Convergence of Identity and Access Management

Jan Lindquist, Cryptomathic

Won Jun, Intercede

Robert Lydic, Wavelynx

Natalie Bannon, Gallagher

Moderator: Jatin Deshpande, Giesecke & Devrient

IDENTITY & PAYMENTS SUMMIT

GOLD STANDARD (ENCRYPTION-BASED) SECURITY

We craft solutions that protect the most sensitive personal data from unauthorized access and meet strict compliance regulations. Our expertise spans four product lines:

KEY MANAGEMENT

MOBILE APP SECURITY

DIGITAL IDENTITIES & SIGNATURES

PAYMENTS

The art of cryptographic security requires us to be at the cutting edge of data and computer science. Every year, we invest millions into Research and Development to keep you and your customers safe.

30+ YEARS OF INNOVATION

30+ BLUE CHIP CLIENTS

30+ COUNTRIES SERVED

20+ INDUSTRIES PROTECTED

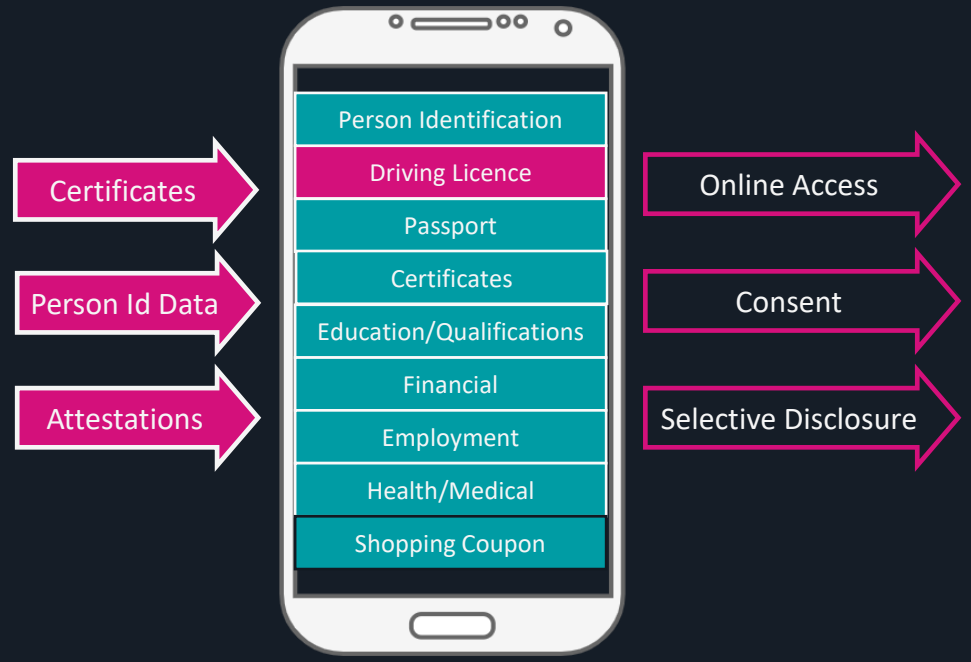
Copyright © 1986-2024 Cryptomathic.

WALLET APP SERVICES

CRYPTOMATHiC

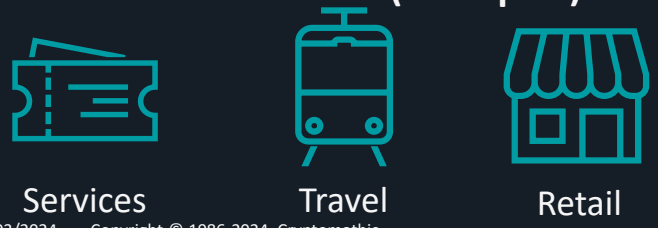
Qualified Providers (Issuers)

Consumer



Relying parties (examples)

Other Providers (Examples)



OpenID mDL

Other Relying Parties (Examples)

Copyright © 1986-2024 Cryptomathic.

