REVISION TO THE MOBILE ID DEVICE BPR

Kickoff Meeting

October 30,2014

WELCOME

- Barbara Guttman
  - Director, Information Access Division

WELCOME!!!

- Looking back… some factoids:
  - It was a long road to the BPR…
    - APB request announced on 08/06/2007
    - The BPR published on 08/21/2009 (746 days)
  - The final comment disposition spreadsheet was 49 pages long (the BPR itself was 55 pages long).
  - In 2009, there was only a handful of devices that were ready for market.

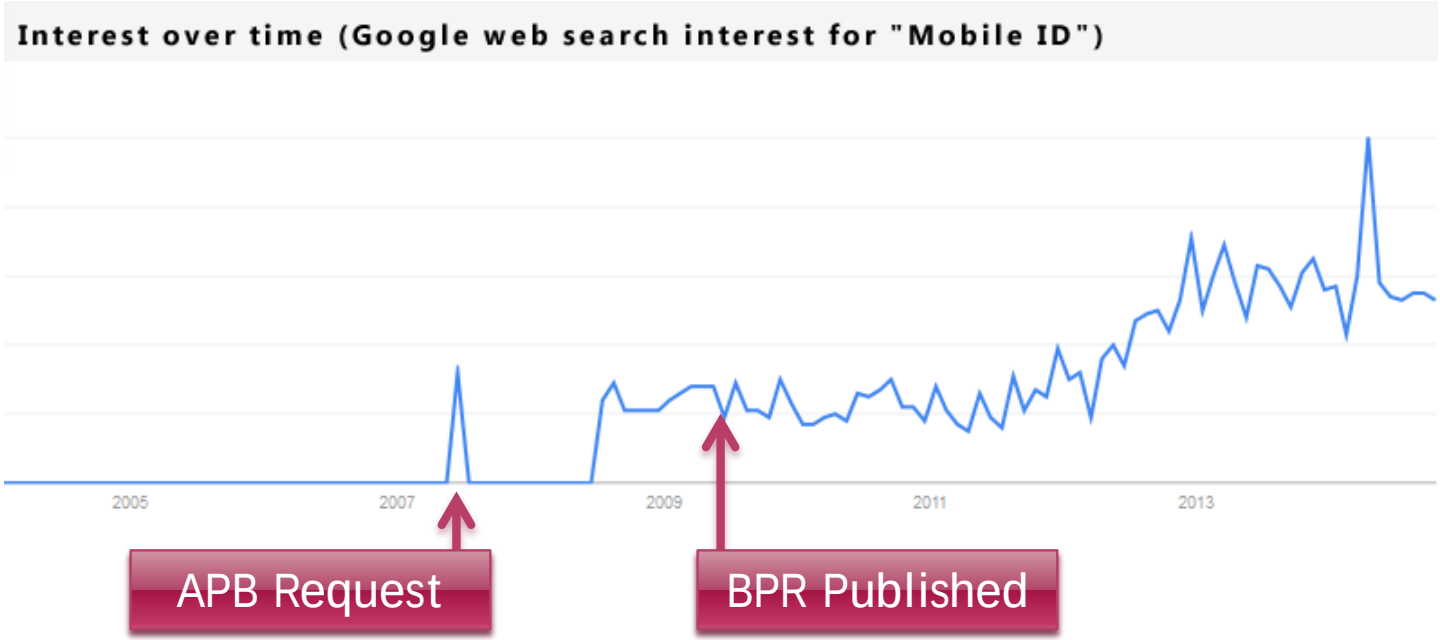
SHAHRAM ORANDI

MUCH HAS CHANGED

- But… its been over 5 years since publication, and much has changed.
  - A mid-range desktop in 2008 could execute 10 BIPS… A smartphone last year hit 18 BIPS.
  - Sensors technology has improved (1000ppi fingerprints, megapixel resolution for even the most basic cameras devices)
  - Data transmission systems have radically transformed (LTE, 802.11, 802.16, Bluetooth)

A LONG ROAD TRAVELLED

- We've come a long way… Lots of devices… FBI-NGI-RISC is in full swing… Lots of new interest…



SHAHRAM ORANDI

IN CLOSING

- The time is right for an update.
- Good to see continued interest and support from everyone!
- Glad to have you here for the next evolution in Mobile ID!

Shahram Orandi
sorandi@nist.gov

NEED FOR AN UPDATE

- BPR originally published in 2009
- ANSI/NIST-ITL standard has incorporated the Acquisition Profiles, and they should be maintained in only one document
- New modalities have matured for biometric and forensic use in a mobile environment
- Referenced Standards have been updated and new ones developed
- Use cases have been further defined
- A mobile ID taxonomy has been developed
- New technology has been developed

BRAD WING

EXCERPTS FROM IBIA LETTER TO NIST DATED MARCH 7, 2014

- Based on input from our member organizations, IBIA is respectfully requesting that the National Institute of Standards and Technology (NIST) consider convening a working group to discuss and review potential updates to NIST Special Publication 500-280 *Mobile ID Device Best Practice Recommendation Version 1.0* (hereafter, Mobile ID BPR), which was published in July 2009. This publication is an important reference document for implementers and suppliers of mobile devices that incorporate biometric technology and is often cited in procurement documents and is used by suppliers in developing product specifications. A number of later documents and standards, such as ANSI/NIST-ITL 1-2011 (NIST Special Publication 500-290), reference the Mobile ID BPR document extensively. However, we believe that some references in the Mobile ID BPR document may be outdated and should be refreshed.

BRAD WING

PROCESS OVERVIEW

- The BPR is a NIST Special Publication, not part of the ANSI/NIST-ITL standard
- We will set up working groups to develop text for the new document
- Much of the document structure will be changed, since the Acquisition Profiles are now in the ANSI/NIST-ITL standard
- Drafts will be circulated for comment
- There will be a poll of interested parties to determine if the draft is acceptable prior to putting through the NIST publication procedure.

BRAD WING

FORMAT OF THE MEETING

- Presentations in limited time slots
  - Questions if there is enough time left in the slot
- Group Discussion in the afternoon

- Think about these questions during the day:
  - What do we want to consider as 'mobile' in the BPR (wearable -- transportable – luggable --mixed ?)
  - What modalities do we want to address?
  - Should we include SOPs? Privacy issues? Etc. or just 'technical' aspects ?
  - Which areas are you willing to chair?
  - Is there anything else that occurs to you as important?

BRAD WING

presentations

USE CASE SCENARIOS

USE OF THE NEXT MOBILE BPR

A DHS S&T Perspective

Patricia Wolfhope
PM
DHD S&T
Resilient Systems Division

Homeland Security
Science and Technology

MOBILE BPR USES?

- Referencing the Mobile BPR in RFI's, RFPs, BAAs . . .
  - Law Enforcement/Military Profiles make it easy
- We have an opportunity to tune the next version to suite our needs
  - Documentation tool for needs and requirements
  - Use cases/scenarios already spelled out
  - Mobile device characteristics in tabular form
  - Guidance on Standards and Best Practices

PATTY WOLFHOPE

EXAMPLES OF SOME NEEDED ADDITIONS

- Forensics
  - Latent finger printing on site at crime scenes
  - Finger printing deceased persons
- Access control
  - To the mobile device itself, facility/area, obtaining services . . .
  - One sentence in section 11.3.1 on Operator Authentication
- BOLOs
  - Ability to receive pictures and criminal history in the field on a mobile device

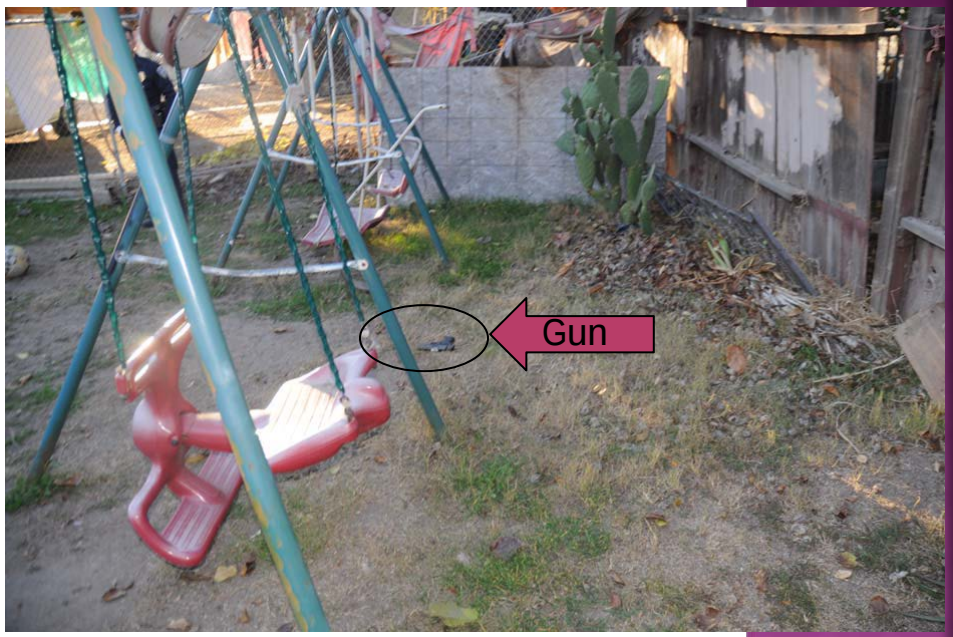
FORENSICS (LATENT PRINTS)

During a traffic stop, an unknown suspect pulled out a firearm and aimed it towards Officer Pierce.

Officer Pierce fired his duty weapon toward the suspect.

The suspect fled on foot with a weapon.

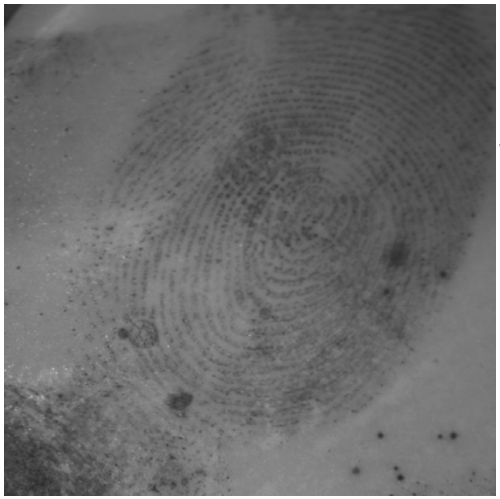
Weapon was located in a nearby back yard.



Field Technician was called out to collect and run latent prints with Fusion at the site. Seventeen prints found to be medium to high quality were submitted and resulted in AFIS hits. An arrest was made.

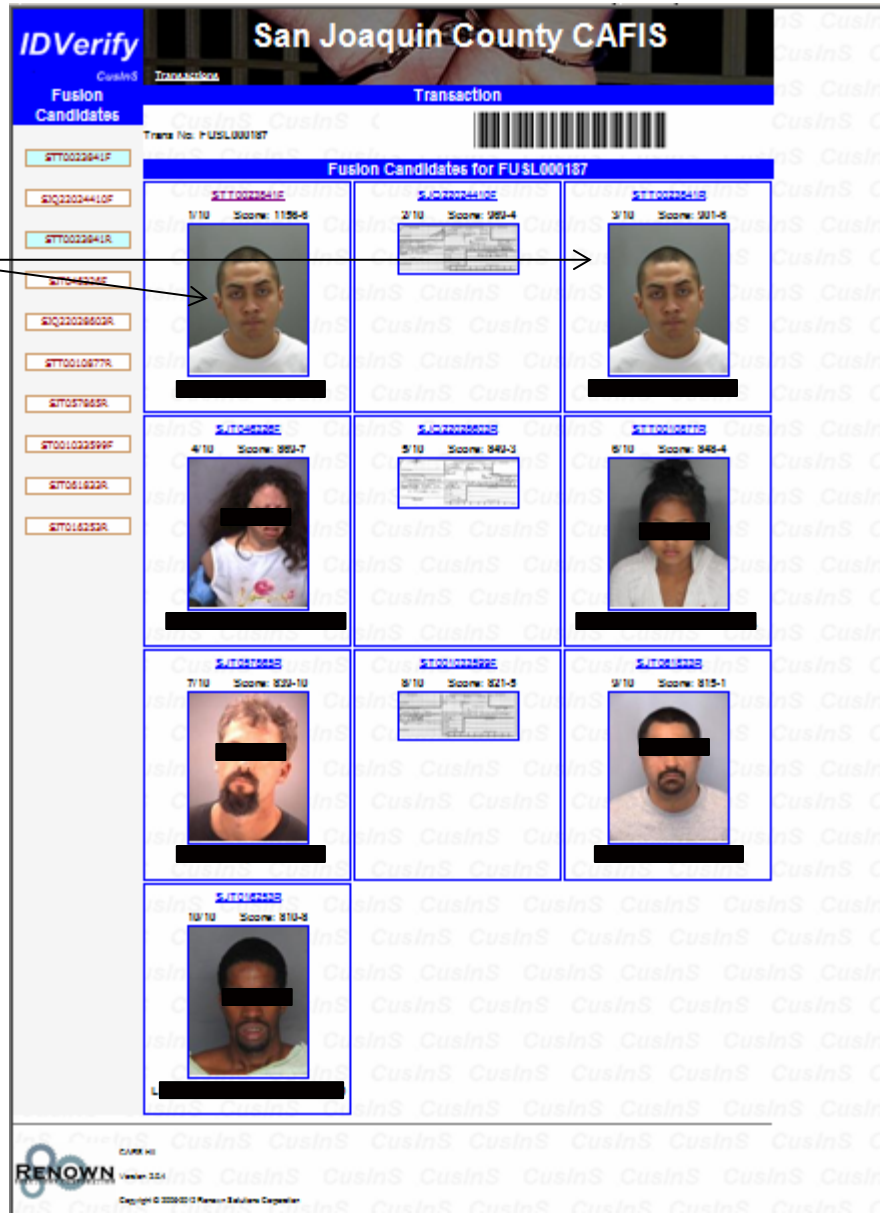
FORENSICS (LATENT PRINTS)

Fusion Image



Suspect

Hit Right Thumb



PATTY WOLFHOPE

FORENSICS (LATENT PRINTS)

SPD CASE [redacted] 417 PC

LATENT LIFT #7B - FROM INTERIOR REARVIEW MIRROR

WITH BLACK POWDER

IDENTIFIED: [redacted]

Lights Out Lifted

Workstation

Lights Out Not Lifted

FUSION #187	LAB AUTO	LAB MANUAL
1290	1493	1020
1083	1236	911
860	919	883
849	907	841
842	902	840
839	875	840
826	865	804
826	857	801
822	854	794
	846	786

PATTY WOLFHOPE

ACQUISITION PLANNING TOOL BY PROFILE

- Acquisition planning tool for operational end users (currently Appendix B)

Description	Law Enforcement	Military
Biometric Data Collection (image sensor capabilities)	flat fingerprints (FAP 10) facial image (SAP 32)	FAP 45 or above SAP 42 or above
Durability / Ruggedness		Ingress Protection Rating: IP65 Must survive multiple drops at 36 inches
Mobility	Field Use and Office Use	Vehicle Use (mounting and charging)
Communications	3G cellular 802.11 (WiFi) Ethernet LAN (RJ-45 connection, for office use)	4G LTE cellular USB 2.0
Inputs	Touchscreen Virtual Keyboard	Physical keyboard peripheral (for office use)
OS	Windows 7	Windows 8
Data Formatting Output(s)		DHS OBIM IXM 6.0 DOJ FBI EBTS 9.3 DOD DFBA EBTS 3.0
Subject Record (data) Storage	200 subject records (storing images, not templates)	
Security	Adherence to DHS 4300A and FBI CJIS Mobile Security policies Data "at rest", "in use" is protected and secured	
Screen Size (inches, diagonal) *(includes platform + accessory)*	Greater than 6 in	Less than 12 in
Dimensions (inches) *(includes platform + accessory)*	Less than 12x10x1.25	Less than 12x10x0.75
Weight (pounds) *(includes platform + accessory)*	Less than 3 lbs	Less than 2 lbs
OPTIONAL Reqrs		
Card Reader		*FIPS-201-1 (e.g. PIV, PIV-I, CAC) [OPTIONAL]*
Biometric Data Collection (Iris and/or latent fingerprint image sensor capabilities)		*IAP 20 or above [OPTIONAL]* *Latent fingerprint capture capabilities [OPTIONAL]*

PATTY WOLFHOPE

ACQUISITION PLANNING TOOL BY USE CASE

Characteristic	Road Stop	Latent Printing	Deceased	Check in/out
Biometric Data Collection (image sensor capabilities)				
Durability / Ruggedness				
Mobility				
Lighting				
Communications				
Inputs				
OS				
Subject Record (data) Storage				
Docking				
Battery				
Security				
Screen Size (inches, diagonal) *(includes platform + accessory)*				
Dimensions (inches) *(includes platform + accessory)*				
Weight (pounds) *(includes platform + accessory)*				
PIV/CAC Card Reader				
Biometric Data Collection (Iris and/or latent fingerprint image sensor capabilities)				

PATTY WOLFHOPE

USE CASES AND SCENARIOS

Rick Lazarick
Chief Czar Scientist - Biometrics
DHD S&T Support Contractor
Computer Sciences Corporation

