Interagency Advisory Board

Meeting Agenda, Wednesday, February 22, 2012

1. **Opening Remarks** *(Mr. Tim Baldridge, IAB Chair)*

2. **Generic Identity Command Set (GICS): Leveraging PIV to Build a Standard Platform for ID Tokens** *(Ketan Mehta, NIST)*

3. **Continuing to Move ICAM into Mobile Computing** *(Owen Unangst, USDA)*

4. **The Movement to Use PIV-I** *(David Belchick, CitiBank)*

5. **NXP and HID Global Enable Mobile Access for NFC Phones Enabling Options for Storing and Managing PIV(-I) Credentials on Mobile Devices** *(Julian Lovelock, HID/Actividentity)*

6. **Cross-Agency Federation: A Demonstration of Federated Identity Trust within the Federal Government and Industry at Level of Assurance 4** *(Tim Baldridge, NASA, and Bob Gilson, DoD)*

7. **Closing Remarks** *(Mr. Tim Baldridge, IAB Chair)*

Options for storing and managing PIV credentials on mobile devices

Julian Lovelock, VP Product Marketing
ActivIdentity, part of HID Global
April 2012

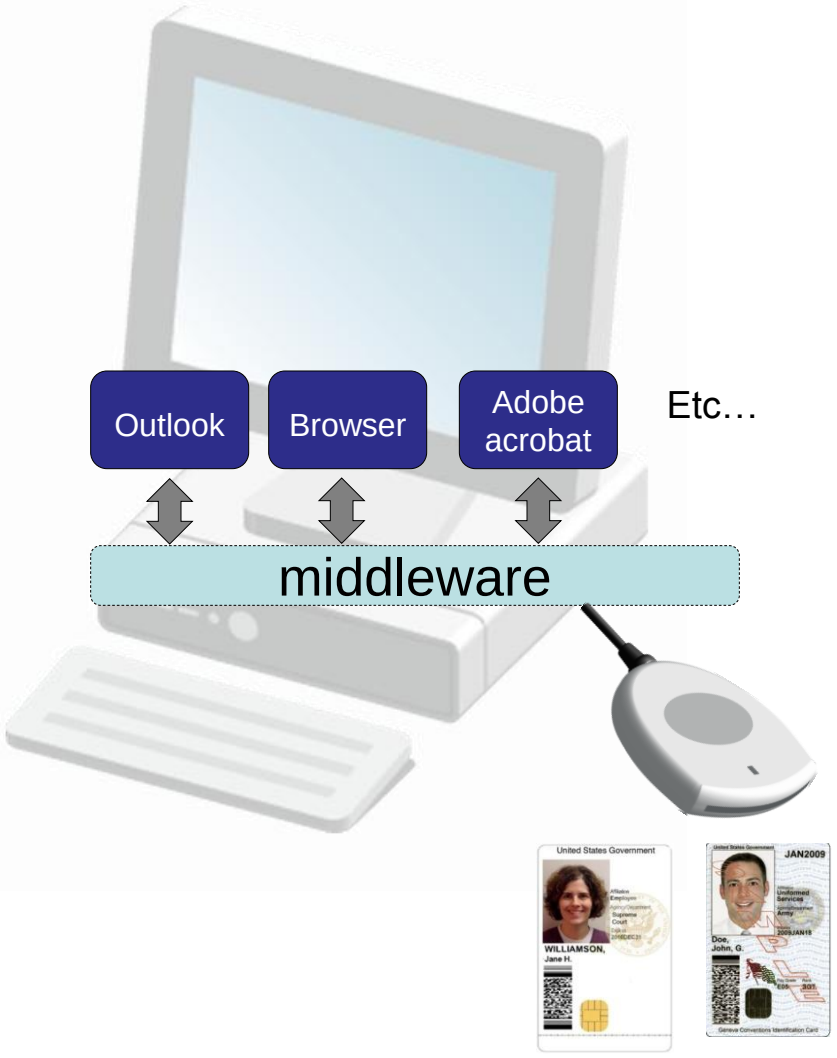
What's the problem we are trying to solve?