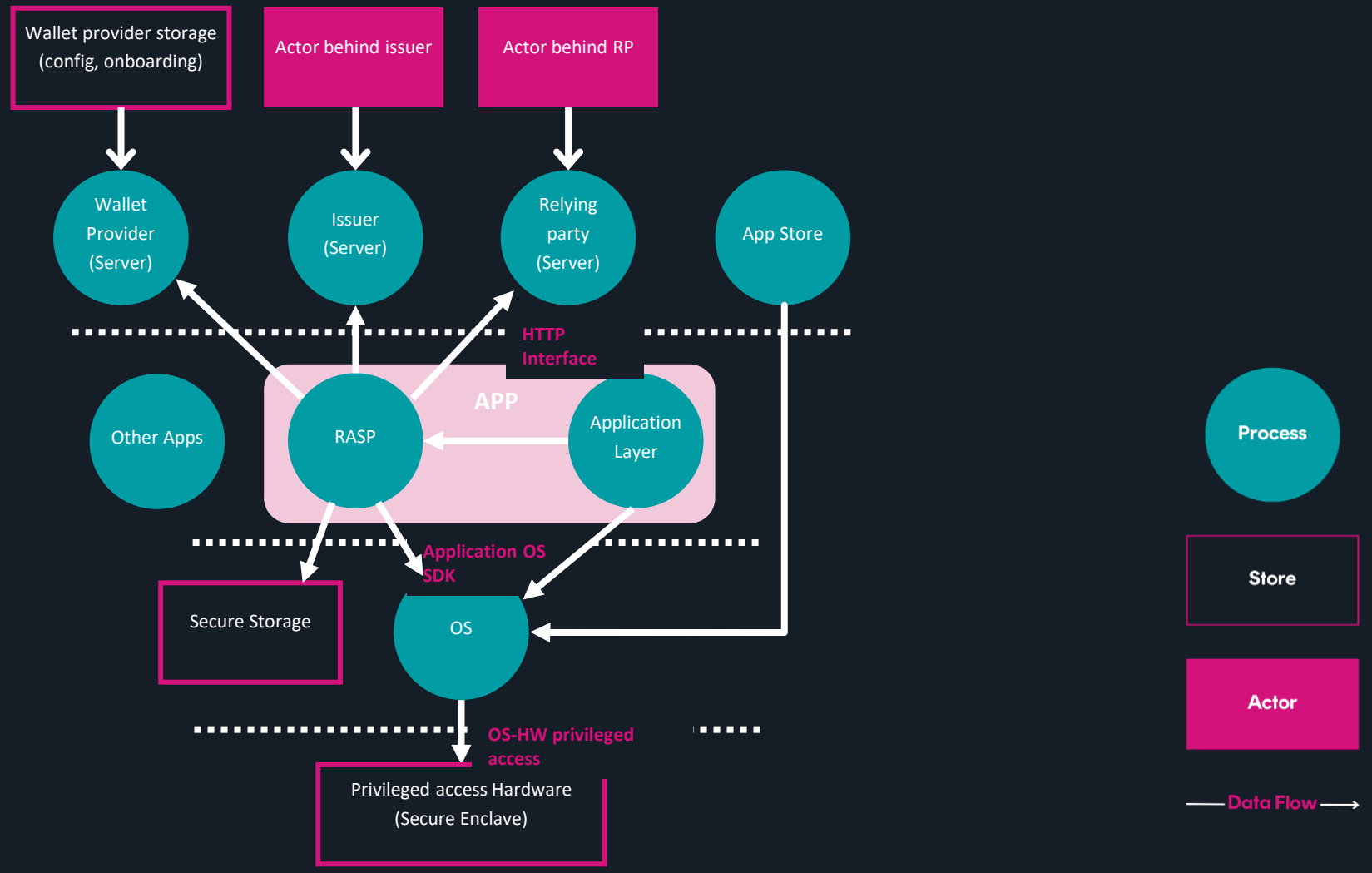
EU Funded Large Scale Projects

1. POTENTIAL – Pilots for European Digital Identity Wallet Consortium
   - Access to government services
   - Opening of a bank account
   - Registration for a SIM card
   - Mobile driving licence
   - eSignatures
   - ePrescriptions
2. EWC – EU Digital Identity Wallet Consortium
   - The storage and display of digital travel credentials
   - The organisation of digital wallets
   - The organisation of payments
3. NOBID – Nordic-Baltic eID Wallet Consortium
   - Authorisation of payments for products and services
4. DC4EU – Digital Credentials for Europe Consortium
   - Educational sector and the social security domain.

Copyright © 1986-2023 Cryptomathic.

APP(WALLET) VULNERABILITY ASSESSMENTS AND THREATS

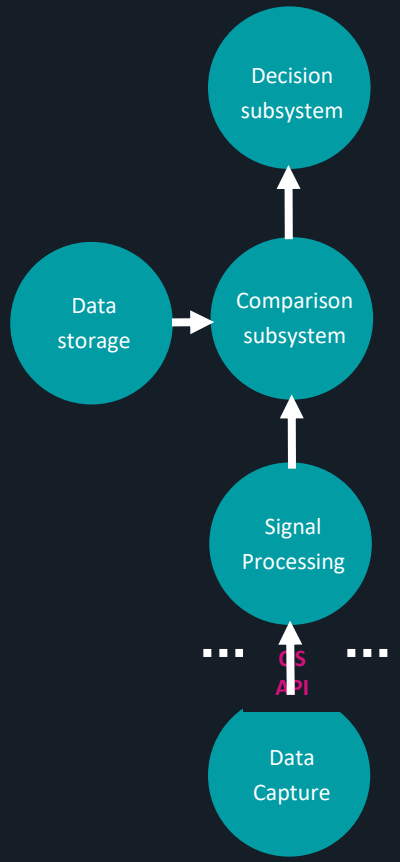
OWASP Threat Dragon is a modelling tool used to create threat model diagrams as part of a secure development lifecycle.



