Advancing Student Identity: Think outside the card

NFC Technology Turns Smartphones Into Into Secure Credentials

Serra Luck

27 May, 2013

Open NFC Versus Secure NFC

- **Open NFC is primarily used for transactions that do not require a high level of security**
  - Does not require the use of a secure element to store identity
  - Drawbacks when used for mobile access extend beyond the lack of security
- **Secure NFC is primarily used for transactions that do require a high level of security**
  - Requires the use of a secure element to store identity
  - Provides a high degree of security, privacy and user convenience

Use of Open NFC or Secure NFC for mobile access control should be based on risk appropriate authentication!

NFC Card Emulation

- Idea:
  - The phone emulates a card, the host does not need to know about it;
  - it can be provisioned remotely;
  - the card becomes virtual
- Which SE technology: SE on SIM, eSE, µSD?
- How to get the virtual card there?
- How many virtual cards can be there simultaneously?
- Can we switch between them?
- How do we provision it from the phone?

The Mobile Access Model

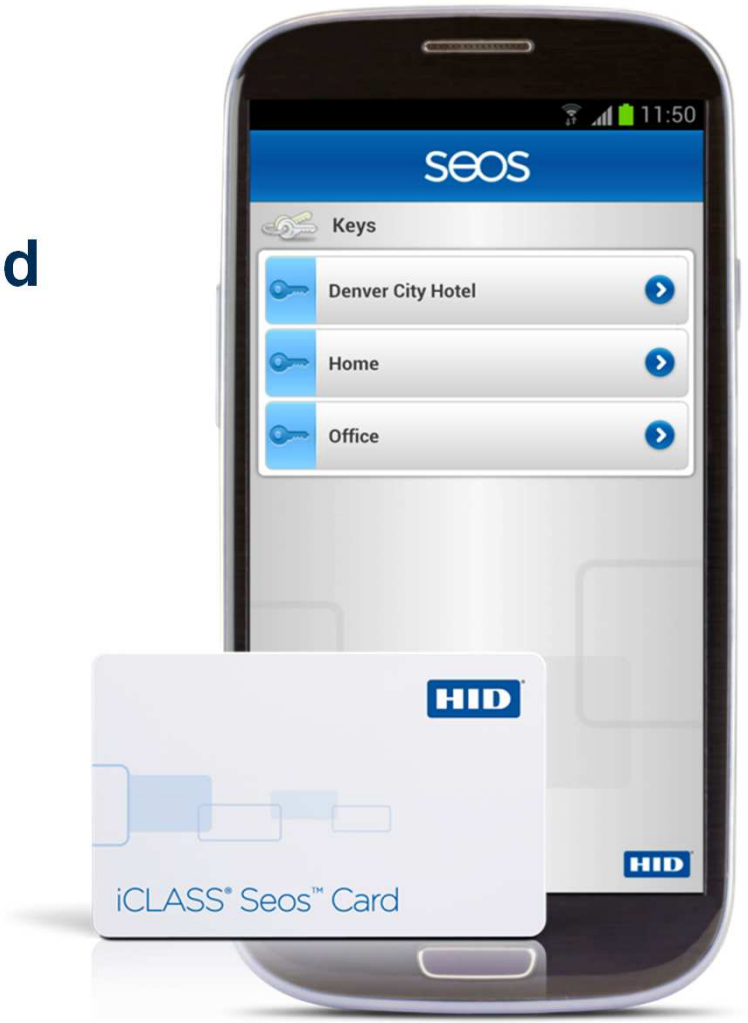
Keys and access cards in your daily life

Converged in your NFC-enabled smartphone

Used to open different types of doors and Windows®

What's Important to Users

- **Users want convenience**
- **System administrators seek flexibility**
- **Multiple digital keys are required simultaneously**
  - And allow me to choose the correct key quickly
- **Digital keys must be secure and private**
- **The solution must be available on multiple types of handsets and in a card form factor**