Homeland Security

Science and Technology

MOBILE BEST PRACTICES WORKSHOP

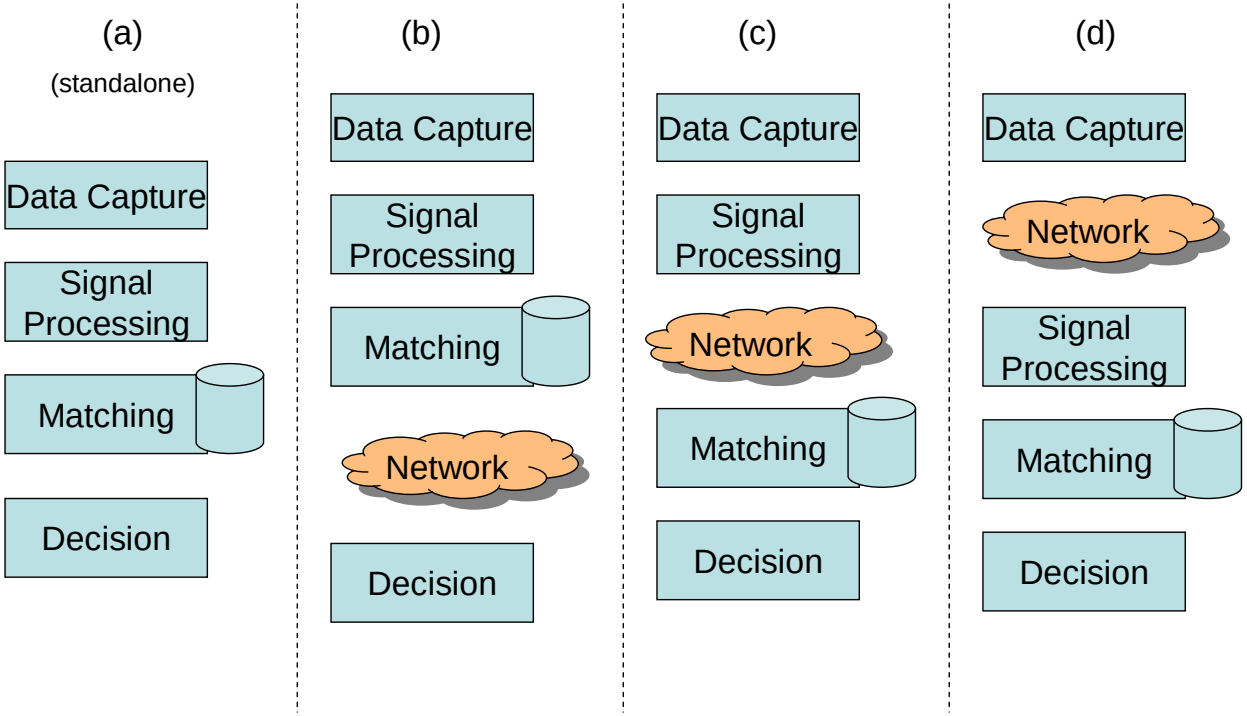
"Use Cases" and "Scenarios"

- Based on 2 sources:
  - NIST Mobile ID BPRS (2009)
  - DHS S&T MBHD (Mobile Biometric Handheld Device) (2011)
- Note reversal of terms

RICK LAZARICK

MOBILE ID BPRS "SCENARIOS"

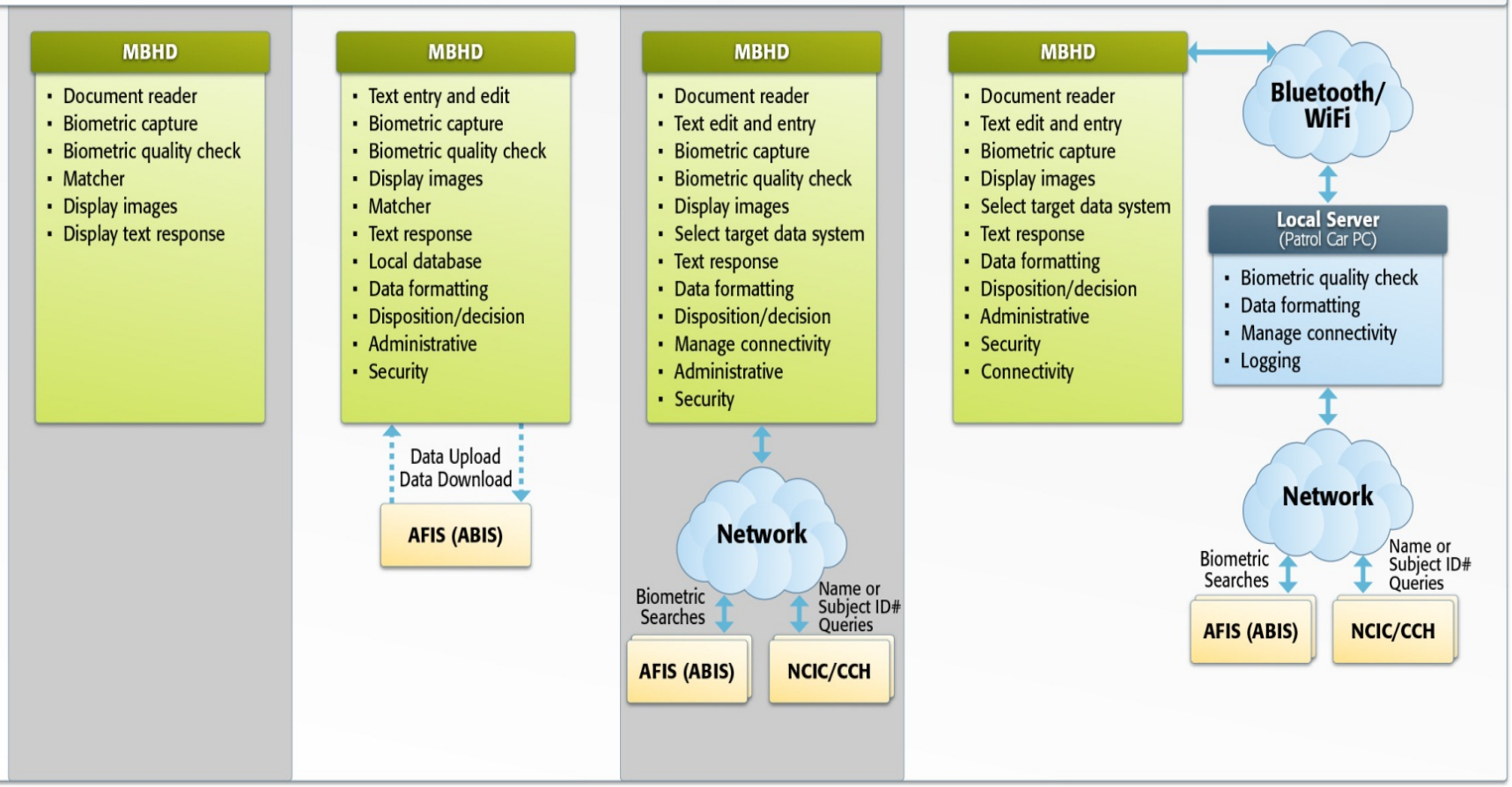
Figure 1 - Tasks Across 4 Basic Scenarios



RICK LAZARICK

MBHD "USE CASES"

Use Case	0	1	2	3
Name	Document Identity Verification	On-board AFIS	Standalone Terminal with Data Query Capability	Remote Server (CMS) Dependent Terminal with Data Query Capability
Function(s)	Verification	Enrollment, Identification, Verification	Enrollment, Identification, Verification	Enrollment, Identification, Verification



MOBILE ID BPRS "USE CASES"

Table 6 - Use cases for risks and functions

Risk to Public Safety/Function	Use Case Example	SAP Level			Notes
		Face	Finger	Iris	
Severe/ Enrollment	Field enrollment into databases with applications where there is a high risk of loss of life or assets. Some situations may require multi-modal biometric enrollment. Enrollment should achieve an equivalent level of quality as if conducted in a controlled environment using non-mobile devices.	42	45+	42	Recommend Capture: • Iris = L&R • Finger = 10 Enrolling all ten fingerprints, multiple views faces including full-face with three to five profiles, both irises, and multiple instances (captures) of each biometric provides additional search capabilities. Note for face enrollments, attempts should be made to control, background expression and lighting where it is practical to do so.
Severe/ Identification	One to many search against a database to identify a subject where there is a high risk of loss of life or assets. Some situations may require multi-modal biometric identification.	42	45+	42	Recommend Capture: • Iris = L&R eyes • Finger = 4+ Note for face identifications, attempts should be made to control, background expression and lighting where it is practical to do so.
Severe/ Verification	1:1 match against a credential or database to verify identity where there is a high risk of loss of life or assets. Some situations may require multi-modal biometric verification.	32+	20+	42	Recommend Capture: • Iris = Either eye • Finger = 2+ Note for face verifications, attempts should be made to control, background expression and lighting where it is practical to do so.

MOBILE ID BPRS "USE CASES" (2)

Moderate/ Enrollment	Mobile booking: Field cite and release when the violation is not high enough to ensure incarceration until arraignment without bail.	42	40+	32	Recommend Capture: • Iris = L&R eyes • Finger = 6+ Note for face enrollments and identifications, ideal lighting conditions should be used. Otherwise, fingerprints or irises should additionally be used.
Moderate/ Identification	In field mobile identification of a subject with questionable or no identification.	42	30+	32	Recommend Capture: • Iris = Either eye • Finger = 4+
Moderate/ Verification	Personal Identity Verification (PIV) Release from custody.	32+	20+	32	Recommend Capture: • Iris = Either eye • Finger = 2+
Mild/Enrollment	The intention is for the biometric enrolment to be of sufficient quality that it shall allow later verification (e.g. e-citations).	32	30+	22	Recommend Capture: • Iris = L&R eye • Finger = 4+
Mild/Identification	Rapid identification in custody prior to formal booking. (Typically done at the jail intake.)	32	10+	22	Recommend Capture: • Iris = Either eye • Finger = 2+
Mild/Verification (finger images).	Court Appearance/Parole/Workhouse, Personal Identity Verification (PIV).	22+	10+	22	Recommend Capture: • Iris = Either eye • Finger = 1+
Mild/Verification (finger minutiae).	Personal Identity Verification (PIV) (using minutiae).	N/A	5+	N/A	Recommend Capture: • Finger = 2+ Not recommended for use between AFIS.

MBHD "SCENARIOS"

Scenarios	Use Case 0	Use Case 1	Use Case 2	Use Case 3
Local Law Enforcement				
Law Enforcement Patrol Activities - Variation A (fingerprint)				X
Law Enforcement Patrol Activities - Variation B (face/iris)			O	X
Law Enforcement Public Event Disturbance			X	
Border Protection				
POE Identity Verification (Document Check)			X	
POE Identity Verification (US-VISIT) (Identity Check)	X			
POE Identification and Verification (US-VISIT)			X	
Maritime				
Coast Guard Interdiction			X	
Maritime Interdiction Operation (DSB Task Force, 2007)			X	
First Responders & Emergency Management				
Disaster Site Operations		X		
DHS First Responders Access Control		X		
Access Control				
Mobile Applications of TWIC	X	O		
Immigration				
Citizenship Application Processing			X	
Scenario Based on United States Border Patrol				
Hospital Scenario			X	
Identification of Deceased			X	
Checkpoint Operations			X	
Joint Operation			X	
Scenario TRADOC				
Hold, detain, release decisions regarding suspects		X		
Identification of local nationals for base access		X		
ScenarioStockton Police Department				
Field Capture Latent Pilot				X
Patrol Mobile Identifications				X
County jail house booking, transfer, and release		O		X

RICK LAZARICK

WAY FORWARD

- Define our terms and stick with them
- Early agreement on *configurations*
- Start with collection of *detailed descriptions*

RICK LAZARICK

Homeland Security

Science and Technology

MOBILE VOICE APPLICATIONS

- Presentation not authorized for distribution

PATRICK GIBBS

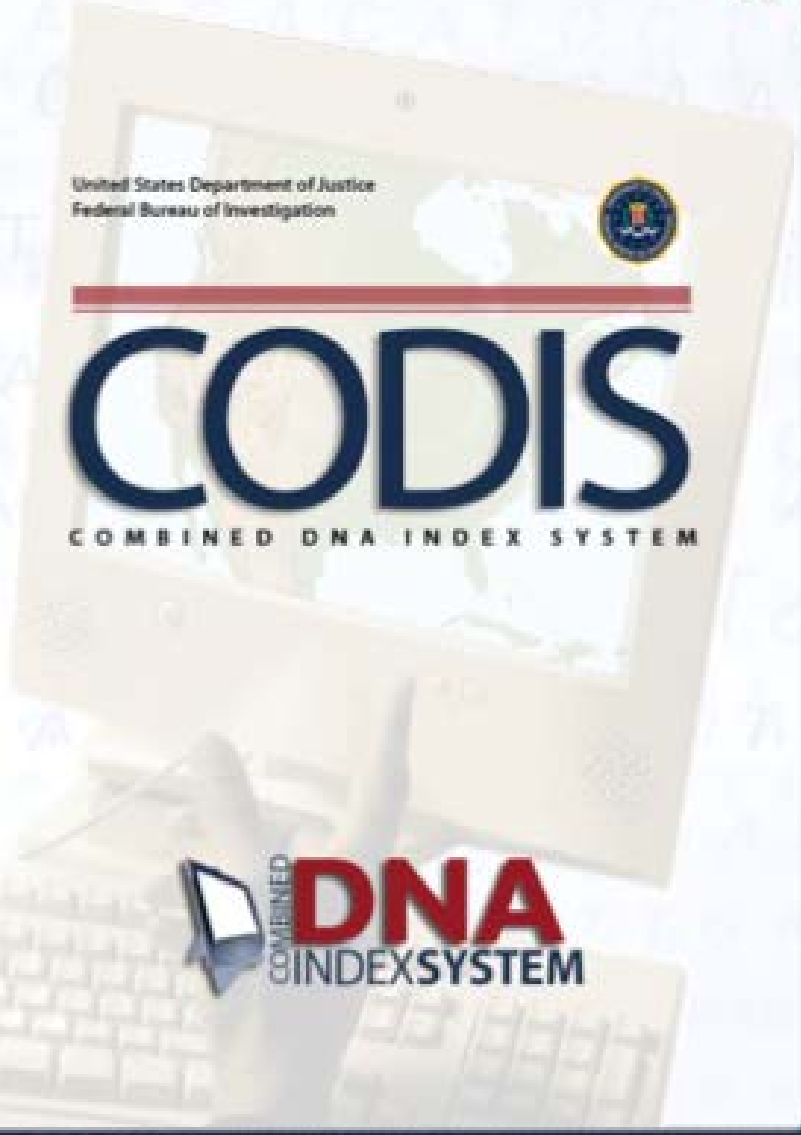
FBI CODIS AND RAPID DNA

- RapidDNA capabilities have been developed and machines deployed around the world
- Some have the capability to export data using ANSI/NIST-ITL 1-2011 format
- FBI/CODIS is not now accepting ANSI/NIST_ITL format
- DHS is testing RapidDNA units in a field environment but not linking to CODIS

KEVIN ELLIS

CODIS DNA Data Exchange Standards

Kevin M. Ellis
Requirements Manager, CODIS Unit
FBI Laboratory
October 31, 2014



Current DNA Data Exchange Formats

- CODIS currently uses an XML file format for adding and modifying specimens in the CODIS database.
- Common Message Format (CMF 3.2) is used to add specimens with STR and Y-STR loci.
- CMF 3.2 was released in July 2003.
- This format is used by commercial vendors that do not use CODIS, but need to provide DNA profiles to CODIS laboratories.

CMF 3.2

An example of an Import CMF 3.2 file results follows:


```xml
<?xml version="1.0" encoding="utf-8"?>
<CODISImportFile xmlns="urn:CODISImportFile-schema">
  <HEADERVERSION>3.2</HEADERVERSION>
  <MESSAGETYPE>Import</MESSAGETYPE>
  <DESTINATIONORI>TXDPS6900</DESTINATIONORI>
  <SOURCELAB>TXDPS6900</SOURCELAB>
  <SUBMITBYUSERID>Kevin.Ellis</SUBMITBYUSERID>
  <SUBMITDATETIME>2014-09-10T00:01:00</SUBMITDATETIME>
  <BATCHID>GFE12345</BATCHID>
  <KIT>GlobalFiler Express</KIT>
  <SPECIMEN SOURCEID="N/A">
    <SPECIMENID>ARRESTEE_01</SPECIMENID>
    <SPECIMENCATEGORY>Arrestee</SPECIMENCATEGORY>
    <LOCUS>
      <LOCUSNAME>CSF1PO</LOCUSNAME>
      <READINGBY>Kevin.Ellis</READINGBY>
      <READINGDATETIME>2014-08-22T19:56:00</READINGDATETIME>
      <ALLELE>
        <ALLELEVALUE>11</ALLELEVALUE>
      </ALLELE>
      <ALLELE>
        <ALLELEVALUE>12</ALLELEVALUE>
      </ALLELE>
```


KEVIN ELLIS

Future DNA Data Exchange Formats

- A new Rapid CMF interface specification is being developed to support the possible integration of Rapid DNA instruments with CODIS.
- Discussion is occurring with Local, State and Federal law enforcement agencies to determine how law enforcement agencies (not on CJIS WAN) can communicate with CODIS.
- Future DNA message exchanges may use the ANSI/ NIST-ITL Type-18 format.
- The FBI Laboratory Division is working with the CJIS Division to create messaging standards for Rapid DNA integration.

