PEOPLE, IDENTITIES AND CREDENTIALS: HOW TO CONNECT THE DOTS

Danny Smith
Executive Vice President, Owner
ColorID

David Stallsmith
Director of Product Management
ColorID
CONNECTING THE DOTS – TODAY’S CARD SYSTEM
WHAT WE’RE TALKING ABOUT TODAY

• We’re trying to figure out which card to go with
• How do we get this mobile thing going?
• Students have to wait for their cards to go live in the (fill in the blank) system
• The guru who wrote our (fill in the blank) system retired
• We have no good way to manage our contractors and guests
• We can only use solutions that are integrated with our one card system
• We can’t get the reports we need
• Our data is a mess and it’s all over the place
• We spend so much time doing things manually
• There are so many things we need our ID system to do that it just can’t do
• How did we get here?
HOW DID WE GET HERE?

The Deferred Maintenance of Identity Management
• All the technology on and in your card
• Each communicates with at least one system
  – Bar code – library, athletic center
  – Mag stripe – payments, door access, printers
  – Contactless smart chip – door access, payments
• Card data is identity data
COLORID
EVERYTHING ON CAMPUS

Access Control  Library  Print/Copy  Book Store

ID Card Issuance

One Card System  Dining, POS

WWW.COLORID.COM  © 2019 -- ColorID, LLC
EVERYTHING ON CAMPUS

One Card System

- Access Control
- Library
- Print/Copy
- Book Store
- Parking
- Transit
- Lockers
- Dining, POS
- Vending
- Laundry
- Library Fees
- Off-Campus

- Attendance
- Exams
- ID Card Issuance
- Contractors
- Visitors
- Summer Campers
- Sports Teams
- Athletic Center
- Residence

WWW.COLORID.COM
© 2019 -- ColorID, LLC
• Often Multiple Days for Service Availability
• Manual Processes
• Email Excel files
  – Department to department
• Flat file transfers
  – Automated
• Feeds
  – After data processing
    • De-duplication
    • Number generation
• 1990s technology, but it works!
IDENTITY MANAGEMENT

Is it a thing?
How we manage identities and their related credentials affect how well our systems work

<table>
<thead>
<tr>
<th>Type of identity</th>
<th>Credential</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital</td>
<td>User name, password; 2FA</td>
</tr>
<tr>
<td>Financial</td>
<td>Banking card; mobile app</td>
</tr>
<tr>
<td>Physical</td>
<td>ID card; mobile ID</td>
</tr>
</tbody>
</table>
• Access to digital data is governed by lots of government regulations in many markets
  – Health care, financial, higher education, corporations
• Physical access is not very well regulated
  – Home Depot example – Verizon audit
• And, as always,
  – Security vs. convenience
If you had all the $$ in the world...

PIV card costs $150

• Background checks verify identity
• Very smart card issued
• For Executive Branch only
  – Federal agency employees

CAC for Department of Defense
• Verify physical identity against PIV (card)
  – Biometrics and PIN – bind person to card
• Access to networks and PCs
• Access to doors - physical access
• Digital certificate on card
  – Encrypted digital identity
  – Tamper proof
• Identity lifecycle concept
  – Certificate authority
  – When something changes with identity, the whole system reacts
WHAT’S GOOD ABOUT PIV

• Tamper-proof card is bound to cardholder
• Any change in cardholder status is distributed
• All systems can know a person’s status at each point of contact
Identity and Access Management
• Usually manages credentials for IT and logical access
• Microsoft product examples
  – Identity Lifecycle Manager, Forefront, MS Identity Manager
  – SailPoint
• Not bound to physical person
  – Protect the system, not the user
IDENTITY ON CAMPUS

How it's done
• Establishing identity – who are you and how do we know that?
• Admissions offices have many channels for validating new students, faculty, staff
  – Application – self service
  – Mailings - address
  – Emails – digital identity
  – Financial aid - financial
  – Other services – 3rd party
Meanwhile over at the Card Office -
- Identity data comes from student information systems to the card database
- “Gotta get a card in their hand”
- Card data is pushed to various systems at issuance
  - Usually just the number on the card for that system
    - One-card system
    - Access control system
    - Other systems – res, library, parking
- Cards stay issued
  - Students, faculty members, staff could be in systems forever
  - Changes handled manually by Card Office
• How will each system know you are who you say you are?
• Issuing and managing multiple credential types
  – Card/cards
    • Multiple credentials on each
  – Mobile credentials – doors, POS
    • See my presentation on mobile on Wednesday at 1:30
  – Biometrics – really physical access!
IDENTITY MANAGEMENT CHALLENGES

• What if someone loses their card or key or credential, or they leave the school?
  – “We have thousands of expired users in our databases”
• Manual processes
  – Removing privileges once student or staff leave campus
  – Updating permissions, re-issuing cards, managing dataflow
• Identity data silos obstruct a consolidated view of identities and access rights
THERE IS THIS PRODUCT...