- US Federal Government has deployed PIV cards
- Government contractors have deployed PIV-I cards
- These are used for
  - Strong Authentication
  - Signing emails / documents
  - Encrypting emails / documents

BUT…

- Employees bring phones & tablets into work
- And they can't use them with PIV / PIV-I cards
- This causes issues such as
  - I can't read an encrypted email on my Android phone
  - I can't send a signed email from my iPhone
  - I can't authenticate to network application from my iPad

The good old days



- Agencies issued their employees with PCs, and administered them
- For each PC, the Agency purchased a card reader and a license for a middleware product
- One Operating System (Windows) dominated
- All PCs came with a USB port to plug in the card reader. Some laptops even came with a card reader built in!
- Agency could install applications from different vendors and these would all use the middleware communicate with the smartcard

Then it got complicated….

Employees brought their own devices into the workplace.

Phones

- Contacts, email & calendar
- Documents not stored on device
- Personal devices
- iOS & Android
- Additional device

Tablets

- Also, documents and applications. Virtualised desktop
- Documents stored and managed on device
- Family devices
- iOS, Windows 8 (& Android)
- PC Replacement

This introduced two challenges

Connection challenge

- Connect the tablet / phone to a PIV(-I) credential

Software challenge

- The operating systems on these devices don't easily support a middleware layer that could be used by multiple apps to access cryptographic service (authentication, signing, encryption) provided by the card

Addressing the “hardware” challenge
How to connect the device to a PIV(-I) credential

Currently the problem can be solved in one of two ways

1. Readers designed for mobile devices. for example
   - iPhone reader sleeve from Precise (Tactivo), plugs into the iPhone port
   - Bluetooth readers (e.g. Omnikey 2061). Connect wirelessly

   Pros: Can use existing cards

   Cons: User experience. Still requires peripherals. Security concerns with Bluetooth

2. Issue a derived PIV(-I) credential onto a secure microSD (with embedded Smart Card chip)
   - Many Android devices have microSD slots
   - MicroSD sleeves are available from vendors such as Device Fidelity

   Pros: Improved user experience.

   Cons: Need to issue and manage derived PIV credentials on a new form factor (dependent on FIPS 201-2). Policy prevents two concurrent active signing credentials.

