DMDC CAC/PKI NFC with OPACITY

Project Technical Manager: Jonathan Shu
CAC Test Lab (CTL), ID Division
Defense Manpower Data Center

Background

Challenges:

- DoD Component - desire to improve usability of PKI on emerging mobile computing environments
    - Dislike of smart card sleds and dongles (due to form factor challenges and bulkiness)

Activity:

- DMDC is working within the Department’s identity management community to examine ways to improve the user experience by conducting several proof of concepts

Tentative Game Plan

1. Discovery: DISA and DMDC frame out a few proof of concepts (POCs) that can be accomplished in between Summer 2012 and 2013— test the "art of the possible".
2. Conduct POCs – Early to mid- 2014
3. Document and share findings
4. Select 2-3 most viable solutions and rundown unknown risk through NSA security assessment
5. Outline implementation challenges, risk, and cost impacts
6. Facilitate discussion on subject and potential DoD-wide solution(s) with DoD Identity Council (IdC) and CIO Executive Board (EB)

Mobility & NFC

Why Pursue NFC with CAC?

- 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
  - Nine out of the top ten smartphone manufacturers have released Near Field Communications (NFC) enabled handsets
- Other business needs within DoD to enable secure contactless transactions with CAC
  - Transit
  - E-purse

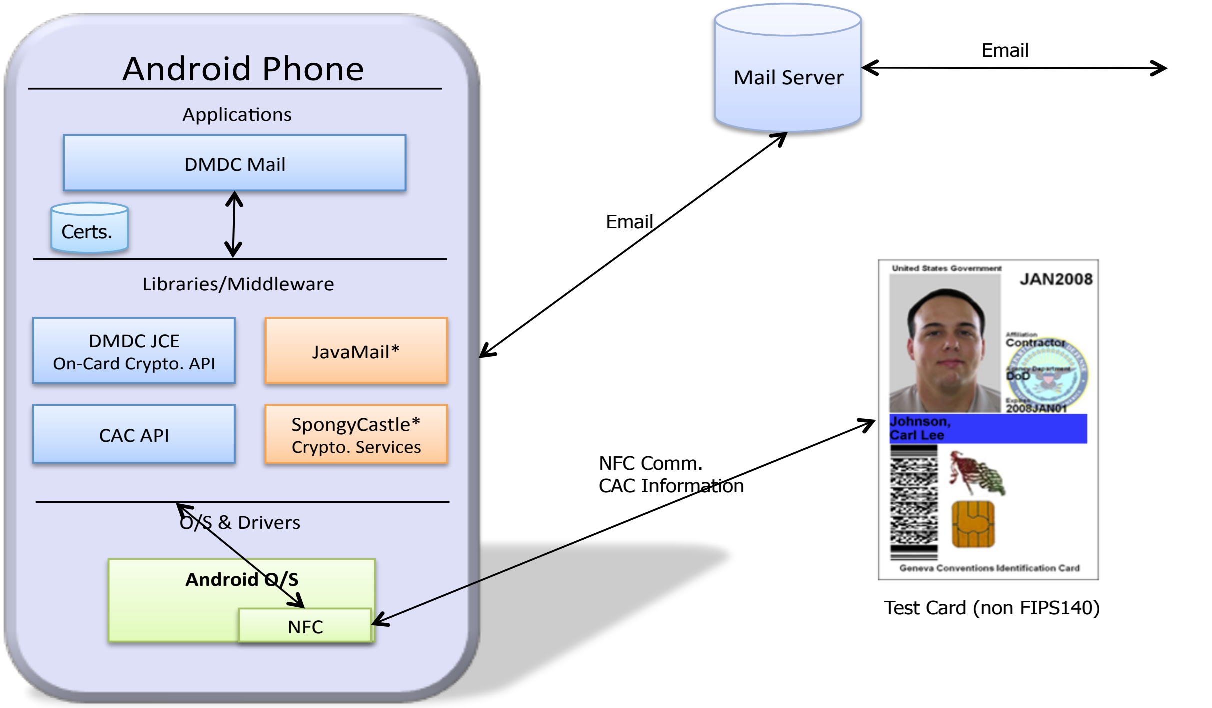
Status Proof of Concept (Part 1)

NFC

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

POC (Part 1) Implementation

NFC POC Architecture



Test Card (non FIPS140)

