Interagency Advisory Board

Meeting Agenda, Tuesday, November 1, 2011

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

2. **FIPS 201-2 Update and Panel Discussion with NIST Experts in Q&A Session** *(Bill MacGregor and Hildy Ferraiolo, NIST)*

3. **Securing Mobile Devices for Government Specific Apps** *(Debb Blanchard, Verizon)*

4. **Enabling HSPD-12 and Biometrics to Secure the Pentagon and Mark Center** *(Derek Nagel and Roger Roehr, PFPA)*

5. **An Example of Enabling HSPD-12 in Multi-Tenant Building by Operating a PACS Platform as a Service** *(Tom Corder, Bridgepoint Systems)*

6. **DoD PIV-I Update** *(Paul Grant, DoD)*

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

Securing Your Mobile Device for Government-Specific Applications: Two-Factor Authentication For Mobile Devices

Interagency Advisory Board (IAB) Presentation

Debb Blanchard

November 1, 2011

Topics

- Government Challenges
- Current State of Mobile Devices
- 4G and LTE

Government Challenges

Authenticated

- Identity Mgmt
- Privacy
- 2/3/4 Factor

Integrated

- Seamless
- Attached
- Collaborative

Secure

- Management
- Data at rest
- Data in transit

Ubiquitous

- Anywhere
- Anytime
- Any Situation

Federal Requirements with Mobile Devices

- Federal Requirements
  - HSPD-12
  - OMB M-11-11
  - Teleworker Act
  - FISMA
- NIST Special Publications
  - SP800-144 – Draft Guidelines on Security & Privacy in Public Cloud Computing
  - SP800-127 – Guide to Securing WiMAX Wireless Communications
  - SP800-124 - Guidelines on Cell Phone and PDA Security
  - SP800-122 - Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
  - SP800-121 - Guide to Bluetooth Security
  - SP800-120 - Recommendation for EAP Methods Used in Wireless Network Access Authentication
  - SP800-114 - User's Guide to Securing External Devices for Telework and Remote Access
  - SP800-111 - Guide to Storage Encryption Technologies for End User Devices
  - SP800-98 - Guidelines for Securing Radio Frequency Identification (RFID) Systems
  - SP800-95 -Guide to Secure Web Services

Current State of Mobile Devices

- FIPS 140-2 certification on consumer popular mobile devices is lacking
  - Federal certification **today** only on RIM and Microsoft OS
  - iOS and Android are in early process
  - To use a non-certified device is a violation of OMB security requirements
- Communication with the smart card, e.g, PIV and CAC
  - Most business laptops have embedded smart card readers
  - Tablets and netbooks, including iPad, need an external smart card reader
  - Communication with smart card and tablet apps need to be via secure Bluetooth or near field communication (NFC)
  - NFC not approved by NIST for the contactless interface
- Technology is still being integrated, however, NIST testing is still in process
- After NIST testing, GSA testing to allow these devices and peripherals on GSA APL for PIV
- 4G network is available now in identified markets

Considerations for Mobile Devices

- Chips must be tested by the *carrier* to ensure FCC compliance
- “Swap out” of chips:
  - May invalidate the manufacturer warranty
  - May not work on the carrier’s network
- Most devices only allow one SIM chip at this time
- Most 4G LTE devices support one microSD and one SIM chips at this time
- Some of the most popular mobile devices are manufactured in China
- Security requirements of the devices and the IT network requirements
- FISMA requirements are not only for the chip but for the *entire mobile device*
- Personal devices used for government business
  - How to validate the device for the network
  - Government-issued identity credential issued/used on the personal mobile device
  - Data ownership stored on a personal mobile device
  - Data security of the data at rest on the personal mobile device
  - Consumer grade products not designed with FISMA security requirements
  - 700 Hz band issues

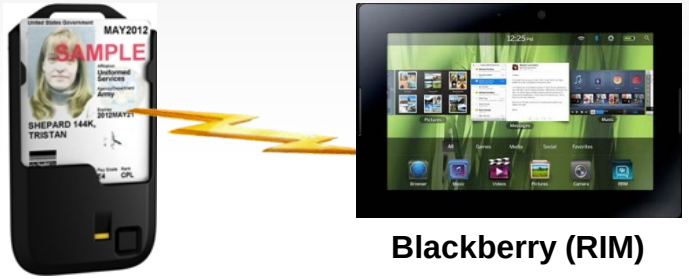
Mobile Devices Under Consideration

iOS)

ndroid)