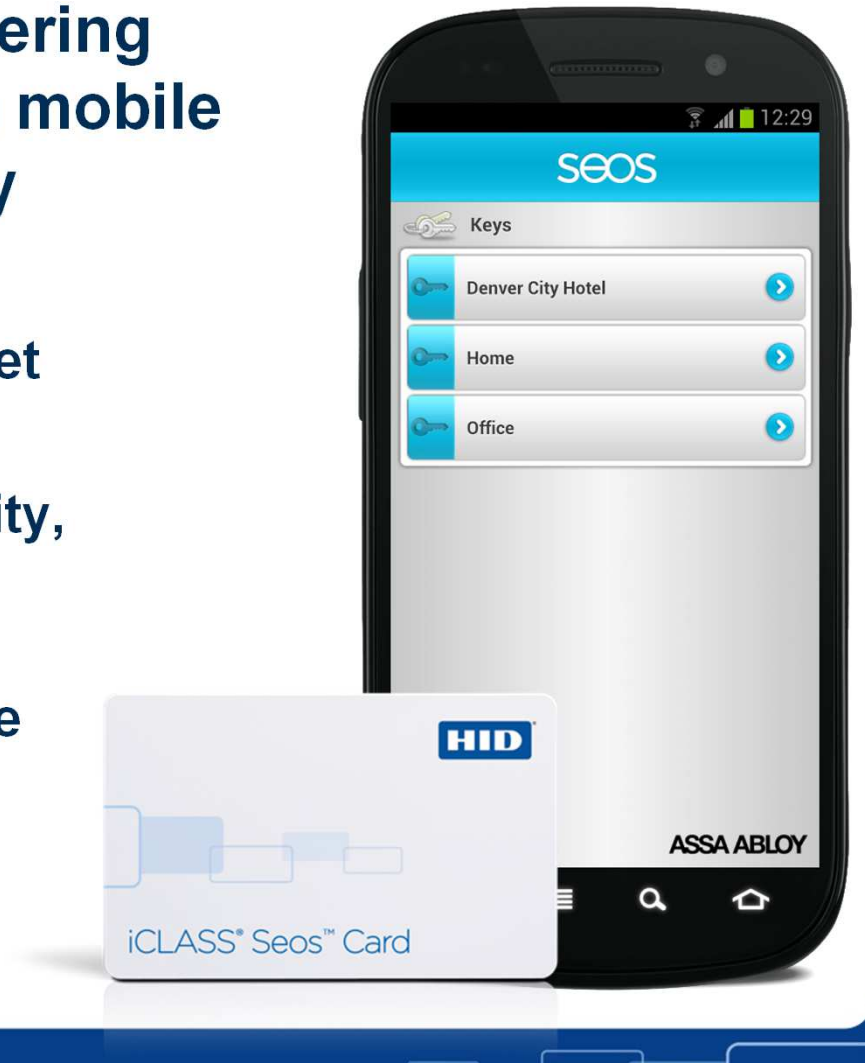


The Technology Vision

- **A single applet instance must:**
  - Support many independent applications (digital keys) simultaneously
  - Offer an “always on” mode such that no end-user intervention is necessary
  - Offer multiple configurations for user selection
  - Be scalable and support fast selection
- **There must be a rich user interface (app)**
  - Offer the ability to see and manage all digital keys from the user interface
- **The technology itself must be:**
  - Easily portable to any standard Java-card based secure element or UICC
  - Based on open architecture based on open standards
  - Highly secure with a high level of privacy

What is Seos?

- Seos™ is the world's first commercial ecosystem for issuing, delivering and revoking digital keys on mobile phones with NFC technology
- Seos is:
  - A legacy free card command set
  - Designed for access control
  - With a specific focus on security, privacy and an enhanced user experience
  - When implemented on a mobile smartphone



A Quick Technical Comparison

Feature	*MIFARE*	*DESFire*	*iCLASS*	*Seos*
Full privacy support		√		√
NSA Suite B Cryptography		√		√
Uses only NIST approved security				√
Full ISO/IEC 14443-4 support				√
Full emulation on standard Java Card				√
Multiple active cards seamlessly		√		√
Decentralized and scalable				√
Mobile extensions				√

The “Nuts And Bolts” Required To Facilitate Mobile Access

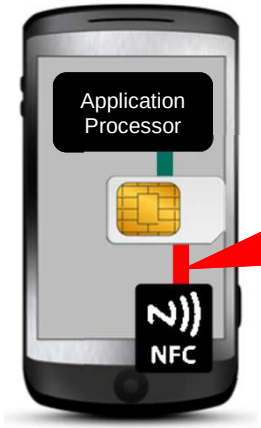
NFC-enabled handsets

NFC-enabled readers, electromechanical locks and a wide ecosystem of third-party hardware

Ecosystem of mobile network operators (MNOs), Trusted Service Managers (TSMs) and others to deliver and manage mobile credentials

Ways to Enable Handsets

- **SIM Centric**
  - Need to integrate with the Mobile Network Operators (MNOs)
- **Embedded Secure Element (eSE)**
  - No need to integrate with the MNOs
  - Must integrate with the handset manufacturers
- **Alternative Form Factors:**
  - NFC microSD cards or add-ons such sleeves/cases
  - No need to integrate with the MNOs or the handset manufacturers