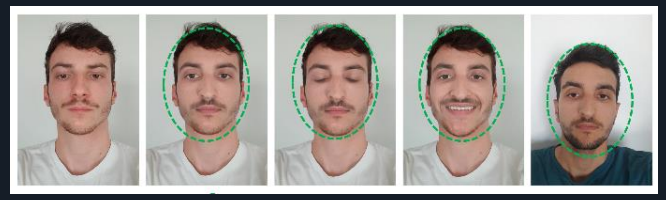
Copyright © 1986-2024 Cryptomathic.

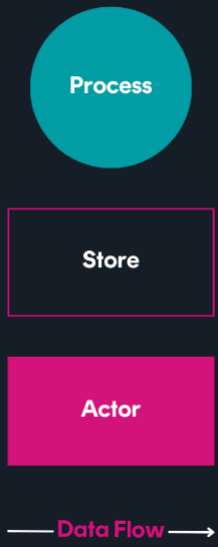
VIDEO CAPTURE VULNERABILITY ASSESSMENTS AND THREATS

OWASP Threat Dragon is a modelling tool used to create threat model diagrams as part of a secure development lifecycle.



How video injection attacks can even challenge state-of-the-art Face Presentation Attack Detection Systems (2023)





Copyright © 1986-2024 Cryptomathic.

THANK YOU

CRYPTOMATHiC

+46 (0) 730684942

Jan.lindquist@cryptomathic.com

JAN LINDQUIST
Product Manager
Mobile Application
Security Core

Copyright © 1986-2024 Cryptomathic.

wavelynx

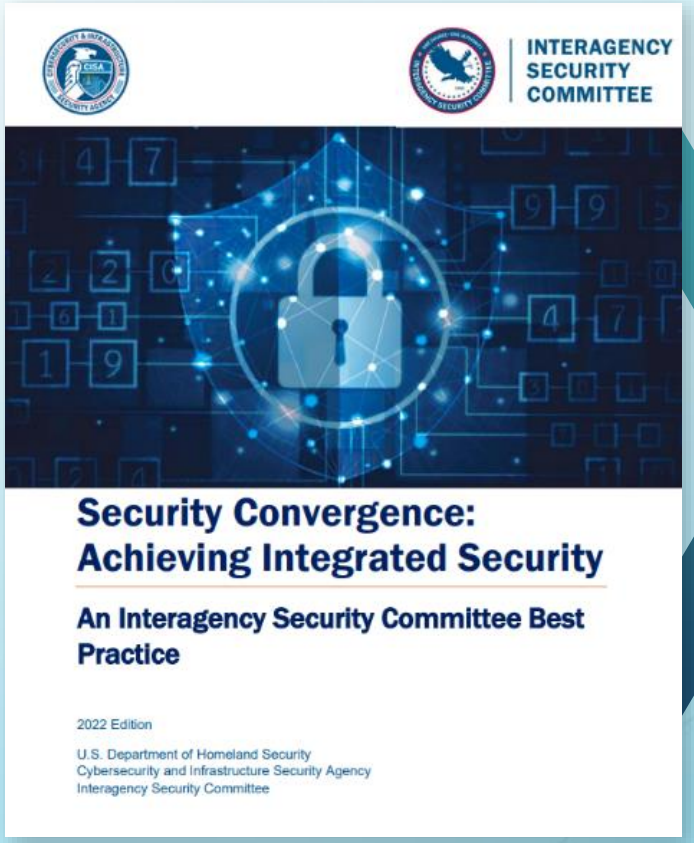
Robert Lydic

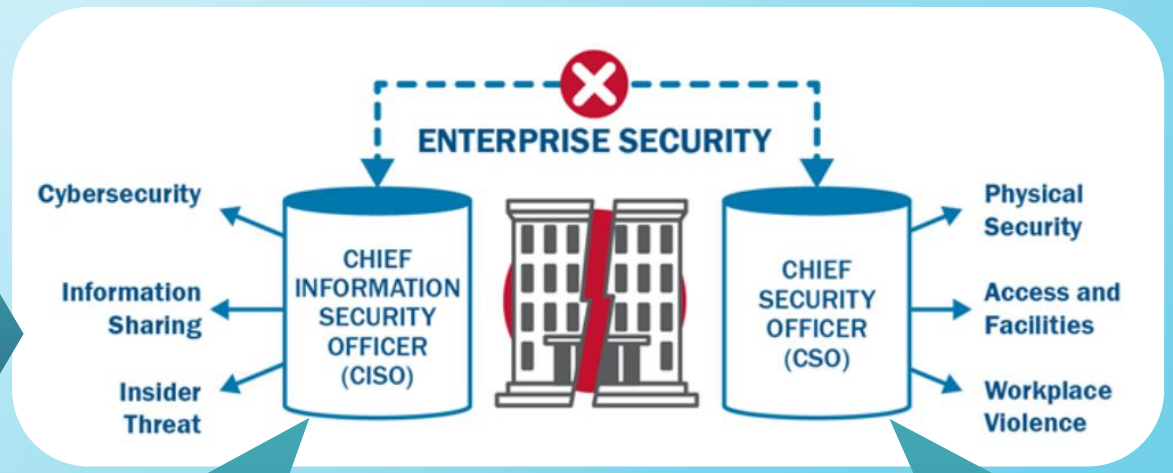
President | Wavelynx Technologies
rob@wavelynx.com
313.587.7300
www.linkedin.com/in/robertlydic/