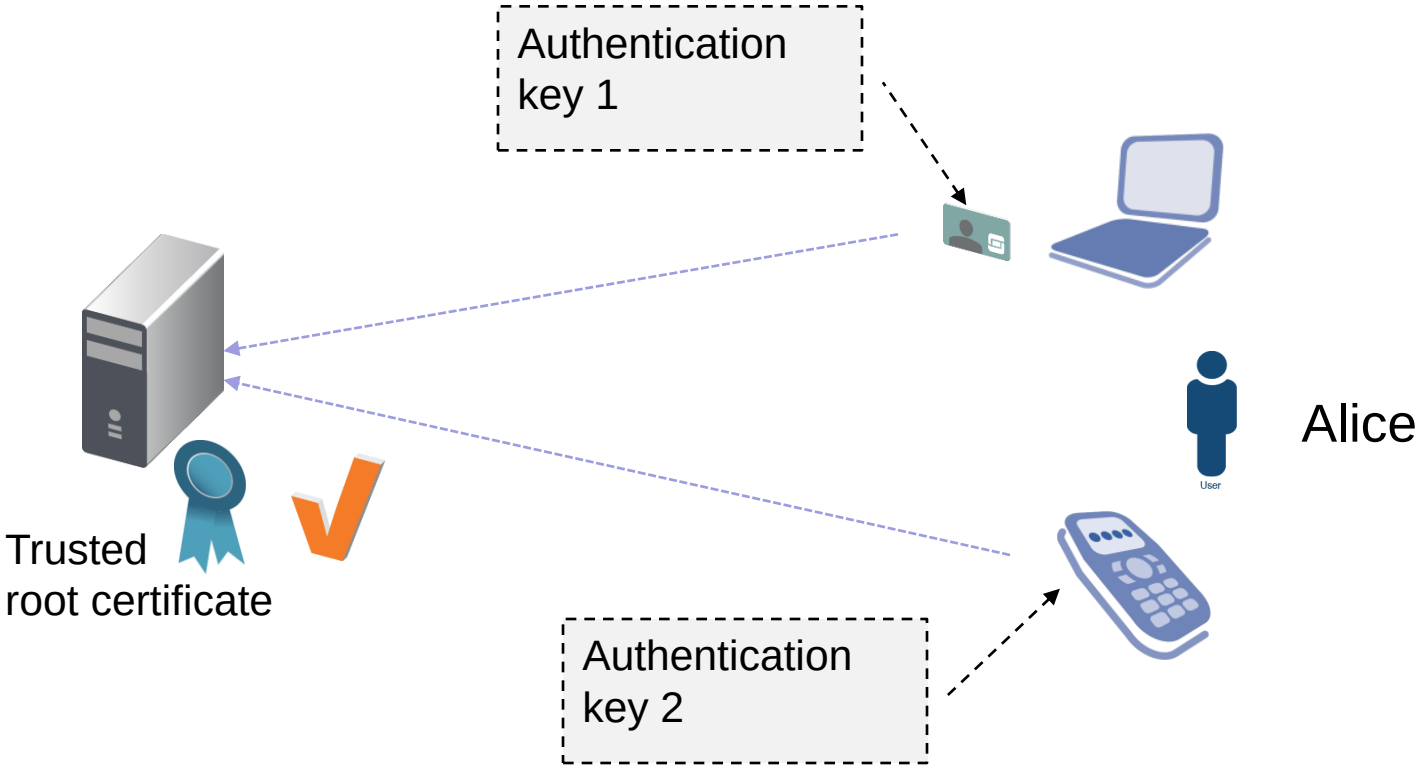
NFC brings two additional options

NFC capable devices leveraging Secure Elements (SE), Embedded or SIM, for storage of NFC services and offer contactless reader capability

