Defense Manpower Data Center
CAC/PKI NFC

Bob Gilson
Jonathan Shu
cacsupport@mail.mil

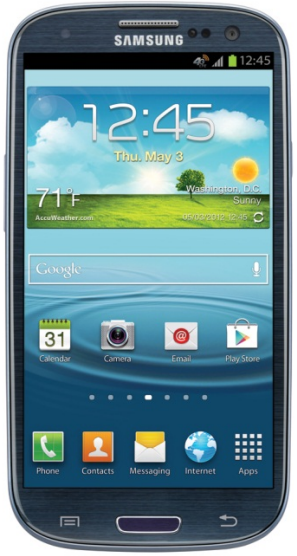

Demo

Authentication in the US Government

- US Government employees must use Personal Identity Verification (PIV) smart cards for authentication
  - HSPD-12 and FIPS 201
  - Office of Management and Budget (OMB) Memorandum M-11-11
- Successful card deployment
  - US Department of Defense has 3.8 million active Common Access Cards

Authentication on Mobile Devices
Available Options

Bluetooth Reader



Derived Credential
Embedded SE

Connected Reader

Derived Credential
Secure microSD

Derived Credential
UICC / SIM

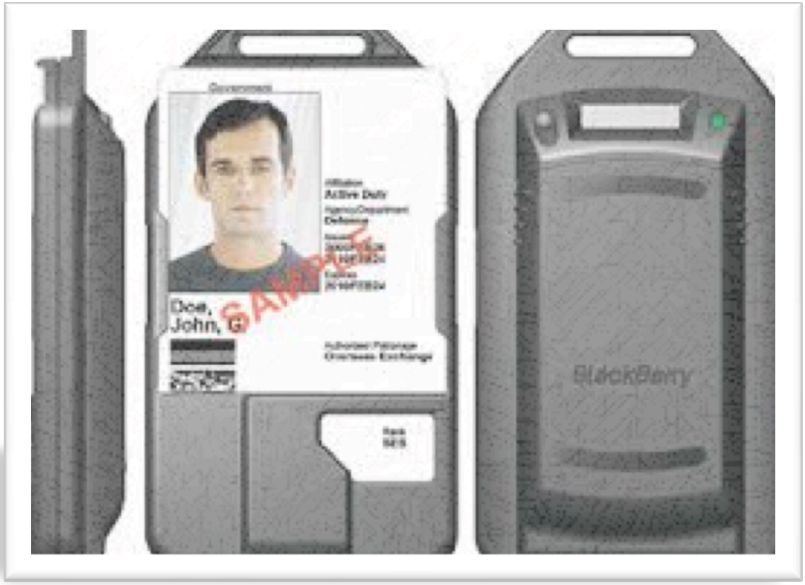
SERVING THOSE WHO
DMDC
SERVE OUR COUNTRY

Authentication on Mobile Devices
Available Options

Method	User Experience	FIPS 201 Compliance	Availability	Cost
Bluetooth Reader	Poor	Yes	Today	$$$$
Connected Reader	Poor to Reasonable	Yes	Today	$$
Derived Credential in secure microSD	Good	In process (FIPS 201-2)	Proof of concept	$$$
Derived Credential in UICC / SIM	Good	In process (FIPS 201-2)	Concept	$$
Derived Credential in Embedded SE	Good	In process (FIPS 201-2)	Concept	$$

Opportunities

- Desire to improve usability of PKI on emerging mobile computing environments
  - Dislike smart card Bluetooth reader
  - BYOD



