress and Emergency Alert Systems
 - Mass Notification Systems

E-PACS / ICAM INTEGRATION



Federal ICAM Program



*IDManagement.gov