Mobile Access is the Killer App
The Path to Flexible, Secure Credentials
Brandon Arcement – Senior Director, Product Marketing
April 8, 2019
Do You Remember the First Time You Saw This?
It's a New World
Credential Requirements

Security

Applications

Mobility

Agenda

The Status Quo

Selecting the Right Credential Solution

Mobile Access

How to Upgrade
The Status Quo - Vulnerabilities
The Status Quo - Vulnerabilities

On “secure” smart cards:

- Unencrypted Card Serial Number
- Poor key management
- Unencrypted data payload
- Identifier marked on the credential
- Open, untracked format
- Reader configuration supporting legacy technology
- Unencrypted communication from reader to panel
The Status Quo – Limited Multi-Application

- Cashless Payment for School Store, Food Service, Vending, Laundry
- Library Check-out
- Logical Access to Workstations and Networks
- Physical Access to Campus Buildings, Labs, Residence Halls
- Secure Print Authentication
- Time and Attendance
- Parking and Transit
The Status Quo – No Path to Mobile

Most technologies deployed today do not provide a path to mobile access

- Reader infrastructure not capable of transition
- Common cross-platform credential model not considered
Disparate Cross-Platform Credential Models

Cards

Mobile Devices

Reader Firmware

Card

iOS App

Android App

iOS eSE

Android eSE

Wearable 1

UID: 123456789
The Status Quo - Summary

- Vulnerabilities in Technology or Implementation
- Limited Multi-Application Support
- No Path to Mobile Access
Selecting the Right Credential Solution

Security
Applications
Mobility
Selecting the Right Solution – Security
A Holistic, Secure Credential Program

- Secure Technology is Foundational
- The Key is Key
- Strong defense has Layers
- Keep Credential Number Private
- Track the Format
- Remove the Weak Link
- Lock the Back Door

Selecting the Right Solution – Security
A Holistic, Secure Credential Program

- Secure Technology is Foundational
- The Key is Key
- Strong defense has Layers
- Keep Credential Number Private
- Track the Format
- Remove the Weak Link
- Lock the Back Door
Selecting the Right Solution - Applications

Leverage technology that makes it possible to incorporate an increasing number of physical, logical, and extended applications:

- Building access
- Secure print authentication
- Time and attendance
- Cashless vending
Selecting the Right Solution - Mobility

Evaluate solutions that offer the freedom to choose

- Device form factors - Card, Phone, Tablet, Wearable...
- Semiconductor platforms - NXP, Infineon, EM...
- Operating systems - iOS, Android, Tizen...
- Readers - Wall readers, Locks, USB readers, embedded devices...
- Communications protocols - NFC, Bluetooth...

...to address your future needs
Mobile Credentials – The Next Frontier

https://www.youtube.com/watch?v=hhvNr3nJ2OA
Common Cross-Platform Credential Model

UID: ????????

Reader Firmware

Seos

Mobile Devices

Cards
Seos Credential Technology

Expanded Device Choice

Multiple Access Applications

Highly Secure Encryption
HID Mobile Access
Bringing the Magic Back to PACS
9 Years of Experience in a Dynamic Market

- **2009**: ASSA ABLOY starts world’s first SIM-based Hotel pilot.
- **2010**: ASSA ABLOY develops SIM-based MIFARE solution.
- **2011**: ASSA ABLOY creates solution with MIFARE and bridge technologies.
- **2012**: Arizona State University pilots microSDs and iPhone Sleeves with HID. Lack of native phone support stops pilot.
- **2013**: HID runs a several SIM-based Seos pilots with different MNOs.
- **2014**: ASSA ABLOY creates HCE proof-of-concept. Apple Pay is launched. Based on NFC and eSE.

**Key Events**:
- **2009**: Mifare4Mobile 1.0 is published. Only one card active simultaneously. Closed environment for managing credentials. Unusable specification.
- **2010**: Slow uptake on NFC phones. Mobile operators struggle to launch SIM solutions.
- **2012**: BlackBerry starts working on an embedded SE solution with MIFARE. Basically no services have been launched.
- **2013**: Samsung announces an embedded SE NFC solution with Visa. Basically no services have been launched.
- **2014**: Apple Pay is launched. Based on NFC and eSE.
Integrated Architecture

