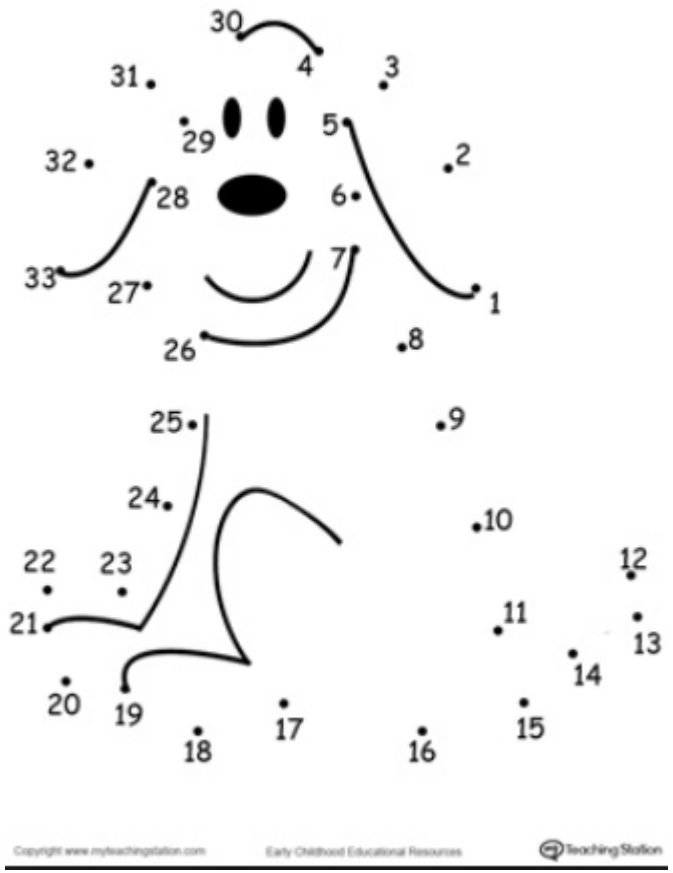
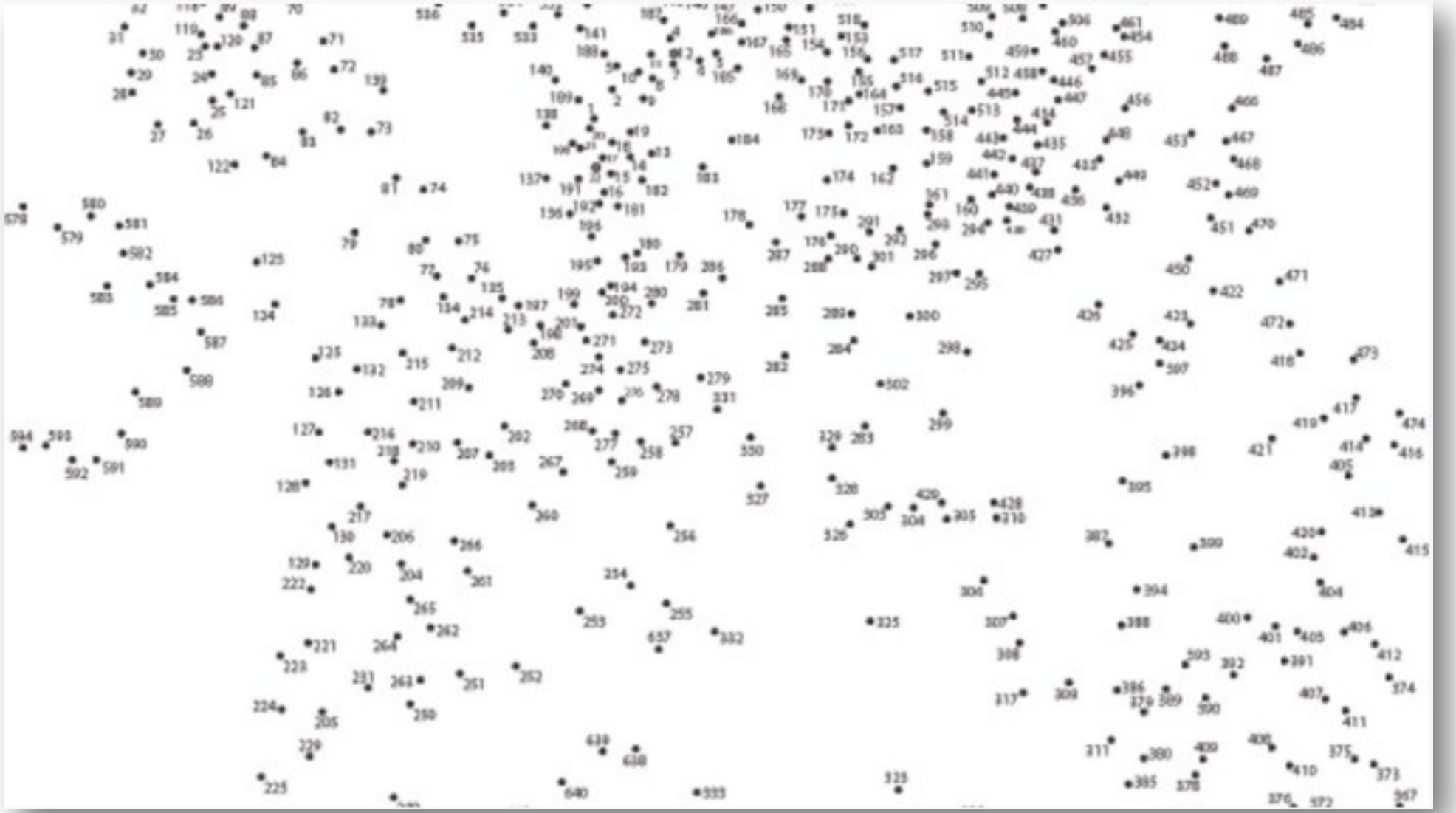
PEOPLE, IDENTITIES AND CREDENTIALS: HOW TO CONNECT THE DOTS

CONNECTING THE DOTS – EARLY CARD SYSTEM



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?

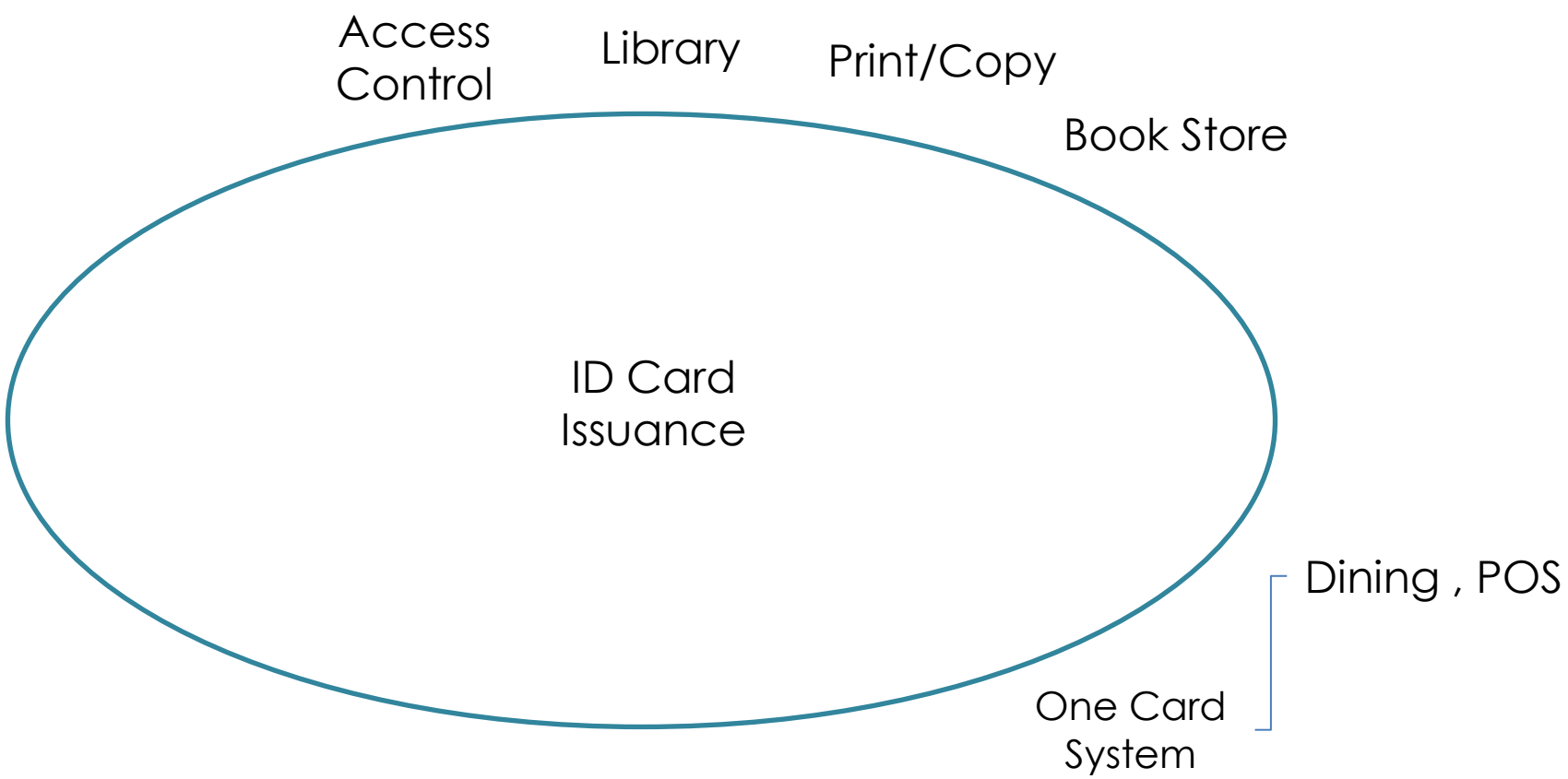
HOW DID WE GET HERE?

