



Tuesday, May 13

Track D
Security & Access Control

Session: Access Technologies & Standards

Time: 1:30 PM – 3:00 PM

Room: W204 D

Moderator:

Gerald Hubbard

Business Development

Datacard Group

Speakers:

Mark Diodati

Analyst--Identity & Privacy Strategies

Burton Group

Christer Wilkinson

Sr. Project Manager

DMJM H&N

Lars Suneborn

Government Program Director

Hirsch Electronics (FIPS 201)

Gary Klinefelter

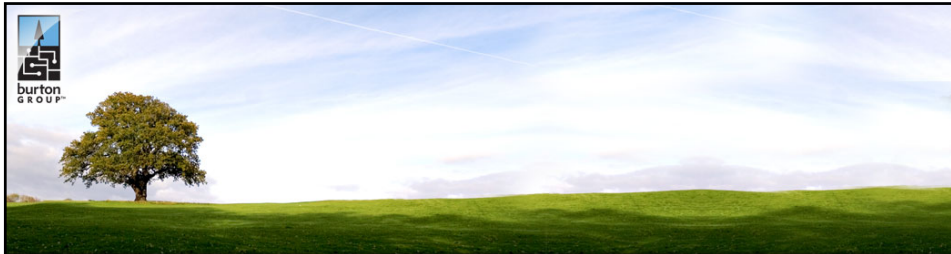

VP Strategic Innovation

HID Global

Walter Hamilton

Chairman

International Biometric Industry Association





Analyst Report: Trends and Obstacles for Security Convergence within the Enterprise

Mark Diodati
Senior Analyst

mdiodati@burtongroup.com
www.burtongroup.com

Tuesday – May 13, 2008

All Contents © 2008 Burton Group. All rights reserved.



Identity and PACS 2

Agenda

- Convergence: What's in a Name?
- PAX Vobiscum: Anatomy of the PACS
- Integration Points and Benefits
- Homeland Security Presidential Directive (HSPD) 12
- Proximity Card Hacking
- Market Trends
- Recommendations
- Q&A



Identity and PACS

3

Agenda

- *Convergence: What's in a Name?*
- PAX Vobiscum: Anatomy of the PACS
- Integration Points and Benefits
- Homeland Security Presidential Directive (HSPD) 12
- Proximity Card Hacking
- Market Trends
- Recommendations
- Q&A



What's in a Name?

4

Physical and logical convergence

- Integration of authentication, authorization, and security event correlation across physical access control systems (PACS) and "traditional" IT applications
- PACS have authorization and management capabilities, so "logical" as a differentiator is insufficient
- While other language may be more accurate, "Physical and logical convergence" has momentum, so we are stuck with it