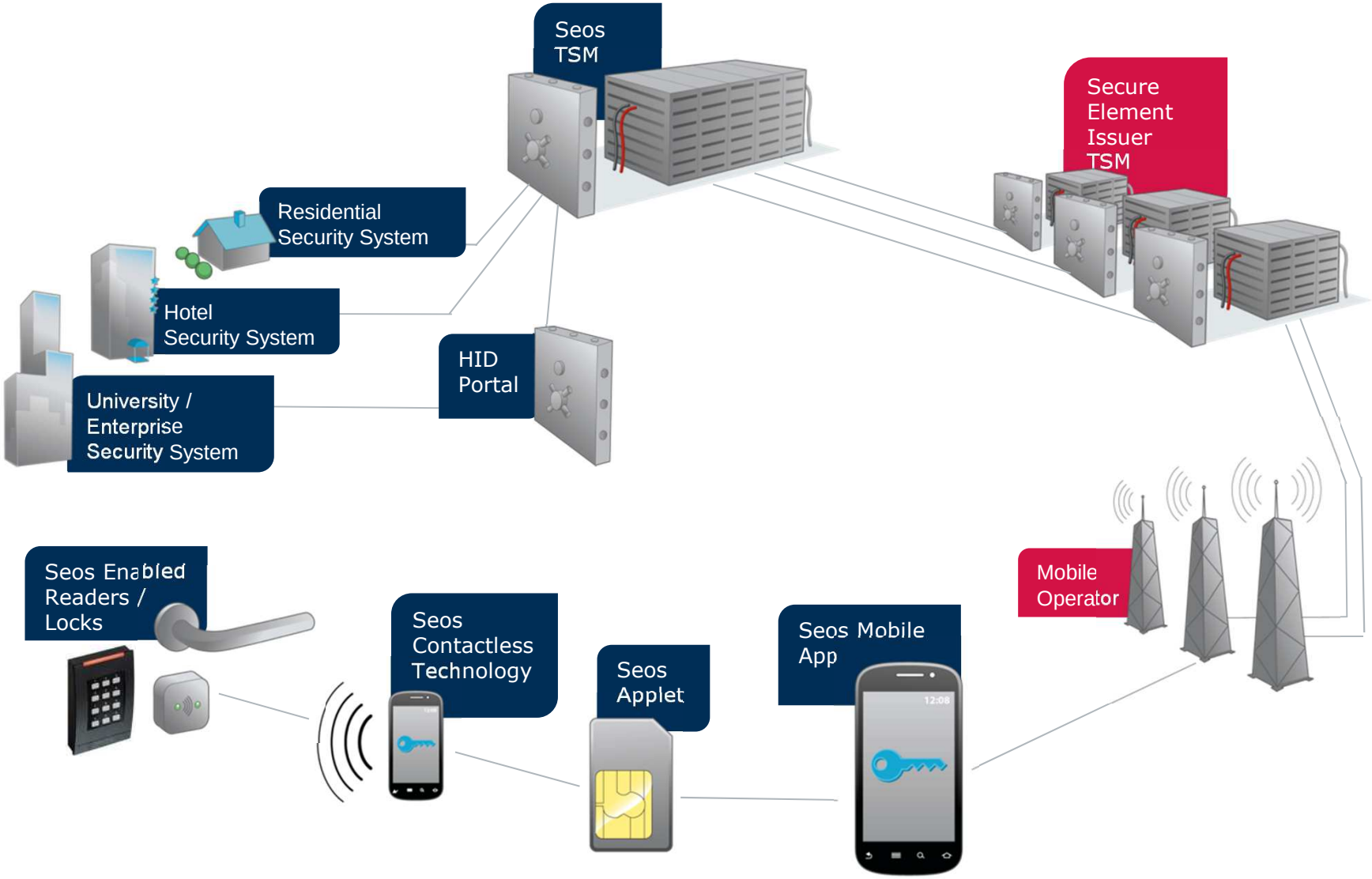
SIM-NFC connection through a single, wired interface

