Towards a Mobile Biometric Test Framework

NIST IBPC | 8 March 2012

Presented by: Eric Kukula, PhD & Frank Shaw

Noblis Team Members:
Eric Kukula, *Technical Lead & Project Manager*
Ann Breckenkamp, Emily Keener, George Kiebuzinski,
Larry Nadel, PhD, Frank Shaw & Rachel Wallner

DHS S&T Team Members:
Patty Wolfhope, *DHS S&T Biometrics Transition Program Manager*
Ryan Bednar, Rick Lazarick & Brad Wing

This work is sponsored by DHS S&T HSARPA
Human Factors Division

Homeland Security
Science and Technology

noblis
For the best of reasons

Background

Why test mobile biometric devices?

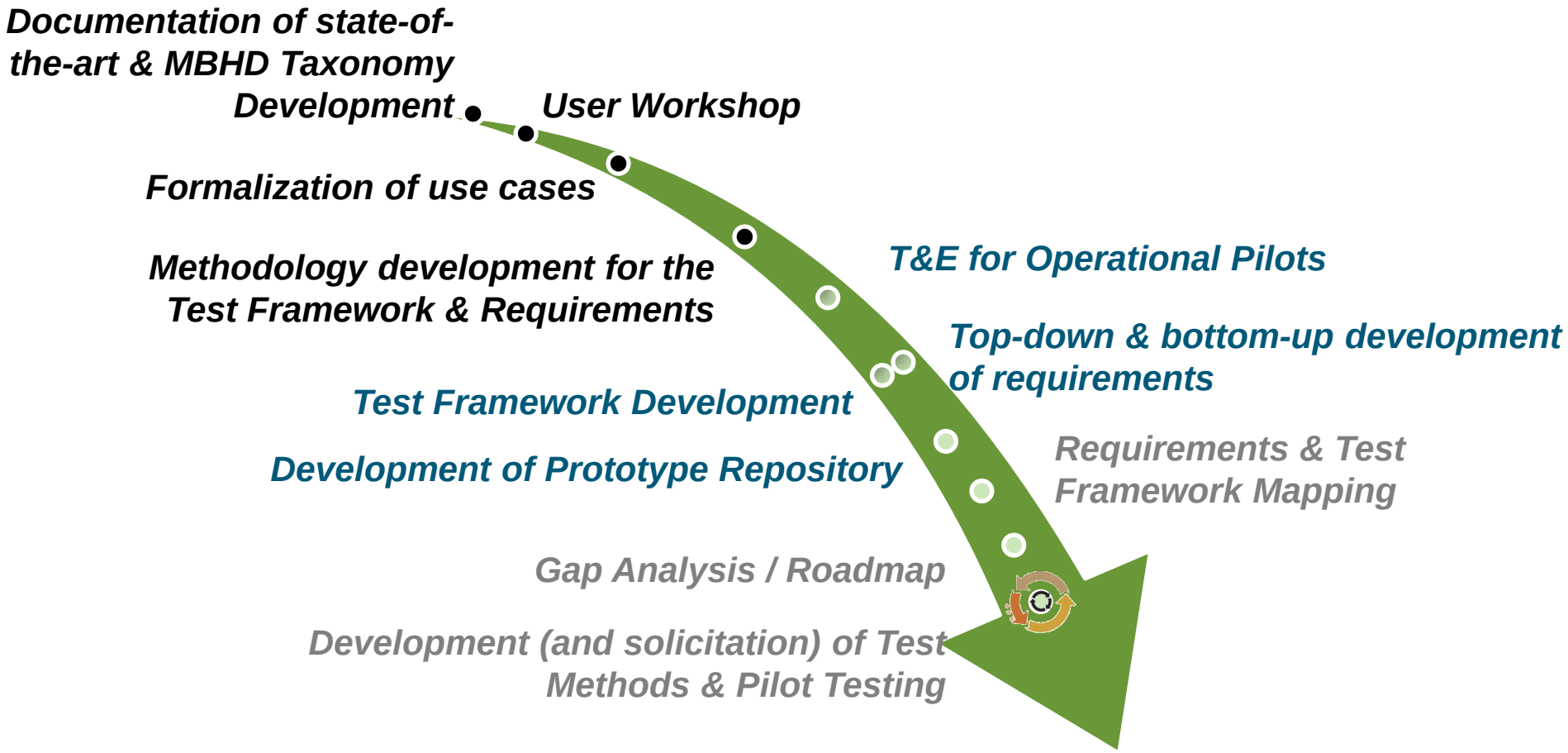
How was the test framework developed?