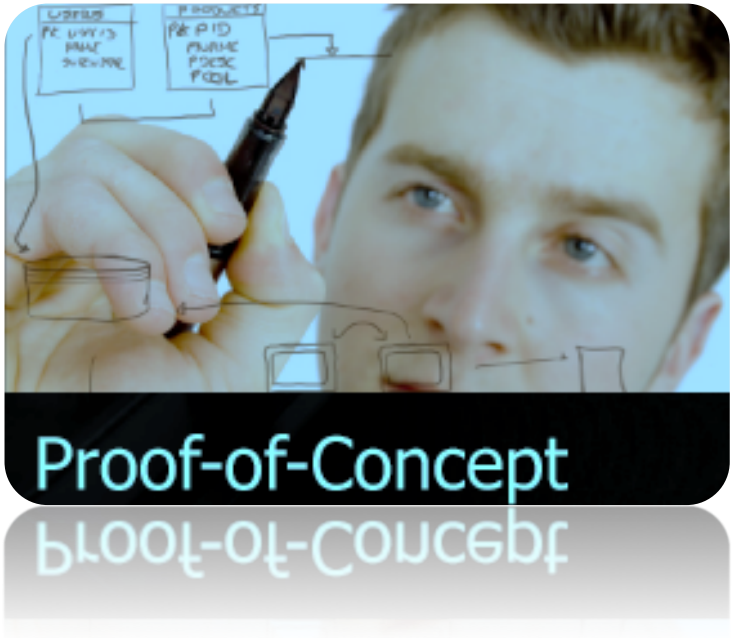
Mobility & NFC

Authentication on Mobile Devices

The NFC Option

- Just place the card on the back of the phone!
- Leverage the user's dual-interface card
- No reader required, with differences based on mobile device
- No new derived credential to procure and manage
- Works with majority of devices
- Good user experience for infrequent operations (e.g. authentication)

POC Short-term Goals



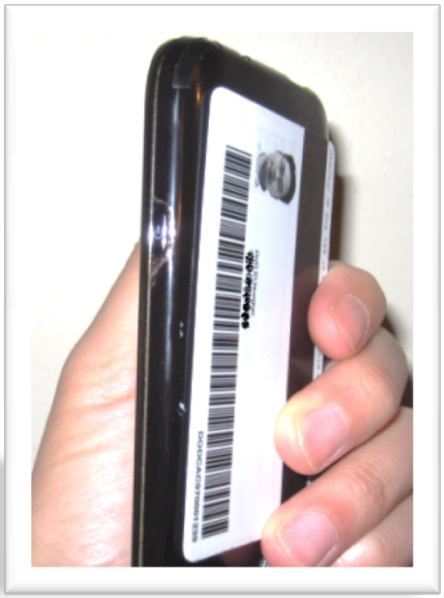
Encrypt/decrypt/sign e-mail

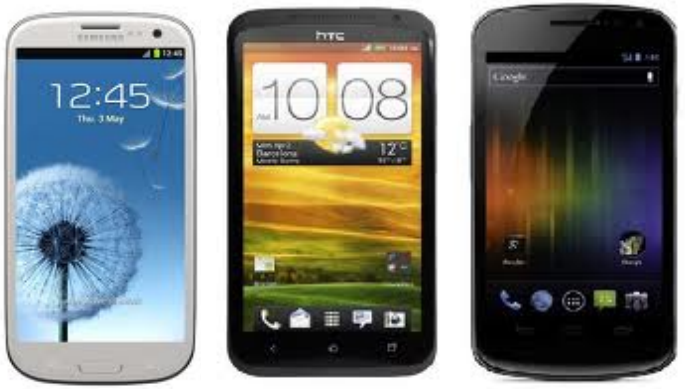
Read demographic data and facial image from CAC

Killer App for NFC Device

is secure email

Status Proof of Concept (Part 1)





Descriptions	Status
NFC Enabled devices in US	✓
Communicate between NFC devices with smart card	✓
Extract CHUID via contactless	✓
Sign/encrypt e-mail via contactless	✓

Proof of Concept (Part 2)

- Expect to conduct test in June/July 2013
- Plug into DISA's test mobile environment with test enterprise e-mail accounts
- Use test DISA managed mobile devices
- communications between the phone and smart card via ANSI 504 Opacity ZKM capabilities
  - Enabling secure contactless access on CAC applets with OPACITY
  - CAC Middleware for Android with OPACITY
  - Professional App: Good for Enterprise, Good Vault

Lessons Learned: Challenges

- Timing between card and mobile device is a problem
  - Android OS needs to provide more time for transactions to complete
  - Current FIPS 140-2 algorithm self-check implementations on smart cards needs to improve (must be faster)
- Need to secure the communication channel between card and device via ANSI 504 Opacity
- Need standard PKCS#11 or Microsoft mini driver implemented on device at OS level

DoD's Vision

- Smart Card Side:
  - CAC implementing draft FIPS 140-3 sequences for cryptographic algorithm self-checks
  - CAC enabled to support PKI function over contactless interfaces
  - CAC containing secure contactless capabilities (i.e., ANSI 504-1 OPACITY ZKM implementation)

DoD Vision Cont.

- Mobile Device (hardware):
  - Support for NFC
  - Support for NFC implementing ISO 7816 PPS like functions or improved timing
- Mobile Device (software)
  - Out of the box SMIME enabled mail client
  - Out of the box PKI enable web browser
  - Native OS certificate management store
  - Native OS implementation of ANSI 504-1 OPACITY enabled PKCS #11 module or mini driver

Take Away Messages

- It is possible to use contactless cards with NFC-enabled mobile devices
- It is possible to use a secure contactless interface compliant with US Government standards
- This represents one of several viable options to provide strong authentication services on mobile devices

Thank you!

cacsupport@mail.mil