IDENTITY & PAYMENTS SUMMIT

CONFIDENTIAL

Convergence is Happening: Physical & Wallet Credentials



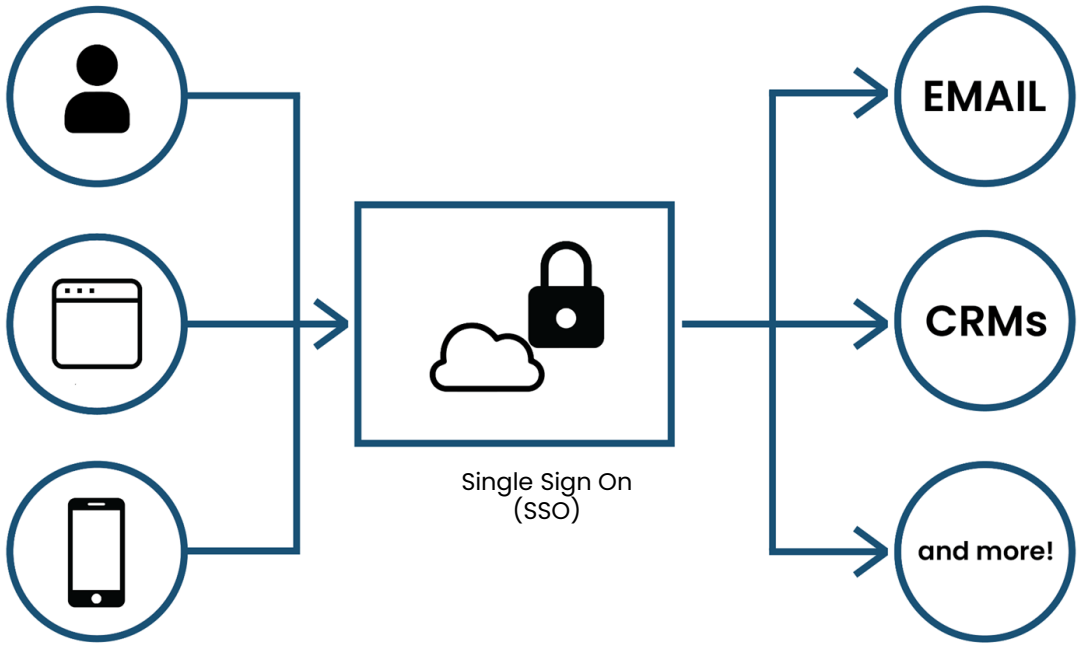


IAM, SSO, MFA, Network Access Credentials

Vetting, ID Credential, On/Off boarding

Access?

All Access to Systems, IP, Documentation



All Access to Facilities

Converged Physical Credential

125 KHz Prox®

DESFire® Ev3
LEAF Standards
NFC

PIV
FIDO passkey

HYPR

IDEMIA

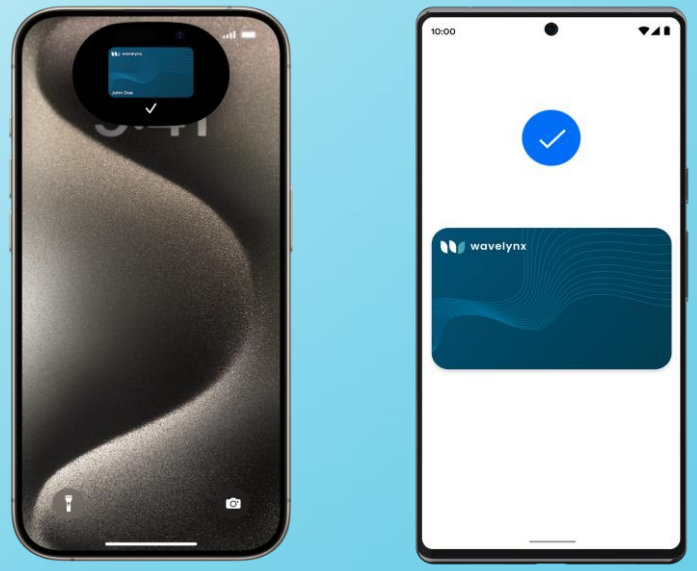
wavelynx

IDENTITY & PAYMENTS SUMMIT

CONFIDENTIAL

How Do Wallet Credentials Solve this?

- Leverage IT platforms for endpoint management to ensure device security
- Leverage IT platforms for SSO to ensure authenticated user
- Integrate physical access control software to automate lifecycle management of users, credentials, and permissions



Wallet Credentials

CONFIDENTIAL

Corporate SSO Identity

Why wallet?