Who will use the test framework and repository?

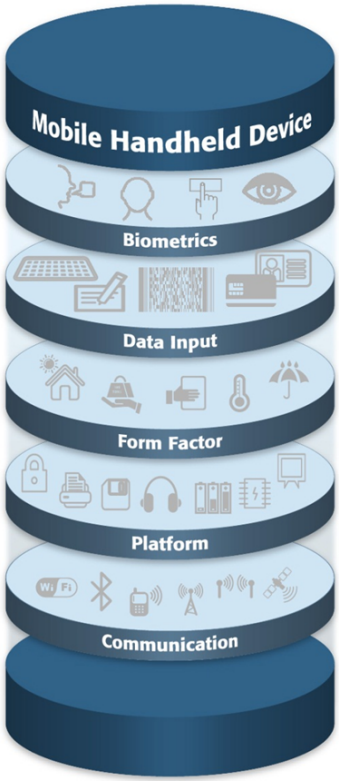
Why Test?

Image references included as hyperlinks. Images without hyperlinks were taken by Eric Kukula. In no case do such references imply recommendation or endorsement by Noblis or DHS S&T.

Methodology & Roadmap



MBHD Taxonomy



System	Biometric				
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	Biometric				
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

noblis

Exists in multiple subsystems

COTS Devices Mapped to the Taxonomy

- Analyzed over 30 COTS MBHD devices*

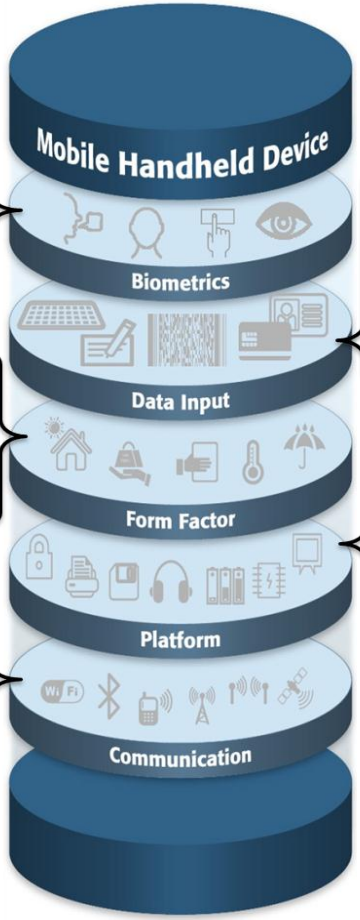
	HIIDE 5	Fusion	SEEK II	Mobile Ident II	MC75	BlueCheck	DSV2+ turbo	Morpholdent	PIER-T
Fingerprint	✓	✓	✓	✓	✓	✓	✓	✓	
Single Flat	✓	✓	✓	✓	✓	✓	✓	✓	
Double Flat	✓		✓						
Rolled	✓		✓						
Face	✓	✓	✓	✓	✓	Optional			
Iris	✓	✓	✓						✓
Single Iris		✓							✓
Simultaneous	✓		✓						
On-board Matching	✓	✓	✓	✓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

	HIIDE 5	Fusion	SEEK II	Mobile Ident II	MC75	BlueCheck	DSV2+ turbo	Morpholdent	PIER-T
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
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
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?					✓	✓			✓

	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	✓				



*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.