The Deferred Maintenance of Identity Management

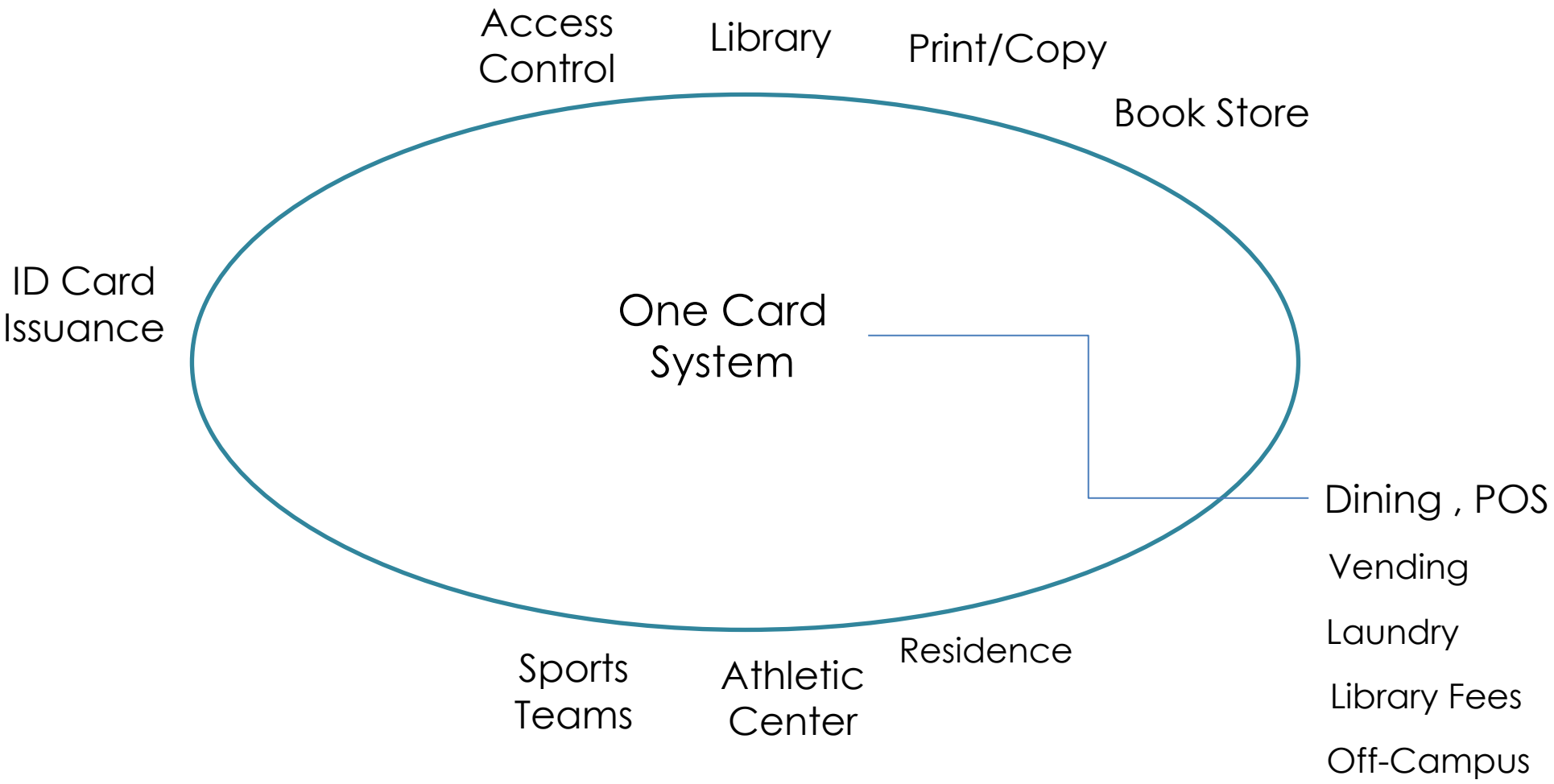
LOOK AT YOUR CARD

- 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

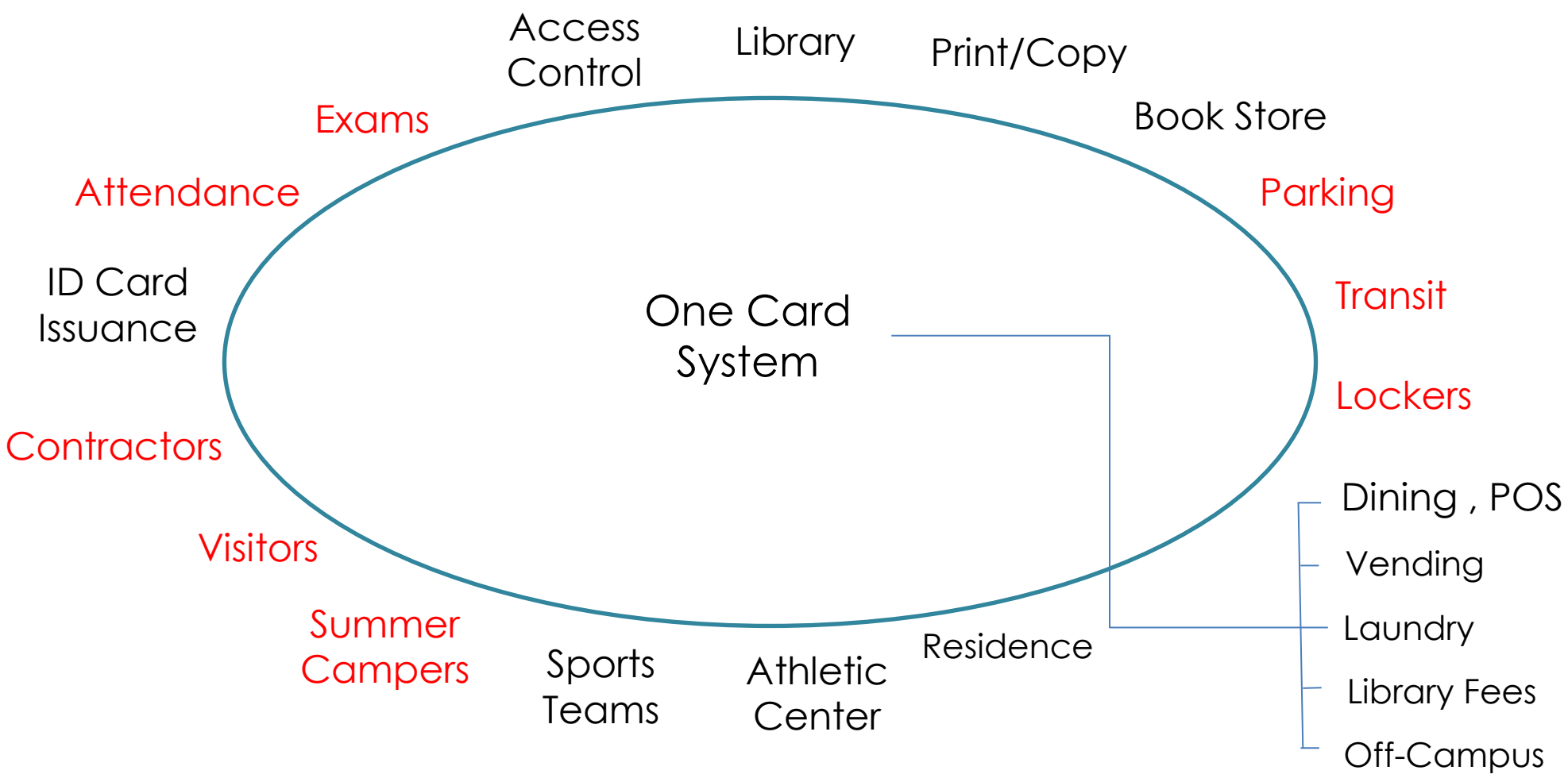
EVERYTHING ON CAMPUS



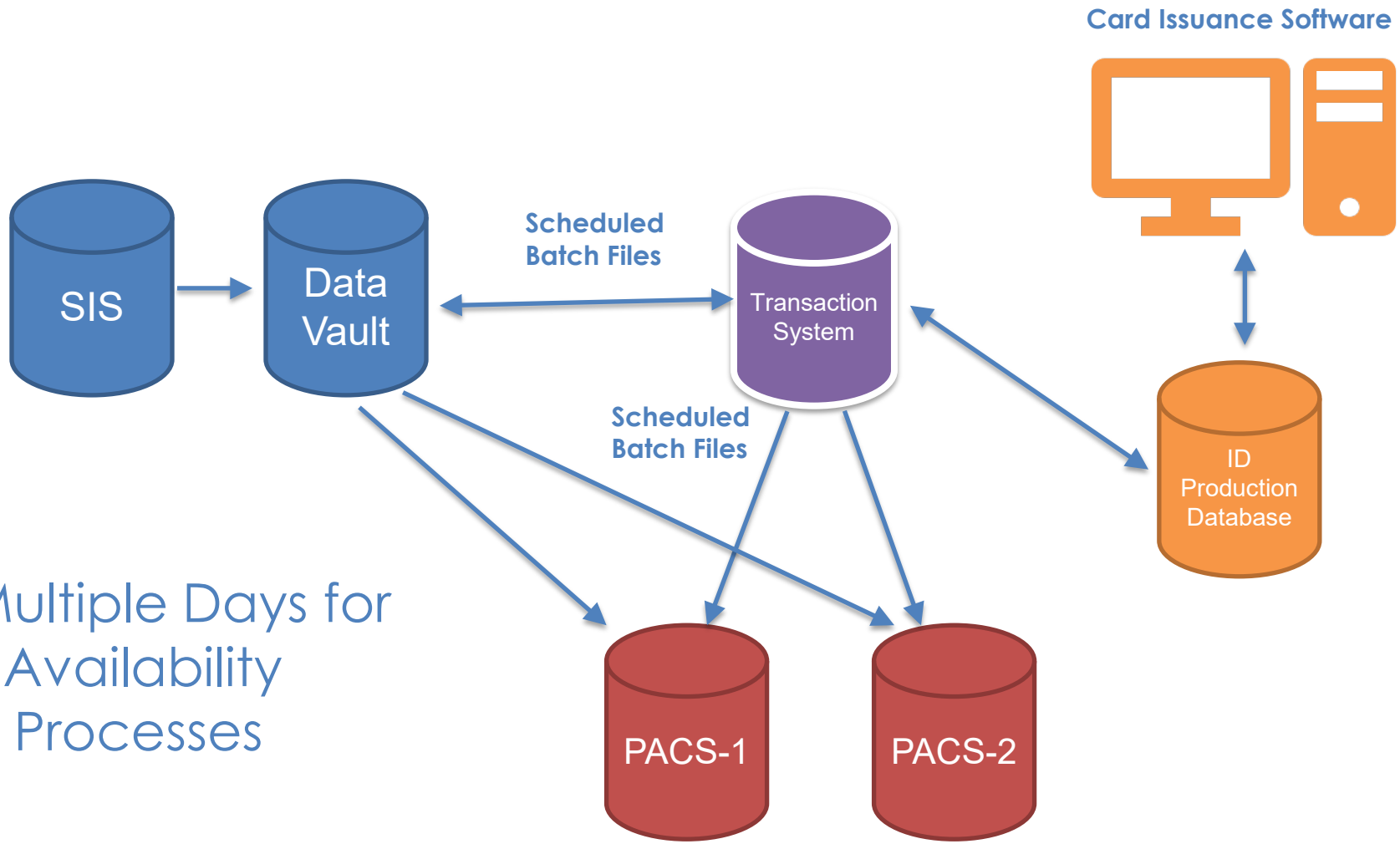
EVERYTHING ON CAMPUS



EVERYTHING ON CAMPUS



UNIVERSITY CARD DATA EXAMPLE



- Often Multiple Days for Service Availability
- Manual Processes

HOW DATA CHANGES AND MOVES

- 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?

IDENTITY IS IMPORTANT

How we manage identities and their related credentials affect how well our systems work

Type of identity	Credential
Digital	User name, password; 2FA
Financial	Banking card; mobile app
Physical	ID card; mobile ID

FINANCIAL IDENTITY

- Your financial institution decides who you are
- They let you use their money to buy a house, car, business, toys
- Financial **identity theft** has been in the headlines for years
  - It's even a movie!
  - Card issuers (banks) don't hold cardholders liable
    - But they give us expensive EMV cards (credentials)

PHYSICAL IDENTITY

- You take up space
- You interact physically with systems
  - Doors
  - Networks
  - Points of Sale
  - Teams and memberships
  - Parking and transit
- Physical persons and possessions have to be safe
  - No tolerance for physical "breach"

IDENTITY AND REGULATION

- 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

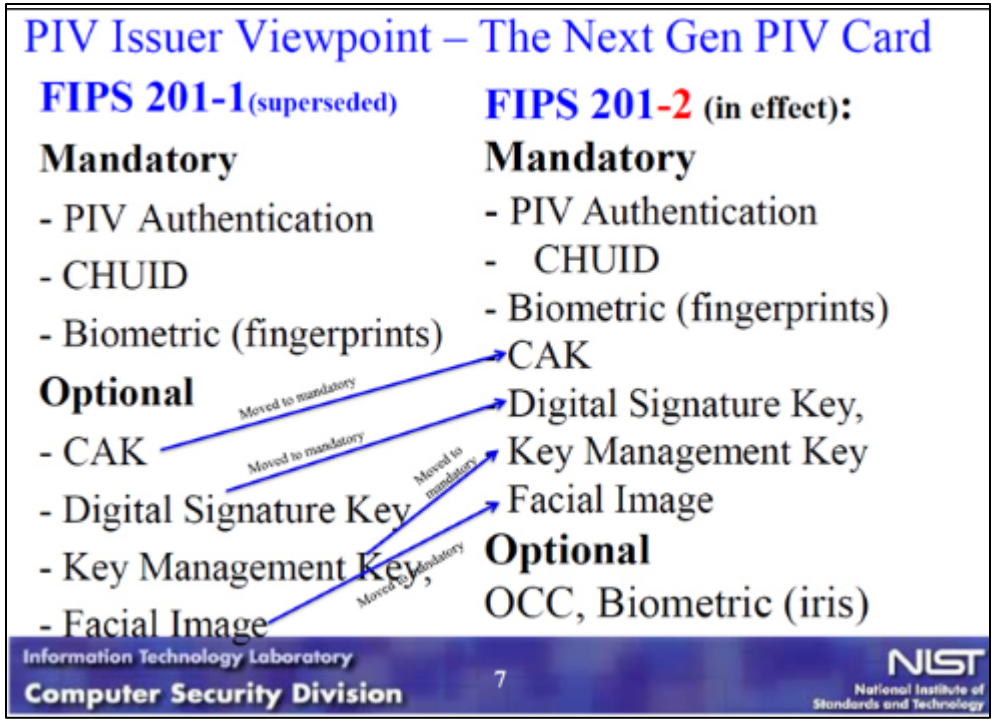
U. S. GOVERNMENT IDENTITY MANAGEMENT

If you had all the $$ in the world…

PIV card costs $150

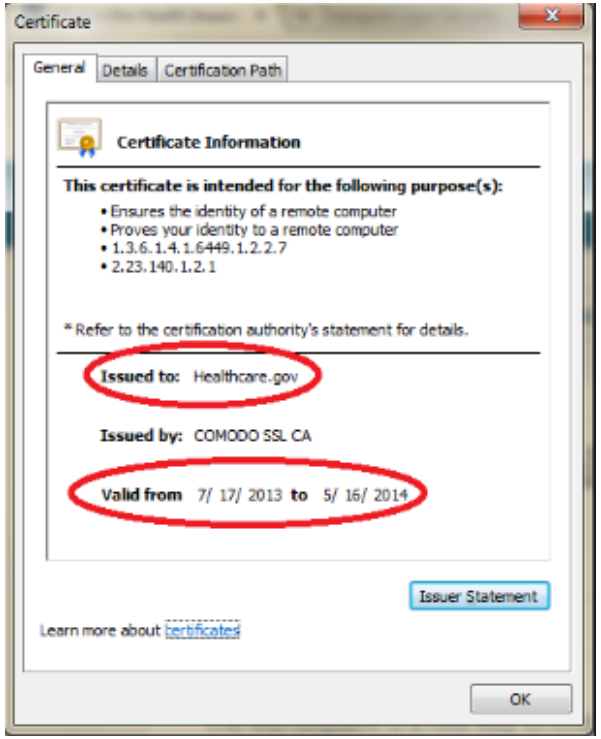
- Background checks verify identity
- Very smart card issued
- For Executive Branch only
  - Federal agency employees

CAC for Department of Defense



MORE ON PIV

- 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

DIGITAL IDENTITY MANAGEMENT - IAM

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

The Gartner IAM Program Maturity Model

IAM Program Maturity Level	1 Initial	2 Developing	3 Defined	4 Managed	5 Optimized
Governance	Ad hoc, informal	Subsumed within InfoSec (and InfoSec governance structures)	IAM governance structure defined and accepted	IAM governance structure fulfilled and refined	IAM governance optimization
Organization	Informal, basic roles, responsibilities decentralized	Technical projects sponsored by BUs and CISO; informal inventory of IAM skills	IAM PMO established, IAM roles and training needs defined	IAM PMO active, RACI matrix defined; proactive skill development	Optimal integration with business; skills optimized
Vision and Strategy	Conceptual awareness at best	Certain business drivers identified; tactical priorities set	Business-aligned vision defined; strategic priorities set	IAM vision and strategy continually reviewed to track business strategy	Periodic optimization of vision and strategy
Processes	Ad hoc, informal	Semiformal BU-specific and target-specific processes	Formal processes defined, consistent across BUs and target systems	Formal processes integrated and refined; aligned with business processes	Process optimization
Architecture and Infrastructure Design	Possible use of target-specific productivity tools	Disjoint technical projects; technology redundancy likely	Discrete IAM architecture defined; rationalization and consolidation in hand	IAM architecture refined and aligned with EA	IAM architecture embedded within EA; optimization
Business Value	None measurable	Tactical efficiency and (maybe) effectiveness improvements; low direct value	Sustained, quantifiable improvements tied to GRC imperative; moderate direct value	Sustained, quantifiable contribution to all key business imperatives; high direct value	Business value optimization; transformational direct value
Legacy Program Maturity Level	Blissful Ignorance	Awareness	Corrective	Operational Excellence	

IDENTITY ON CAMPUS

How it's done

UNIVERSITY PHYSICAL IDENTITY MANAGEMENT – p. 1

- 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

UNIVERSITY PHYSICAL IDENTITY MANAGEMENT – p. 2

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

CREATING A VARIETY OF CREDENTIALS

- 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!