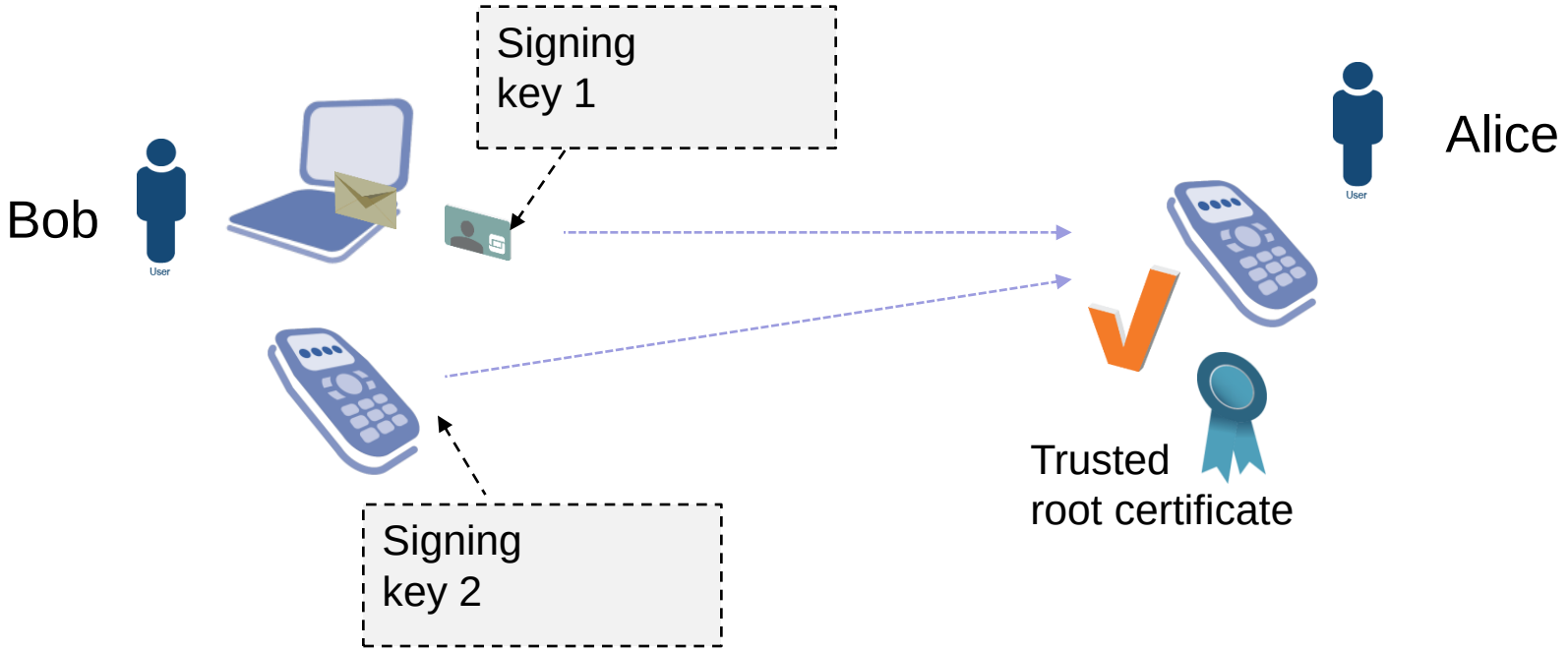
1. Derived PIV credential stored ‘on-board’ the NFC Secure Element
   - *Pros. User convenience. No sleeves required*
   - *Cons: Separate lifecycle management of derived credentials. (addressed in FIP 201-2) Need to FIPS 140-2 certify multiple device SEs*

2. Interface with PIV card via the NFC reader
   - *Pros. Use the existing card (provided it’s dual interface)*
   - *Cons: Against PIV credential usage policy (signing and encryption keys cannot be used over contactless interface. Performance issues over contactless interface. (addressed in GICS by OPACITY).*