User Workshop :: 31 March 2011

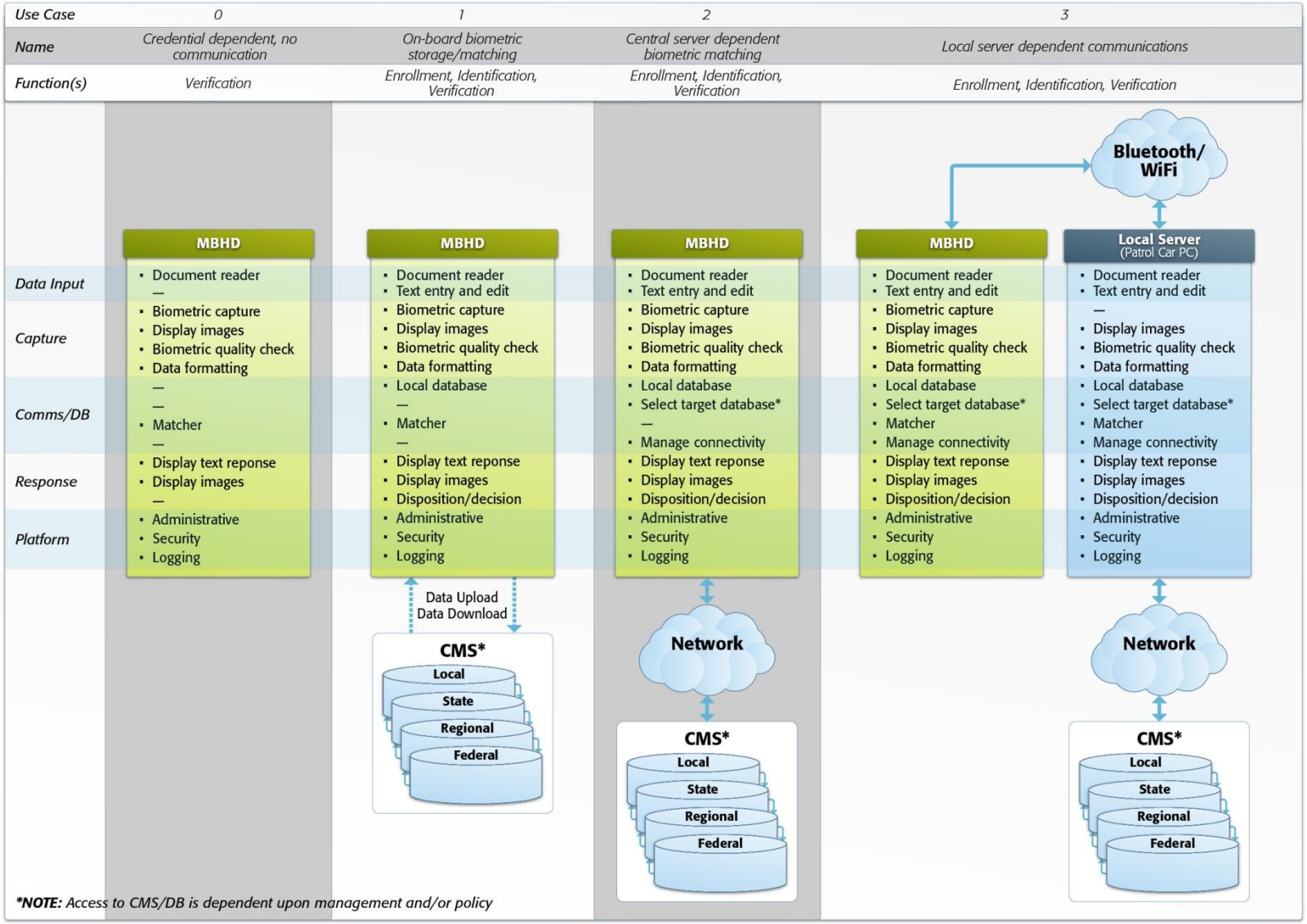
Tucson Border Patrol Sector HQ

- *Report for the Mobile Biometric Technology Workshop for Developing a Test Framework and Supporting Requirements*
  - Workshop context, rationale, and purpose
  - User Survey Results and Analysis
  - User/Participant Presentation Summaries
  - Use Cases
  - Scenarios
  - Mapping of Scenarios to Use Cases
  - Results
  - Conclusions
  - Recommendations