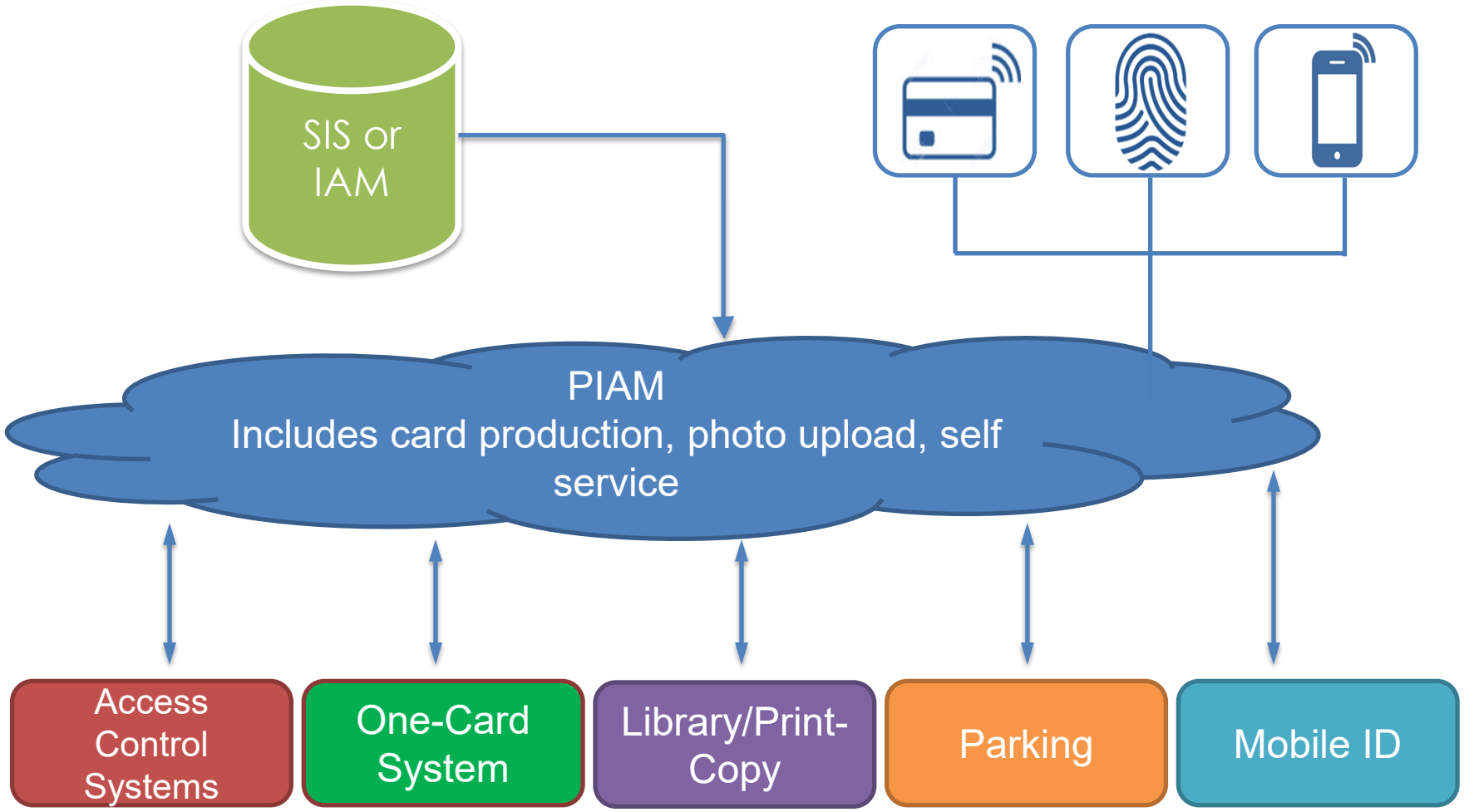
IDENTITY MANAGEMENT CHALLENGES

- 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

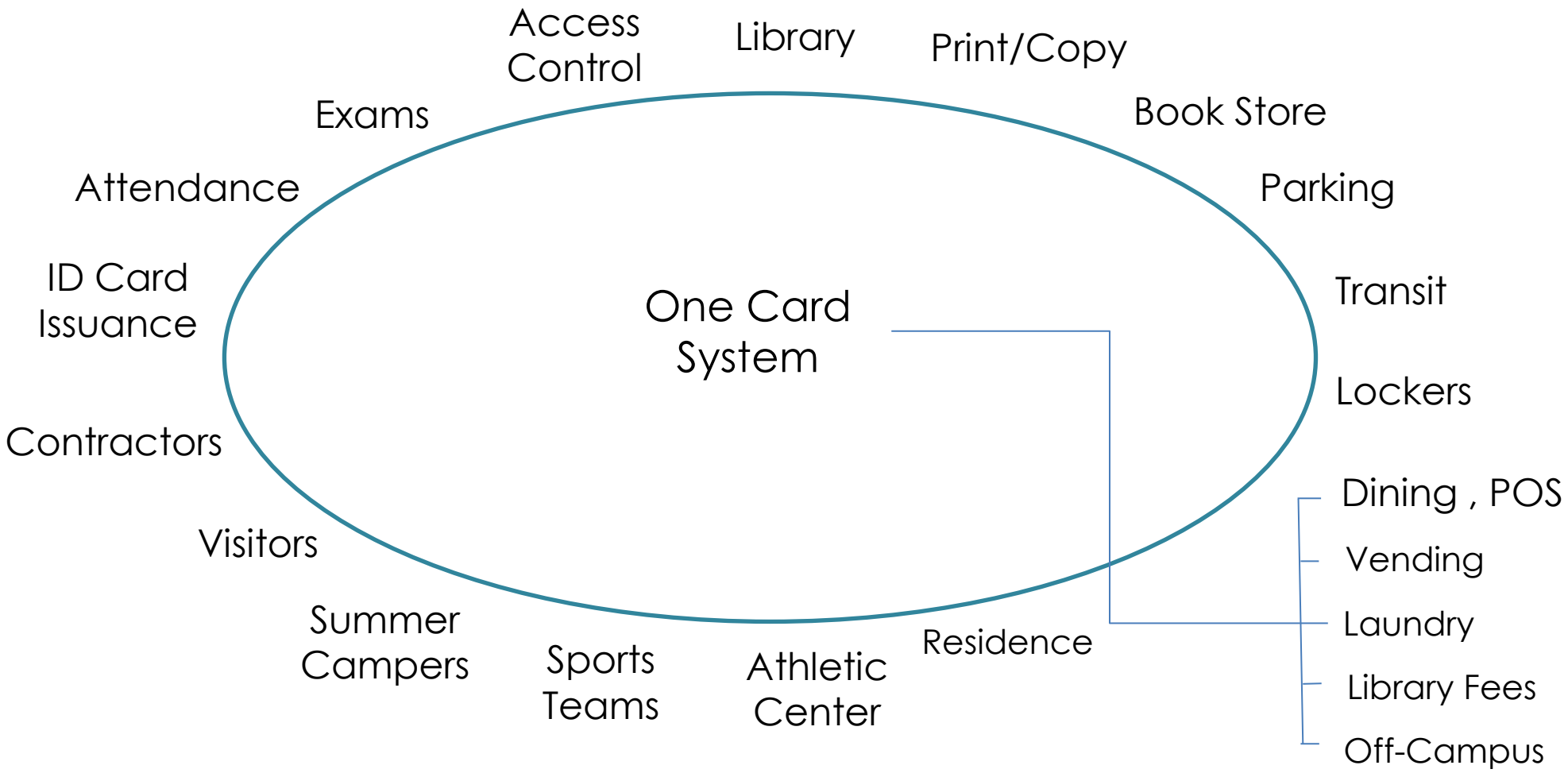
THERE IS THIS PRODUCT…

PIAM = Physical Access and Identity Management

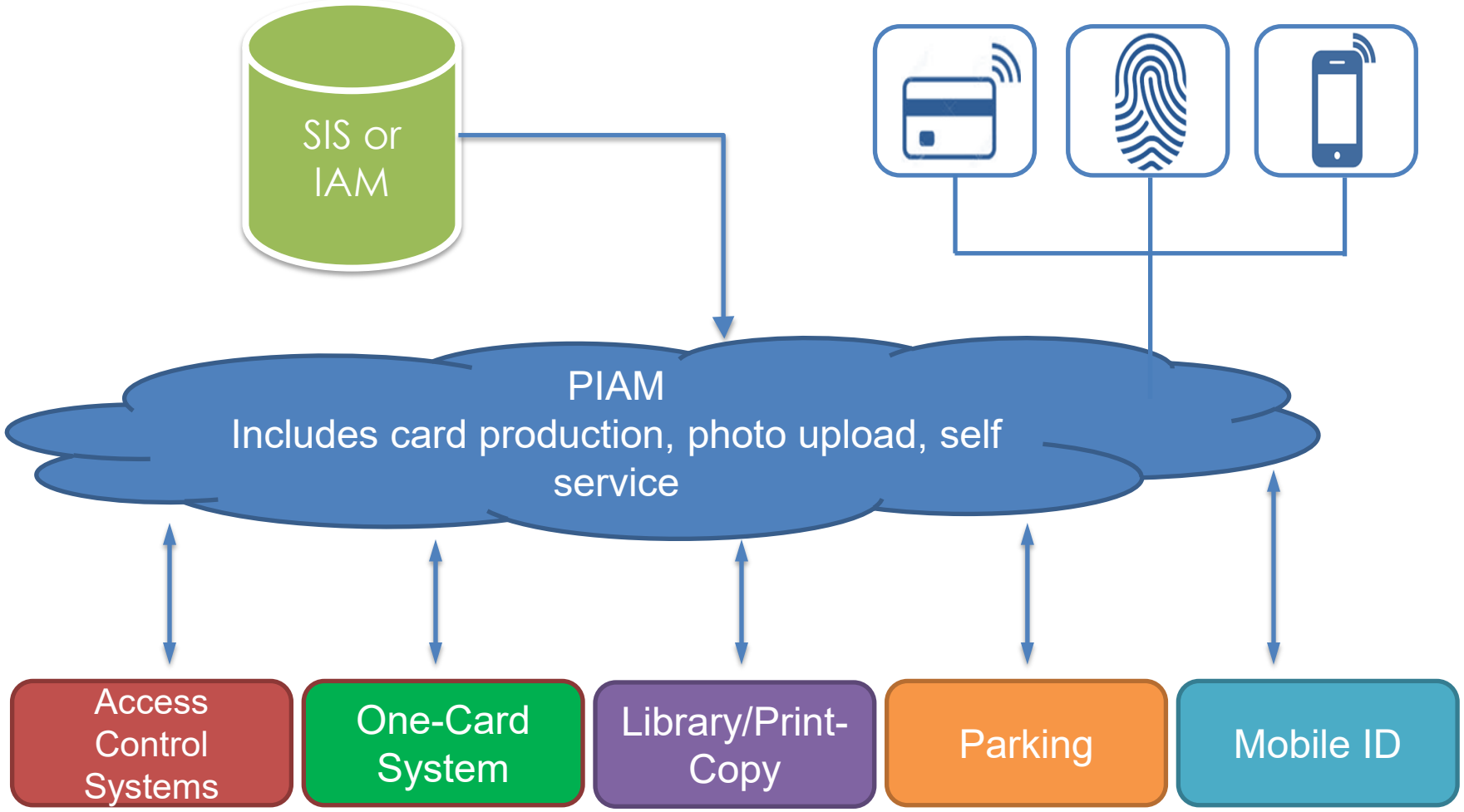
PIAM MOVES CREDENTIAL DATA



EVERYTHING ON CAMPUS