Identity and PACS

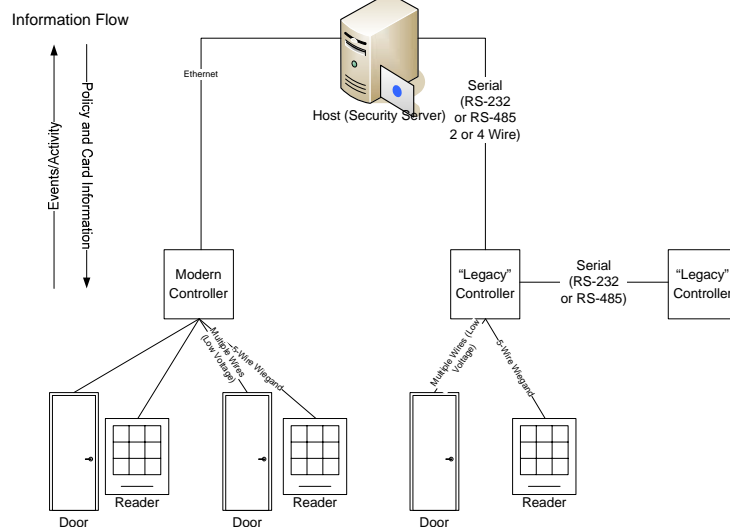
Agenda

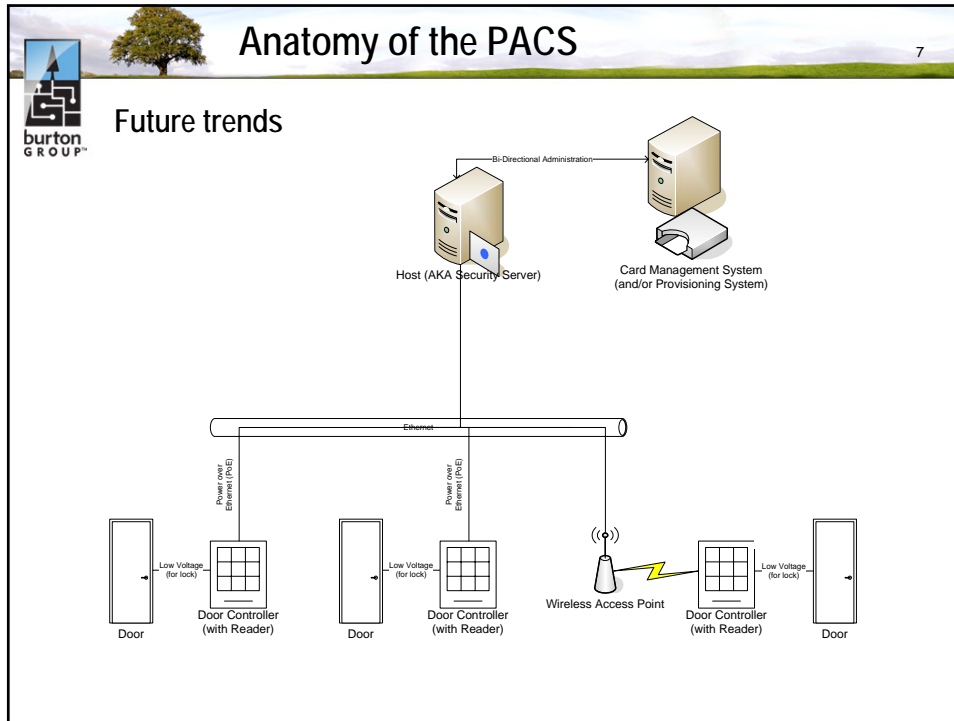
- Convergence: What's in a Name?
- **PAX Vobiscum: Anatomy of the PACS**
- Integration Points and Benefits
- Homeland Security Presidential Directive (HSPD) 12
- Proximity Card Hacking
- Market Trends
- Recommendations
- Q&A





Anatomy of the PACS

"Typical" PACS





- Anatomy of the PACS** 8
- Challenges**
- There are many vendors and technologies
 - AMAG Technology, GE Security, HID Global, Hirsch Electronics, Honeywell, Johnson Controls, Lenel, Siemens, and Tyco International (Software House)
 - Most organizations have multiple, heterogeneous PACS systems
 - Separate administration consoles and islands of identity
 - Mix of different components (hosts, cards, readers, controllers)
 - The organization may not own the PACS due to tenancy

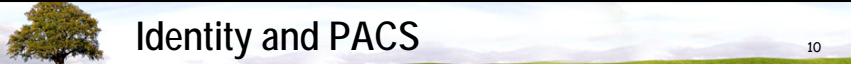



Anatomy of the PACS

9

Challenges

- The proprietary, embedded wiring schemes makes wholesale upgrade to more modern technologies extremely difficult
 - In particular, presents a challenge to HSPD-12 deployments
 - Use of the PIV card's advanced authentication features requires upgrading (at a minimum readers and controllers)



Identity and PACS

10

Agenda

- Convergence: What's in a Name?
- PAX Vobiscum: Anatomy of the PACS
- **Integration Points and Benefits**
- Homeland Security Presidential Directive (HSPD) 12
- Proximity Card Hacking
- Market Trends
- Recommendations
- Q&A



Integration Points and Benefits

Converged card

- The use of a single card for access to both physical and logical applications
 - “Swiss army knife”
- Contact interface for logical applications
- Contactless interface for PACS
 - Most common cards are HID Prox and MIFARE Classic
- Achievable using productized technology
- Benefits
 - Enhanced security (visual identification, PACS and logical authentication)
 - Ease of use
 - Potential reduction in the number of devices and sign-ons



Integration Points and Benefits

Converged card

Name	Description	Image
hybrid card	Smart card and proximity (prox) card “bolted together” “Separate silicon” (processing and storage) Most common P/L access card deployed	
dual interface card	Two interfaces, common processing and storage Greater functionality for physical access (read/write, security, features) Usually ISO 14443A/B contactless specification “Card of the future”	
tri-interface card	At least three interfaces (typically one contact, two contactless) to enable compatibility with multiple PACS technologies (HID Prox, PIV, MIFARE)	