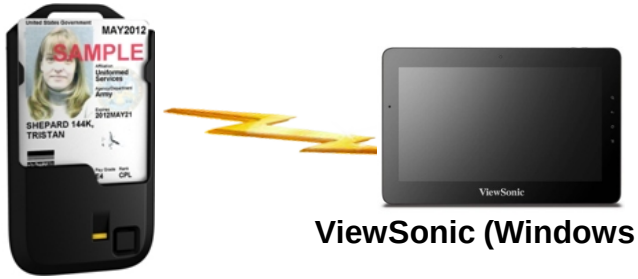
iMac (iOS)

NOT CERTIFIED AS OF TODAY!



Blackberry (RIM)

Windows Tablet (Windows OS)



ViewSonic (Windows OS)

DISA approved Bluetooth security with FIPS 140-2 crypto module

Fully supports Microsoft CAPI and PC/SC interfaces

Open front provides maximum card visibility as required by FIPS-201

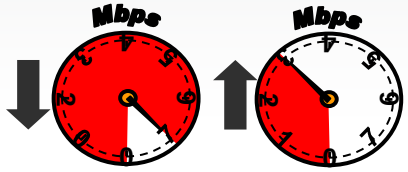
Inactivity timeout options for longer battery life

Multi-colored LEDs provide connectivity and charging status

OTA upgradeable middleware, firmware and drivers for additional smart card functionality

verizon

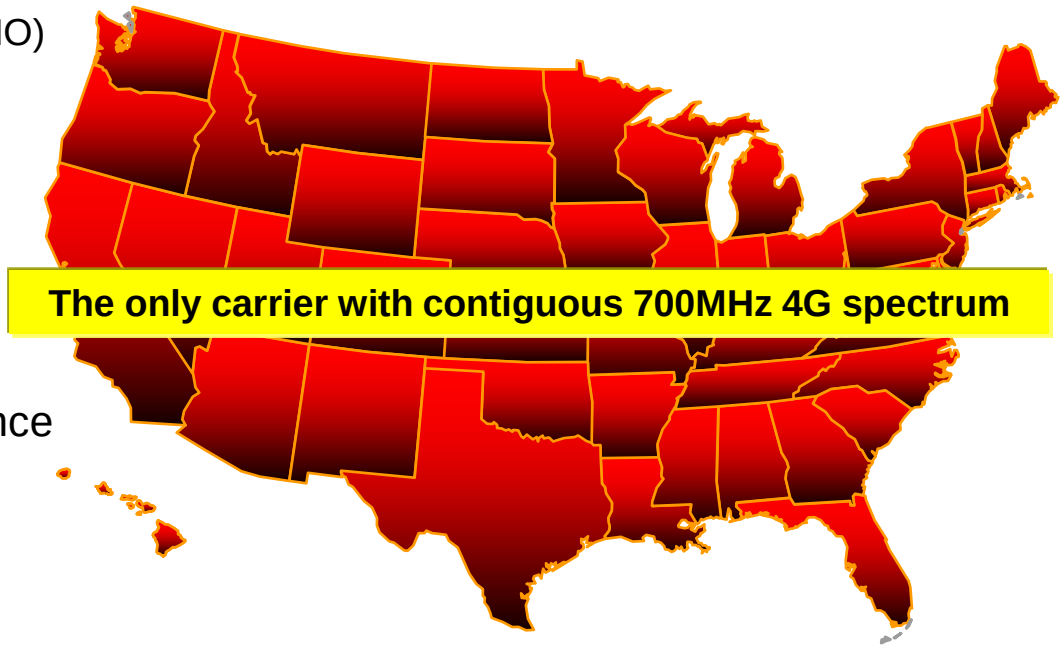
- New Technology Advancements
  - Radio Technology
    - Orthogonal Frequency Division Multiple Access (OFDMA)
  - Antenna
    - Multiple Input-Multiple Output (MIMO)
- Evolved Packet Core
  - Flat IP-based architecture
  - Flexible bandwidth options
- IP Multi-Media Subsystem
  - Wireless and Wireline Convergence
  - Network Based Services – Gateways/Servers