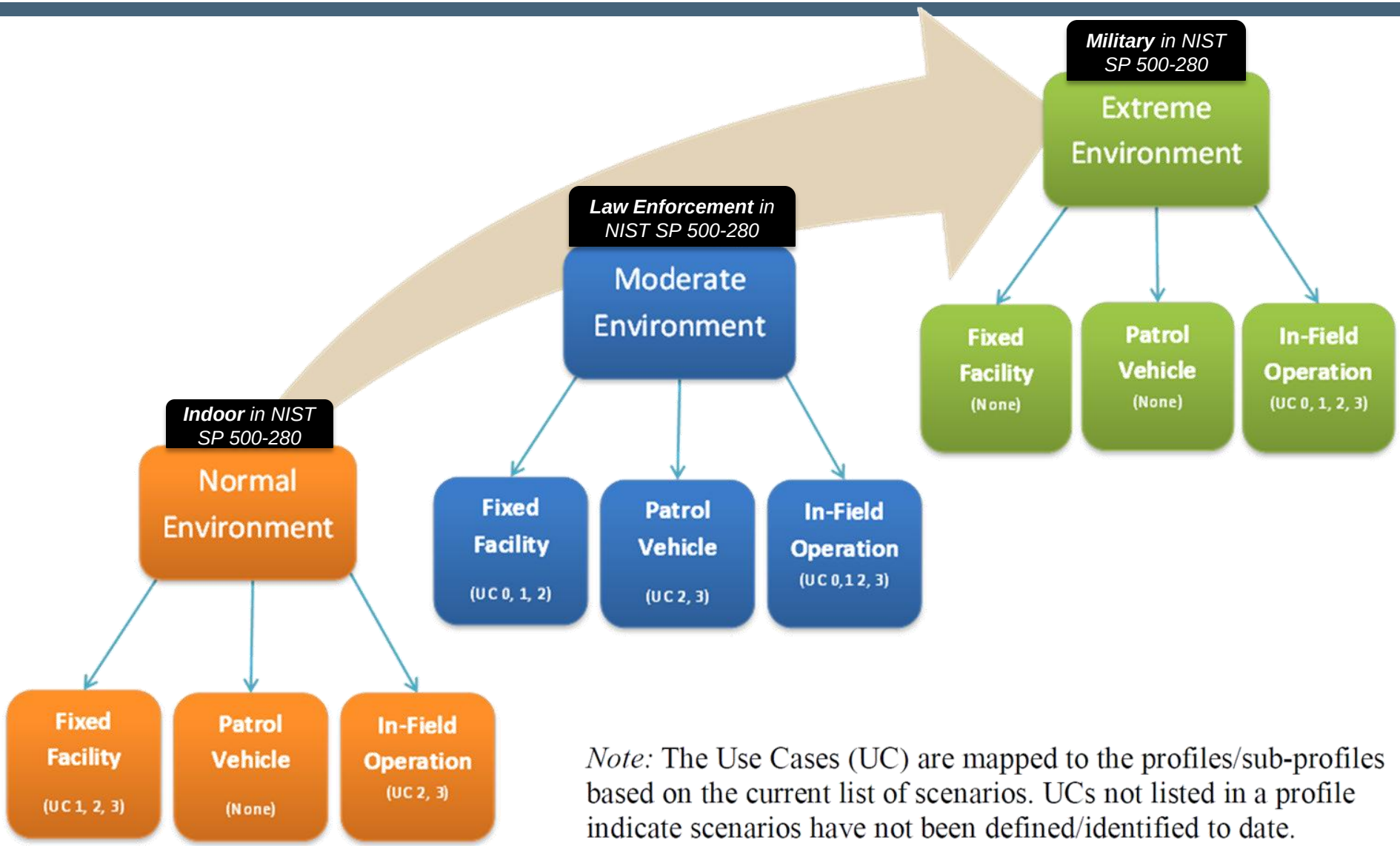
Homeland Security
Science and Technology