Managing Derived credentials Authentication Credentials

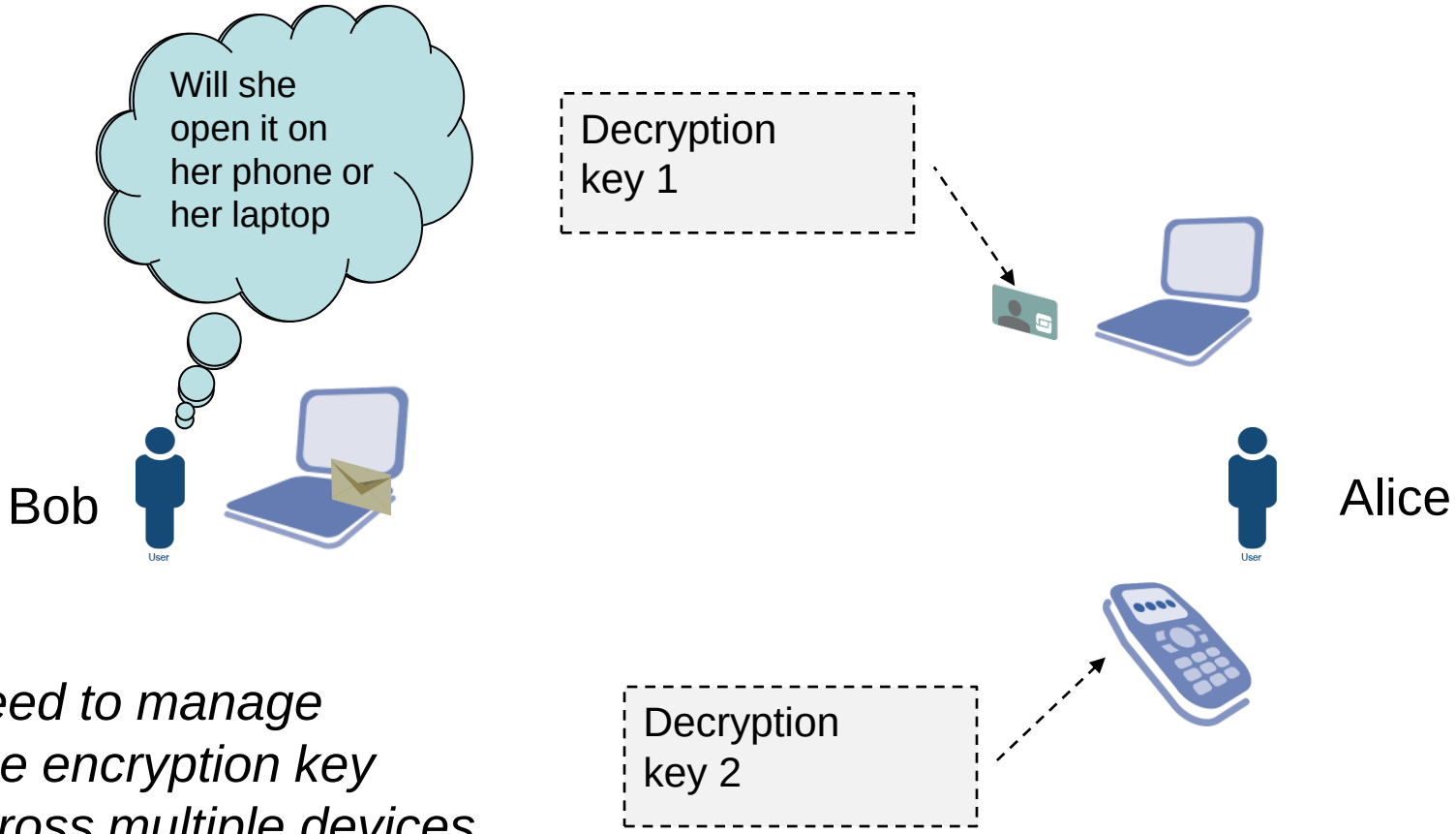


Managing Derived credentials Signing Credentials



An ASSA ABLOY Group brand
PROPRIETARY INFORMATION. © 2012 HID Global Corporation. All rights reserved.

Managing Derived credentials Encryption Keys



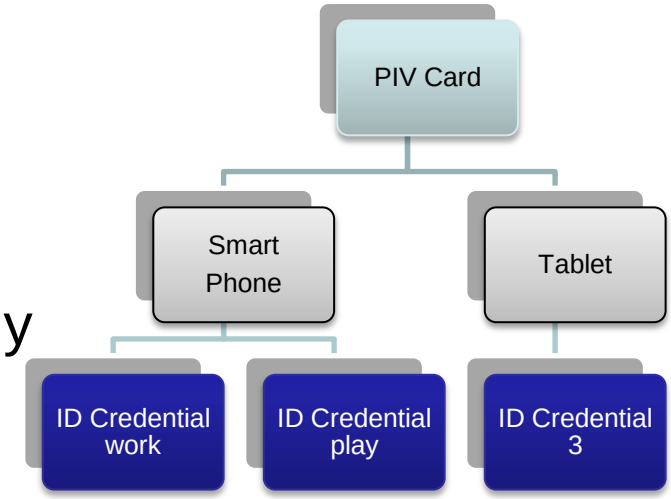
Need to manage one encryption key across multiple devices