card images source: <http://www.idwholesaler.com>



Integration Points and Benefits

13

Common identity management

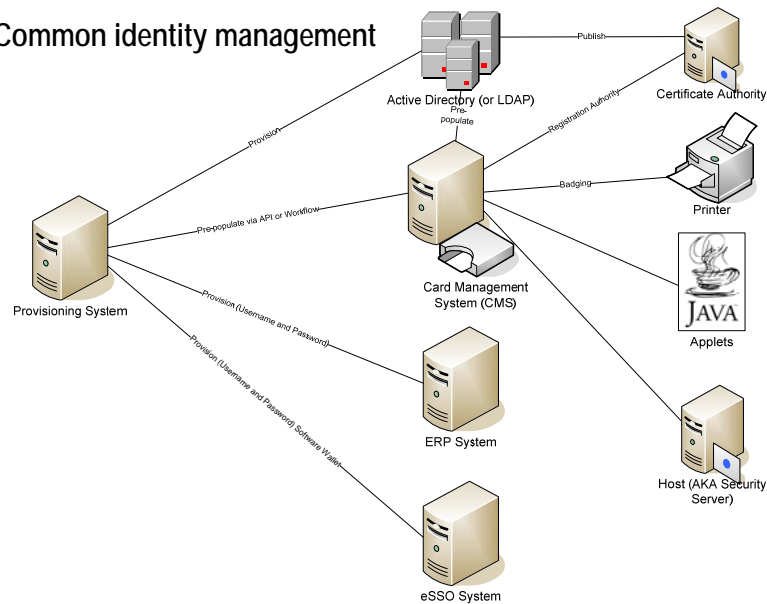
- Manage user credentials and access rights across physical and logical resources from a single administrative console
 - Or reduced number of consoles
- Requires significant customization effort
- Benefits
 - Better lifecycle management
 - Quicker on-boarding and termination
 - Better authorization (access) policies
 - Macro level view into access rights
- New trend: using the PACS to drive logical identity changes



Integration Points and Benefits

14

Common identity management





Integration Points and Benefits

15

Security event correlation

- The view of user activity across physical and logical systems
- Readily achievable via security information and event management (SIEM) products
 - May require mapping of user identities and aggregation of physical locations
- Benefits
 - 360 ° view of user activity for auditing and (perhaps more importantly) quicker forensic investigations



Integration Points and Benefits

16

Contextual authorization

- Making access decisions based upon the user's current physical or logical status
- Benefits
 - Enhanced security
- Examples
 - Imprivata OneSign
 - Only known productized capability for contextual authorization
 - Exchange/PACS integration
 - Only those people invited to the meeting can access the conference room
 - Requires significant integration work between Exchange and PACS



Identity and PACS

17

Agenda

- Convergence: What's in a Name?
- PAX Vobiscum: Anatomy of the PACS
- Integration Points and Benefits
- **Homeland Security Presidential Directive (HSPD) 12**
- Proximity Card Hacking
- Market Trends
- Recommendations
- Q&A



HSPD-12

18

Smart card credential for every Federal employee and contractor

- Personal Identity Verification (PIV) card
- NIST did a credible job on standards (FIPS 201, SP 800-73)
 - ANSI 378 for biometric template
 - ISO 14443 for contactless interface

"Card of the Future"

- Dual interface/single chip enables advanced authentication options for PACS
 - Biometrics, X.509

Agencies were required to begin issuing cards by 10/27/06



HSPD-12

19

Most agencies are challenged and are behind schedule

- FIPS 201 approved products did not appear until the summer of 2006
- The FIPS 201 identity proofing and issuance process is daunting
 - But arguably commensurate with assurance levels to sensitive resources
- The PIV card is incompatible with most agencies' PACS systems
 - Some are adopting tri-interface cards or Wiegand-compatible readers
- Many agencies opted to integrate with provisioning systems
 - Some of these provisioning systems are new



Identity and PACS

20

Agenda

- Convergence: What's in a Name?
- PAX Vobiscum: Anatomy of the PACS
- Integration Points and Benefits
- Homeland Security Presidential Directive (HSPD) 12
- **Proximity Card Hacking**
- Market Trends
- Recommendations
- Q&A



Proximity Card Hacking

21

Hacking

- Skimming – surreptitious reading of a contactless card
 - Does not require possession, only proximity
- Cloning – creating a mirror image of the contactless card

Attacks

- HID Prox (125 kHz) attacked demonstrated at the 2007 RSA Conference
 - Card does not support encryption
- MIFARE Classic attack proved several weeks ago
 - Proprietary encryption algorithm broken
 - Attack is particularly damaging as these cards are used in payment systems (e.g., tollway and transportation)