PIAM = Physical Access and Identity Management
PIAM MOVES CREDENTIAL DATA

SIS or IAM

PIAM
Includes card production, photo upload, self service

Access Control Systems
One-Card System
Library/Print-Copy
Parking
Mobile ID
PIAM MOVES CREDENTIAL DATA

Includes card production, photo upload, self service

SIS or IAM

Access Control Systems

One-Card System

Library/Print-Copy

Parking

Mobile ID
• It’s the 21st century!
  – No patience for laggy data
• RESTful APIs
• Native DB connections
• ODBC
• Flat file transfers still have a place
• 24-72 hour feeds are no longer acceptable
HID SAFE SELF-SERVICE BADGING PROCESS

Student requests new ID card

Approver notified

Approver approves request

Card Office

Prints the ID card

Existing Card is updated or Security prints. Workflow is documented for Audit and Compliance

Self-Service Portal

Student notified

Card is printed

Downstream systems, PACS, Library, Parking auto-updated with new badge numbers

© 2019 -- ColorID, LLC
SAFE HAS SOME INTELLIGENCE

• Physical access control example:
  – Policy
  – Integration
• HID SAFE has intelligence built in
• Ensure each identity has the right access, to the right areas, for the right length of time
PIAM MANAGES FULL IDENTITY LIFECYCLE

- Enroll/Hire/Pre-register/Contract
- Authorize/Vetting
- Issuance of Campus ID Cards or Mobile Tokens
- Check-In Kiosks
  - can include issuance of temp badge
- Reports Operational/Predictive
- Access Audit and Compliance
- Provision

Disenroll/Terminate/Check-out

Students
Staff
Visitors
Vendors
Contractors

© 2019 -- ColorID, LLC
COME TOGETHER

PIAM is a group effort
How are the credentials and the permissions that go with them shared with campus systems?

- Across distributed campuses
- Across multiple systems
- Do you have silos?
SAFE IDENTITY MANAGEMENT – LIKE GOOGLE DOCS

- On-boarding & Badging
- Visitor Management
- Access Management
- Privacy & Compliance
- Analytics

www.colorid.com
SAFE IDENTITY MANAGEMENT – LIKE GOOGLE DOCS

On-boarding & Badging
Visitor Management
Access Management
Privacy & Compliance
Analytics

Needs to restock badges

Needs to know when identities are on-boarded
SAFE IDENTITY MANAGEMENT – LIKE GOOGLE DOCS

On-boarding & Badging
Visitor Management
Access Management
Privacy & Compliance
Analytics

Responsible for visitor & event management campus wide

WWW.COLORID.COM
They now reside on campus.

Changed their major a month ago.

Needs to audit access for off site Hospital Research.

They report to him.

Research Staff who work in a Govt high security area.

On-boarding & Badging
Visitor Management
Access Management
Privacy & Compliance
Analytics

SAFE IDENTITY MANAGEMENT – LIKE GOOGLE DOCS

WWW.COLORID.COM
Needs to compile compliance report for all sites
On-boarding & Badging
Visitor Management
Access Management
Privacy & Compliance
Analytics

SAFE IDENTITY MANAGEMENT – LIKE GOOGLE DOCS

Needs to understand which sites are violating tailgating policies
IDENTITY MANAGEMENT FOR THE ENTERPRISE

Managing identities at the enterprise level solves problems and provides opportunities.
TEMPORARY IDENTITIES

Just stopping by
TEMPORARY IDENTITIES

• How do we create and manage identities for visitors, conferences and events?
• Timed events
  – Visitors to residence halls
  – Any other visitors
    – Conferences
      • Academic
    – Summer programs
  – Contractor management
    • Example – Often no vetting, name only, extended terms for cards, no way to check change in status
Question for you. We are looking at Visitor Management for some of the loaner cards we print for guests and contractors. These cards do not currently fit into our badging process as cleanly as we want so ideally looking for a solution that would allow sponsors to pre-enroll guests and then print badges as needed.

We also need help with bulk enrollment processes. For instance Housekeeping is contracted out and they request 50 cards at a time. I want a way to set them up for bulk printing.

I would really love a way for the system to help automate audits of these guest/contractors cards as well. Also a way for these sponsors to re-certify that the cards are still in use/possession.
REPORTING AND COMPLIANCE

What just happened?
• We need to know who, what, when, where, and maybe why, identities and credentials were:
  – Created
  – Used
  – Revoked
• ID systems may store some of this data
  – How to pull it together?
Identity Management for the Enterprise

HID SAFE Enterprise

Enhances Local Functions:
- Record of Approval
- Record of request

And Adds New Capabilities at the Enterprise-level:
- Audit Attestation
- Policy Enforcement
- 24/7 Compliance Reports
- SLA management
• May, 2018
• Covers any data stored for EU persons
• Requires personal consent to use data
• Requires data removal after use
• Fines for non-compliance
  – Maximum of 4% of global annual turnover or €20 million
• Manage risk profiles per person
  – These can change after enrollment
  – Observed behavior on campus
    • Files accessed
    • Doors accessed
  – Behavior off campus
    • External databases log this
  – Manage threats
    • Insider cyber attacks
    • Physical attacks
DIFFERENT APPROACHES

Is there another way?
OTHER APPROACHES TO “PIAM”

• Take a “best of breed” approach
• Many new solutions for identity management
  – New, robust ID issuance software products
    • Powerful data handling capabilities
    • My presentation at 3:15 today, Rm. 25
  – Move and manipulate data across many systems
    • Swiftdata
  – Photo upload products
    • CloudCard, MyPhoto
  – Real time reporting
    • Tableau, Qlic, Domo, Splunk
WHAT TO DO?

• What gaps do we have, both in security and in convenience?
  – Identity management directly impacts the “user experience”
  – Deferred maintenance of identity management?
• Can departments pull together around Physical Identity and Access Management?
• Are our current systems locking us into a future of limited options regarding identity and credentials?
THANK YOU