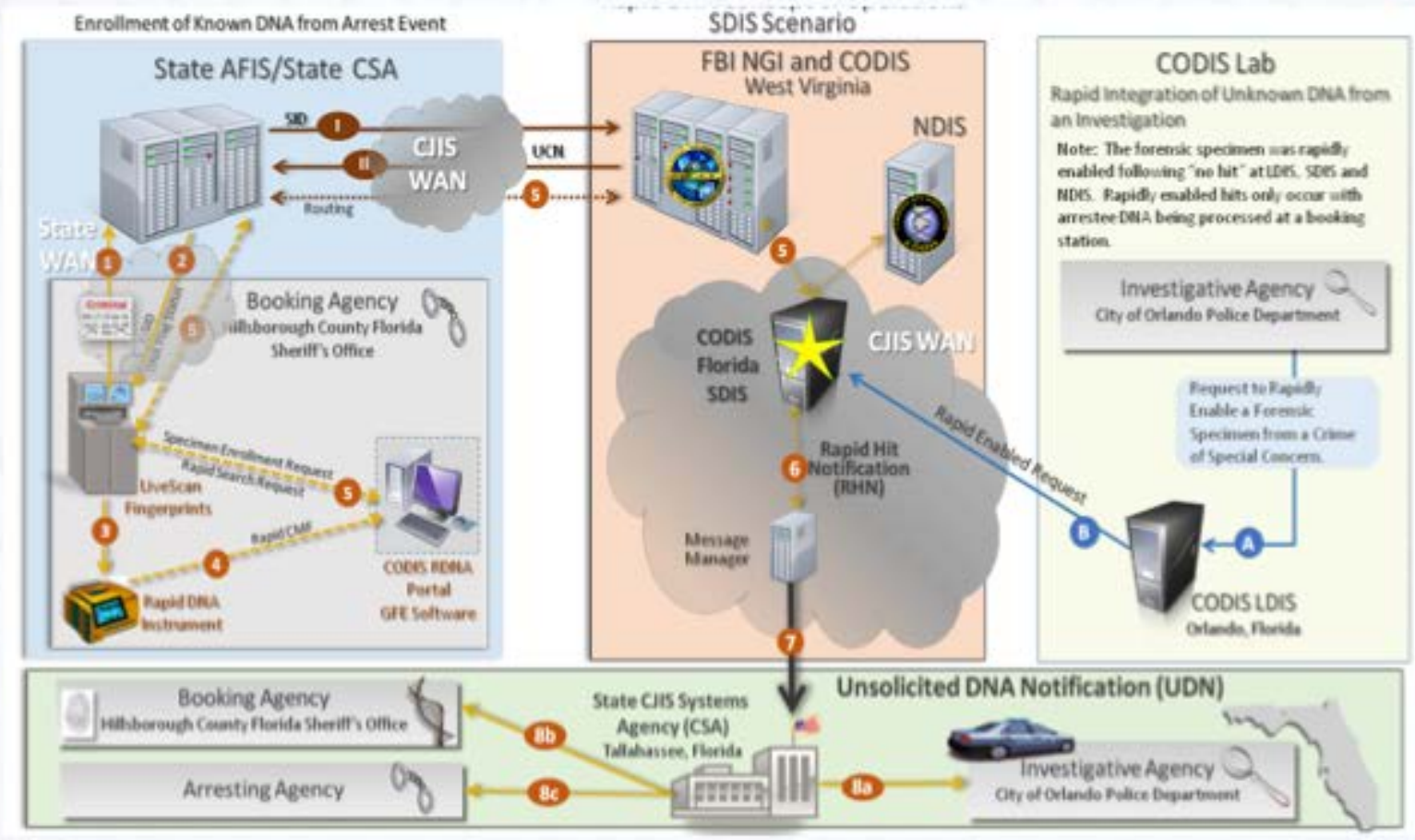
KEVIN ELLIS

Goals of FBI Rapid DNA Initiative

- Rapid DNA is being designed for use in the law enforcement booking process to analyze DNA in near real-time
- Produce CODIS-compatible DNA profiles from arrestee reference samples in the booking station environment
- Use the existing CODIS structure to search a DNA database to determine if the arrestee is linked to an unsolved crime while the individual is still in police custody

KEVIN ELLIS

Draft Rapid DNA Message Flow



Thank You

Kevin M. Ellis
CODIS Unit
703-216-2852
Kevin.Ellis2@ic.fbi.gov

MOBILE DEVICE USABILITY FOR BIOMETRIC ACQUISITION

Kristen K. Greene
NIST Visualization and Usability Group

KRISTEN GREENE

NIST DISCLAIMER

- Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology nor does it imply that the products mentioned are necessarily the best available for the purpose.

KRISTEN GREENE

OUTLINE

- Usability
- Mobile device constraints
- WSABI (Web Services for Acquiring Biometric Information)
- Designing for touch and gesture

KRISTEN GREENE

USABILITY MATTERS

- It matters A LOT
- Better usability = faster task completion times, fewer errors
- Better usability = less training

KRISTEN GREENE

USABILITY: ISO 9241

- Usability is defined (ISO 9241, 1998) as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use."

KRISTEN GREENE

USABILITY: ISO 9241

- **Effectiveness**: Accuracy and completeness with which users achieve specified goals.
- **Efficiency**: Resources expended in relation to the accuracy and completeness with which users achieve goals.
- **Satisfaction**: Freedom from discomfort, and positive attitudes towards the use of the product.
- **Context of use**: Users, tasks, equipment (hardware, software and materials), and the physical and social environments in which a product is used.

KRISTEN GREENE

DEVICE SIZE MATTERS

- Smaller devices = BIGGER usability problems
- Smaller buttons and keys
  - Onscreen keyboards
- Lack of tactile feedback
- Icon sizing and spacing
- Can’t port directly from desktop to mobile

KRISTEN GREENE

ONSCREEN KEYBOARDS

- Sizes vary *between* mobile devices
  - Based on physical differences in maximum available touchscreen real estate
- Sizes vary *within* a single device
  - Depending on device orientation (landscape versus portrait mode)
  - "splitting" the keyboard, which changes the relative distance between some keys more so than others

KRISTEN GREENE

WSABI

- Web Services for Acquiring Biometric Information
- Touchscreen interface for multimodal biometric capture
- Has undergone formal usability testing
- https://github.com/NIST-BWS/wsabi2
- http://dx.doi.org/10.6028/NIST.IR.8003
  - Design and Testing of a Mobile Touchscreen Interface for Multi-Modal Biometric Capture

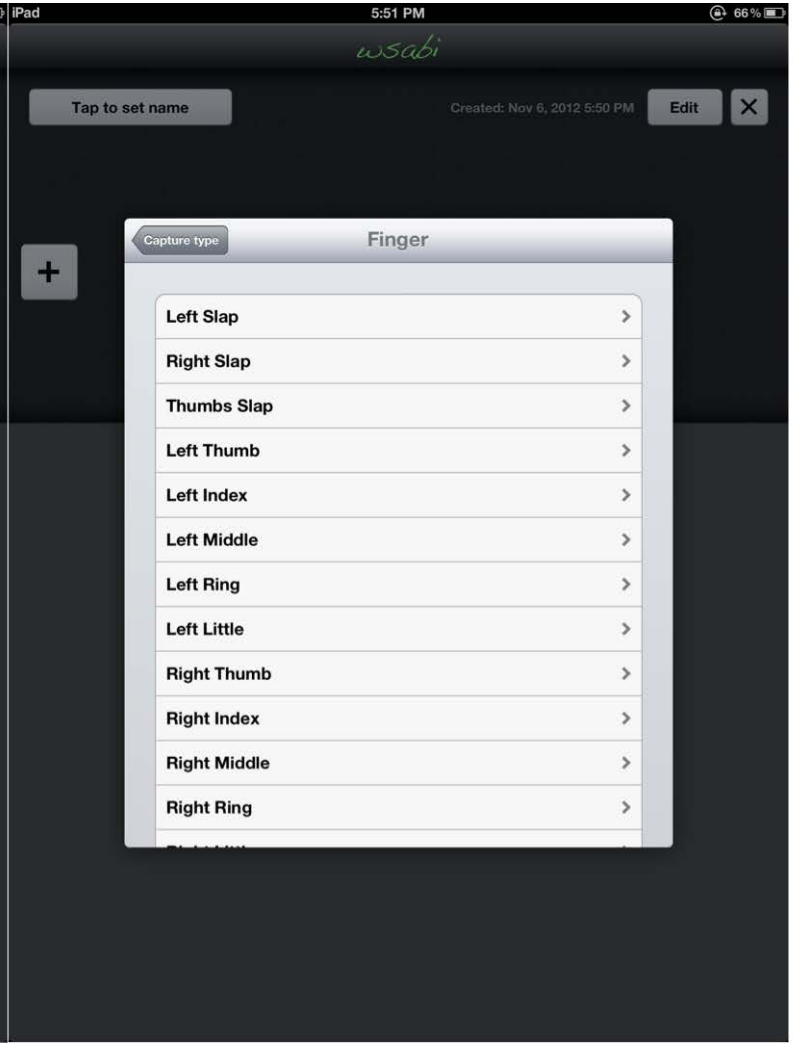
KRISTEN GREENE

WSABI

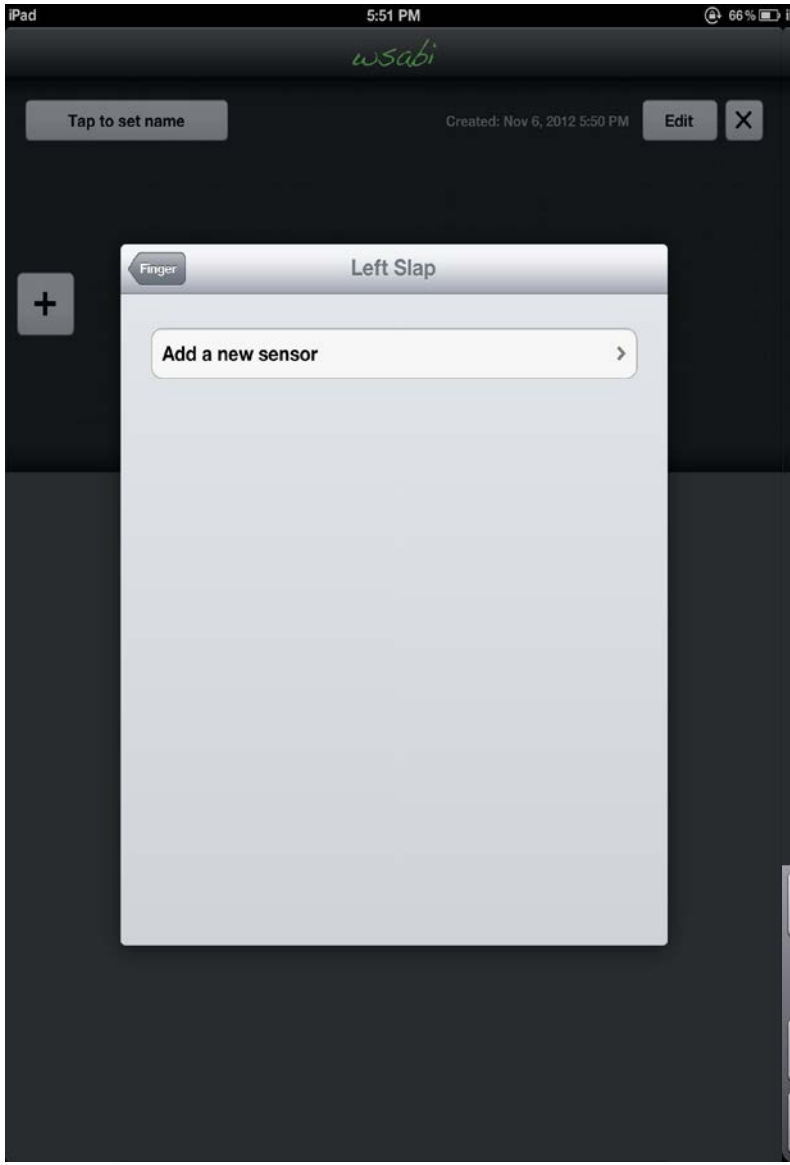
- Consistency is key
- Regardless of the biometric modality or sensor, users perform same actions to capture, annotate, clear, and retake biometric data
- Same method of sensor setup regardless of biometric modality or sensor

