intercede

ID anywhere • mobile | smart cards | devices

www.intercede.com | @intercedemyid

Derived Credential Issuance

Chris Edwards
Chief Technology Officer

Smart Card Alliance • Washington DC • October 2014

Intercede and MyID

- US and UK based mobile and smart card solutions and services provider
- Identity and credential management software vendor
- Responsible for the MyID IDCMS suite
- Trusted Application Management (TAM) cloud service provider
- Government, aerospace and defense, finance, manufacturing, healthcare, telecoms...
- Key supplier to US Federal identity market
- High security and usability

Why do we need derived credentials?

- **Mobile workforce demands**
  - Phone as a token for local authentication
  - Phone as a gateway to enterprise cloud services
  - Phone access to corporate VPN
  - Communication signing and decryption*

- **But**
  - Card-readers are not ubiquitous
  - Full NFC use is not supported for existing cards
  - Limited standard security architecture on mobile devices
  - Many use cases go beyond the proposed derived credential content

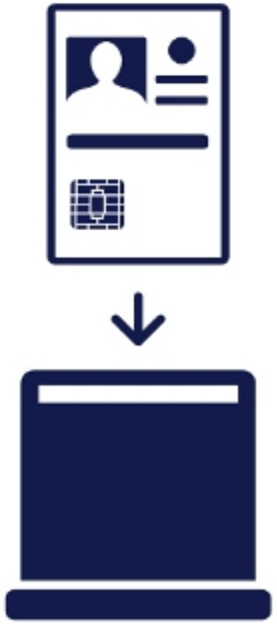
Where can derived credentials exist?

- **Cryptographic keystore options**
  - Software 'keychain' or app storage – LOA3
  - UICC (SIM)
  - Embedded secure element
  - Trusted execution environment
  - NFC chip – internal or external
  - Secure microSD
  - Coupled devices – physical, Wi-Fi, Bluetooth
- **Derived credential 'extensions'**
  - CHUID or device authentication certificate in the UICC, NFC SE, µSD or HCE for PACS
  - Signed, verifiable images for visual identification

How can we deliver derived credentials?

- **Direct connection**
  - Wired installation from management tool on workstation
  - Removable secure elements can be provisioned directly
- **Over the air**
  - Suitable for UICC resident credentials
  - Bound to a MNO and/or TSM
- **Over the internet**
  - WiFi or GSM internet transport from private or public CMS
  - Requires an app on the device to marshal the installation

Welcome to the MyID Kiosk
Insert your card to begin



Enter your PIN

1 2 3

4 5 6

7 8 9

0 ←

Next

Place your finger on the fingerprint scanner

Welcome Sam C. Jones

Do you have the MyID Identity Agent on your mobile?