- More secure than all other credentials
- Superior provisioning and administration
- Unparalleled user experience for all users

CONFIDENTIAL

Convergence of Identity and Access Management

Won J. Jun
Solutions Architect
Intercede

intercede

IDENTITY & PAYMENTS SUMMIT

About Intercede

MyID software manages millions of digital identities worldwide

Trusted by governments, large enterprises, military and police

More than 20 years domain expertise - feature-rich product and expert staff

Supported by a global partner network and our own UK and US offices

intercede

IDENTITY & PAYMENTS SUMMIT

Intercede capabilities

Registration and ID Verification

- Biographic data capture
- Fingerprint capture
- Facial biometric capture
- ID document validation
- Background checks
- 1:Many biometric matching

Credential Management

- Issuance policy
- Central and local issuance
- Lifecycle management
- Audit and reporting
- Key management
- PKI integration
- FIDO

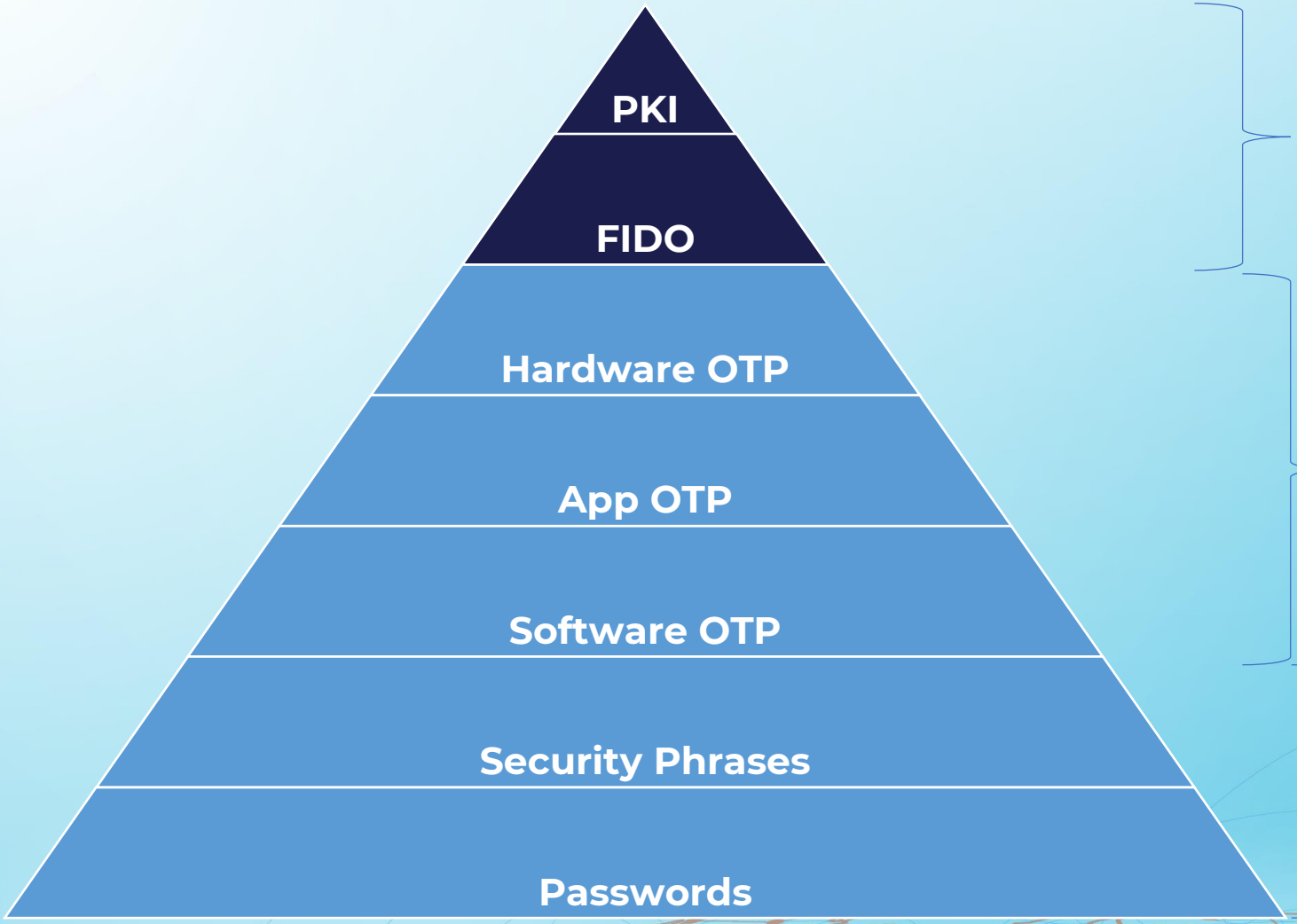
Multi-Factor Authentication

- FIDO
- Hardware OTP
- Push notifications app
- Software OTP
- Deviceless PIN grid OTP
- OTP over SMS

Password Security Management

- Compromised password check
- Password policy
- Policy enforcement

Stronger authentication from passwords to PKI



MyID CMS

MyID MFA

MyID PSM

intercede

IDENTITY & PAYMENTS SUMMIT

History of convergence in LACS and PACS

- 1990's: PACS was king. LACS was emerging.
- 2000's: LACS became more prominent. Visions of integrated LACS and PACS. iPhone introduced (2007).
- 2010’s: More advancement in convergence. FIDO introduced (2012). The mobile team emerges.
- 2020's: Disparate LACS and PACS convergence.