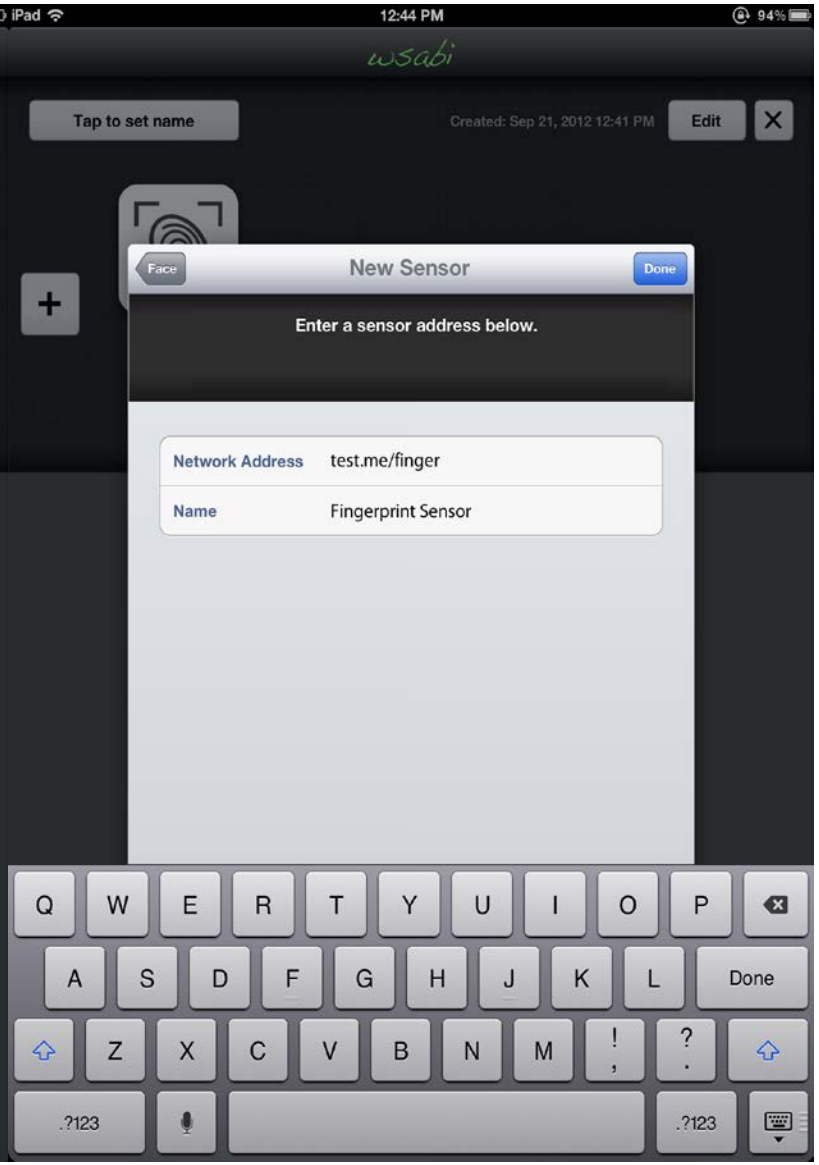
KRISTEN GREENE

KRISTEN GREENE

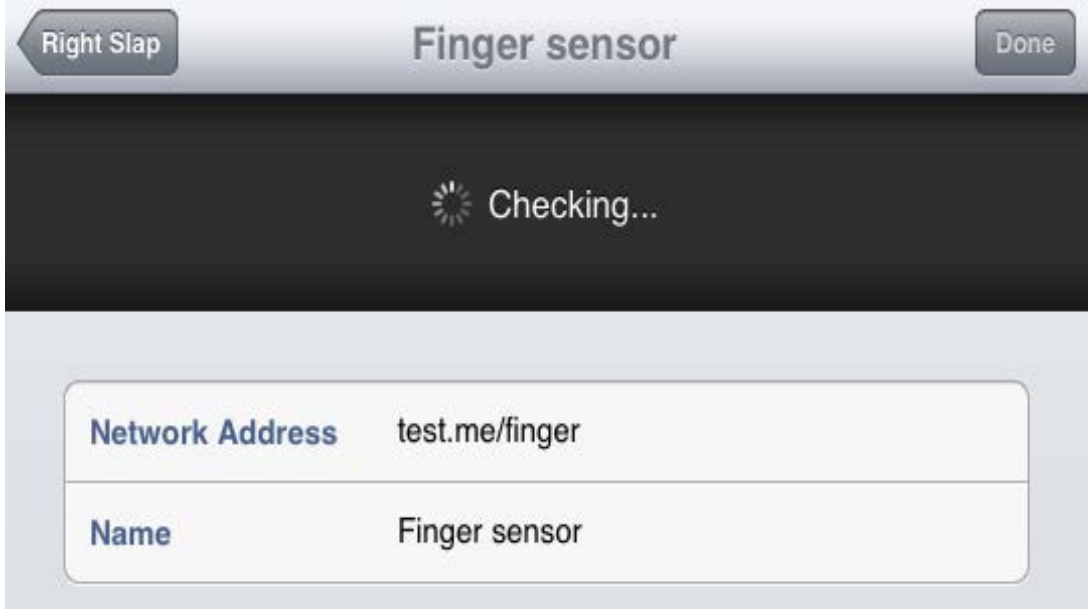


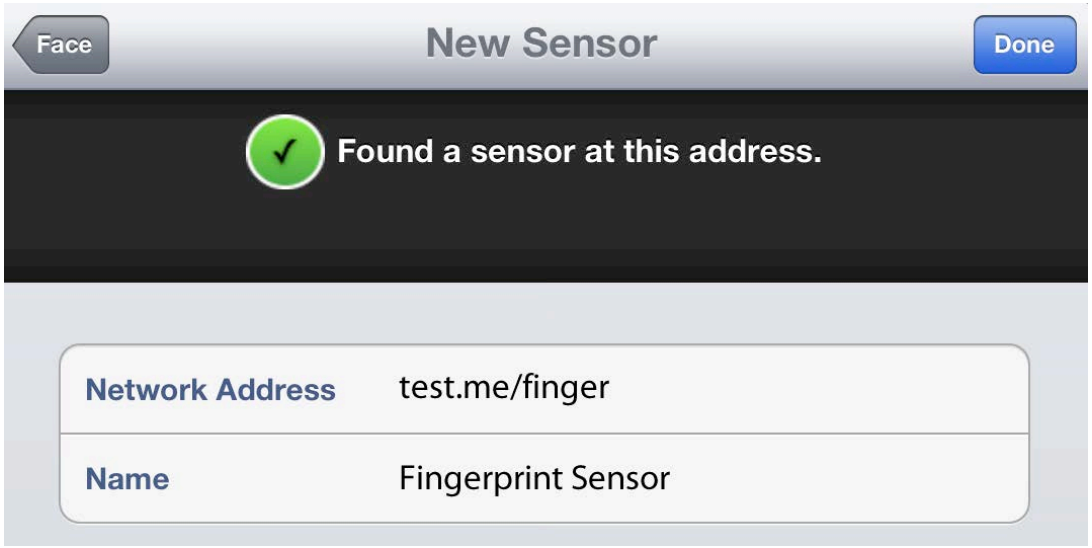
KRISTEN GREENE



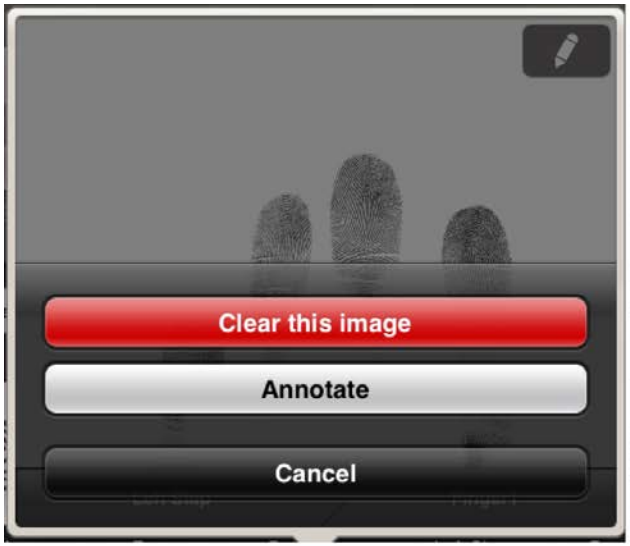


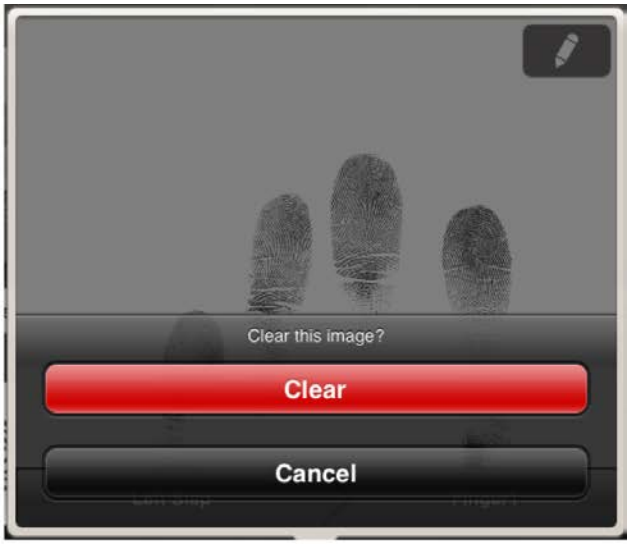
KRISTEN GREENE

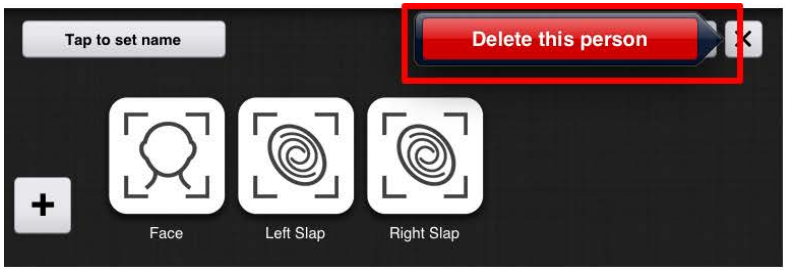


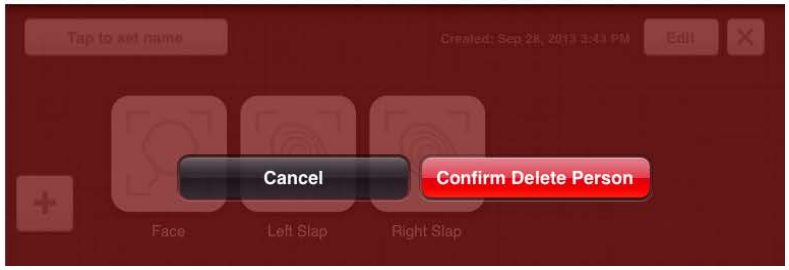


KRISTEN GREENE









KRISTEN GREENE

DESIGN GUIDELINES (A FEW)

- Design biometric acquisition software to be user- rather than sensor-centric
- Keep the core capture primitives constant
- Be consistent
- Use internationally tested, standardized symbols where possible
- Be aware of differences between desktop and mobile computing paradigms

KRISTEN GREENE

QUESTIONS?

- http://dx.doi.org/10.6028/NIST.IR.8003
  - Design and Testing of a Mobile Touchscreen Interface for Multi-Modal Biometric Capture
- kgreene@nist.gov
- bws.nist.gov

KRISTEN GREENE

BORDER PATROL USE OF IRIS IN A MOBILE ENVIRONMENT

- Remote Subject Identification
  - 1:N based on iris only
  - 1:N multimodal
  - Tablet device (peripheral or built in camera)
- Detainee Management
  - 1:1 based on iris only
  - Tablet device, multiple use cases
    - Verify identity before transfer of custody
    - Verify deportation at point of departure
    - Track detainee movement using iris

PAUL GOOD

FBI MOBILE ID SCENARIOS

PETER ALEX

GIU Biometric Tools Initiative

- MISSION: to give FBI users the tools to access the biometric identification power of the US Government in real time at any point on the planet in support of operations.

- VISION: to be the premier United States government provider of mobile identification solutions by delivering 1) the best tools, 2) and the most data, 3) with the fastest speed, 4) to the most locations, 5) for the greatest operational impact.

PETER ALEX

QCP - Components

- Current
  - Quick Capture Platform: backpack (laptop, scanner, battery, camera)

Panasonic Toughbook Laptop

Air card
(Not in all kits

BGAN Satellite
(Not in all kits)

Fingerprint Scanner

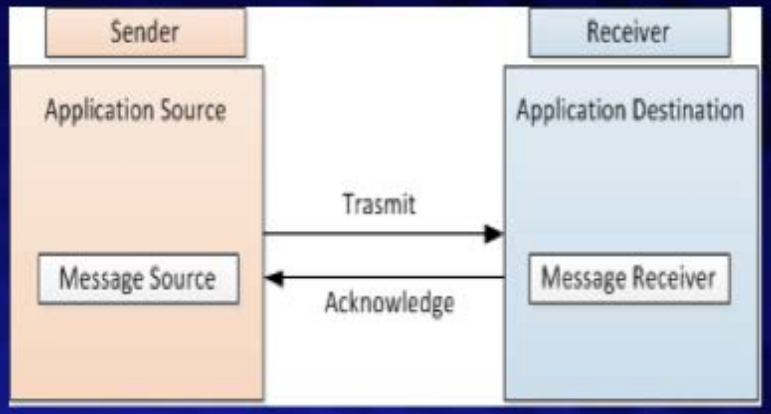
PETER

ALEX

Basic messaging model

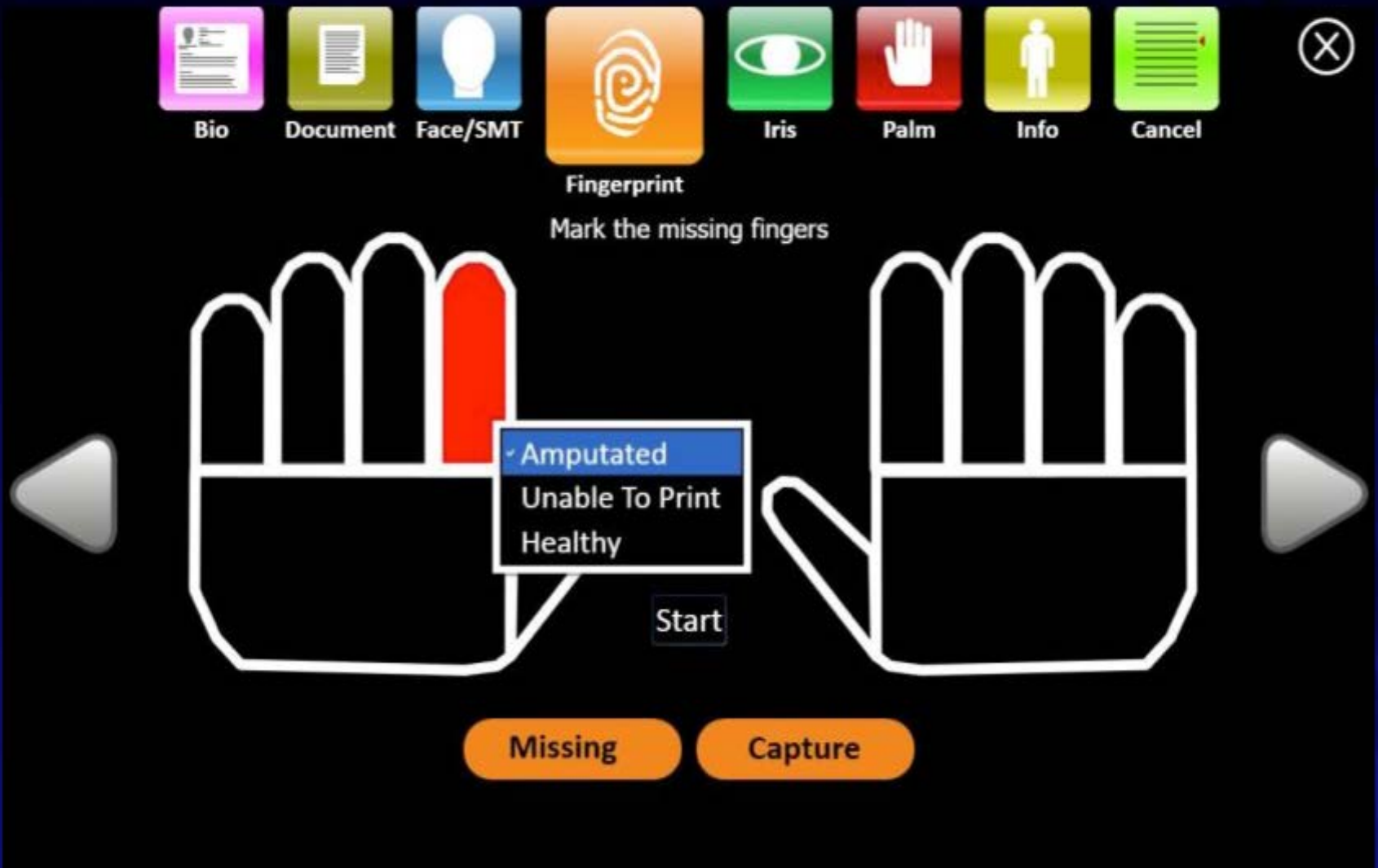
- End user
- Create transaction through application
- Open communication path
- Open transaction manager
- Transmit transaction to CJIS

- Response sent back to the transaction manager
- Notification can be viewed on the device



PETER ALEX

BCIP Software



PETER ALEX

Transaction manager

PETER ALEX

Transaction manager (Possible Rap Sheet)

Transaction Manager - TRAINING

NONIDENT: E2013295999000000004

ORI: WVIAFIS0Z
TOT: SRE
Date: 20131022
Name: NOVA,TESTING
Transaction Type: NonIdentification [SRE]
Status: Processed
Last Action: 10/22/2013 10:21:34 AM

Search

IDENT: sscn2009020000000000

ORI: USVISIT0Z
TOT: SRE
Date: 20090430
Name: TEST,TEST
Transaction Type: Identification [SRE]
Status: Processed
Last Action: 10/22/2013 10:21:35 AM

Rapsheet

This record is being sent for identification purposes only. It does not convey the individual's immigration status and is not an immigration detainer.

Statement on Disclosure of Visa Records

According to the Immigration and Nationality Act, section 222(f): The records of the Department of State and of diplomatic and consular offices of the United States pertaining to the issuance or refusal of visas or permits to enter the United States shall be considered confidential and shall be used only for the formulation, amendment, administration, or enforcement of the immigration,

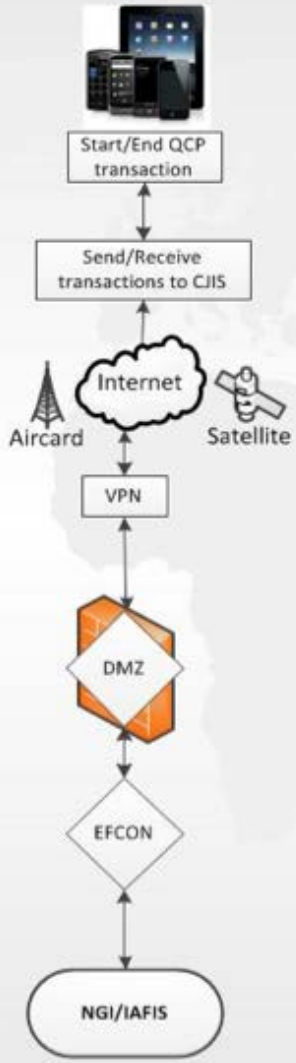
NONIDENT: 6831786

ORI: WVD0D0000
TOT: SRE
Date: 20100423
Name: NOVA,TESTING
Transaction Type: NonIdentification [SRE]
Status: Processed
Last Action: 10/22/2013 10:21:35 AM
File Name: efts.sub

10:21 AM
10/22/2013

PETER ALEX

Current Communication Path



PETER ALEX

Mobile Device

- Laptop (Current)
- Size (footprint)
  - Large
- Weight
  - Weight: Heavy
    - ~5 lbs

- Tablet (Interim)
- Size (footprint)
  - Medium
- Weight
  - Weight:
    - Light
      - ~1 lbs

- Phone (Future)
- Size (footprint)
  - Small
- Weight
  - Weight:
    - Light
      - ~5 ounces

PETER

ALEX

Mobile - Capabilities

Laptop

Primary Capabilities

- Fingerprint
- Face
- Iris

Future Capabilities

- Voice
- …

Smartphone/Tablet

Primary Capabilities

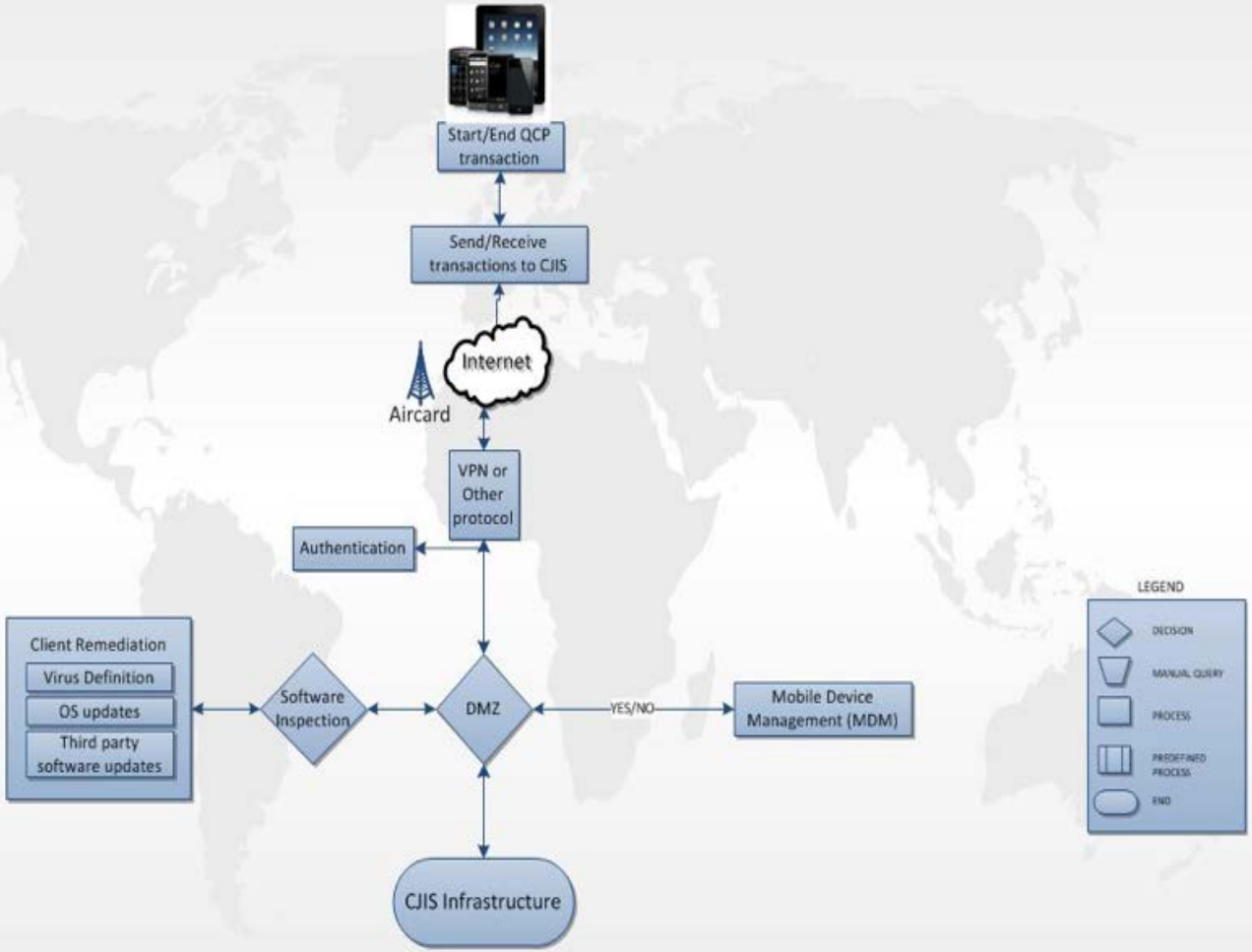
- Fingerprint

Future Capabilities

- Face
- Iris
- Voice
- …

PETER ALEX

Future Communication Path



PETER ALEX

Transmission

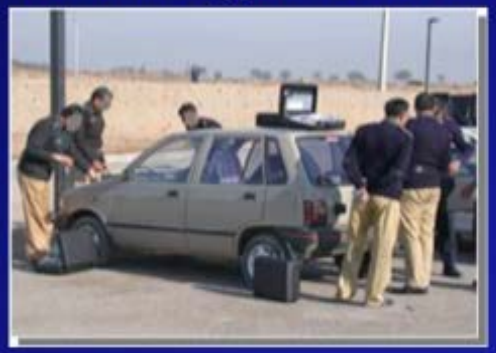
- Desktop/Laptop (Current)
  - Software
    - EBTS compliant (ebts files)
  - Communication
    - Air/Satellite
    - VPN – Cisco AnyConnect
- Mobile (Future)
  - Software
    - EBTS Compliant (ebts files)
  - Communication
    - Cellular, ….???
    - VPN, Web Service,….???