NFC-Enabled Reader Hardware

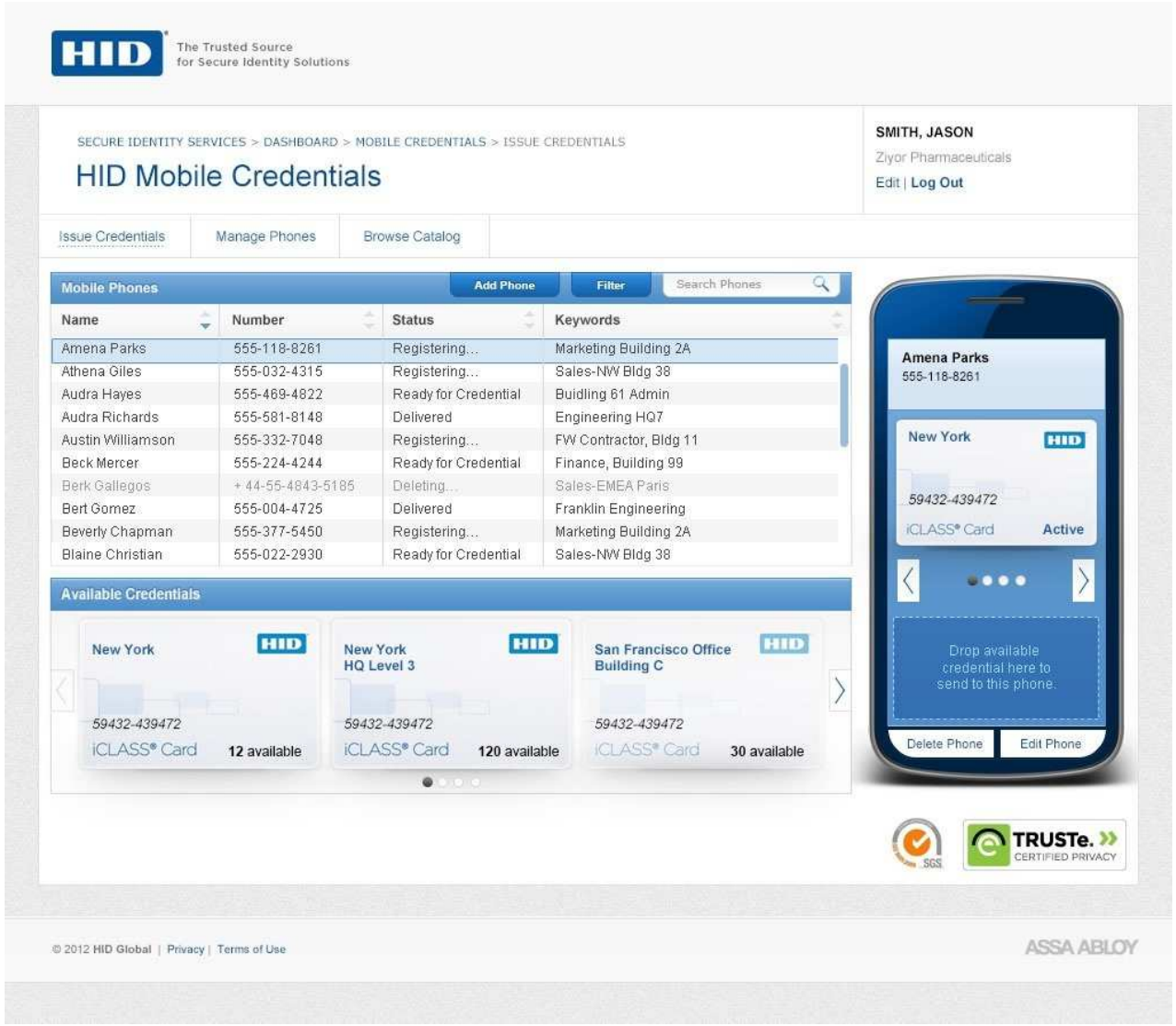
Seos-enabled NFC smartphones require complementary hardware:

- On-line HID iCLASS SE® readers
- Electromechanical locks
- Residential Locks
- Desktop readers
- Third-party hardware for a variety of applications:
  - Time and attendance
  - Secure print authentication
  - Biometric template storage