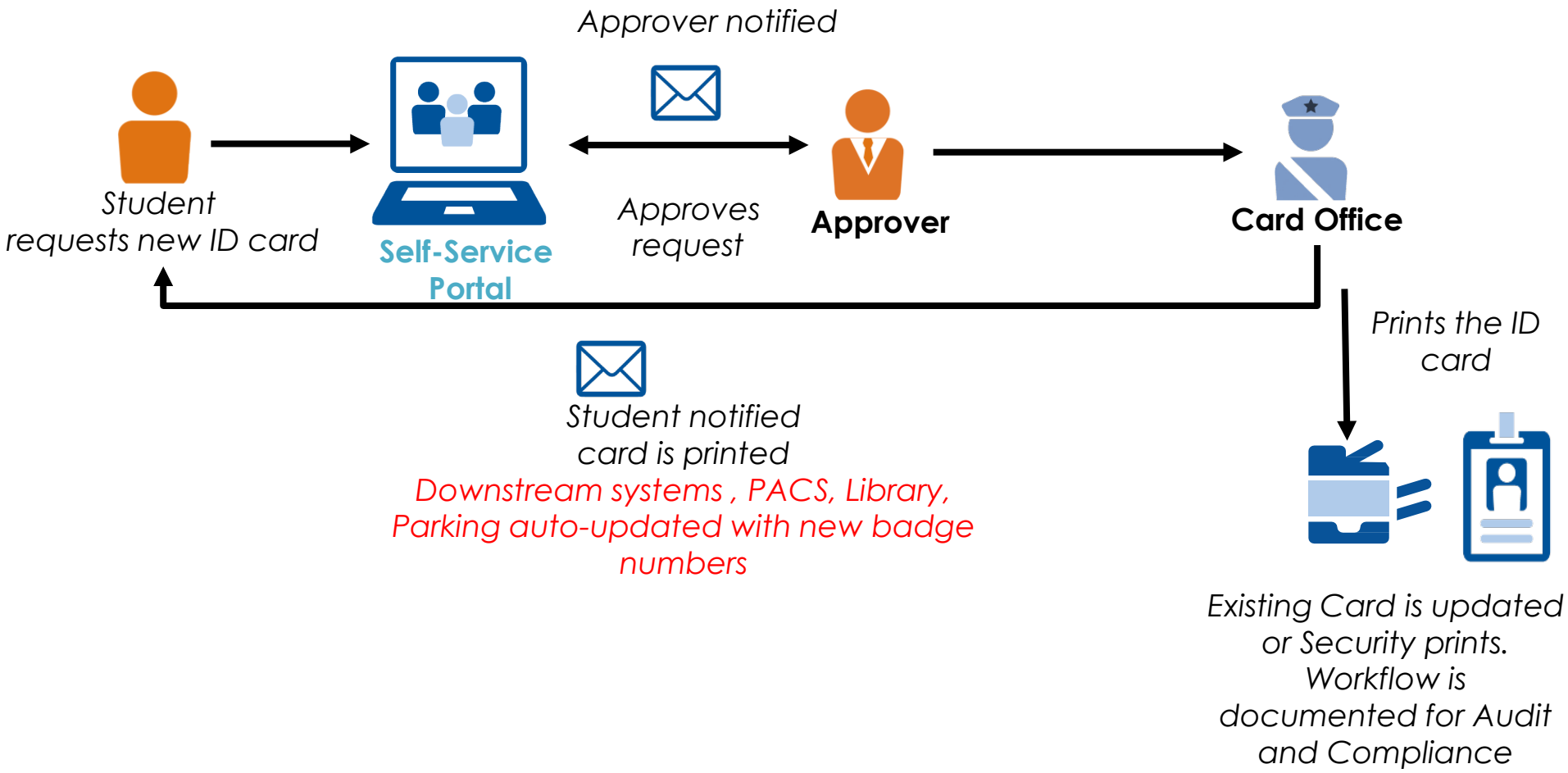
PIAM MOVES CREDENTIAL DATA



DATA CONNECTIONS

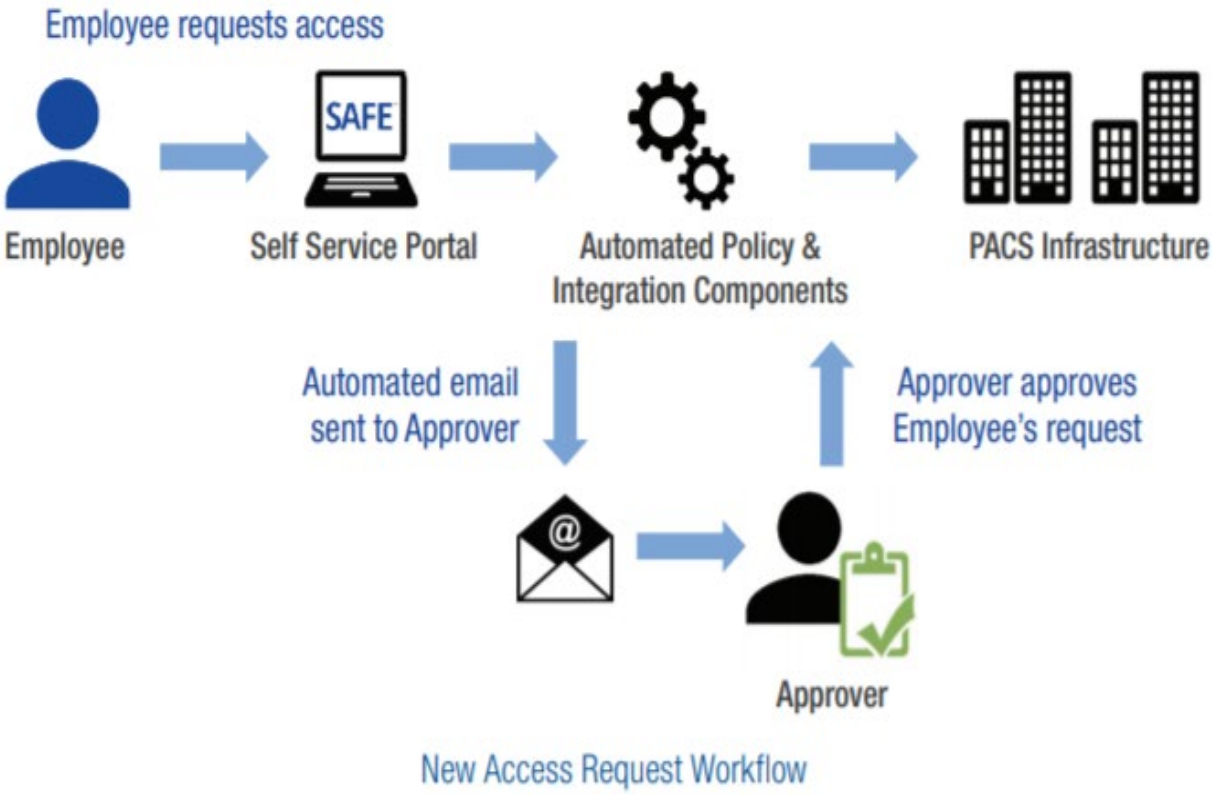
- It's the 21st century!
  - No patience for laggy data
- RESTful APIs
- Native DB connections
- ODBC
- Flat file transfers still have a place
- 24-72 hour feeds are no longer acceptable