PETER ALEX

Scenarios

- Scenario 1
  - A SWAT Agent is going into a house with a potential suspect. The area the house is located has optimal cellular communication for laptop to be set up or mobile device.

- Scenario 2
  - A CAC Agent is conducting a prostitution sting operation in a hotel in a major city. Cellular communication for laptops and mobile phones will either be good or bad depending on the buildings and the city.



PETER ALEX

Scenarios

- Scenario 3
  - An VC agent is going to be traveling to a remote dessert location in New Mexico where an unidentified person of interest has been located. Cellular communication is spotty, at best.

- Scenario 4
  - A CTD agent is going to a foreign country for an operation. Cellular connectivity is very low to nonexistent.

PETER

ALEX

Scenarios

- Scenario 5
  - An team of NYC agents are conducting a mass arrest. Cellular communication is typically good depending on the building material and location.

- Scenario 6
  - A natural disaster occurs, i.e. Hurricane Katrina. Cellular connectivity can be very low to nonexistent. Agents conduct fingerprinting on the bodily remains to help identify individuals.

PETER ALEX

Questions?

Peter Alex
Global Initiatives Unit
304-625-5019
Peter.Alex@ic.fbi.gov

PETER ALEX

BIOMETRIC USABILITY: STANDARDS

Mary Theofanos

Yee-Yin Choong

National Institute of Standards and Technology
U.S. Department of Commerce

ISO/IEC SC 37 24779 INFORMATION TECHNOLOGY - PICTOGRAMS, ICONS AND SYMBOLS FOR USE WITH BIOMETRIC SYSTEMS HAS 4 ACTIVE PARTS

- Part 1: General
- Part 4: Fingerprint
- Part 5: Face
- Part 9: Vascular

MARY THEOFANOS

24779: PART 1 INFORMATION TECHNOLOGY - PICTOGRAMS, ICONS AND SYMBOLS FOR USE WITH BIOMETRIC SYSTEMS — GENERAL

General guidance for use with all biometric systems/modalitie

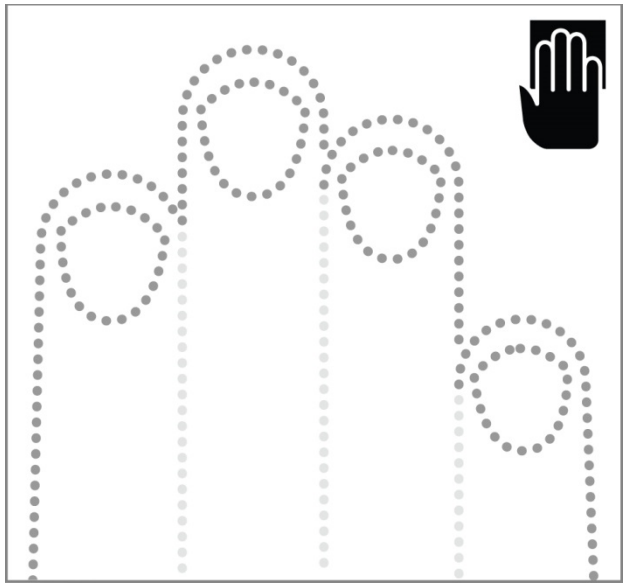
- Move forward
- Move backward
- Move left
- Move right
- Failure
- Success
- Retry
- Seek Assistance

MARY THEOFANOS

PART 4: FINGERPRINT APPLICATIONS - EXAMPLE SYMBOLS

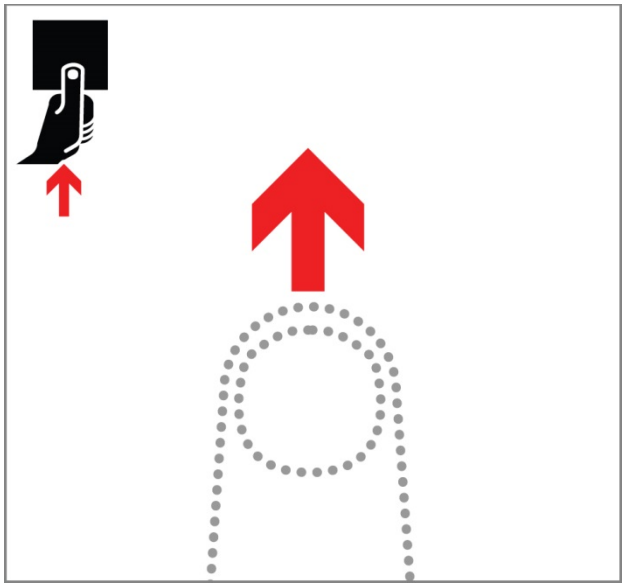
General guidance

- General overlay guide for slap



Hand positioning corrections:

- Move forward - thumb;



MARY THEOFANOS

Also have animated symbols

24779: PART 5 INFORMATION TECHNOLOGY - PICTOGRAMS, ICONS AND SYMBOLS FOR USE WITH BIOMETRIC SYSTEMS – FACE

Symbols Include:

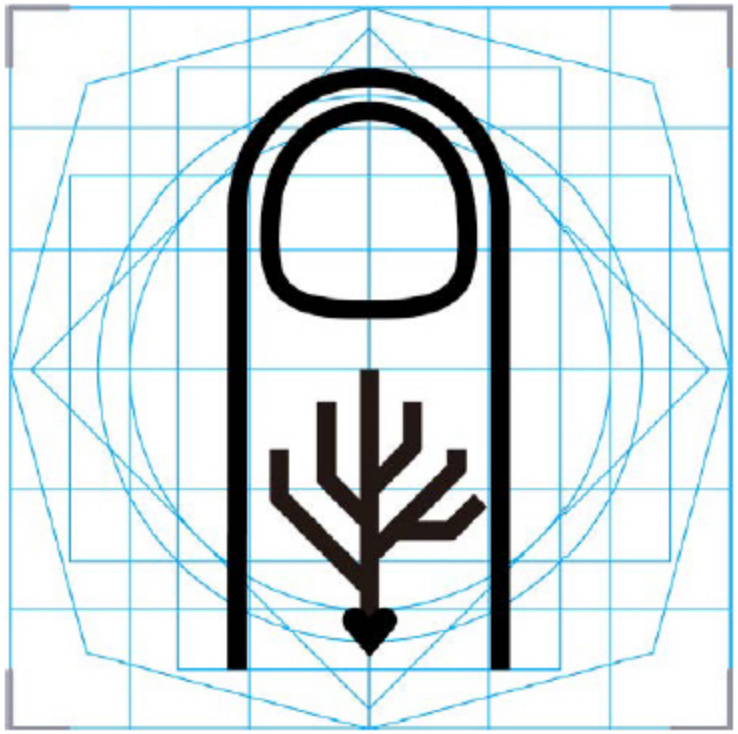
- Facial Image Capture
- Look at a point
- No Hats
- No glasses
- Move hair away from face

MARY THEOFANOS

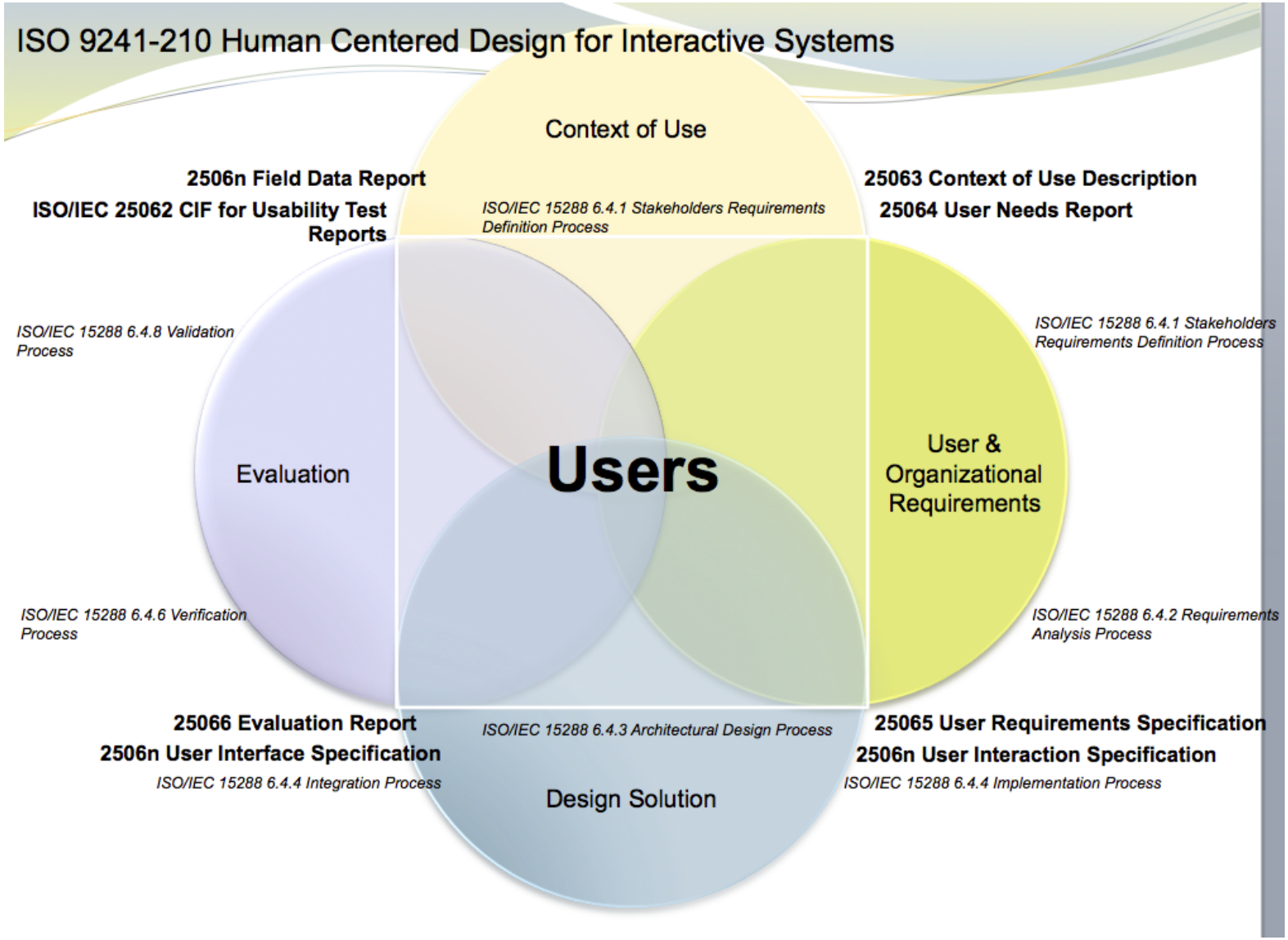
24779: PART 9 INFORMATION TECHNOLOGY - PICTOGRAMS, ICONS AND SYMBOLS FOR USE WITH BIOMETRIC SYSTEMS – VASCULAR

Symbols Include:

- Vascular Image Recognition
- Hand Vascular Image
- Finger Vascular Image

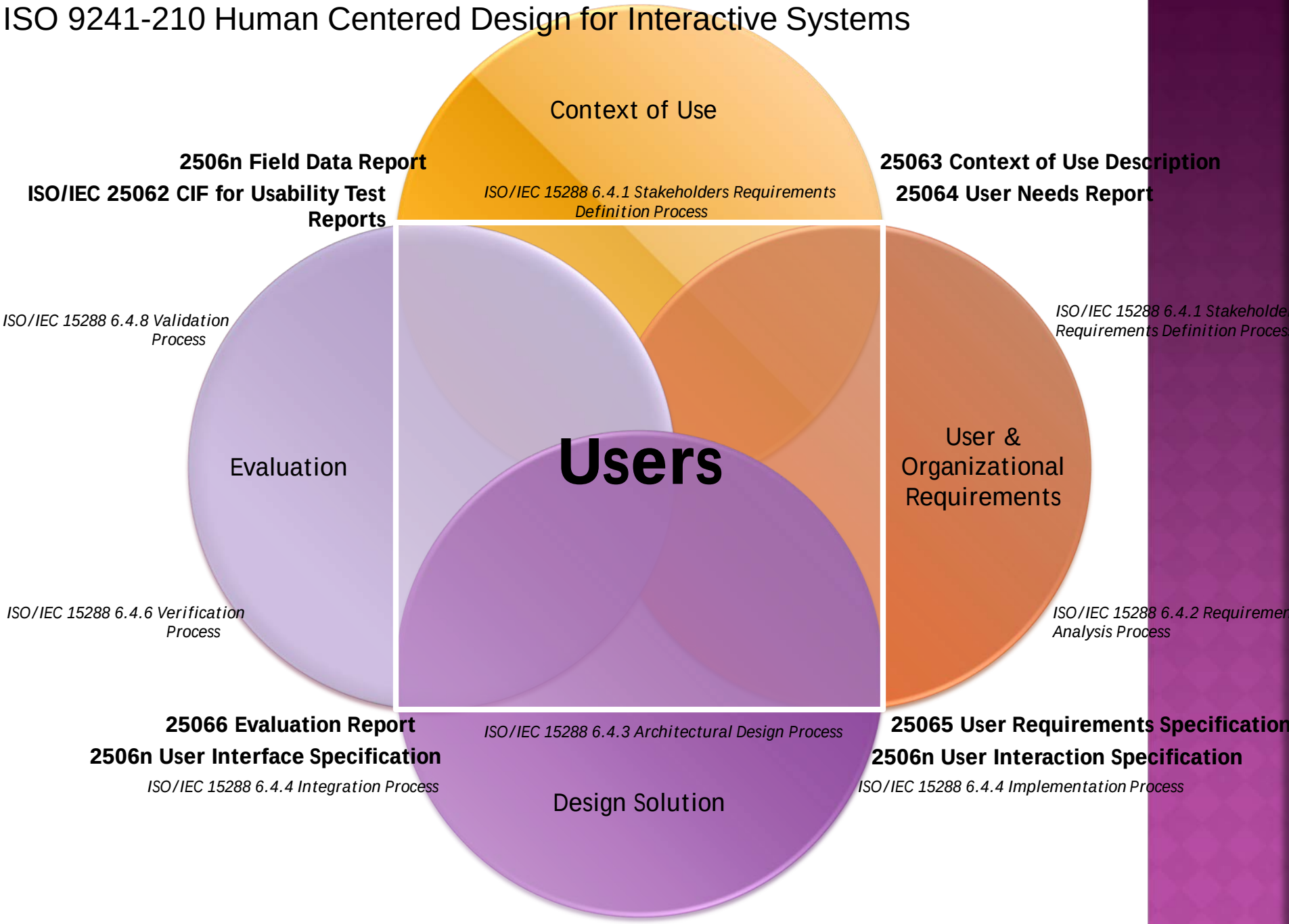


MARY THEOFANOS



MARY THEOFANOS

ISO 9241-210 Human Centered Design for Interactive Systems



CONTACT INFORMATION

Mary Theofanos

National Institute of Standards and Technology

maryt@nist.gov

Acknowledge: Department of Homeland Security Science and Technology Directorate for their support of this research