~5-12 Mb ~2- 5 Mb

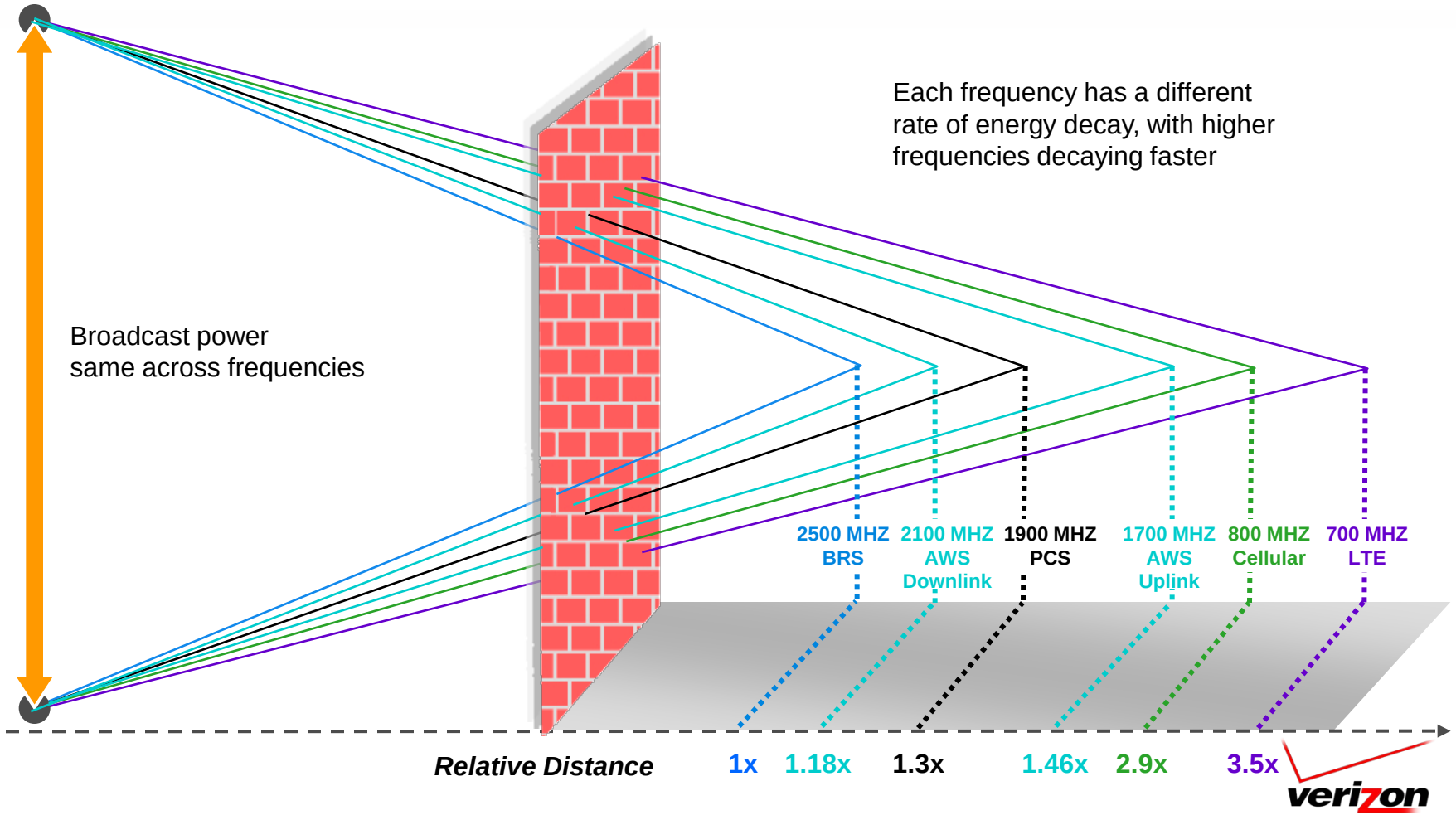
30 ms

150 ms

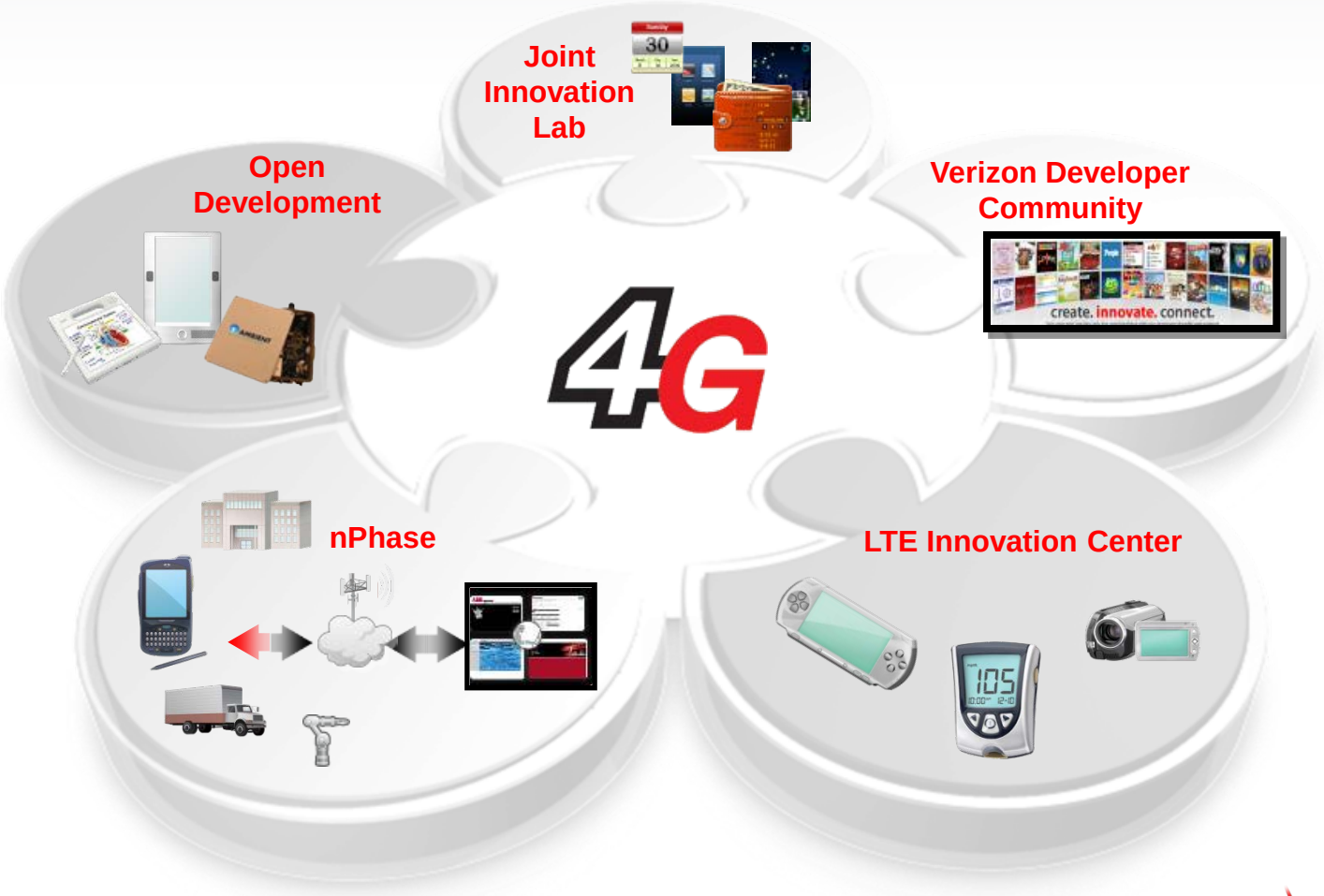


Building Penetration Comparison

700 MHz Delivers Superior Building Penetration



Leadership In Innovation



Extending the Enterprise

Continuity of Operations (COOP)
Provides secure wireless access to critical content such as disaster plans, floor plans & emergency communications.

Dashboards
Software that enables business applications and dashboards on Blackberry and WM devices.
Knowledge dashboards, IT Help Desk & field Service.

Field Agent Safety
Management, Tracking and Dispatch applications on Blackberry, Windows and Android Devices

Video Surveillance, Recognition and Identity Management software solutions using Smartphones IP cameras and Bio-Metric peripherals to complete a solution.

Wireless Routers
Quickly set up small or temporary Work Groups

29

Summary

- Applications and workstations are starting to accept smart cards natively
  - Dell/HP
  - Microsoft
  - Adobe
- Need to ensure that PK-Enabled applications have access to the following:
  - Trusted identities
  - Certificate chains
- Each IT department has different policies on the configuration policies for mobile devices, workstations and applications
- OMB security and certification requirements are applicable to all mobile devices, including RIM, Microsoft, iOS, and Android, including FIPS 140-2 certifications
- Policy and testing issues need to be addressed soon! Agencies are moving forward – in some cases violating OMB.

Thank you!