Proximity Card Hacking

22

Impact to PIV deployments

- Most PIV deployments will use compatibility mechanisms with existing PACS systems
 - Effectively “dumbs down” the security of the PIV card
- The identity assurance provided by PIV cards used this way is diminished
 - Some agencies recognized this and are going to “native” FIPS 201 systems

Bottom line

- No authentication mechanism is bulletproof
 - Including lost or stolen cards
- Additional controls are required in addition to PACS
 - Security event correlation, video surveillance



Identity and PACS

23

Agenda

- Convergence: What's in a Name?
- PAX Vobiscum: Anatomy of the PACS
- Integration Points and Benefits
- Homeland Security Presidential Directive (HSPD) 12
- Proximity Card Hacking
- **Market Trends**
- Recommendations
- Q&A



Market Trends

24

Early adopters of integration include the following verticals

- Aerospace
 - Physical security concerns
- Pharmaceutical
 - Paperwork reduction provided by smart cards
- Oil and Gas
 - Compliance initiatives
- Financial
 - High physical security needs

Interest is expanding in these and other verticals, due to:

- Compliance/security goals
- Maturity of integration products



Market Trends

25

We're beginning to see vendors self-identify with "convergence"

- Imprivata
 - Integrates with PACS
 - Provides security event correlation and contextual authorization
- Quantum Secure
 - Provides a single provisioning console for multiple, heterogeneous PACS
 - Integrates with the major provisioning systems, also has an SPML interface
- Privaris
 - Provides single authenticators that can support multiple card technologies
 - Also has USB smart card and RSA SecurID OTP support



Market Trends

26

Additional vendors

- ArcSight
 - Security event correlation across PACS and traditional IT applications
- ActivIdentity
 - Leading CMS vendor for enterprise smart card deployments
 - Currently productizing PACS integration
 - Best integration with major IdM provisioning systems



Identity and PACS

27

Agenda

- Convergence: What's in a Name?
- PAX Vobiscum: Anatomy of the PACS
- Integration Points and Benefits
- Homeland Security Presidential Directive (HSPD) 12
- Proximity Card Hacking
- Market Trends
- **Recommendations**
- Q&A



Recommendations

28

Evaluate the costs and benefits

- Enhanced security first, ROI second

Win executive sponsorship

- Convergence is dead without it

Build consensus

- Across HR, IT Security, Facilities, Software Support
- Otherwise, ostensible technical challenges will kill the project

Be opportunistic

- Ride workstation refresh and PACS upgrades, even when it is not convenient from a project management perspective



Recommendations

29

Embrace Heterogeneity

- Multi-protocol cards and readers can smooth over differences and aid in migration

Don't skimp

- Thoroughly integrate CMS, provisioning, PACS, and AD
 - Otherwise, user and administrative burden will be too great
- Get budget approval upfront
 - Avoid "going back to the well"
 - Otherwise, you risk losing credibility and killing the project



Recommendations

30

Implement robust emergency access procedures

- Strike the balance between usability and security
- For most organizations, "go home and get it" will not be satisfactory
 - but don't make it too easy to forget the card

Sweeten the deal

- Deploy enterprise single sign-on (eSSO)
- Workstation software is required anyways, why not give the user's some added convenience?



Conclusion

31

The integration of identity and physical access control systems can provide usability benefits and increased security, but careful consideration is required

Deployment of a common card for physical and logical access is usually a multi-year process that requires cross functional collaboration

- However, other integration points exist which don't require deployment of a converged card

Proximity card hacking is one of several concerns associated with most cards

- Organizations should implement additional controls to improve identity assurance



Identity and PACS

32

Agenda

- Convergence: What's in a Name?
- PAX Vobiscum: Anatomy of the PACS
- Integration Points and Benefits
- Homeland Security Presidential Directive (HSPD) 12
- Proximity Card Hacking
- Market Trends
- Recommendations
- Q&A



RTCA Committee 207
Airport Security Access Control Systems

Christer J Wilkinson
Chairman RTCA 207



What is RTCA?

RTCA, Inc. is a private, not-for-profit corporation that develops consensus-based recommendations regarding communications, navigation, surveillance, and air traffic management (CNS/ATM) system issues.

www.rtca.org



How does it work?

RTCA functions as a Federal Advisory Committee.

Its recommendations are used by the Federal Aviation Administration (FAA) as the basis for policy, program, and regulatory decisions and by the private sector as the basis for development, investment and other business decisions.

Like every other Federal Advisory Committee the member participation is pro-bono and decisions are by consensus.

What is committee 207?