ICE

Consolidated Use Cases

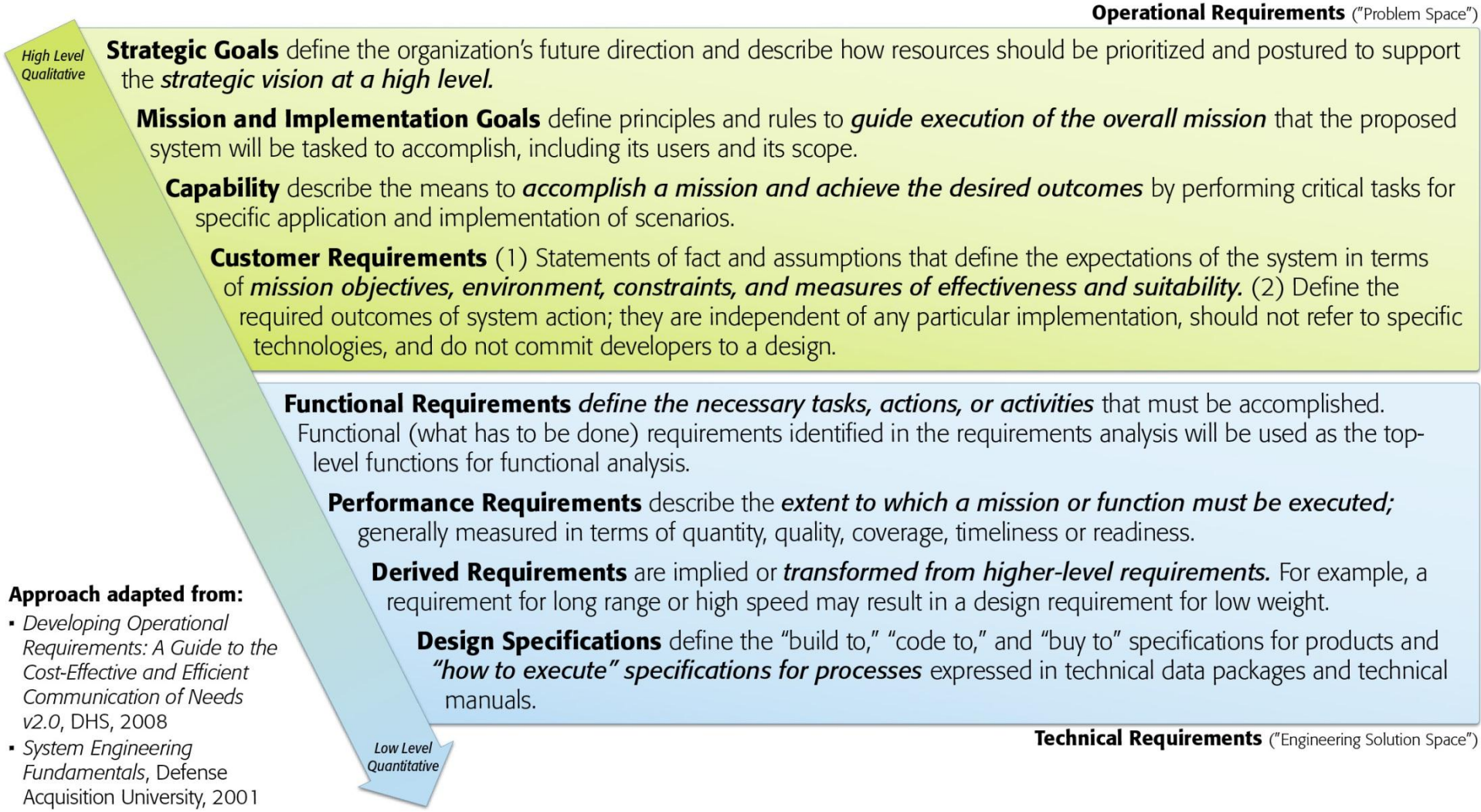


Requirement Profiles & Sub-Profiles



Note: The Use Cases (UC) are mapped to the profiles/sub-profiles based on the current list of scenarios. UCs not listed in a profile indicate scenarios have not been defined/identified to date.

Requirements Methodology



Approach adapted from:

- *Developing Operational Requirements: A Guide to the Cost-Effective and Efficient Communication of Needs v2.0*, DHS, 2008
- *System Engineering Fundamentals*, Defense Acquisition University, 2001