HID SAFE SELF-SERVICE BADGING PROCESS

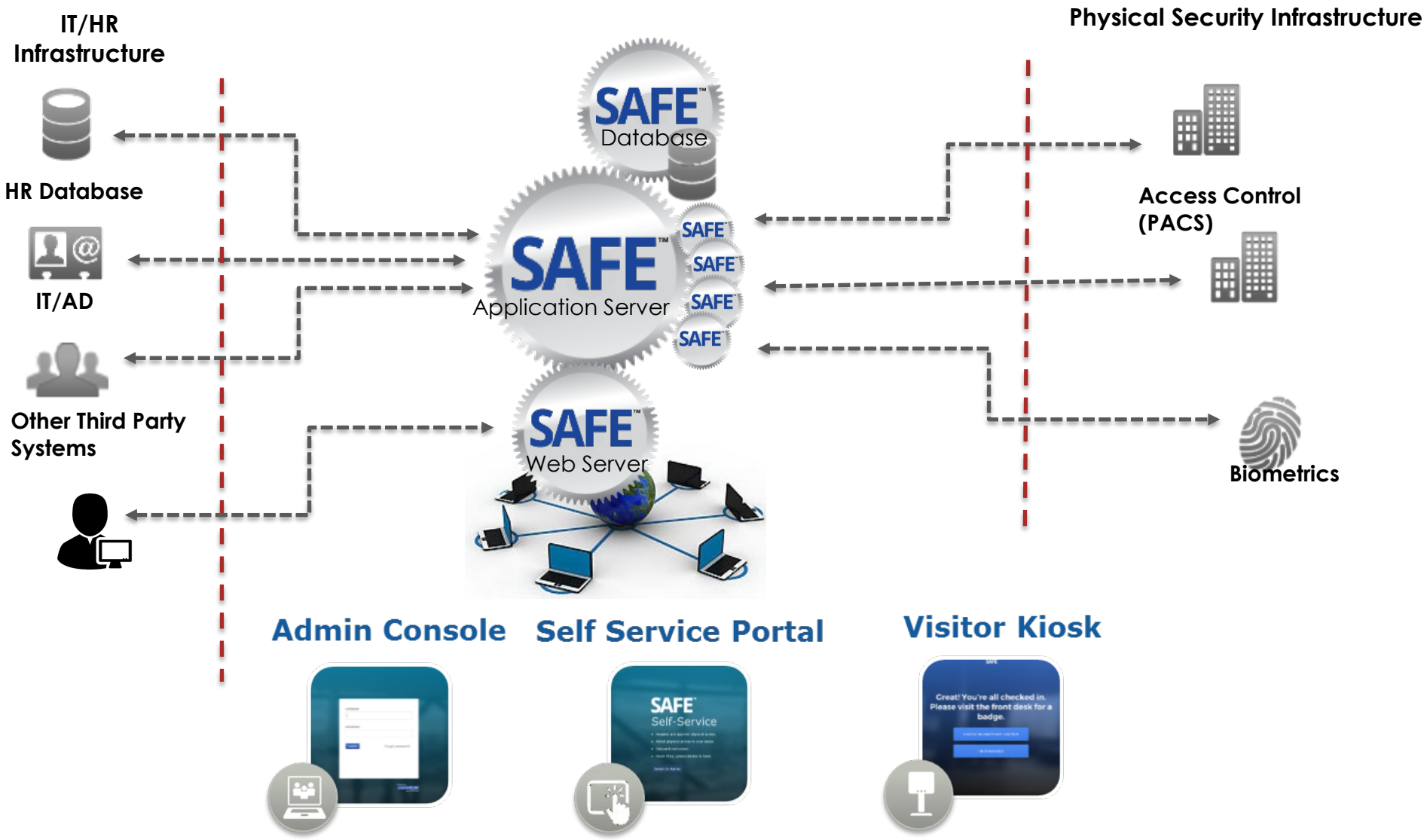


SAFE HAS SOME INTELLIGENCE

- Physical access control example:
- HID SAFE has intelligence built in
  - Policy
  - Integration
- Ensure each identity has the right access, to the right areas, for the right length of time