MARY THEOFANOS

NETWORK & COMMUNICATION CONSIDERATIONS FOR DIFFERENT MOBILE ARCHITECTURES

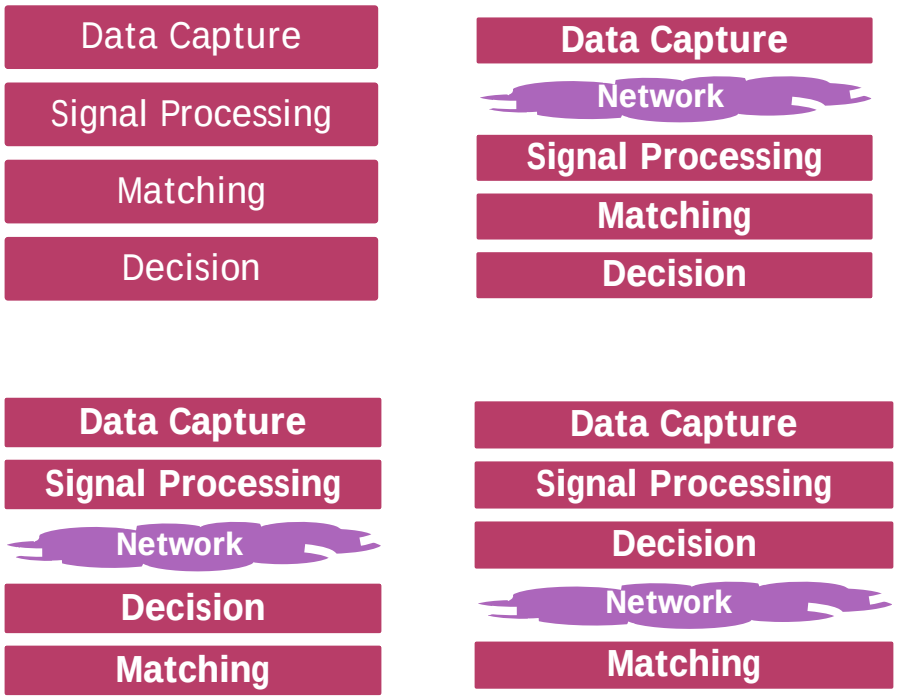
Ross J. Micheals

NIST

Mobile Best Practices Update Workshop

30 Oct 2014

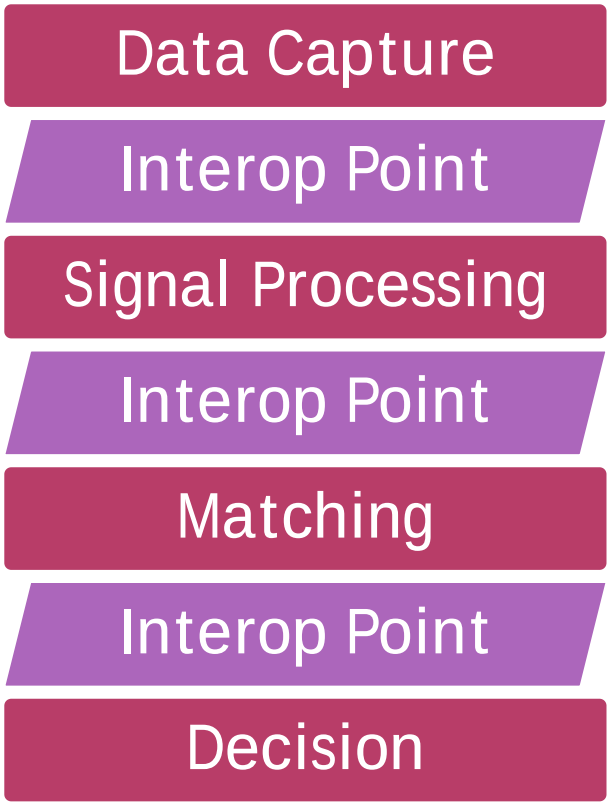
ARCHITECTURAL MODEL FROM BPR



BPR recognizes that different components may be separated by a network

Ross Micheals

PROPOSED UPDATE



- Generalize the "network" to an interoperability point; crossing a logical or physical boundary
- Multiple interop points (e.g. networks) are not just possible, but likely

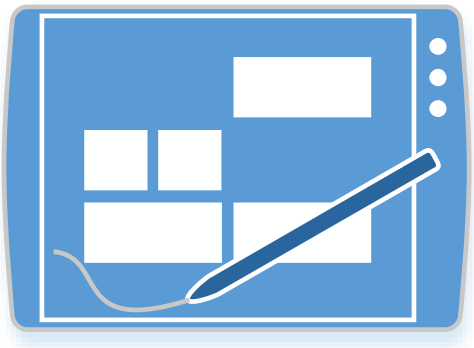
Ross Michaels

EXAMPLE ARCHITECTURES

- Consider two components
  - **sensors: (data capture and signal processing)**
  - **matchers: (matching and decision)**
- Different ways they might be ‘componentized’
- Illustrative and intended to stimulate discussion; not authoritative or a comprehensive treatment of all possible architectures

Ross Micheals

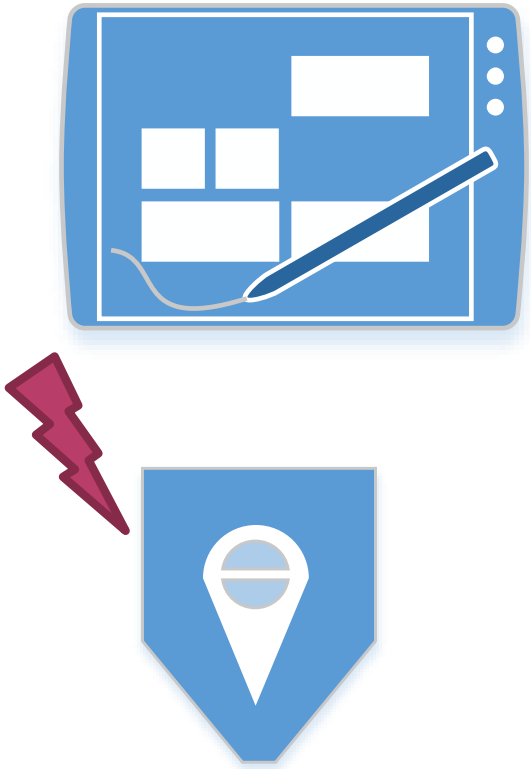
SENSOR—ALL EMBEDDED



- Most flexible with respect to interoperability points
- Explicit interoperability points may not be present; if they are, they would not require traversing a physical network
- Component communications could happen in within the same process or though a variety of interprocess communications
- Easier to make decisions that resist changes later

Ross Micheals

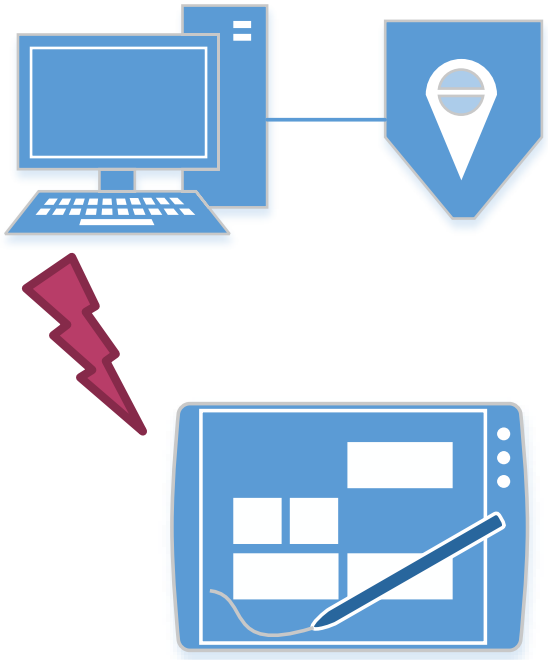
SENSOR—CLIENT DEVICE TO EMBEDDED



- Network traversal as client device requests capture and gets results
- Degree of signal processing may vary (e.g., does a template or an image come back?)
- (Typically) wireless communication might be Bluetooth, NFC, WiFi, or proprietary; **suggestion: make wired backup a best practice**
- Physical and logical integration is a sliding scale, (e.g. an intelligent ‘sleeve’)

Ross Michaels

SENSOR—CLIENT DEVICE TO TETHERED SENSOR



- Ability to leverage a great deal of computational and communications capabilities
- Network: Wireless/wifi (with Ethernet backup?)
- Enables the use of the widest variety of sensors with mobile devices:
  - Legacy
  - Luggable (e.g., DNA)
  - Fixed location (e.g., high resolution palm)

Ross Michaels

MATCHER—NO MATCHER

- Different scenarios may use a matcher at different stages during their usage
  - Data input preparation for a deployment
  - Offline matching
  - Research & development
- Systems supporting these must be designed to accommodate stages in which a matcher may not be ‘online’

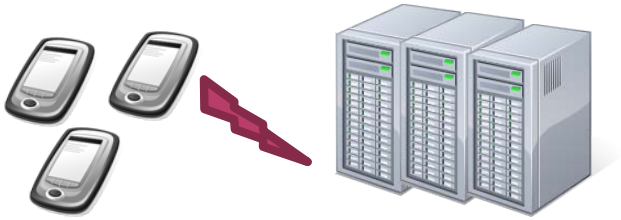
Ross Micheals

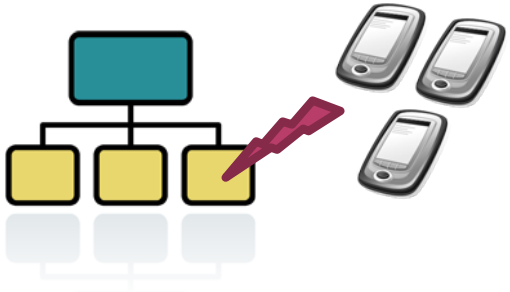
MATCHER—LOCAL MATCHER

- Matcher lives “inside” device; i.e., local ‘watch list’ with persons of interest;
- Similar to fully integrated client device
  - Most flexible with respect to interoperability points
  - Explicit interoperability points may not be present; if they are, they would not require traversing a physical network
  - Component communications could happen in process or though a variety of interposes communications
  - Easier to make decisions that resist changes later

Ross Micheals

MATCHER—REMOTE





- **Different scenarios may require different payloads**
- Scenario/deployment
  - Centralized station specific to an incident response (ad hoc server)
  - Proprietary or "local" data formats may be okay
- Large-scale matcher
  - Cellular or satellite communications
  - Formal, "curated" formats (think EBTS, ANSI/NIST)
- Branch office
  - Matcher specific to a municipality;
  - Wifi or law enforcement-dedicated communications network
  - Could be a hybrid of custom and curated formats

Ross Micheals

WEB SERVICES

- Can be applied across a diverse set of architectures (even the all embedded)
- Use the protocols that underlie the web for machine-to-machine communications
  - Evolution of existing practice (e.g., SMTP for IAFIS)
  - Nearly universal; COTS friendly
  - Well tested

Ross Michaels

OPEN BIOMETRIC WEB SERVICE SPECIFICATIONS

- OASIS Biometrics TC
  http://tinyurl.com/biometricstc
- **Biometric Identity Assurance Services (BIAS)**
  - *biometric operations (enroll, verify, identify)*
  - OASIS Standard SOAP Profile; based on INCITS 442:2010
- **WS-Biometric Devices**
  - *command and control of a biometric sensor*
  - OASIS Biometrics TC: Committee Specification Draft

Ross Michaels

QUESTIONS?

rossm@nist.gov

http://bws.nist.gov

http:// tinyurl.com/biometricstc

Ross Micheals

OTHER ISSUES TO CONSIDER

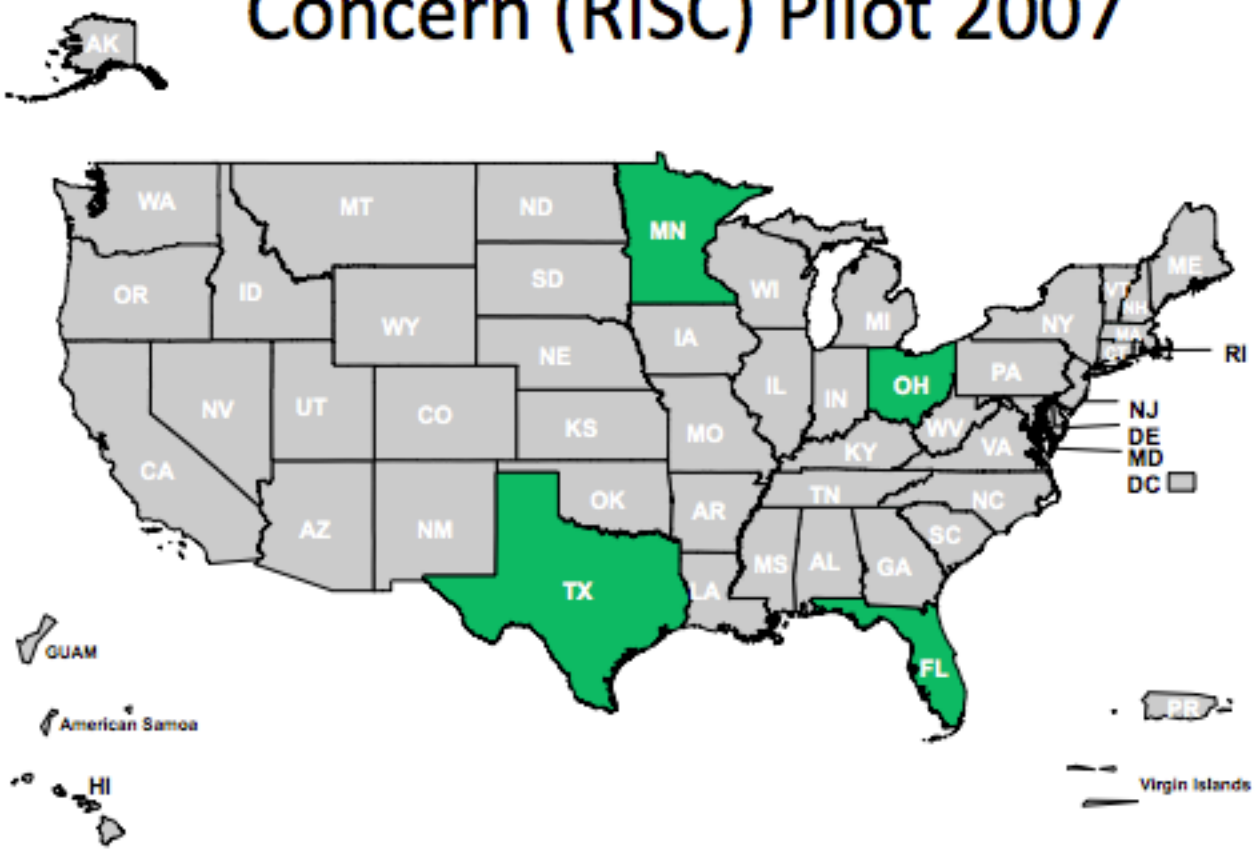
REMOVING GLASSES: IMPACT ON FACIAL RECOGNITION

- Slides presented separately

DELIA McGARRY

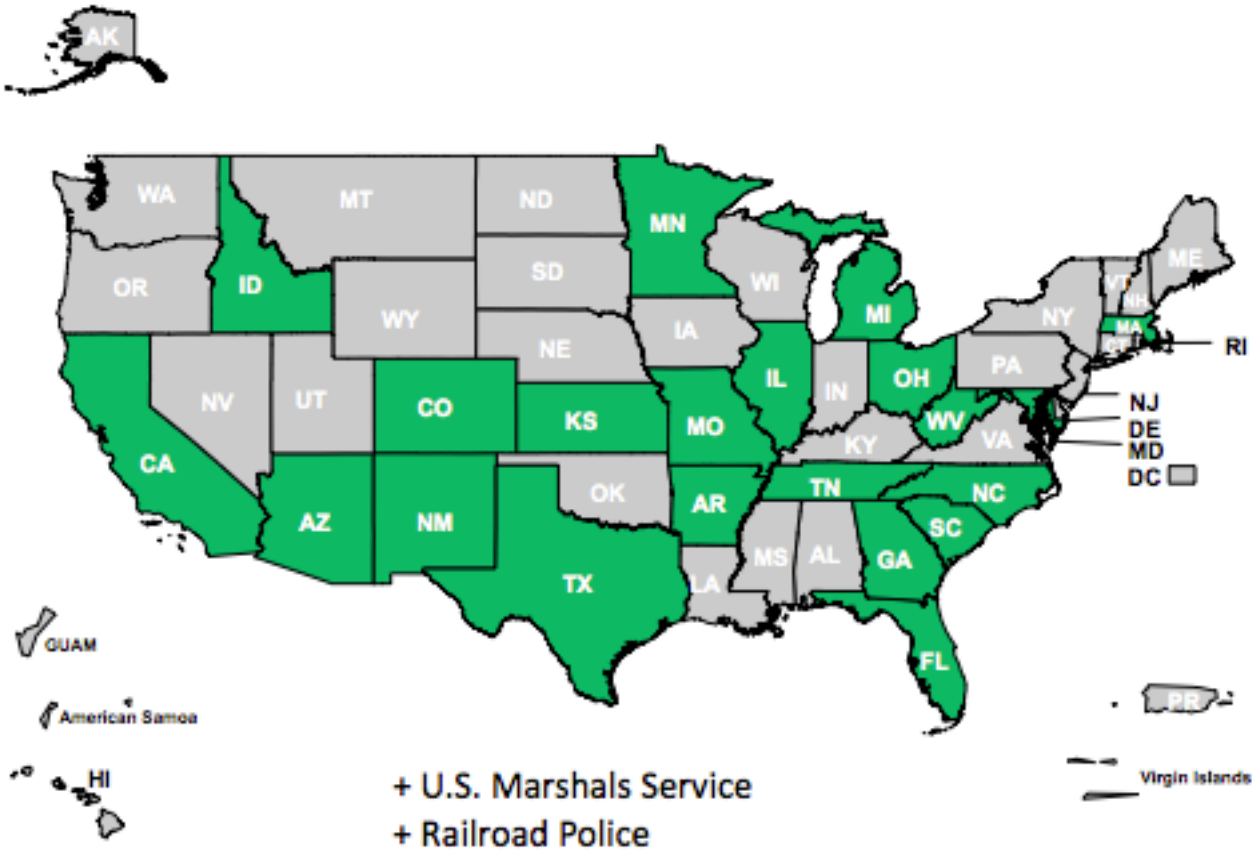
FINGERPRINT ACQUISITION PROFILES - THE FBI EXPERIENCE

Repository for Individuals of Special Concern (RISC) Pilot 2007



DAVID JONES

RISC Deployment 2014



+ U.S. Marshals Service
+ Railroad Police

DAVID JONES

RISC Stats

Over 1.3 Million Transactions Processed

- **Average Daily Submissions**
  - 1,605 (Peak 3,082)
- **Average Response Time**
  - 4.71 seconds
- **Average "Hit" Rate**
  - 4.16 %

Yellow Responses = 0.39 %

  - Yellows to "Red" = 72.5 %
- **Reject Responses** = 0.14 %

DAVID JONES

NIST Study

As a result of a CJIS Advisory Policy Board (APB) request, an independent study was conducted to examine the impact of Fingerprint Acquisition Profiles (FAPs) on the accuracy of RISC

In March 2014 the National Institute of Standards and Technology (NIST) completed a study titled:

NISTIR 7950

Examination of the Impact of Fingerprint Spatial Area Loss on Matcher Performance in Various Mobile Identification Scenarios

DAVID JONES

NIST Study

RISC Testing / Summary

- FPIR "False Positive" performance between FAP10 & FAP30 on the NGI RISC matcher appears to not be impacted significantly.
- FNIR "False Negative" performance between FAP10 & FAP30 is significant for #2 and #7 two finger submissions
  - 3.272% @FAP10
  - 1.844% @FAP20
  - 1.616% @FAP30
- If you must keep your FAP10 device, you may be able to get near-FAP30 performance by using FAP10 with 4 fingers (#2, #3, #7, #8 with FNIR of 1.714%) but sequencing errors may cause other headaches.
- EBTS- Study Results will be highlighted in a TOU and the document will be referenced in EBTS

DAVID JONES

FAP 10 and FAP 30

- CJIS "highly recommends" agencies deploying mobile ID devices searching RISC to procure FAP 30 or higher devices.
  - If agencies want to meet the RISC accuracy rate and submit only two fingerprint images, a FAP 30 device is optimal.
  - Agencies continuing to submit only two fingerprint images with FAP 10 devices may accept some risk.