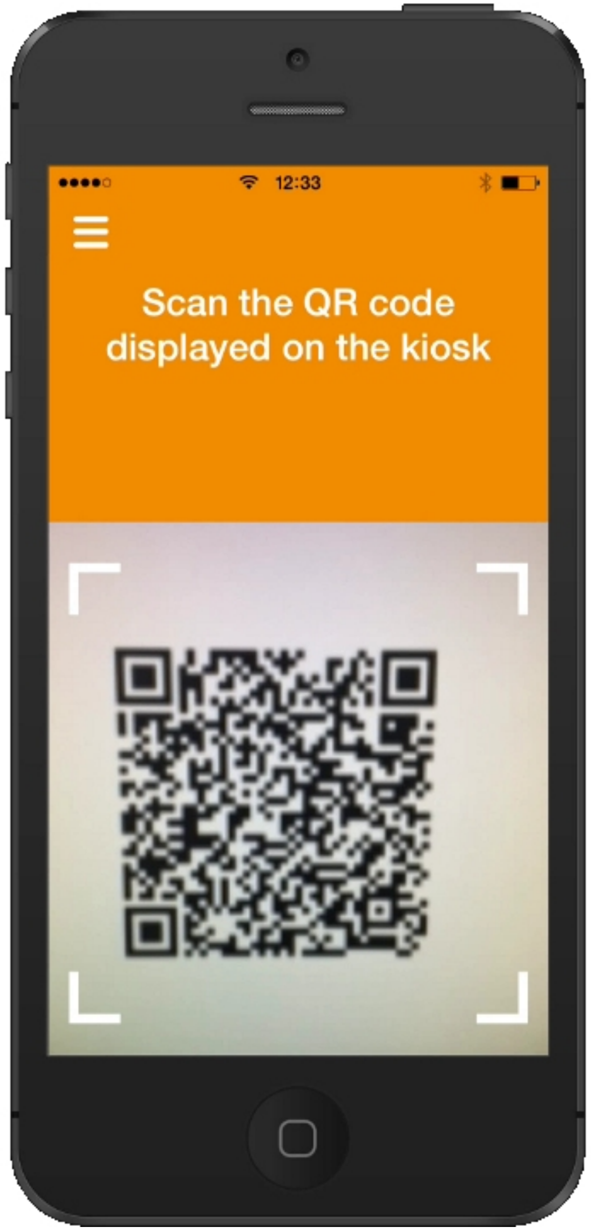
Yes

No

Using the MyID Identity Agent on your mobile,
scan the QR code

Back

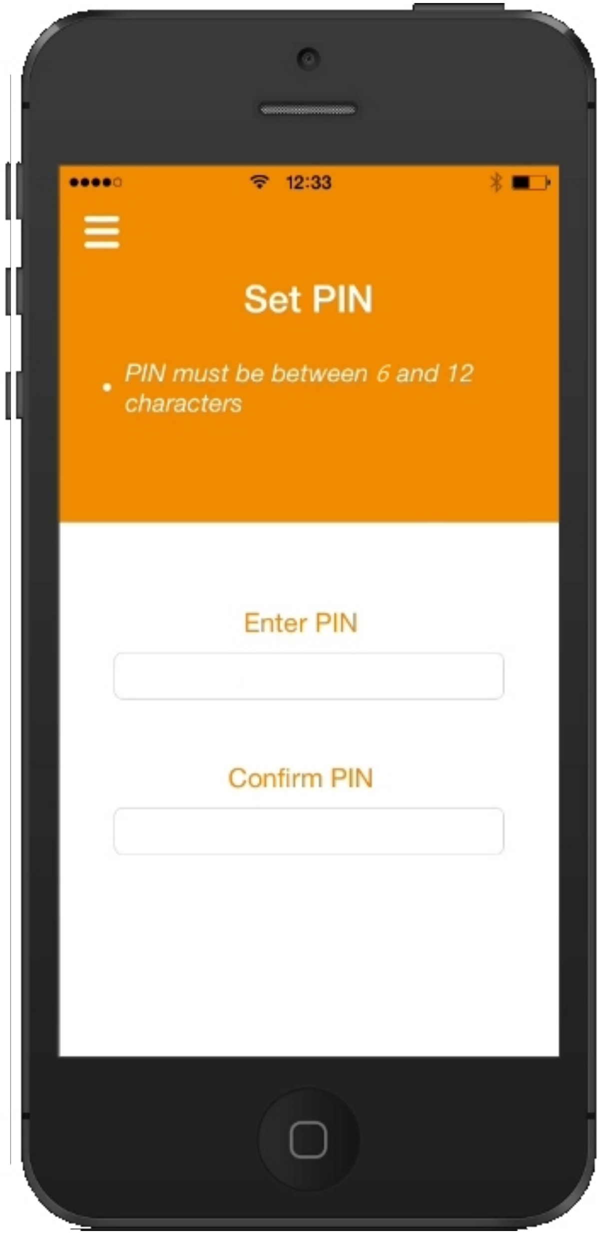
The phone app now takes over…



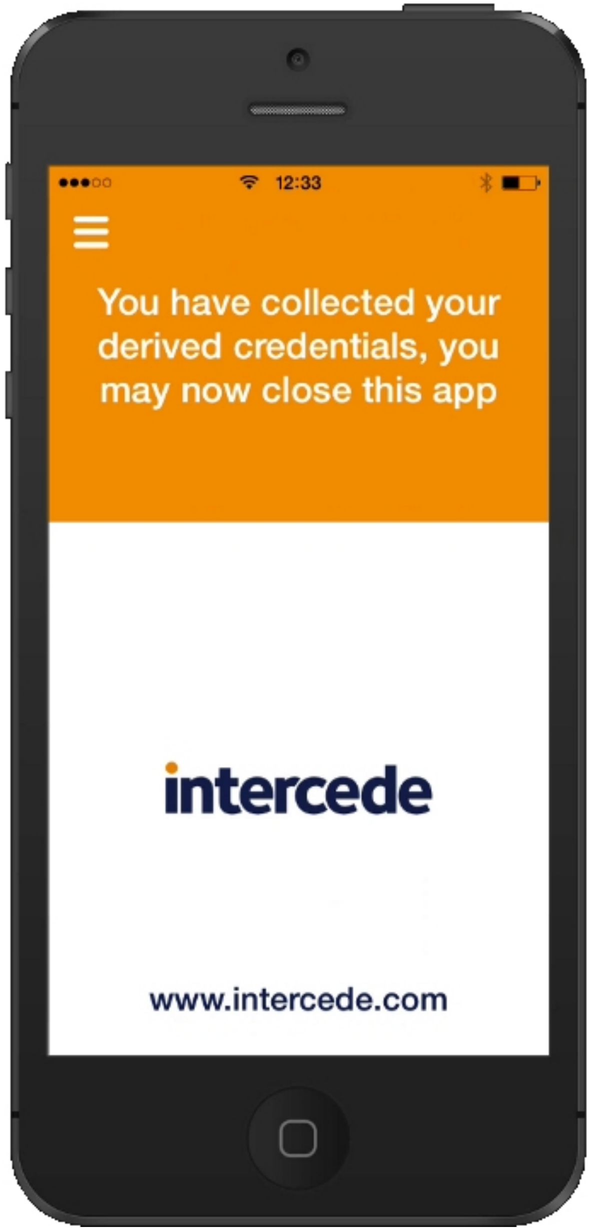
Remove your card and follow the instructions on your mobile