SOLUTION ARCHITECTURE



PIAM MANAGES FULL IDENTITY LIFECYCLE

COME TOGETHER

PIAM is a group effort

SHARING IDENTITIES AND RELATED CREDENTIALS

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

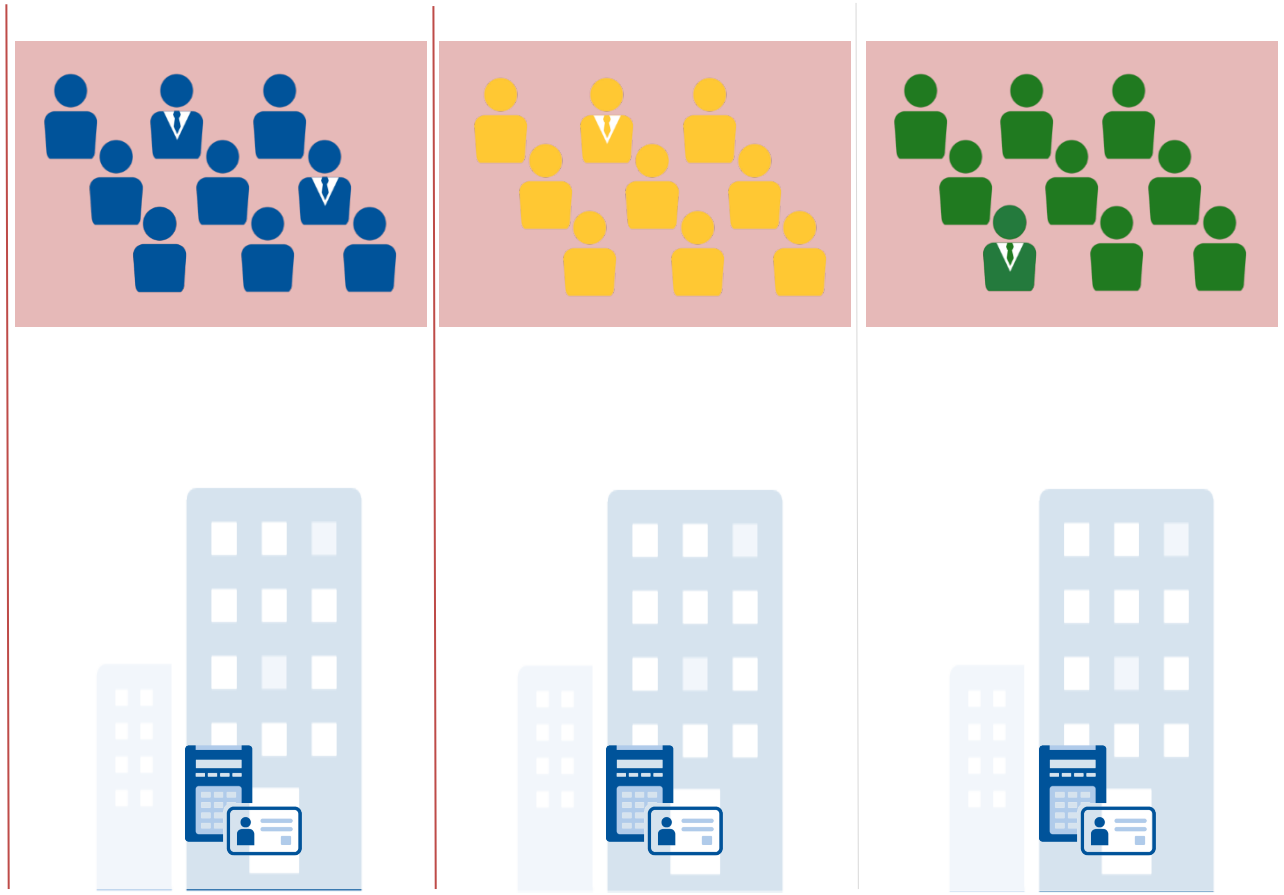
On-boarding & Badging

Visitor Management

Access Management

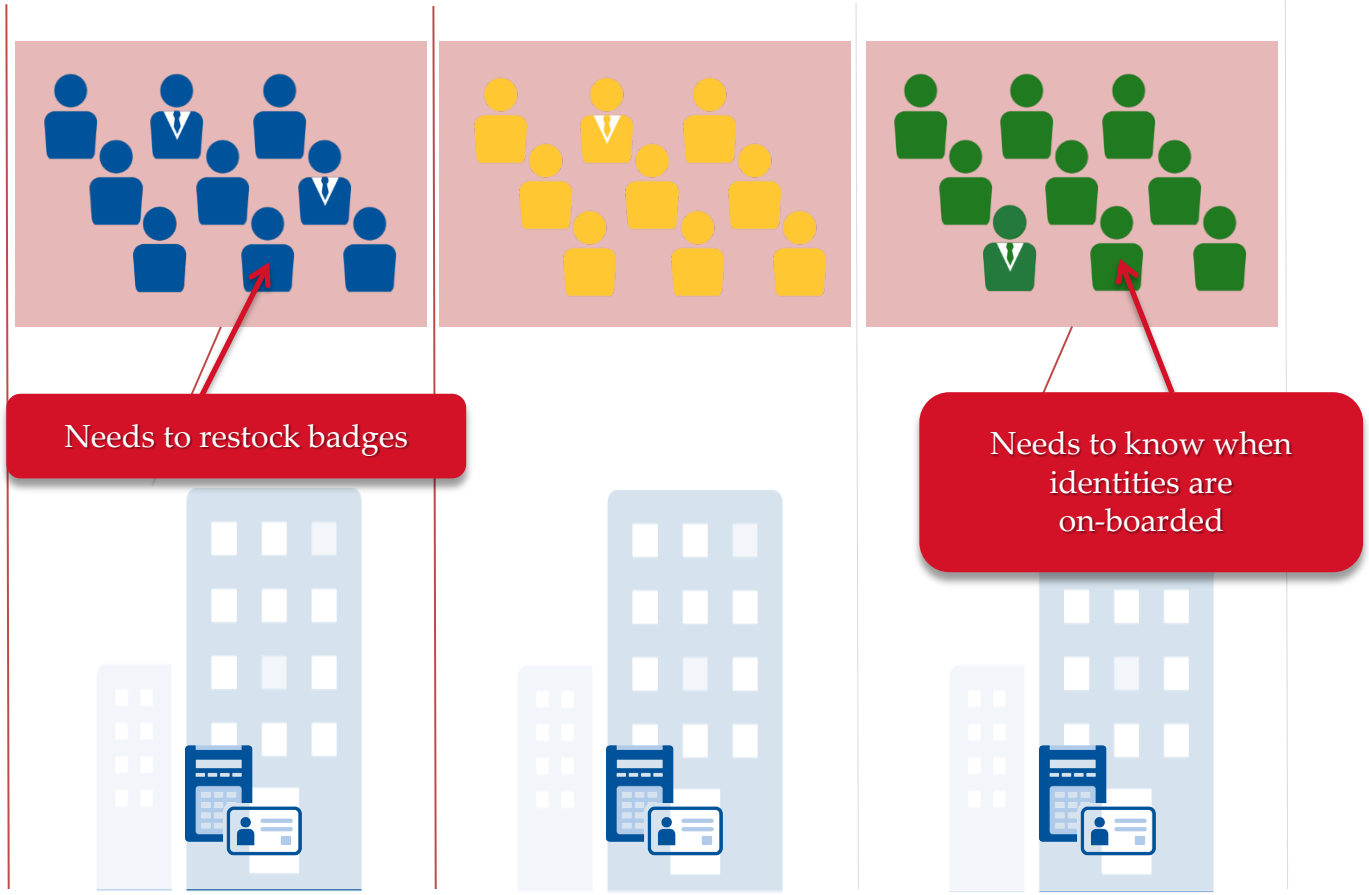
Privacy & Compliance

Analytics