Managing Derived credentials Lifecycle Management

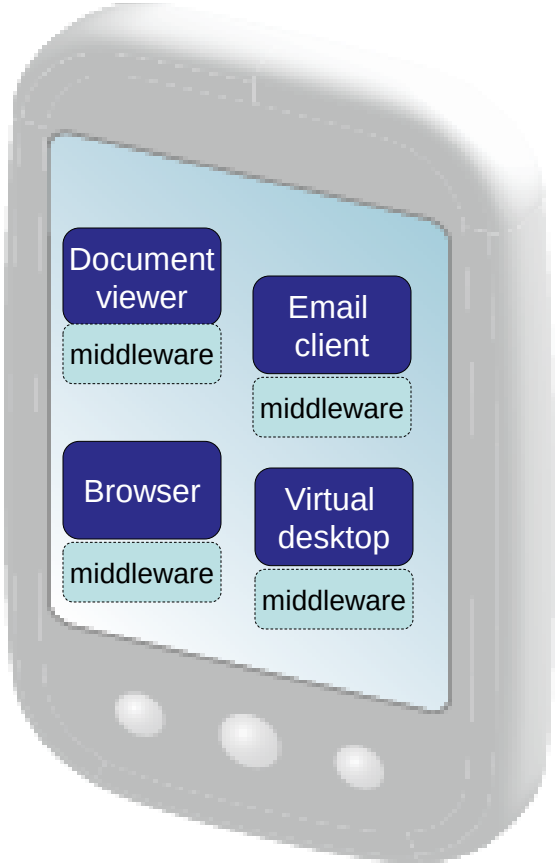
ACTIVIDENTITY part of HID Global

- Containerized between work, home, play
- Need to support derived credentials
  - E.g. ID credential derived from PIV card

- Containerization and derived credentials require hierarchical lifecycle management:
  - Loss of mobile device revokes all credentials
  - Revocation of PIV card automatically revokes ‘work’ mobile ID credential



Addressing the software challenge



- Instead of deploying a shared middleware service layer
- Middleware may need to be statically bound with the different apps running on the mobile device

Middleware model (by platform)

- Supports shared middleware services
- Has a well established trust model

- Supports shared middleware services
- Application trust model is not well established

- Requires middleware to be statically compiled into every app

- Supports shared middleware services
- Has a well established trust model

Windows 8 & TPMs

Forrester recommends that most OEMs who are selling "pure" Android tablets today switch to Windows 8.

- Intel based tablets may have TPMs
  - PIV credentials managed on TPM?
  - Shared middleware services
- ARM based devices
  - Unlikely to have a TPM / may not support smartcards

Deployment by device (phones)

	Hardware (pre NFC)	Middleware
iPhone *Minimal form factors, No microSD slot,*	Secure microSD in sleeve (P) Connected reader (A) Bluetooth reader (LR)	Embedded in apps
Android phones *Multiple form factors, Sometimes microSD slot,*	Secure microSD in slot (P) Bluetooth reader (LR) Connected reader (LR)	Embedded in apps / Could be shared Middleware Services
Blackberrys *Limited form factor, microSD slot*	Secure microSD in slot (P) Connected reader (LR) Bluetooth reader (LR)	Shared Middleware Services

(P) – Preferred, (A) Acceptable, (NA) Not Available, (LR) Last resort

Deployment by device (tablets)

	Hardware (pre NFC)	Middleware
iPad *Minimal form factors, No microSD slot,*	Secure microSD in sleeve (P) Connected reader (A) Bluetooth reader (A)	Embedded in apps
Android tablets *Multiple form factors, Usually microSD slot.*	Secure microSD in slot (P) Bluetooth reader (A) Connected reader (A)	Embedded in apps / Could be shared service
Windows 8 tablets *Multiple form factors.*	TPM (P) Secure microSD in slot (P) Bluetooth reader (A) Connected reader (A)	Shared middleware services

(P) – Preferred, (A) Acceptable, (NA) Not Available, (LR) Last resort

Challenges

- Embedding of middleware in app vendors is in early stages
- No defined agreed standard for Middleware Services on platforms
- Multiple different combinations – Operating system, phone model, secure element form factor. Which combination do vendors bet on?
- No vendor yet provides a phone sleeve and a FIPS 140-2 Level 3 compliant microSD
- Dependency on FIPS 201-2 to validate secure micro SD as PIV compliant platform
- Lifecycle Management of derived credentials