Reasons for slow convergence

- The tale of “two kingdoms”
- Shifting requirements
- Infrastructure changes
- Different vendor sets
- Technological advancements

Evolving requirements and landscape

- Mobile technology – “the third kingdom”
- Multiple personas (identities) and roles
- MFA options (software, hardware, hybrid)
- FIDO (Consumer → Enterprise)
- Password security management

Current trends in convergence

- Federated IDs and open specifications
- Smart cards and tokens
- Mobile (MDMs)
- FIDO (Enterprise)
- Biometrics
- Digital wallets

“Everything is converging”– One size does not fit all.

Convergence from our customers' view

- Higher assurance logical and physical access (Gov, Intell)
- Modernization of PACS. REST API integration. (e.g., On-demand revocation)
- Identity and access management governance
  - On-boarding
  - Process integration

  (Ex.: Onboard in Sailpoint, pass identity into CMS, then to LACS and PACS.)
  - Central identity orchestration point
  - Can reduce cost, increase security
- Data breaches addressed

Thank you!

Won J. Jun
Solutions Architect

Email: won.jun@intercede.com
Office: +1 888 646 MYID

https://www.linkedin.com/in/wonjun/
www.Intercede.com

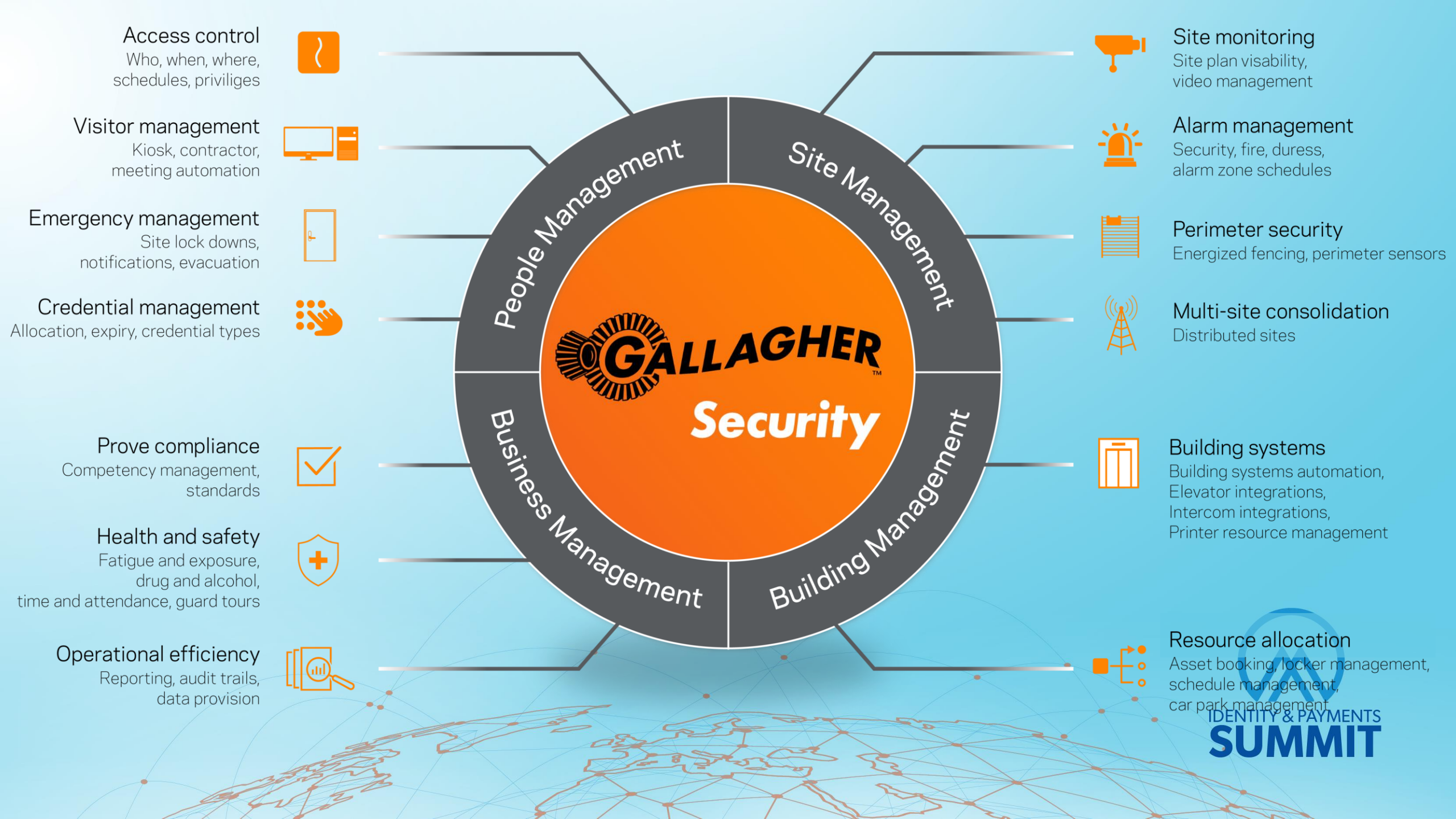