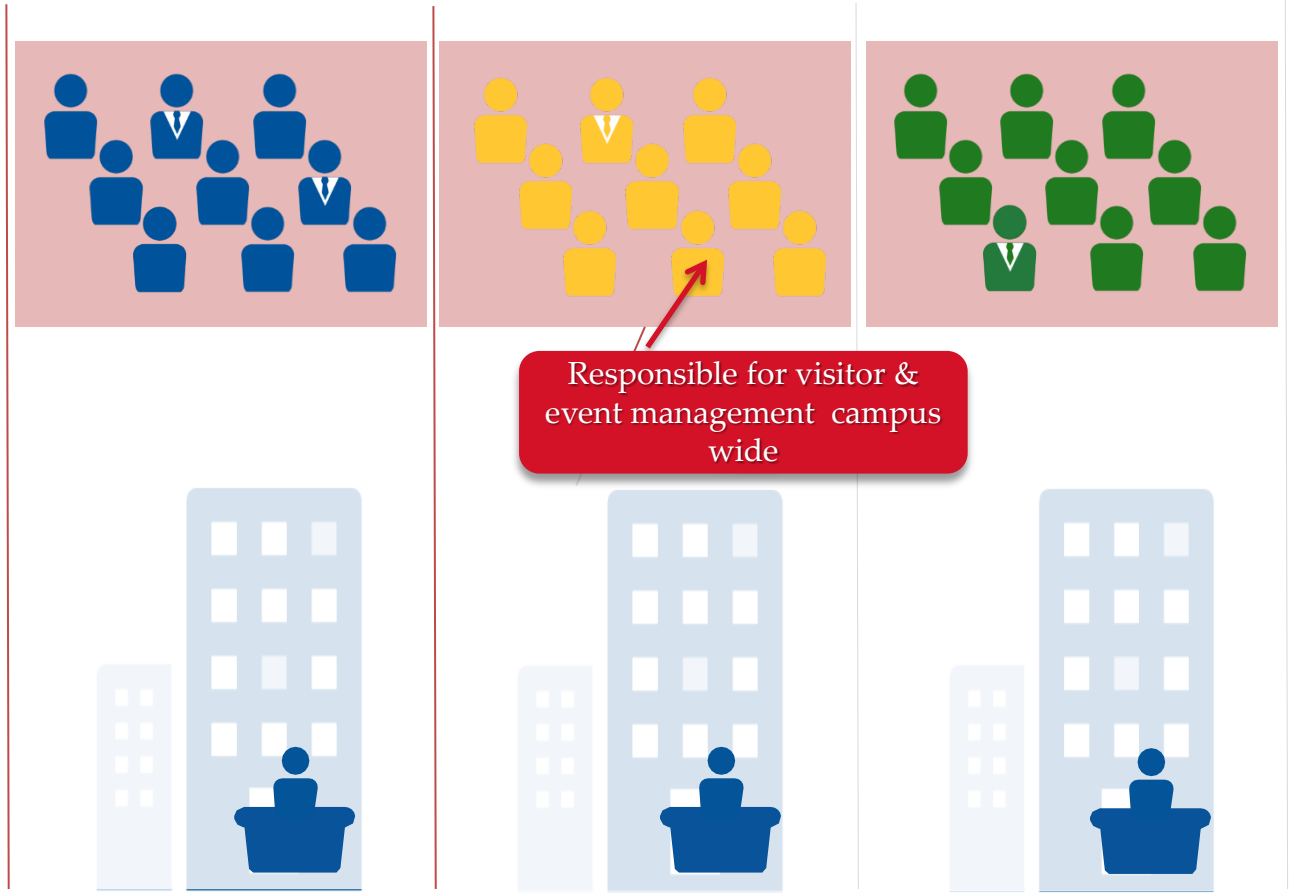
SAFE IDENTITY MANAGEMENT – LIKE GOOGLE DOCS

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



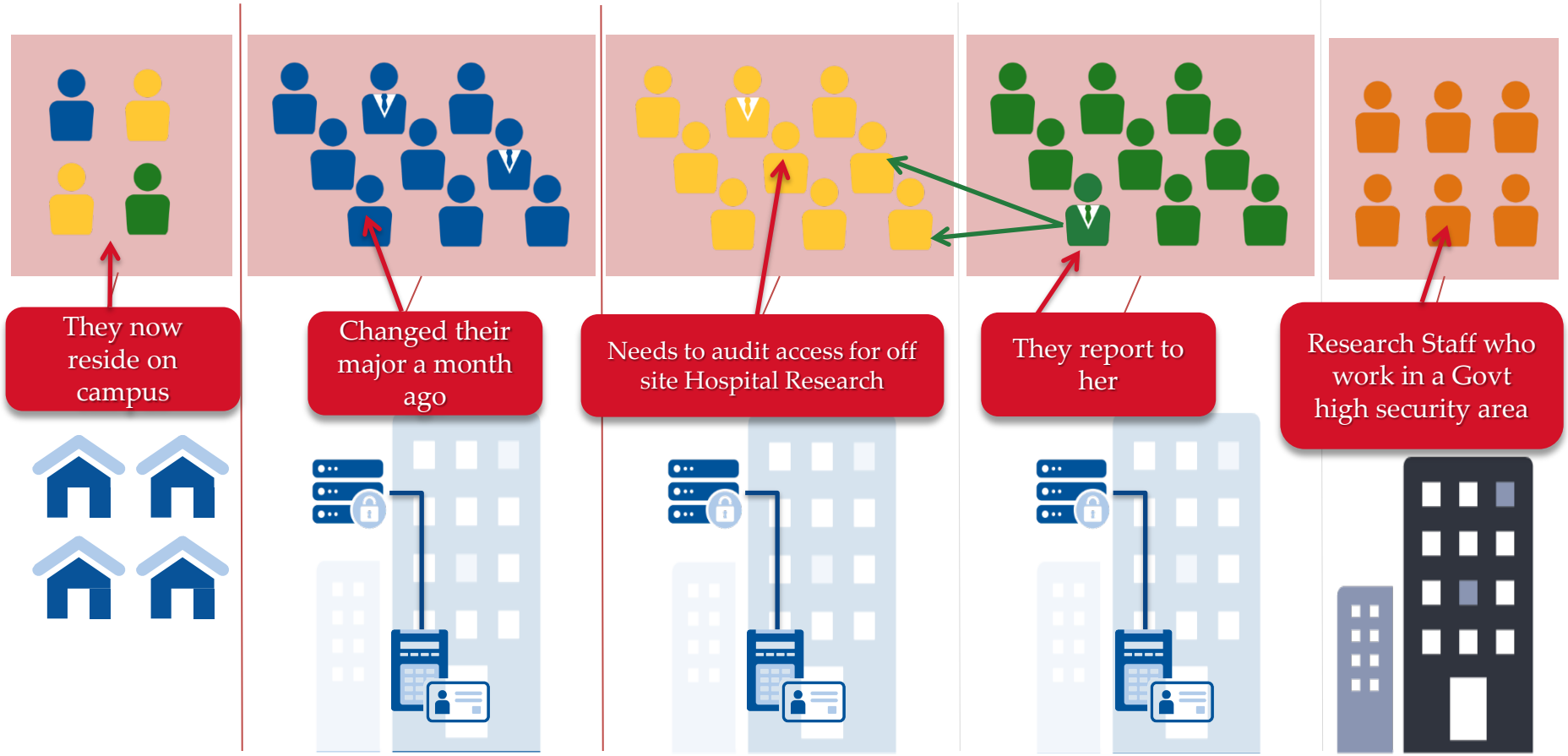
SAFE IDENTITY MANAGEMENT – LIKE GOOGLE DOCS

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



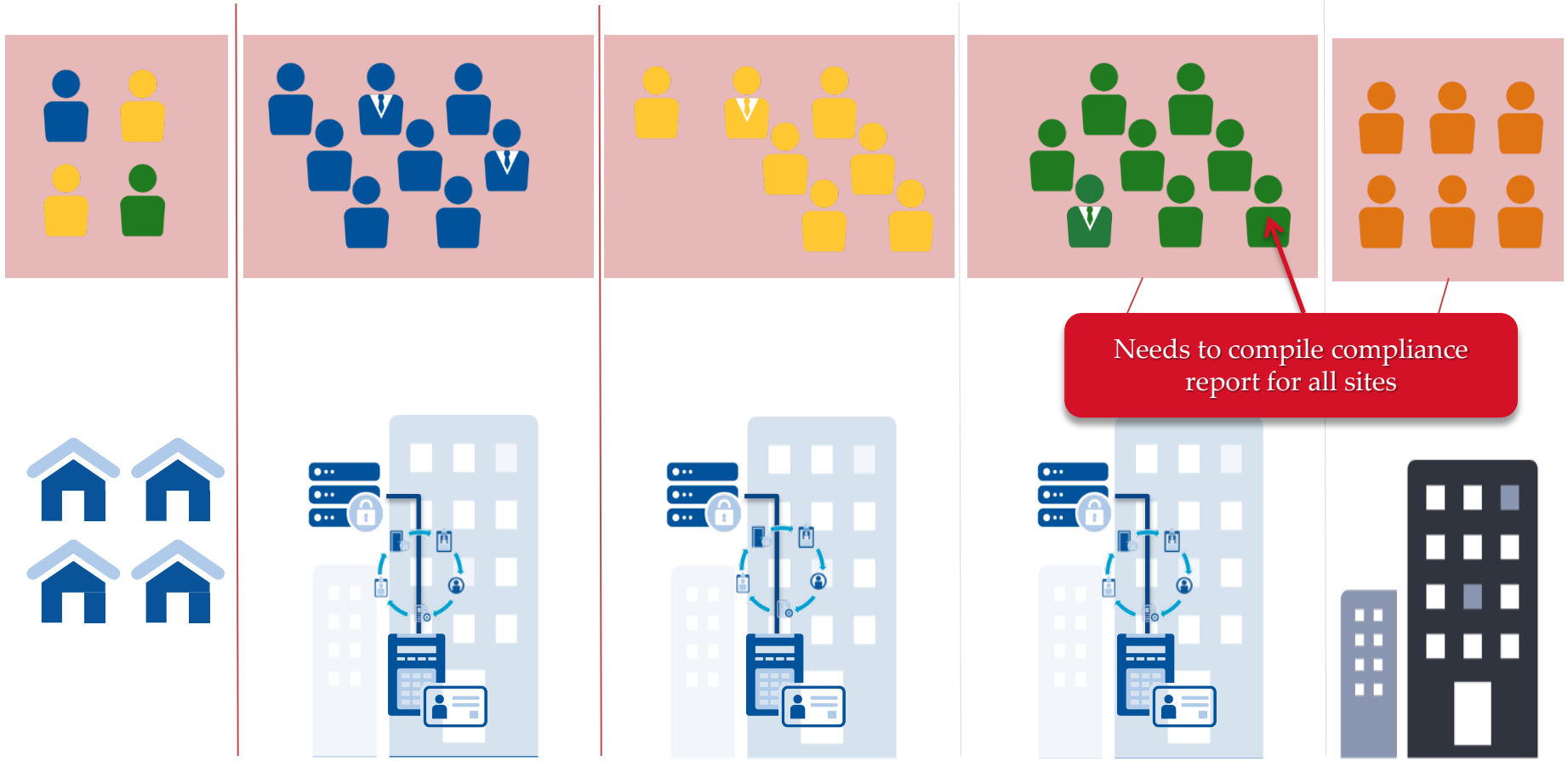
SAFE IDENTITY MANAGEMENT – LIKE GOOGLE DOCS