Special Committee (SC) 207 was established at the request of the Airport Consultants' Council. SC-207 is tasked to revise RTCA DO-230A - *Standards for Airport Security Access Control Systems* issued in April 2003.

What is standard DO230?

DO 230 was originally issued to give guidelines to airports following the announcement and subsequent regulation of new access control security measures in 1989.

What is the general scope of DO230?

DO 230 provides guidance on the implementation of airport staff access control systems and supporting systems at airports nationwide

What is **not** in the scope of DO230?

DO 230 does not address the issue of passenger screening
DO 230 does not address the issue of checked baggage screening
DO 230 does not address blast mitigation issues
DO 230 does not address radiological, bacterial or chemical threats

Also note:

RTCA standards are **not** regulatory requirements.

History of standard DO 230

DO 230	was issued in 1996
DO 230A	was issued in 2003
DO 230B	will be issued in June 2008

Each of DO 230 and DO 230A were used in over 100 airport access control system implementations, in addition to casual non recorded use.

How was it developed?

Like all RTCA standards it is developed by a series of formal public plenaries plus informal working groups on individual chapters.

This standard has 9 sections and took 19 plenary sessions. Over 175 people contributed, from the Public, Industry groups, FAA and TSA.

The final document is nearly 300 pages.

All work was performed pro bono

DO 230B approach:

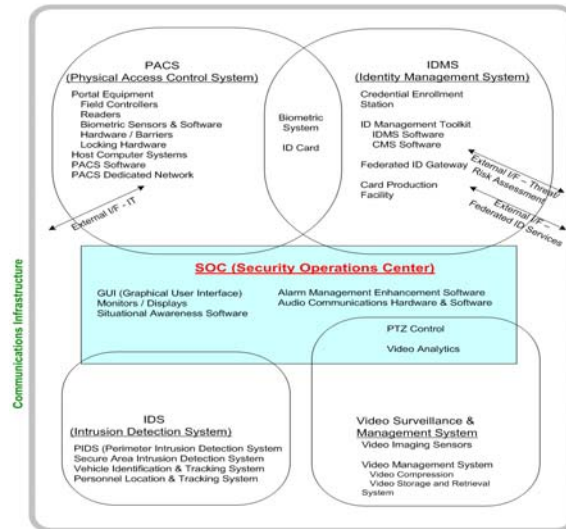
New title:

“Integrated Security System Standard For Airport Access Control”

- Provides guidance on systems for existing regulations
- Provides guidance for systems for anticipated regulations
- Provides guidance on system migration
- Provides guidance on industry best practices

DO 230B Content

1. Introduction
2. System level requirements
3. Identity management
4. Physical access control
5. Intrusion detection systems
6. Video management
7. Security operations centers
8. Communication infrastructure
9. Procurement guidance



Current Aviation Practices

- Airports issue their own Access Credentials
- Regulations require Security Threat Assessments and Criminal History Checks prior to issuing a credential.
- Currently these functions are normally provided by TSA and by the Transportation Security Clearing House both via communication gateways.
- State and municipal requirements are in addition and vary between states and airports.
- Distribution and nature of functions determined by both law and regulation and thus is not amenable to conventional operational variation

Scale of requirement:

- Around 400 regulated airports with access control systems
- Vary in size from airports with 5 doors to some with 1500 portals,
- Probably around 100,000 portals in total
- Probably around 1.5 staff with various types of credential

Current airport technology access media

- around 2% Use Smart card
- around 50% Use Proximity cards
- around 40% Use Magnetic stripe
- around 1% Use Operational biometrics.

TSA Policy with regard to Aviation

- Since 9/11 the long term policy was to move to smart cards and biometrics and interoperability.
- Numerous test programs (TWIC) and pilot studies (AACPP) undertaken
- Scale and difficulty of transformation underestimated
- Recognition of need to enhance the credential issuance process
- Recognition of need to move towards biometric based identity verification at both issuance and in use.
- Current initiative is "ACIS" (Aviation Credential Interoperability Solution) not TWIC.

The DO 230B Standard thus reflects:

- Anticipated identity management requirements based in industry best practices based on FIPS 201
- Best practices for Airport Physical access control systems and migration strategies to smart cards
- Eventual migration towards an interoperable solution

It also includes:

- SOC design and operation guidance
- Video system design and guidance
- Communication system design and guidance
- Intrusion detection design and guidance.



Availability

- DO 230B will be available in late June 2008.
- It will be available via www.rtca.org.



RTCA Committee 207 Airport Security Access Control Systems

Christer J Wilkinson
Chairman RTCA 207
christer.wilkinson@aecom.com