Color Legend: 🟩 Standard Android Software 🟧 Open Source Port 🟦 CTL Development

* Required modifications

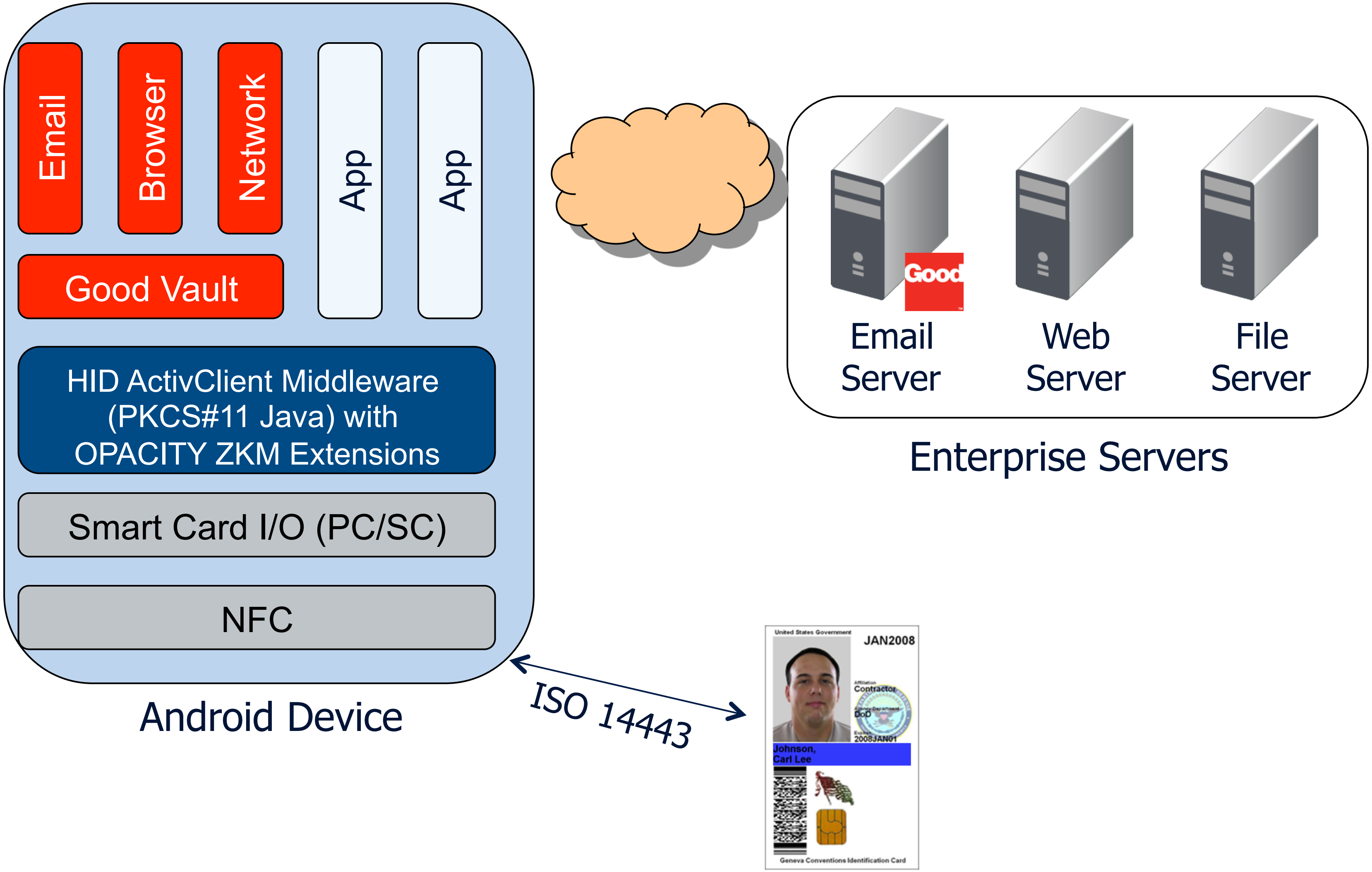
Lessons Learned: Challenges

- 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

Proof of Concept (Part 2)

- Test mobile environment with test e-mail accounts with JITC X509 test Certs.
- Use Samsung S3 mobile devices
- Use commercial SMIME client
- Secure communications between the phone and smart card via ANSI 504 Opacity ZKM capabilities
- Very near

POC (Part 2) Implementation



Email

Browser

Network

App

App

Good Vault

HID ActivClient Middleware (PKCS#11 Java) with OPACITY ZKM Extensions

Smart Card I/O (PC/SC)