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



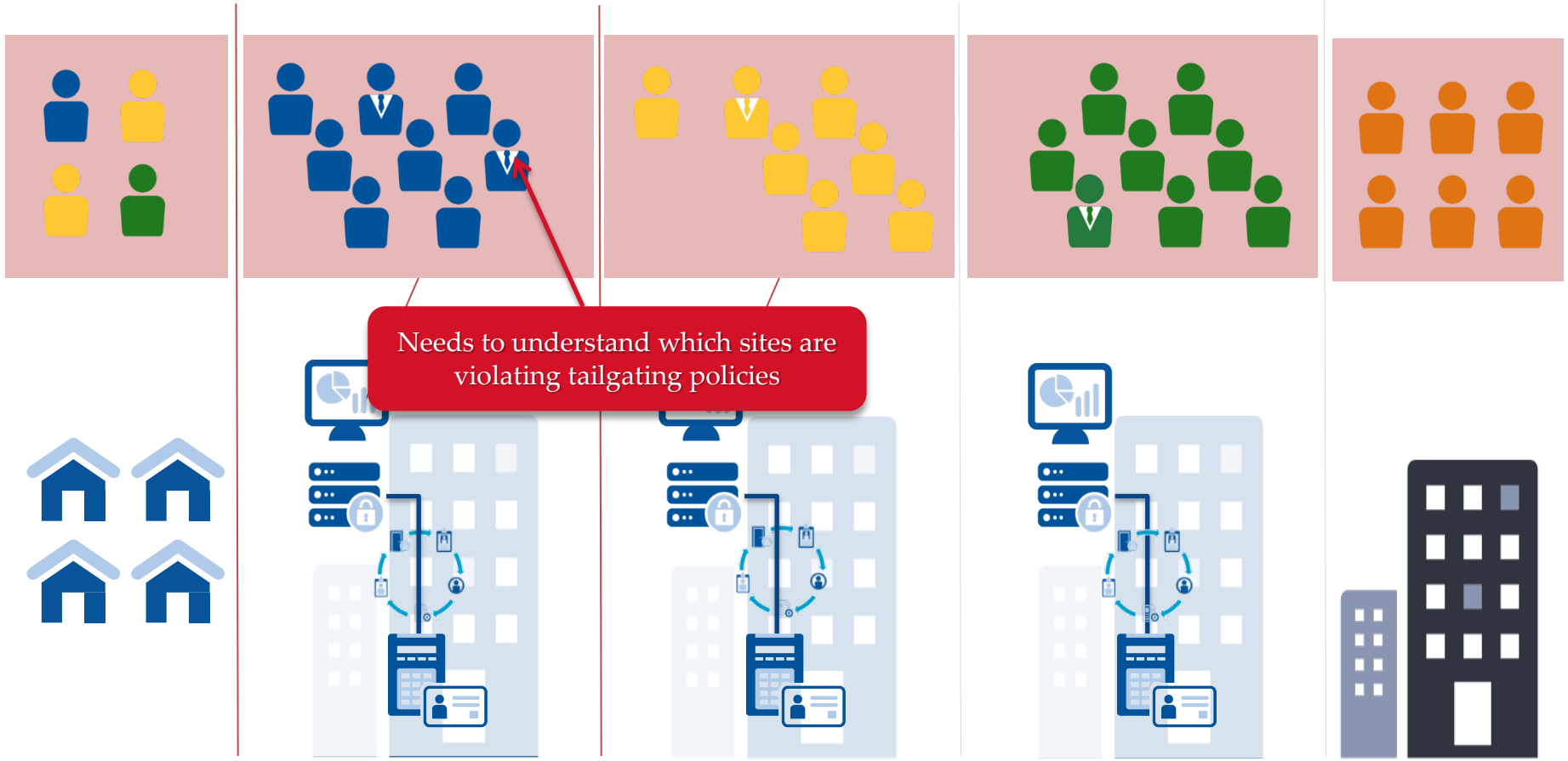
SAFE IDENTITY MANAGEMENT – LIKE GOOGLE DOCS

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

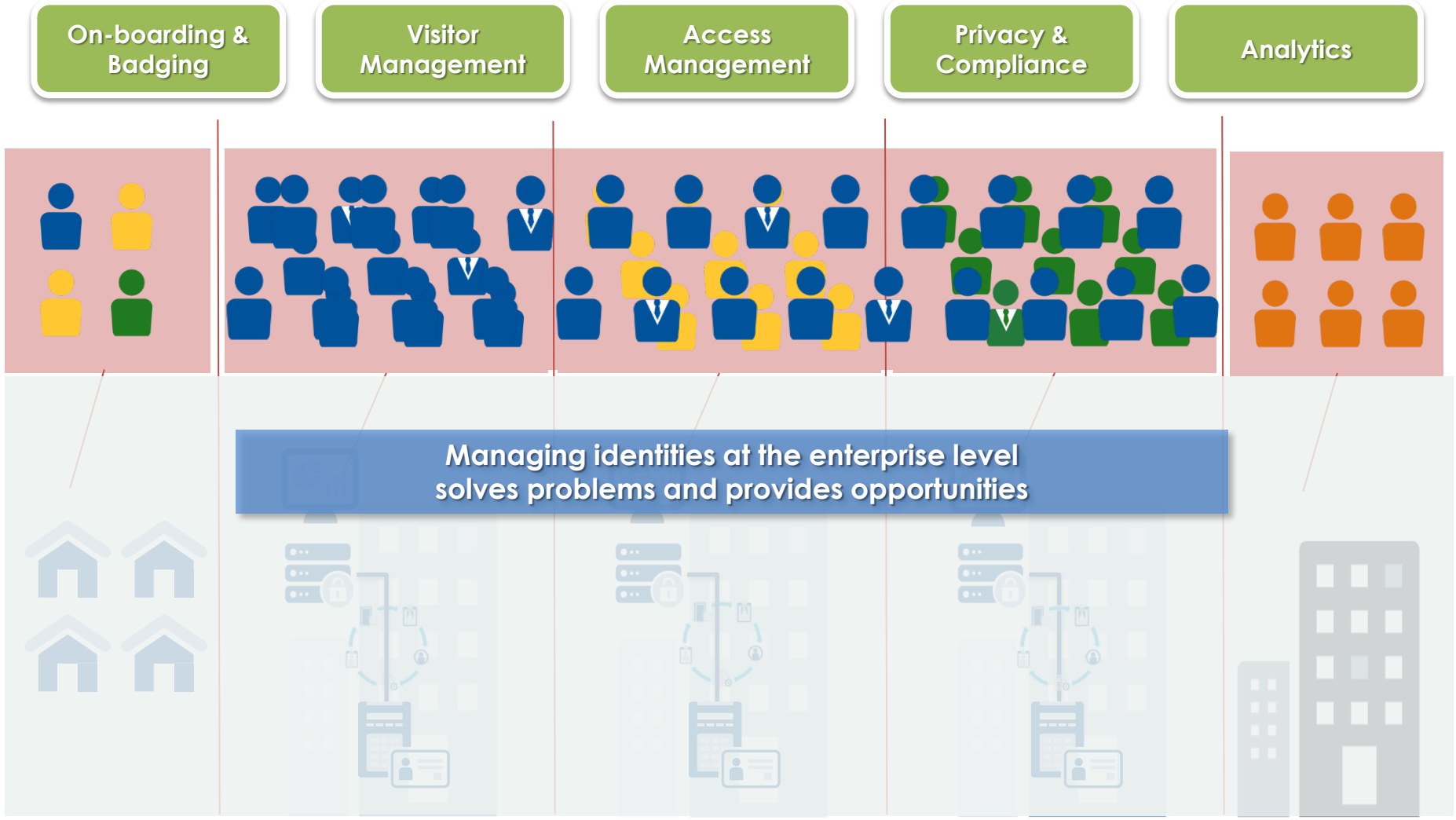


SAFE IDENTITY MANAGEMENT – LIKE GOOGLE DOCS

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



IDENTITY MANAGEMENT FOR THE ENTERPRISE



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

TEMPORARY ID CARDS – USE CASE

- 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?

REPORTING AND COMPLIANCE

- 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?

EU GDPR – GENERAL DATA PROTECTION REGULATION

- 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

IDENTITY ANALYTICS

- 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

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

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
  - Move and manipulate data across many systems
    - Swiftdata
  - Photo upload products
    - CloudCard, MyPhoto
  - Real time reporting
    - Tableau, Qlik, 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