IDENTITY & PAYMENTS SUMMIT

intercede

Business Value of Identity Convergence in Physical Access

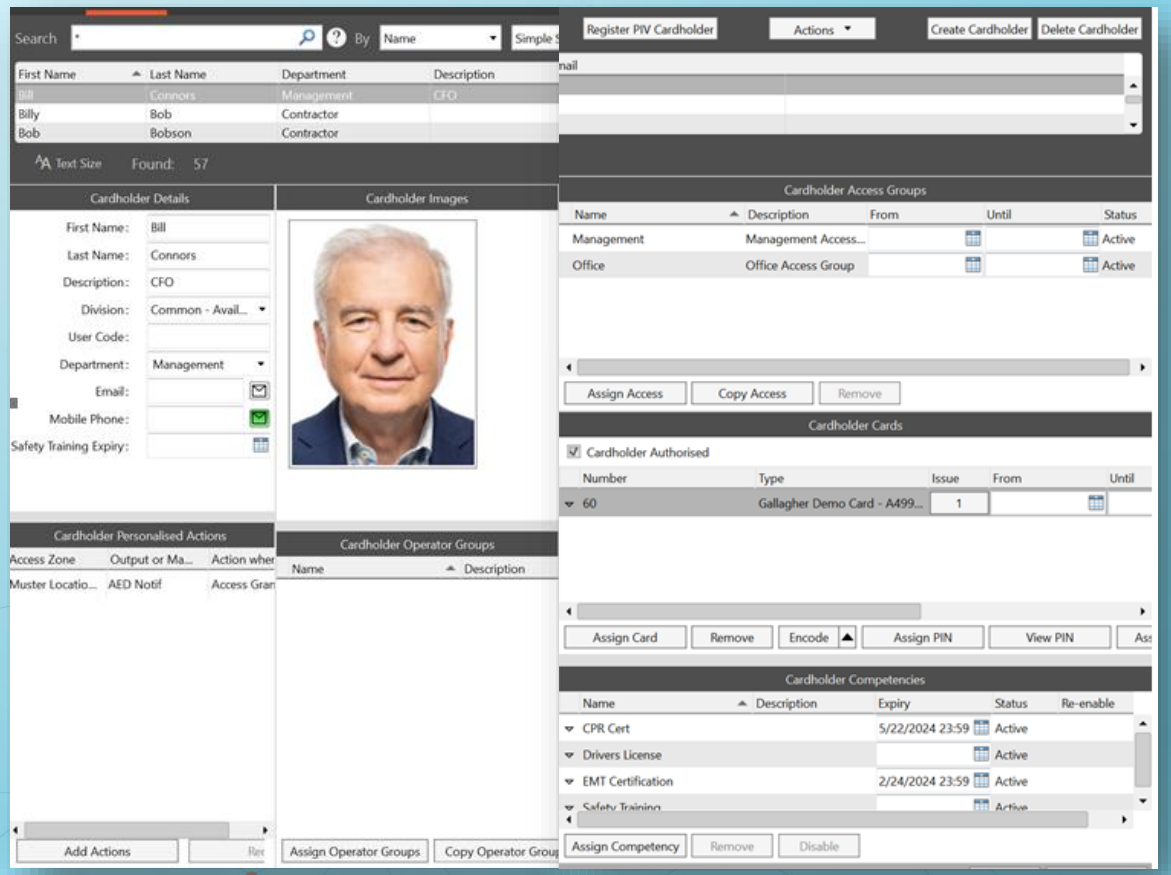
Natalie Bannon
Director Strategic Alliances, Americas
Gallagher Security
natalie.bannon@gallagher.com | 314.591.4605

IDENTITY & PAYMENTS SUMMIT


Access control
Who, when, where, schedules, priviliges
Visitor management
Kiosk, contractor, meeting automation
Emergency management
Site lock downs, notifications, evacuation
Credential management
Allocation, expiry, credential types
Prove compliance
Competency management, standards
Health and safety
Fatigue and exposure, drug and alcohol, time and attendance, guard tours
Operational efficiency
Reporting, audit trails, data provision
People Management
Site Management
Business Management
Building Management
GALLAGHER
Security
Site monitoring
Site plan visability, video management
Alarm management
Security, fire, duress, alarm zone schedules
Perimeter security
Energized fencing, perimeter sensors
Multi-site consolidation
Distributed sites
Building systems
Building systems automation, Elevator integrations, Intercom integrations, Printer resource management
Resource allocation
Asset booking, locker management, schedule management, car park management
IDENTITY & PAYMENTS
SUMMIT