Policy determines keystore location and protection

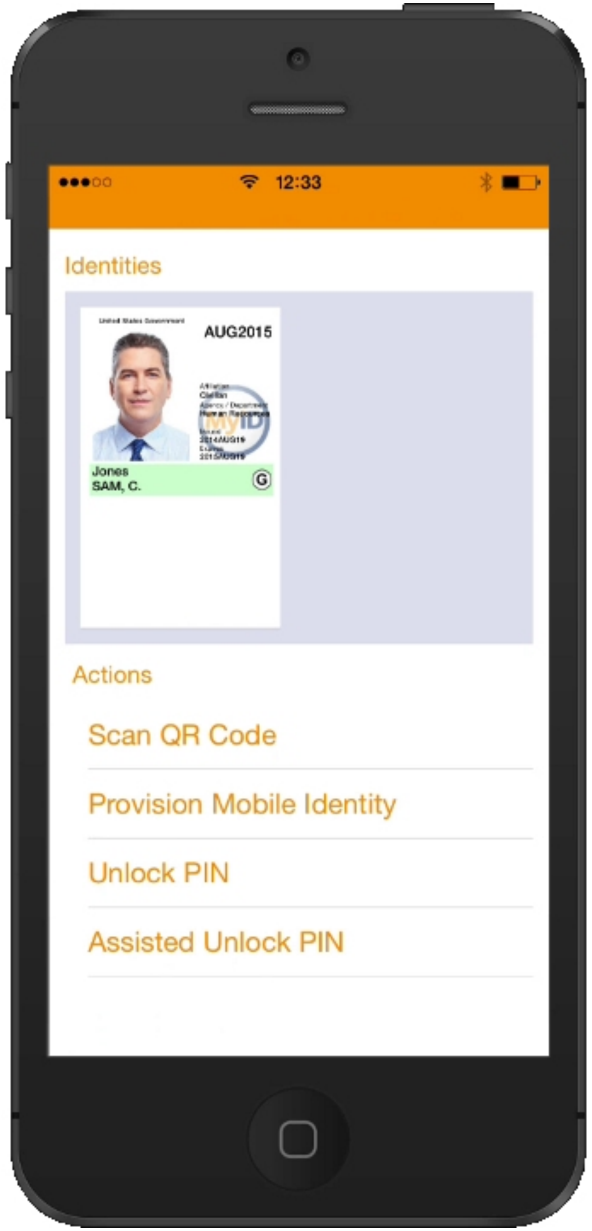
intercede



Keys, certificates and optional data are installed



A visual component is included



LOA3 versus LOA4

- **LOA3**
  - Software keystore
  - Self-service allowed
  - Card + PIN authentication
  - FIPS 140-2 Level 1

- **LOA4**
  - Hardware keystore
  - Attended issuance only
  - Card + PIN + biometric authentication
  - FIPS 140-2 Level 2/3

Policy enforcement

Lifecycle management

intercede

- A derived credential management system (DCMS) is used
- The original PIV card is a ‘breeder’ document
- That PIV card may be revoked or replaced independently
- If the *cardholder* has their PIV rights revoked, the derived credential must be cancelled
- The original IDMS/CMS provides cardholder status changes to the DCMS
- To retain the linkage between accounts, the IDMS/CMS must notify when replacement cards are issued

Using your enhanced derived credentials

intercede

Mobile apps

- Email
- Browsers
- Document signing
- VPN

Cloud services

- Document repositories
- SSL client
- Webmail

As an NFC token

- Desktop logon
- Authentication
- PACS

Question time

Chris Edwards | chris.edwards@intercede.com