



GOVERNMENT
CONFERENCE
October 29–30, 2014 WASHINGTON, DC

MOBILITY & IDENTITY TRACK

IMPLEMENTING MOBILE DERIVED “PIV” CREDENTIALS

CHRIS TAYLOR
ENTRUST



BUSINESS DRIVERS

- Problem:
 - Provide users same level of access to enterprise resources on mobile devices as they have on their desktops



- Business Requirements

- Address the demand by federal employees to use mobile devices in the workplace and abroad
- Security on mobile devices meets policy
- Reduce roadblocks that impede PIV adoption
- Secure alternative auth method to the PIV card
- Compliance to security policies
- Centralized control to manage Derived PIV Credential (PIV-D)





POLICY REQUIREMENTS

The following policies are required to be adhered to:

- FIPS-201-2
- SP800-157
- SP800-63-2
- SP800-73-4
- Common policy certificate policy
- E-Auth/ICAM





REQUIREMENTS

• Use Cases

- SCLO
- VPN
- protected websites
- Exchange (email)
- Document signing
- Support Mission Apps

Desktop

✓

✓

✓

✓

✓

x

Mobile

N/A

✓

✓

✓

✓

✓



- System requirements
 - Low total cost of ownership
 - MDM integration
 - Flexible deployment models
 - runs on the majority of mobile devices deployed (GFE today and BYOD tomorrow)
 - Scalable security mechanism of protecting the private keys
 - Integration into their existing eAuth environment
 - Self-Service portal





CHALLENGES

- 800-157 and 800-73-4
 - Not finalized as of yet
- Common policy certificate policy
 - Can't issue a PIV-D until updated



- Need flexible solution
 - utilize the SSP and NFI CA cert types in a manner that best matches the PIV-D intent until the standard is approved
 - on premise vs hosted



- Integrations with other products
- Derived credential is useless with out apps!



DERIVED PIV CREDENTIAL SOLUTION

- Entrust Federal SSP
- Entrust IdentityGuard Management Server/Self Service Module
- Entrust Mobile Smart Credential application
- Thursby Eco-system
- MobileIron





IMPLEMENTATION STRATEGY

- Initial Proof-of-Concept
 - Investigated potential solutions
 - Selected a solution
 - Evaluated for 12 months
- Limited agency pilot – 1H 2015
 - Build out documentation and support structure
 - Provide to key stake holders within the organization
- Agency wide deployment to all GFE mobile devices
 - Build Production environment in summer 2015
 - To begin in 2H 2015



A blue-tinted photograph of a city street at night. In the foreground, a wide crosswalk with white stripes is visible. Several pedestrians are walking across the street, their figures slightly blurred. The background features tall buildings with many windows, some of which are lit up. Streetlights are visible, casting a glow on the scene. The overall atmosphere is urban and nocturnal.

WRAP-UP

- It's a partnership – a collaborative approach to be successful
- Extending beyond GFE Mobile users – BYOD
- Hosting PIV-D solution for other federal agencies
- Consulting with other federal agencies for deploying their own PIV-D solution
- Expand use cases, e.g. mission critical apps



THANK YOU

www.datacard.com

www.entrust.com