Cardholder Info Pull from Systems

- Personal Information
- Competencies
  - Trainings
  - Certificates
- Access
  - Locations
  - Machines
  - Workstations
  - Parking Spots
- Personal Data Fields
  - Computer User ID
  - Parking Pass #
  - Contractor Name
  - Favorite Ice Cream Flavor
- Credentials



IDENTITY & PAYMENTS SUMMIT

Shuttle Bus Use Case

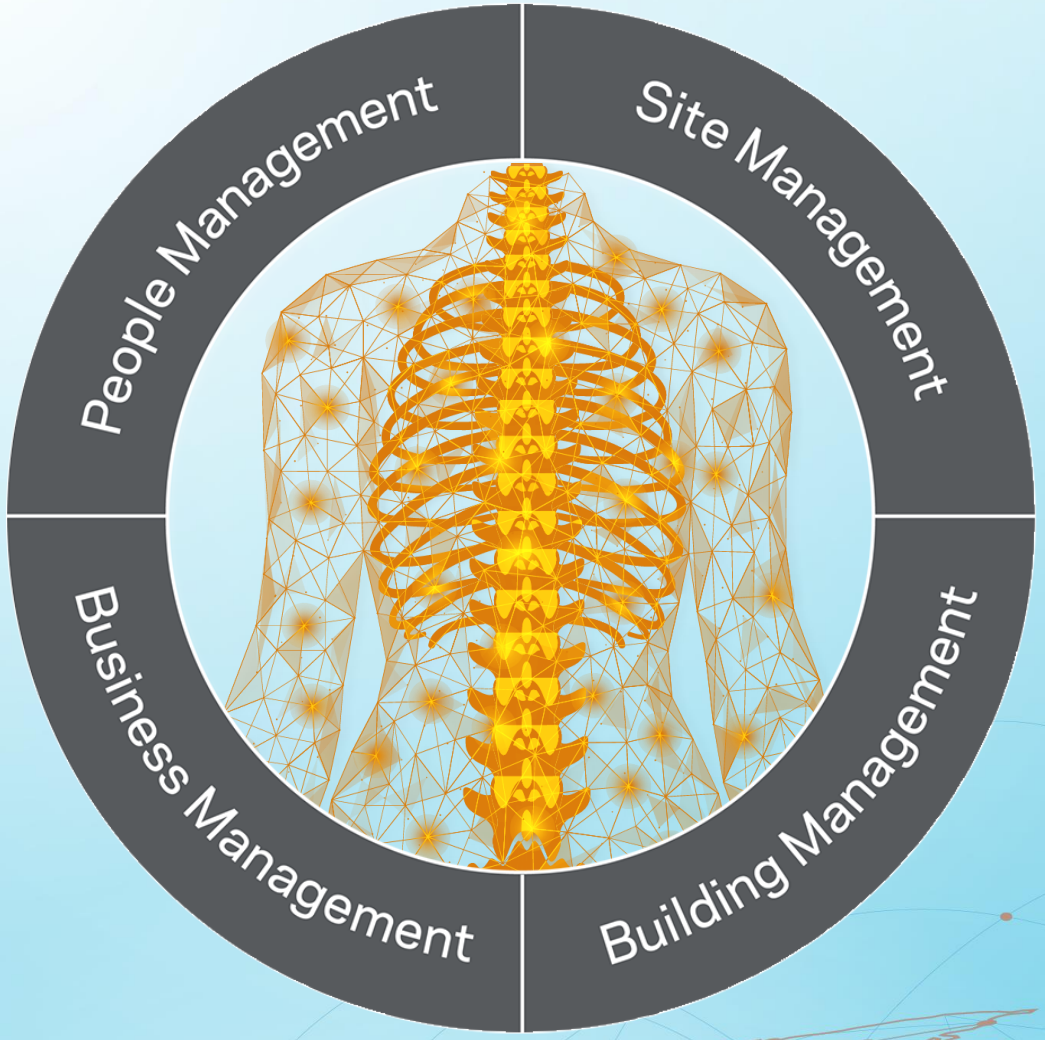
- Access control not to open doors
- Identity leveraged to know who they are
- Business continuity benefits
  - Show up for shift
    - Tied to HR scheduler
  - Additional worker needed
  - Mining – ability to clear blast zones quickly

IDENTITY & PAYMENTS SUMMIT

Forklift / Machinery Use Case

- Enforcing compliance requirements
- Tied to LMS
- Notifications & alerts, warnings
- Audit trails & reports

Global Customer Example



14 Systems
26 Integrations

- Automatic provisioning & access from AD & HR systems
- Space Utilization – conference rooms, parking spaces, lockers
- Employee location tracking
- Shuttle bus
- Ordering corporate clothing
- Time & attendance
- Credential management
- Competency management – machine safety, workstation access
- Randomized drug testing
- Temperature checks during pandemic
- Reports, event data analysis
- BACnet integration for HVAC & lights
- Access control & intrusion
- Perimeter detection – multiple solutions

IDENTITY & PAYMENTS SUMMIT