DAVID JONES

Questions?

David L. Jones
Lead Analyst
david.jones3@ic.fbi.gov
304-625-4850

DAVID JONES

ADDING A NEW FAP 55 CODE FOR 3.2” X 2.0” IN MOBILE PLATFORMS

Capture[1]	SAP Levels								
	5	10	20	30	40	45	50	60	55
Acquire flat images	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Acquire rolled images	No	No	No	No	Optional	Optional	Optional	Optional	optional
Minimum resolution	500 ppi ± 10 ppi	500 ppi ± 10 ppi	500 ppi ± 10 ppi	500 ppi ± 10 ppi	500 ppi ±10 ppi [2]	500 ppi ± 5 ppi	500 ppi ± 5 ppi	500 ppi ± 5 ppi	500 ppi ± 5 ppi
Minimum Gray levels	256	256	256	256	256	256	256	256	256
Minimum Image Dimensions (wxh)	.5” x .65”	.5” x .65”	.6 ”x .8”	.8 ”x 1.0”	1.6 ”x 1.5”	1.6 ”x 1.5”	2.5” x 1.5”	3.2” x 3”	3.2” x 2”
Minimum image area	.325 sq in	.325 sq in	.48 sq in	.8 sq in	2.4 sq in	2.4 sq in	3.75 sq in	9.6 sq in	6.4 sq. in.
Compression algorithm[3]	N/A	WSQ	WSQ	WSQ	WSQ	WSQ	WSQ	WSQ	WSQ
Maximum compression ratio	N/A	10:1	10:1	10:1	15:1	15:1	15:1	15:1	15:1
Simultaneous number of fingers	1	1	1	1	1 to 2	1 to 2	1 to 3	1 to 4	1 to 4
Sensor certification	PIV	PIV	PIV	PIV	PIV	Appendix F	Appendix F	Appendix F	Appendix F
Minutiae extractor certification	PIV	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Interchange									
Image / template	Minutiae	Image	Image	Image	Image	Image	Image	Image	Image
Standard used	INCITS 378-2004	ANSI/ NIST Type-4 or Type-14	ANSI/ NIST Type-4 or Type-14	ANSI/ NIST Type-4 or Type-14	ANSI/ NIST Type-4 or Type-14	ANSI/ NIST Type-4 or Type-14	ANSI/ NIST Type-4 or Type-14	ANSI/ NIST Type-4 or Type-14	ANSI/ NIST Type-4 or Type-14

TOM BUSS

ADDING A NEW FAP 55 CODE FOR 3.2” X 2.0” IN MOBILE PLATFORMS

- FAP45 (two finger) sensors OK for ABIS field enrollment
- FAP45 not accepted by FBI/CJIS/Police for field booking.
- Need for mobile field enrollment is growing in US and international

Current situation

- LES (film/TFT based) FAP55 sensor can take shape compatible with cell phone size and thickness goals.
- FAP55 (3.2” x 2”) size meets “type 4” enrollment standard suitable for field booking (10print rolls)

Reasons for adding FAP55

presentations

STANDARDS AND REFERENCE MATERIALS

ANSI/NIST-ITL

- ANSI/NIST-ITL has been updated to include new modalities that may be useful in mobile applications
  - Voice
  - DNA
- The Acquisition Profiles of the first BPR have been incorporated into the standard for face, fingerprint and iris.
- Updated data acquisition and data storage requirements and data transmission fields should be reflected in the new BPR

BRAD WING

MOBILE ID TAXONOMY

- Based on DHS S&T Mobile Biometric Handheld Device (MBHD) Testing & Evaluation (2010-12)
  - Work was sponsored by DHS S&T HSARPA Resilient Systems Division (RSD)
  - Scope included:
    - Scenario & Use Case Analysis
    - Requirements Development
    - Test Framework Development

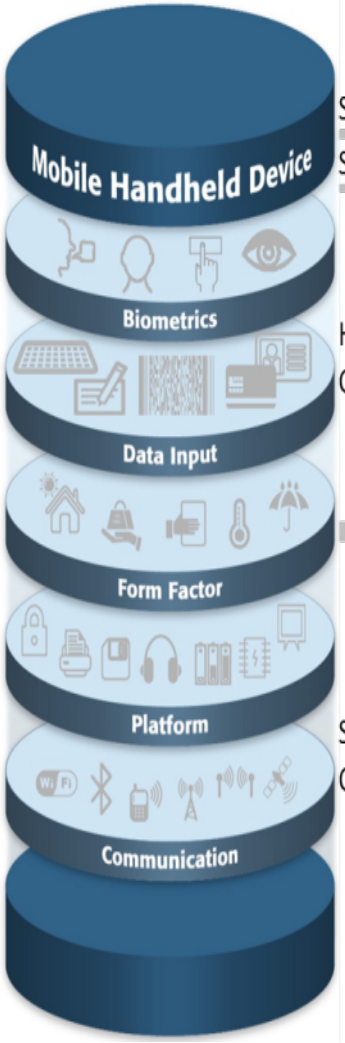
ERIC KUKULA

MBHD TAXONOMY

- Structural decomposition that provides a defined way to depict a mobile biometric handheld device into 5 subsystems
  - Each subsystem consists of components
    - Hardware
    - Software

ERIC KUKULA

MBHD TAXONOMY



System	Mobile Biometric Handheld Device				
Subsystem	***Form Factor***	***Biometrics***	***Data Input***	***Platform***	***Communication***
Hardware Components	Chassis Ingress Protections Battery Casings Access Panels	Imager (size/characteristics) Processor/Controller Imager Housing Illuminator	Keyboard Programmable Buttons Pointing Devices Touchscreen Microphone Readers Other	Processor & Memory Power Output Display Device Storage Interfaces Feedback	Wired Connectivity Wireless Connectivity
Software Components	N/A	Data Acquisition Signal Processing Matching Data Management Template Generator* Interface Control Biometric Status Monitoring Dynamic Workflow Manager Spoofing/Evasion	Acquisition Encoding/Decoding Metadata Management	Operating System Applications Formatting/Template Security Template Generator* Protocol Management	Network Management Protocols

**** Exists in multiple subsystems***

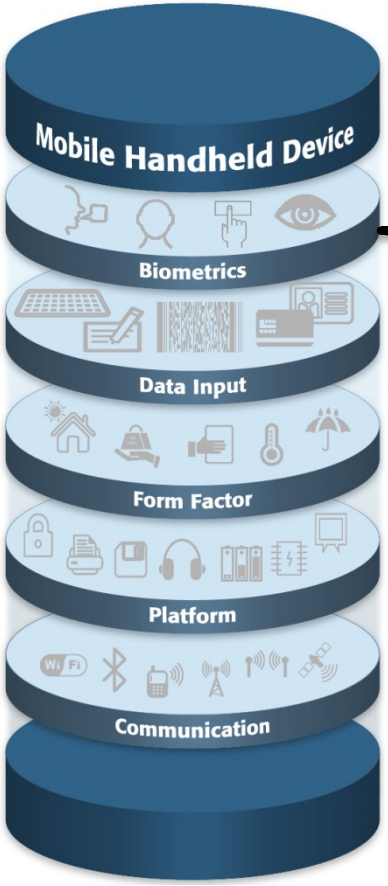
MBHD EXPANDED TAXONOMY

System	Mobile Biometric Handheld Device				
Subsystem	***Form Factor***	***Biometrics***	***Data Input***	***Platform***	***Communication***
Hardware Components	**Chassis** **Ingress Protections** **Battery Casings** **Access Panels** External Connectors Switches	**Imager (size/characteristics)** Camera Sensor Other **Processor/Controller** **Imager Housing** Frame Seals Protective Coating **Illuminator** Optical Flash Multi-Spectral IR	Keyboard Programmable Trackpad Mouse Touchscreen Stylus Microphone **Readers** Magnetic Stripe Bar Codes Smart Card RFID MRZ / OCR **Other**	**Processor & Memory** CPU Memory **Power** Battery Charging Circuit Charge Status Indicator Charger Interface Docking Station Interface* **Output** Speaker Printer **Display Device** Backlight **Storage** Internal Fixed External Remove **Interfaces** SAM SDIO Memory Expansion RS-232* Ethernet* USB* Firewire* Docking Station Interface* Wiegand Interface* **Feedback** LEDs Symbols/Pictograms Aural Tactile (Haptic)	**Wired Connectivity** RS-232* Ethernet* USB* Firewire* Docking Station Interface* Wiegand Interface* **Wireless Connectivity** **PAN** BlueTooth Body Area Networks ZigBee **LAN** IEEE 802.11 a/g/n IEEE 802.11af **WAN** GSM/GPRS/EDGE/UMTS 1xEV-DO HSPA and HSPA+ WiMAX (IEEE 802.16e and IEEE 802.16m) LTE and LTE-Advanced **Mobile Satellite Communication Systems** **Global Navigation Satellite Systems (GNSS)**
Software Components	N/A	**Data Acquisition** **Signal Processing** Segmentation Quality Feature Extraction Template Generator* **Matching** On-Board (Biometric Module) Host/API/Software Workstation CMS **Data Management** Storage Case Management **Template Generator*** **Interface Control** **Biometric Status Monitoring** **Dynamic Workflow Manager** **Spoofing/Evasion** Liveness	**Acquisition** **Encoding/Decoding** **Metadata**	**Operating System** **Applications** General Status Monitoring Dynamic Workflow Manager Output Formatting **Formatting/Template** Compression Encryption Transmission Template Generator* **Security** Physical Access Control Logical Access Control Hard Drive Encryption Cryptography **Template Generator*** **Protocol Management**	**Network Management Protocols** Secure Communications Mobile Virtual Private Network

Exists in multiple subsystems

ERIC KUKULA

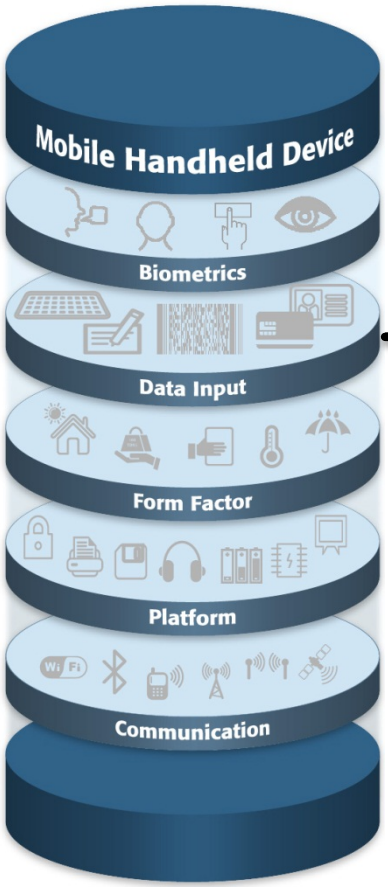
DEVICE COMPARISONS - BIOMETRICS



	HIIDE 5	Fusion	SEEK II	Mobile Ident II	MC75	BlueCheck	DSV2+ turbo	MorphoIdent	PIER-T
Fingerprint	✓	✓	✓	✓	✓	✓	✓	✓	
Single Flat	✓	✓	✓	✓	✓	✓	✓	✓	
Double Flat	✓		✓						
Rolled	✓		✓						
Face	✓	✓	✓	✓	✓	Optional			
Iris	✓	✓	✓						✓
Single Iris		✓							✓
Simultaneous	✓		✓						
On-board Matching	✓	✓	✓	✓	✓	✓	✓	✓	

*Trade names and company products have been listed in the text above. In no case does such identification imply recommendation or endorsement by Noblis or DHS S&T, nor does it imply that the products are necessarily the best available.

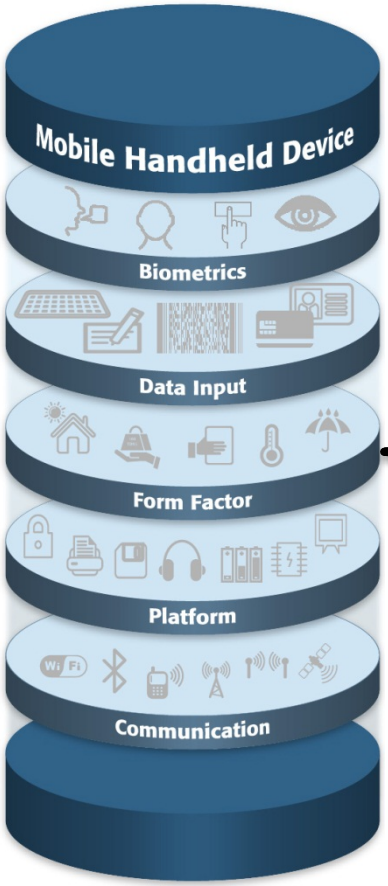
DEVICE COMPARISONS - DATA INPUT



	HIIDE 5	Fusion	SEEK II	Mobile Ident II	MC75	BlueCheck	DSV2+ turbo	MorphoIdent	PIER-T
Physical Keyboard		✓	✓		✓				
Touchscreen	✓	✓	✓	✓	✓		✓	✓	
Programmable Buttons					✓		✓	✓	✓
Readers									
Contact Smartcard	✓		Optional		Optional		✓		
Contactless Smartcard					Optional		✓		
Barcode Reader					✓		✓		
Magnetic Stripe Reader				✓					
MRZ Encoding			Optional						

*Trade names and company products have been listed in the text above. In no case does such identification imply recommendation or endorsement by Noblis or DHS S&T, nor does it imply that the products are necessarily the best available.

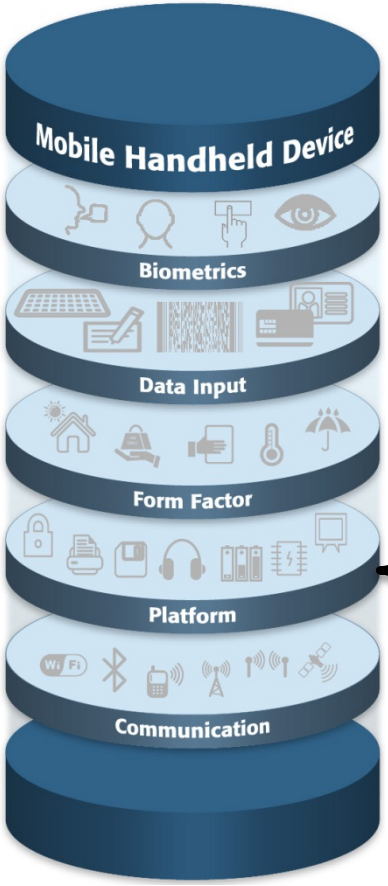
DEVICE COMPARISONS - FORM FACTOR



	HIIDE 5	Fusion	SEEK II	Mobile Ident II	MC75	BlueCheck	DSV2+ turbo	MorphoIdent	PIER-T
Weight									
< 1 lb				✓	✓	✓		✓	✓
1 - 3 lbs		✓					✓		
> 3lbs	✓		✓						
Size (LxWxD)	5 x 8 x 3	8.74 x 4.61 x 2.91	8.75 x 5.5 x 3.5	6 x 3.15 x 1.30	6 x 3.1 x 1.7	4.45 x 1.69 x 0.87	7.3 x 7.3 x 2	5.2 x 2.6 x 0.7	3.5 x 5.0 x 2.6
S/M/L	Large	Large	Large	Medium	Medium	Small	Large	Small	Medium
MIL-STD-810F	✓	✓	✓				✓		
IP Rating	54	65	65		54		54		

*Trade names and company products have been listed in the text above. In no case does such identification imply recommendation or endorsement by Noblis or DHS S&T, nor does it imply that the products are necessarily the best available.

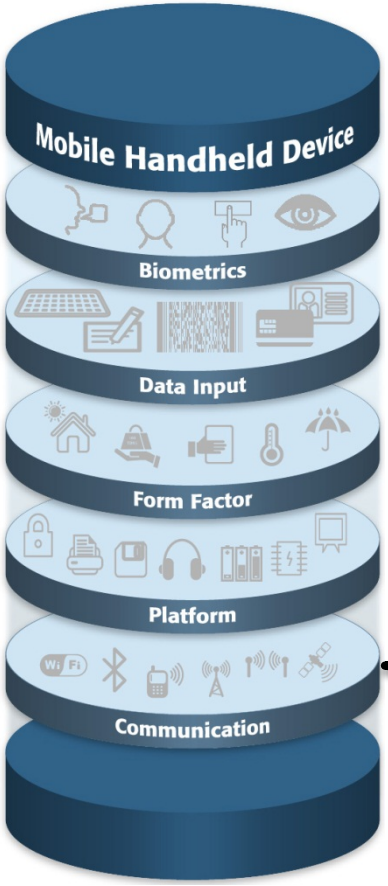
DEVICE COMPARISONS - PLATFORM



	HIIDE 5	Fusion	SEEK II	Mobile Ident II	MC75	BlueCheck	DSV2+ turbo	Morpholdent	PIER-T
CPU	Intel Atom				Intel Xscale		Renesas SH4 7760		TI dual core
Storage	80 GB SSD	128 MB Flash	64 GB SSD	128 MB Flash	256 MB Flash	2MB Flash	256 MB Flash		64 MB Flash
Display									
Size	5"	3.5"	4.1"	3.5"	3.5"		3.5"	2.4"	
Resolution	800x480	320x240	800x480	320x240	640x480	96x64	240x320	320x240	220x176
Battery									
Hot-swappable		✓	✓		Optional				
Lasts 8+ Hours	✓	✓			✓		✓	✓	
Peripheral Required?					✓	✓			✓

*Trade names and company products have been listed in the text above. In no case does such identification imply recommendation or endorsement by Noblis or DHS S&T, nor does it imply that the products are necessarily the best available.