NFC

Android Device

ISO 14443

Email Server

Web Server

File Server

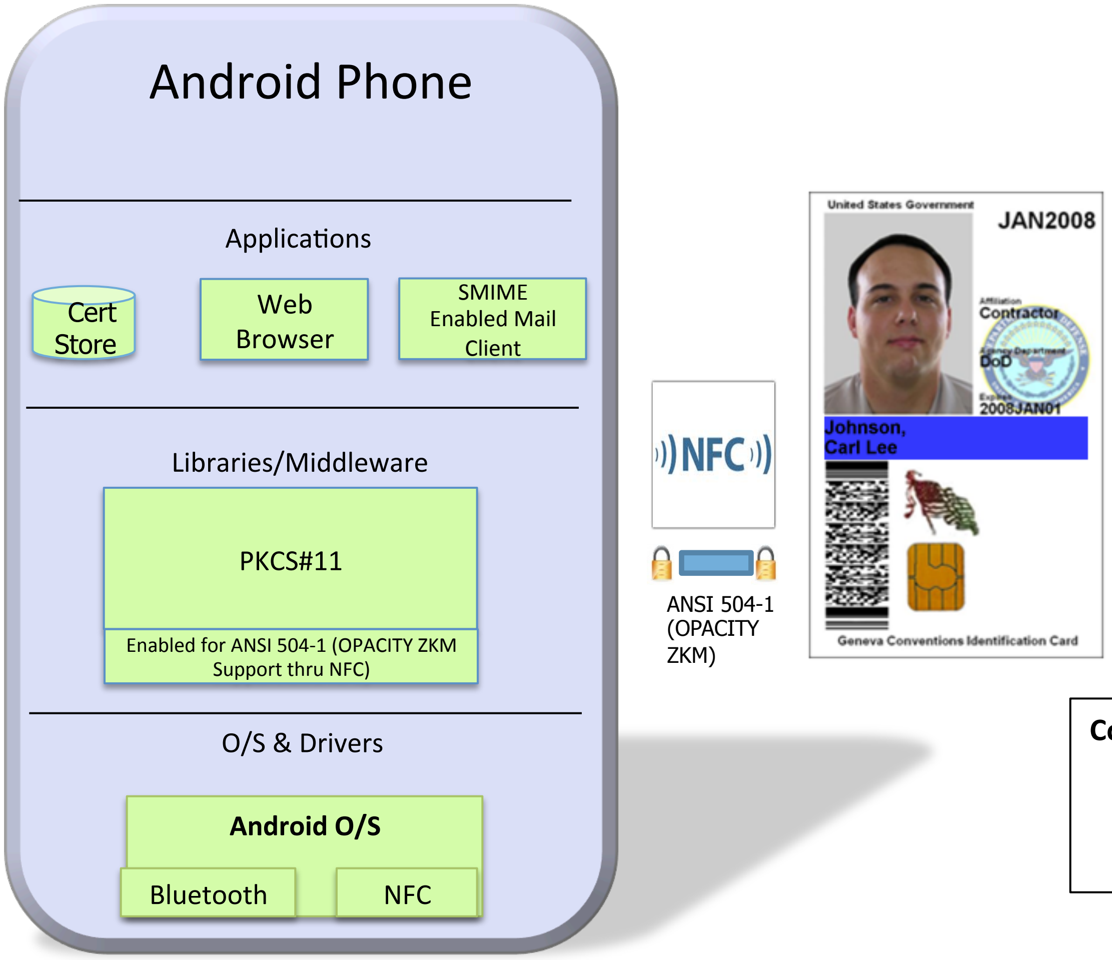
Enterprise Servers

DoD's Vision

- Smart Card Side:
  - CAC implementing draft FIPS 140-3 or modified FIPS 140-2 sequences for selective cryptographic algorithm self-checks
  - CAC enabled to support PKI function over contactless interfaces
  - CAC containing secure contactless capabilities (i.e., ANSI 504-1, Pilot OPACITY ZKM implementation and ANSI 504-2 for full rollout)
    - Information on implementation/standard is posted on Smart Card Alliance website at http://www.smartcardalliance.org/resources/pdf/OPACITY_Overview%203.8.pdf
- 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 ZKM enabled PKCS #11 module or mini driver

NFC and Smart Card Architecture

(Mobile Device Mfg./Android—Future view from DoD Perspective)



Android Phone

Applications

Cert Store

Web Browser

SMIME Enabled Mail Client

Libraries/Middleware

PKCS#11

Enabled for ANSI 504-1 (OPACITY ZKM Support thru NFC)

O/S & Drivers

Android O/S

Bluetooth

NFC

ANSI 504-1 (OPACITY ZKM)

Color Legend:

🟩 Mobile device mfg./Android

DMDC CAC/PKI NFC with OPACITY

Bob Gilson

Irving.r.gilson.civ@mail.mil