Next Generation Physical Access Control Systems
– A Smart Card Alliance Educational Institute Workshop

Standards and Interoperability

Adam Shane
Product Manager, AMAG Technology
Standards and Interoperability

This session covers the standards that are guiding next generation Physical Access Control System designs, the new requirements they place on PACS and the impact that they will have on interoperability.

- Standards
- Requirements
- Interoperability
PACS Legacy System
Standards Drive Down Costs

Why the race to standards-based solutions?

- Systems based on standards have lower total cost of ownership

- Challenges:
  - Wide variety of standards exist
  - Standards are not stable
  - New standards being released
  - Pseudo standards
Total Cost of Ownership

TCO is a buzz word and not a science

- Installation costs
- Lifecycle costs
  - Maintenance
  - Repair
  - Licensing/support
- Salvage and Replacement
PACS Installation

Consider many scenarios

- Replacing legacy solutions – migration is critical
- Re-use of cabling, readers, cards – or NOT
- PACS Integration to other services
  - IDMS (Sal D’Agostino)
  - LACS (Roger Roehr)
  - Cryptographic Services (Nathan Cummings)

- Infrastructure
  - Switch ports
  - PoE
  - Routers/Firewalls
PACS Maintenance Costs

Lifecycle costs can outweigh installation costs

- Software Support – traditional
- Software as a Service (SaaS) – new, for PACS
- Maintenance – batteries, testing, cleaning
- Updates to SW / HW
PACS Salvage Value

At the system’s end of life what can be re-used or re-purposed?

- Traditional thinking held PACS useful life at 10-15 years
- IT systems perform technology refresh in 3-5 years
- Example
  - FIPS 201 released in 2005
  - NIST SP800-116 released in 2009

What’s Next???
The Challenge of Standards

A wide variety of standards exist in the market – sometimes competing

- IEEE – Ethernet, PoE, TCP/IP, WiFi
- SIA – OSIPS
- NIST – FIPS 201 (Mike Kelley) and many others
- PSIA
- SEIWG
- Unpublished (restricted) standards
- Other regulations - ROHS
Standards Evolve

As we learn more about unexpected consequences of our actions, standards evolve to limit misuse

- FIPS 201 will be revisited, again, next year
- NIST SP800-73 is in revision 3
- This affects all standards
Manufacturers have a long development cycle

- Standard is released in final form
- End user demand builds
- Manufacturer becomes expert on facets of the standard
- Development time
- Testing – where are those test cards?
- Release
Caveat Emptor

Buyer Beware! Which standard does the product support?

- Don’t try to drive a PTZ camera with IEEE 802.11af (PoE). You’ll need 802.11at (PoE Plus).

- How long does it take for the Approved Products List to refreshed?
Requirements

Standards and expectations impose requirements on the PACS

- Support various identifiers on the credential
- Provide a mechanism for migration
- Integrate with other systems/services
- Consideration for future needs
Hello World

PACS have been on segregated networks

- Isolate network traffic
- Prevent hacking
- No support from IT department

Paradigm shift

- IT support, IT provided infrastructure/equipment
- Network bridged to internal and external services

Property of the Smart Card Alliance © 2009
“...it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).”
FIPS 201 is designed to foster interoperability at the card level

- Readers must support correct standards
- Readers must support card edge commands
- Approved Product List
- Larger data structures (FASC-N compared to Prox card)
SP800-116 Goes Further

SP800-116 illuminates the false assumptions of the past

- Authentication of data cannot be considered a factor unless we trust the source providing the authentication.
- Something you have
- Something you know
- Something you are
Interoperability

- At the card – cards from all agencies can be read at readers at all agencies
- At the panel – PACS hardware all operates the same and can be mixed and matched across systems
- At the software – PACS server software can relay information from one system to another
Putting the Pieces Together

- Standards are a moving target
- High expectations on manufacturers to provide solutions that are flexible
- Expansion of the definition of authentication

- How do we get there?
Integration

While the ability to support integration puts specific requirements on the product, it allows the system to off-load all of the specialized tasks.

Allow various systems to specialize in their own functions, yet share data in sufficient detail as to make the operation transparent to the user.
PACS Legacy System
Example Integrated System
Integration Challenges

Integration is not without its own set of challenges

➢ Change management
  ▪ If upgrading one component, verify overall solution is still compatible

➢ One-off solutions vs. COTS
  ▪ One-off solutions are not easily (or inexpensively) upgraded to add new features
In conclusion, **standards** provide a framework to allow various systems to share data.

Specific implementations of standards are dictated by project **requirements** which further define the interface.

The goal of **interoperability** must be taken in context of the true objectives of the solution. For PIV this would be a single card for all types of authentication (logical and physical) to provide government wide consistency of identity verification.

**Integration** is the mechanism by which the pieces fit together.
Speaker Contact Information

Adam Shane
AMAG Technology
adam.shane@amag.com · Phone: (800) 874–1091
www.amag.com