DEVICE COMPARISONS - COMMS



	HIIDE 5	Fusion	SEEK II	Mobile Ident II	MC75	BlueCheck	DSV2+ turbo	MorphoIdent	PIER-T
WiFi	✓	✓	✓	✓	✓		Optional		
Bluetooth	✓	✓	✓	✓	✓	✓	Optional	✓	
GSM	✓	✓		✓	✓		Optional		
CDMA	✓	✓		✓	✓		Optional		
4G	✓								
Ethernet	✓		✓						
USB	✓	✓	✓	✓	✓	✓	✓	✓	✓
Docking Station						Optional	✓		
GPS	✓	✓	✓	Optional	✓				

*Trade names and company products have been listed in the text above. In no case does such identification imply recommendation or endorsement by Noblis or DHS S&T, nor does it imply that the products are necessarily the best available.

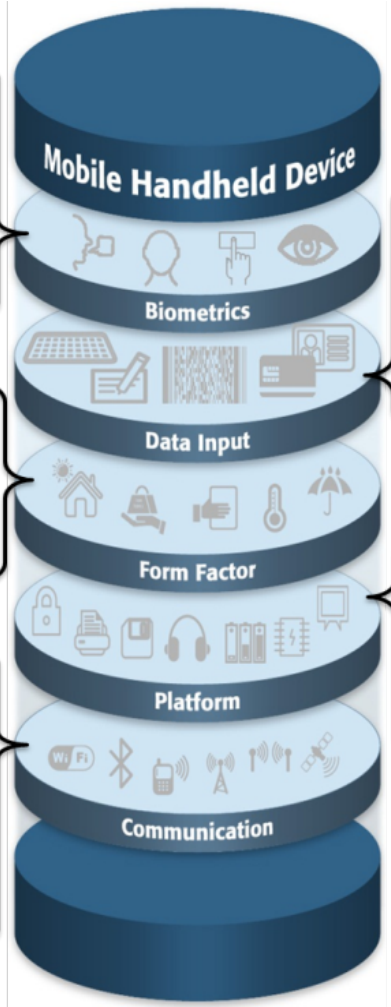
COTS DEVICES MAPPED TO THE TAXONOMY (2011-12)

- Analyzed over 30 COTS MBHD devices*

	HIIDE 5	Fusion	SEEK II	Mobile Ident II	MC75	BlueCheck	DSV2+ turbo	Morpholdent	PIER-T
Fingerprint	✓	✓	✓	✓	✓	✓	✓	✓	
Single Flat	✓	✓	✓	✓	✓	✓	✓	✓	
Double Flat	✓		✓						
Rolled	✓		✓						
Face	✓	✓	✓	✓	✓	Optional			
Iris	✓	✓	✓						✓
Single Iris		✓							✓
Simultaneous	✓		✓						
On-board Matching	✓	✓	✓	✓	✓	✓	✓	✓	

	HIIDE 5	Fusion	SEEK II	Mobile Ident II	MC75	BlueCheck	DSV2+ turbo	Morpholdent	PIER-T
Weight									
< 1 lb				✓	✓	✓		✓	✓
1 - 3 lbs		✓					✓		
> 3 lbs	✓		✓						
Size (LxWxD)	5x8x3	8.74x4.61x2.91	8.75x5.5x3.5	6x3.15x1.30	6x3.1x1.7	4.45x1.69x0.87	7.3x7.3x2	5.2x2.6x0.7	3.5x5.0x2.6
S/M/L	Large	Large	Large	Medium	Medium	Small	Large	Small	Medium
MIL-STD-810F	✓	✓	✓				✓		
IP Rating	54	65	65		54		54		

	HIIDE 5	Fusion	SEEK II	Mobile Ident II	MC75	BlueCheck	DSV2+ turbo	Morpholdent	PIER-T
WiFi	✓	✓	✓	✓	✓		Optional		
Bluetooth	✓	✓	✓	✓	✓	✓	Optional	✓	
GSM	✓	✓	✓	✓	✓		Optional		
CDMA	✓	✓	✓	✓	✓		Optional		
4G	✓		Optional						
Ethernet	✓		✓						
USB	✓	✓	✓	✓	✓	✓	✓	✓	✓
Docking Station						Optional	✓		
GPS	✓	✓	✓	Optional	✓				



	HIIDE 5	Fusion	SEEK II	Mobile Ident II	MC75	BlueCheck	DSV2+ turbo	Morpholdent	PIER-T
Keyboard		✓	✓		✓				
Touchscreen	✓	✓	✓	✓	✓		✓	✓	
Programmable Buttons					✓		✓	✓	✓
Readers									
Smartcard	✓		Optional		Optional		✓		
Smartcard					Optional		✓		
Barcode Reader					✓		✓		
Reader				✓					
MRZ Encoding			Optional						

	HIIDE 5	Fusion	SEEK II	Mobile Ident II	MC75	BlueCheck	DSV2+ turbo	Morpholdent	PIER-T
CPU	Intel Atom				Intel Xscale		Renesas SH4 7760		TI dual core
Storage	500,000+	100,000+	60,000			1,200 - 6,000			
Display									
Size	5"	3.5"	4.1"	3.5"	3.5"		3.5"	2.4"	
Resolution	800x480	320x240	800x480	320x240	640x480	96x64	240x320	320x240	220x176
Battery									
Hot-swappable		✓	✓		Optional				
Lasts 8+ Hours	✓	✓			✓		✓	✓	
Peripheral Required?					✓	✓			✓

*Trade names and company products have been listed in the text above. In no case does such identification imply recommendation or endorsement by Noblis or DHS S&T, nor does it imply that the products are necessarily the best available.

SECTION 12.2 WIRELESS COMMUNICATION

Original BPR Sections

- Wireless Connectivity
- Cellular Connectivity
  - GSM/GPRS/EDGE/UMTS
  - CDMA/1XRTT/EVDO/EVDM
  - HSDPA/WCDMA
- Satellite Communications
- 802.11 b/g
- Bluetooth
- Global Positioning System (GPS)
- Integrated Wireless Antenna
- Wireless Connection Status

Updates needed to reflect current technology

- Wireless Personal Area Networks (WPANs)
  - BlueTooth® (IEEE 802.15.3)
  - ZigBee (IEEE 802.15.4)
  - 6loPAN (IEEE 802.15.4)
  - Mesh sensor networks (IEEE 802.15.5)
  - Body Area Networks (IEEE 802.15.6)
- Wireless Local Area Networks (WLANs)
  - IEEE 802.11a/g/n/ac
- Wide Area Networks (WANs)
  - HSPA and HSPA+
  - WiMAX (IEEE 802.16e and IEEE 802.16m)
  - LTE and LTE-Advanced
- Regional Area Networks (TV White Space) [IEEE 802.22]
- Mobile Satellite Communication Systems
- Global Navigation Satellite Systems (GNSS)

Note: List is non-exhaustive.

ERIC KUKULA

SECTION 13 ENVT CONSIDERATIONS - UPDATES NEEDED?

Environmental Profile	Description
Indoor (Normal)	office environments such as an office building, court of law, etc. Operating temperatures: From 32°F to 104°F (0°C to 40°C) Storage temperatures: From 14°F to 122°F (-10°C to 50°C) Relative humidity: max. 85% non condensing Ingress Protection Rating (IP Code): IP 40 or higher
Law Enforcement (Moderate)	Indoor/outdoor, i.e. patrol officer or in patrol car Operating temperatures: From 14°F to 122°F (-10°C to 50°C) Storage temperatures: From -4°F to 140° F (-20°C to 60°C) Relative humidity: 10% - 90% non condensing Ingress Protection Rating (IP Code): IP 54 or higher, in operational configuration, with any existing expansion port closed Drop resistance: Resistance to multiple drops on concrete from a height of 3 feet (91 cm).
Military (Extreme)	harsh environments, such as extreme temperatures, exposure to dust, sand, rain, water splashes, vibrations, and dropping of the device. Operating temperatures: From -20°F to 140°F (-29°C to 60°C) according to MIL-STD-810F Method 501.4 Procedure II at 140°F MIL-STD-810F Method 502.4 Procedure II at -20°F Storage temperatures: From -20°F to 140°F (-29°C to 60°C) according to MIL-STD-810F Method 501.4 Procedure I at 140°F MIL-STD-810F Method 502.4 Procedure I at -20°F Relative humidity: MIL-STD-810F Method 507.4 Rain: MIL-STD-810F Method 506.4 Procedure I Ingress Protection Rating (IP Code): IP 65 or higher, in operational configuration, with any existing expansion port closed Drop resistance: The devices should comply with MIL-STD-810F Method 516.5 – Procedure IV (Transit Drop), in non-operational configuration. If the devices do not contain a hard drive, compliance is required also in the operational configuration. Vibration resistance: The devices should comply with MIL-STD-810F Method 514.5 – Procedure I (General Vibration), in both operational and non-operational configurations.

ERIC KUKULA

WEARABLE BIOMETRIC CAPTURE DEVICES

- Several different types, some including multiple modalities (usually face and voice)
  - Google glasses
  - Near-field communications
    - Disney's MyMagic wristband
    - Bionym electrocardiogram bracelets
  - Cameras worn by police to record incidents
    - Built-in facial recognition to compare against local watchlists
    - Voice capture for later forensic analysis
  - Medical device monitors
  - Helmets with iris recognition (to ID wearer) in goggles
  - Micro-feature recognition and gesture recognition
  - Biometrically verified weapons use
  - And more!

SOME CHALLENGES FOR MOBILE ID THAT MAY BE DIFFERENT THAN FIXED LOCATION UNITS

- 3D printing of body parts / Reconstructive surgery
- Spoofing and non-cooperative / un-cooperative behavior that is not likely or typical at fixed location units
- Failure-to-acquire protocols
- Privacy and use of data (particularly for DNA)
- Disposal of the mobile unit (including erasure of data)
  - Some units may designed for one-time or limited use
- Protocols for data handling (including erasure of data) during field ops
- Remote or timed disabling operations of the unit (if stolen or misplaced)
- Mobile medical screening combined with biometrics
- Admissibility of data / match results for law enforcement applications
- Interoperability and verified linking of data
- Additional automated modalities (hair pattern growth on face, ear shape, ocular region, blood type, classifiers for 'soft' biometrics: height / weight / age / ethnicity / gender / tattoo and scar, etc.)
- Combination with / in devices designed to show exposure to explosives, illegal drugs, pathogens, etc.
- Combination with / in devices to detect health and responsiveness of persons under medical care, in battlefields, or under supervised detention or quarantine
- Operation in harsh environments and under dangerous situations
- Verification of identity of the unit operator and data entry personnel

BRAD WING

IRIS ACQUISITION GUIDANCE

James Cambier, Ph.D.
Crossmatch Technologies, Inc.

- MobileID BPR for iris images should be consistent with current and emerging standards:
  - ISO/IEC 19794-6:2011 Information technology – Biometric data interchange formats – Iris image data
  - FDIS 29794-6 Information technology – Biometric sample quality – Iris image data
- Three areas of inconsistency
  - Image MTF and pixel resolution
  - Illumination wavelength
  - Minimum distance (margin) from iris outer boundary to closest image boundary

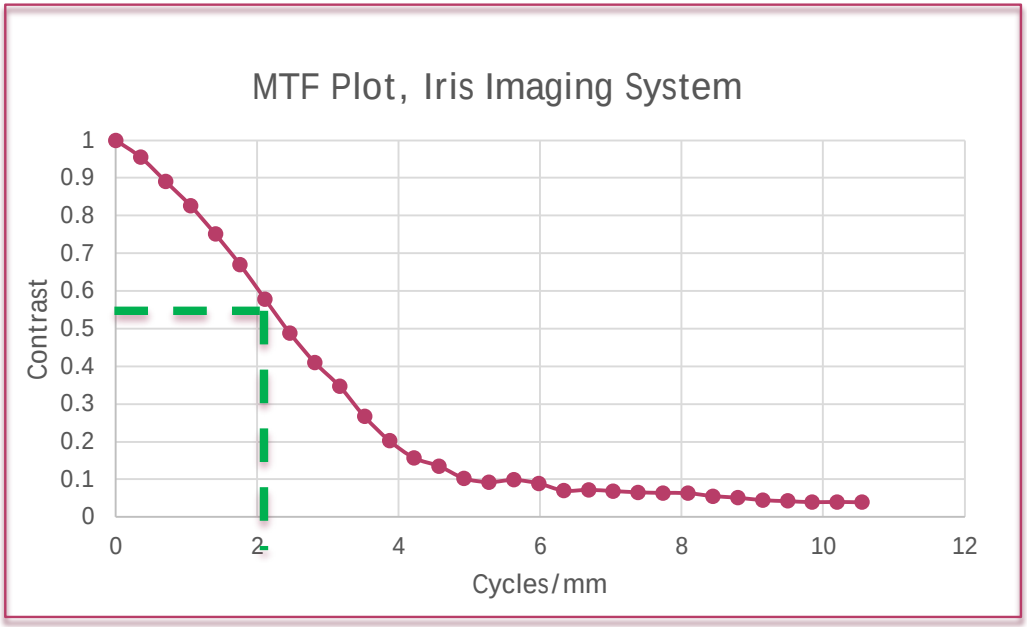
MTF AND PIXEL RESOLUTION

Attribute	MobileID BPR	19794-6	29794-6
Contrast		0.60	0.50
Spatial frequency, cycles/mm		2	2
Spatial sample rate, pixels/mm	10.8 – 21.0*, no upsampling	10	15.7

*derived from specified range of iris diameter in pixels (140 – 210) and typical range of iris diameter of 10mm – 13mm

JAMES CAMBIER

MTF AND PIXEL RESOLUTION

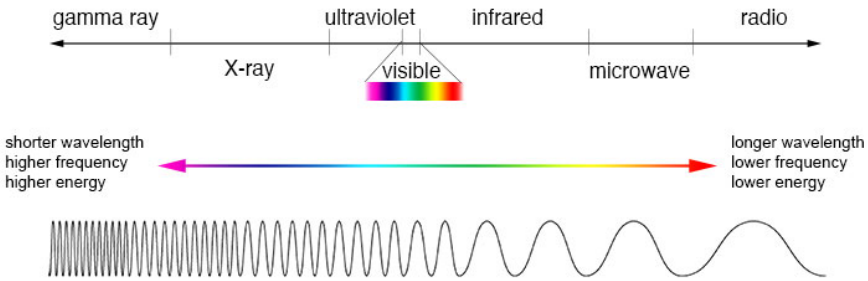


Recommendations:

- Specify spatial sampling rate directly in pixels/mm, not iris diameter
- Adopt MTF recommendations of 19794-6:2011.
- Spatial sample rate of 10 pixels/mm is reasonable estimate of Nyquist rate for typical imaging system using COTS optics
- Allow upsampling from 10 pixels/mm if algorithms require higher minimum iris diameter (in pixels)

JAMES CAMBIER

ILLUMINATION WAVELENGTH



- Iris imaging systems use near-IR illumination within the 700-900 nm wavelength range
- Experience indicates that a wide range of wavelengths is needed to accommodate a variety of eye colors
- Mobile devices may require more limited spectral distributions to reduce size and power requirements

JAMES CAMBIER

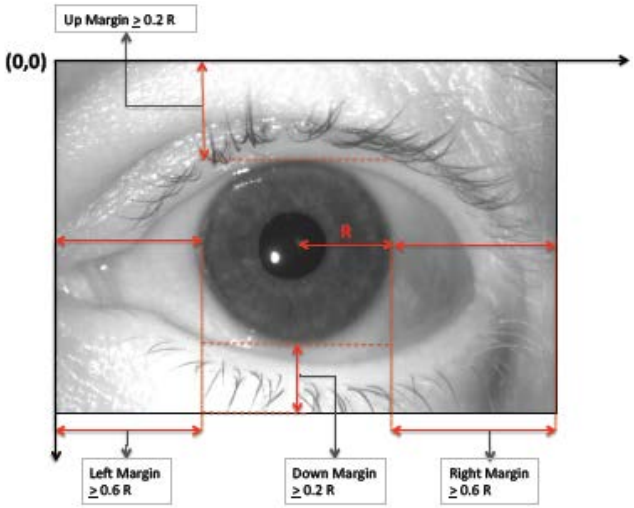
ILLUMINATION WAVELENGTH

MobileID BPR	19794-6	29794-6
Any 100 nm band within 700-900 nm must contain ≥ 35% of total energy	Illumination energy should be emitted at wavelengths in 700-900 nm range, and should be ≥5° off-axis to prevent "red-eye" effect	≥90% of energy shall be within 700-900 nm band; ≥35% of energy in 700-900 nm range shall be within 800-900 nm band

Recommendation: Adopt specification from 29794-6 to provide maximum design flexibility for mobile devices

JAMES CAMBIER

IMAGE MARGIN REQUIREMENTS



Parameter	MobileID BPR	19794-6	29794-6
Vertical margin	0.5 x diameter	0.2 x radius	0.2 x radius
Horizontal margin	0.25 x diameter	0.6 x radius	0.6 x radius

Recommendation: Adopt 19794-6, 29794-6 specifications

JAMES CAMBIER

OPEN DISCUSSION

- Additional topics to be considered
- Formation of subject matter groups
- Selection of working group leads
- Development of a timeframe

BRAD WING

ADJOURN