You Choose:
- HID User Interfaces
- Cloud API & App SDK

PACS / IAMS

Credential Admin

API

HID Platform

Mobile ID
HID Mobile Access
Two Original Modes of Operation

**Tap**

Like with prox cards

**Twist & Go**

Closest door will unlock
Android Wear & Apple Watch
Widget & 3-D Touch

- Swipe Right
- Press Firmly
Supported Devices List

250+ Devices
NFC vs. Bluetooth

**NFC Card Emulation**
- Supported by iCLASS SE readers
- Short Range
  - Tap only
- Performance similar to card
- Android only

**Bluetooth**
- Supported by iCLASS SE readers
- Short & Long Range
  - Tap, Twist & Go, Wearables, Widget, 3-D Touch
- Less consistent than card
- Android & iOS
Apple June Announcement

ASSA ABLOY Helps Enable Contactless Student IDs in Apple Wallet

ASSA ABLOY will leverage its expertise in mobile access to support Apple’s efforts to make it easier to access dorm rooms with contactless student IDs.

Nico Delvaux
CEO; ASSA ABLOY
Mixed Populations
Mobile Devices with Legacy Credentials
Benefits of Mobile Access

- More User Convenience
- Greater Operational Efficiency
- Higher Security
Benefits of Mobile Access

**More User Convenience:**
Enable building occupants to use smartphone, tablet, or wearable to enter controlled areas

- Fewer items to carry
- Lost or forgotten cards no longer a problem
- Remote, over-the-air credentialing
- Extended read range for special applications
- Adds to perception of innovative environment
- No online connectivity required; Background operation
Benefits of Mobile Access

Greater Operational Efficiency:
Make physical access administration easier with digital, online processes

- Physical credential management transforms to digital experience
- Over-the-air credentialing of remote workers and visitors
- Streamlined operations with easy integration to PACS, visitor management, and other systems
- Sustainable process with reduced waste and lower carbon footprint
Benefits of Mobile Access

**Higher Security:**
Provide higher levels of authentication

- Seos technology used to secure credential
- Mobile devices are rarely forgotten, lost, or stolen
- Missing mobile devices are reported almost immediately
- Easily de-provision unauthorized devices; revoke credentials over-the-air
- Applications can be protected with biometric and/or passcode
- Vulnerabilities can be addressed quickly through remote update
Common Concerns About Mobile Access

Won’t Work with Dead Battery

No Visual Authentication of Identity

Express Cards with power reserve
If iOS isn’t running because iPhone needs to be charged, there may still be enough power in the battery to support Express Card transactions.

Supported iPhone devices automatically support this feature with:
• A transit card designated as the Express Transit card
• Student ID cards with Express Mode turned on
Simple and Free to Register

How to Upgrade
Steps to Upgrade
Best Practices
Cation Areas
## Migration Options – Pros/Cons

<table>
<thead>
<tr>
<th>Single Tech Cards</th>
<th>Cost neutral credentials</th>
<th>Reconfigure all readers More expensive readers Replace all credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi Tech Cards</td>
<td>Replace only remaining legacy credentials</td>
<td>Reconfigure all readers More expensive readers More expensive credentials (temp)</td>
</tr>
<tr>
<td>Readers First</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multi Tech Cards</td>
<td>No reconfiguration of readers Less expensive readers Replace credentials only once Risk appropriate reader upgrades</td>
<td>More expensive credentials</td>
</tr>
<tr>
<td>Credentials First</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
How to Upgrade
Best Practices

✔ Site survey and complete inventory of existing technologies as a first step

✔ Support as few legacy technologies as possible

✔ Choose new solution capable of mobile access

✔ Build your own mobile app

✔ Start small – execute successfully at one building, then repeat
How to Upgrade
Caution Areas

- Don’t procrastinate: Set target dates for completion
- Consider and manage performance expectations
- Use common, managed credential format
- Set expectation for reader hardware refresh cycle
- Validate service provider security assertions
  - Ask about key management practices
  - ISO27001 Certification
Invest in Solutions that Demonstrate **Choice**

Supports:
- Cards and Mobile Devices
- Smartphones, Tablets, and Wearables
- Multiple Secure Element Hardware Platforms
- iOS, Android, and Other operating systems
- NFC, Bluetooth, and beyond

Independent of:
- Transaction System
- Access Control Host
- Reader/Credential service provider
For more information

Brandon Arcement - barmacemt@hidglobal.com
Brett St. Pierre - bstpierre@hidglobal.com