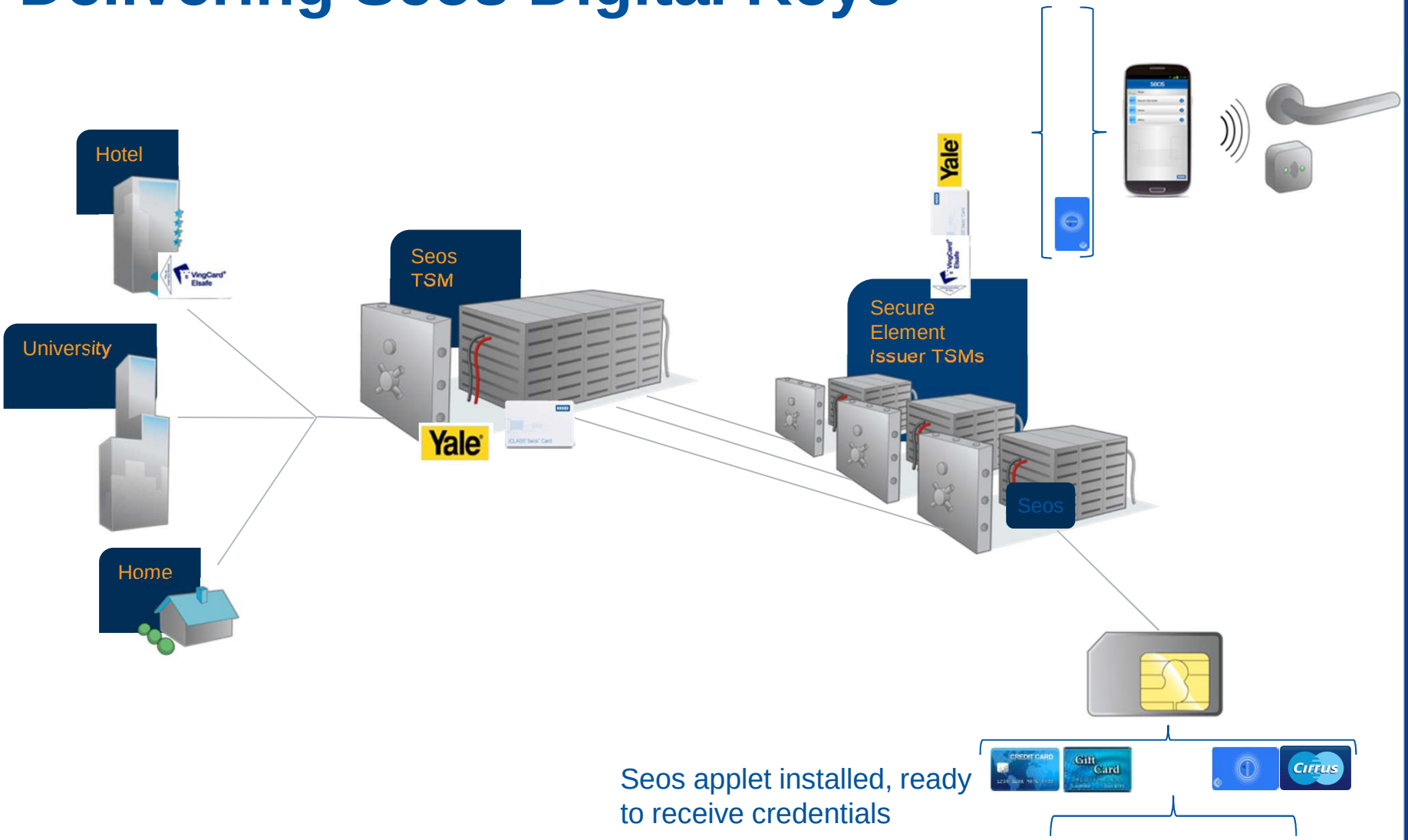
Seos: Powering Mobile Access



HID Secure Identity Services™ Portal



Delivering Seos Digital Keys



Seos applet installed, ready to receive credentials

Handset Update

- **RIM / BlackBerry® Devices**
- **Android™ Devices**
- **Microsoft / Windows® 8 Devices**
- **Apple® iOS Devices**
  - iPhone 5 does not have NFC

Seos Provides…

- **Convenience to users**
- **Flexibility for system administrators**
- **Simultaneous use of multiple digital keys**
  - The reader can choose the key for the user
- **Secure and private digital keys**
- **Functionality on multiple handsets, SIMs and embedded secure elements, and cards**

What Should I Do Now?

- **Prepare for the future use of mobile access by installing and using iCLASS SE readers**
  - These readers support a wide range of technologies including HID and Indala proximity, iCLASS, MIFARE and Seos for mobile access
  - These readers will also support Seos cards and mixed environments
- **Become educated about the "nuts and bolts" of mobile access**
  - Understand the various mobile access offerings and how to differentiate between them
- **Ask your mobile network operator to support Seos in NFC-enabled smartphones**
  - Mobile network operators need to know that the market is ready to embrace the use of NFC for mobile access control

Videos

- Arizona State University: http://www.youtube.com/watch?v=d4NmYdMAAHU
- Netflix: http://www.youtube.com/watch?v=KLEoF8wwAKA
- Good Technologies: http://www.youtube.com/watch?v=AHVk1UJqkGE
- Seos: http://www.youtube.com/watch?v=hM5enp7vvcM

For More Information…

Serra Luck

Director, Mobile Access Solutions
HID Global
+49 174 3141498

+90 546 5141498
sluck@hidglobal.com