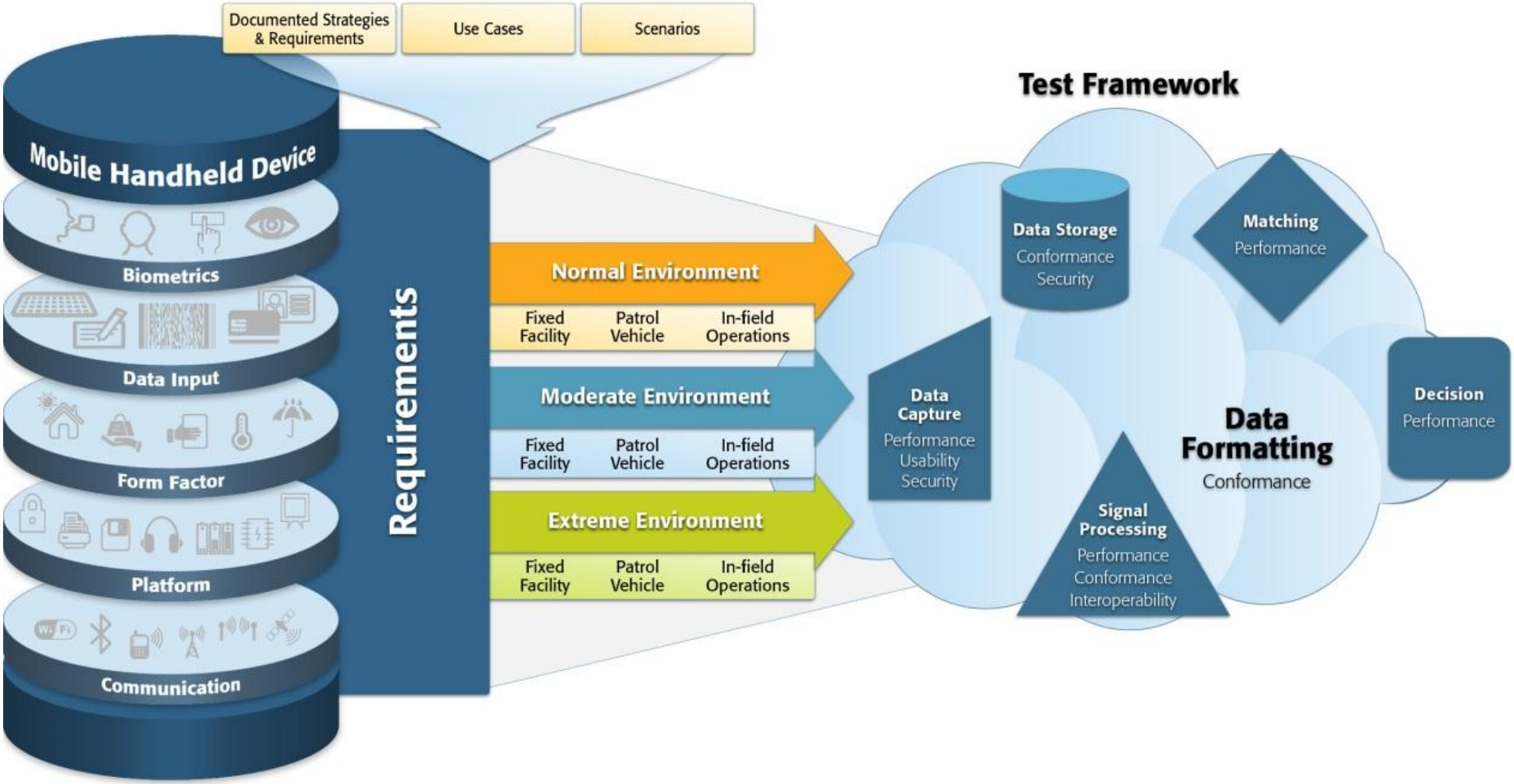
Operational Requirements

Strategic Goals Through Customer Requirements

Strategic Goals	Top Strategic Goal: Ensure the safety and security (includes preventing and reducing the vulnerability of terrorist attacks) of the American people, the Homeland, America's allies, and America's national interests.						
	Strategic Goal #1: Prevent the inflow and outflow of harmful and illegal people, business, and goods across the National borders	Strategic Goal #2: Enable quick recovery from man-made and natural disasters	Strategic Goal #3: Prevent and reduce crime and illegal activity (transnational and domestic)	Strategic Goal #4: Respect for universal values	Strategic Goal #5: Protect the nation's critical infrastructure, leaders, and events		
Mission & Implementation Goals	Protect the maritime, air and land transportation systems from terrorism, harmful people, and harmful goods.	Protect national leaders and leaders of ally governments	Protect vulnerable sites and events and prevent suspicious or unauthorized persons from gaining access to secure or sensitive areas	Protect key resources of the United States	Enforce the nation's immigration laws to support national security, public safety, and integrity of the borders	Prevent and disrupt the trade, production and usage of illegal drugs	Prevent the illegal trade of goods and facilitate in lawful goods crossing the national borders
Capabilities	Identify persons attempting to enter the U.S. illegally, who have violated immigration laws, or who are previous deportees	Identify individuals who are on terrorist or other watch lists	Identify encountered individuals wanted for criminal activity	Detect and identify suspicious persons at a distance in a lawful manner	Determine the identity of hurt or deceased persons	Verify the identity of a person carrying a credential/documentation	Verify the identity of a person claiming an identity without documentation (credential)
	Detect threats and report these threats back to authorities in near/real time.	Provide access to necessary data for mission related activities	Protect individuals from physical harm	Protect the privacy of individuals	Create records for lawbreakers		
Customer Requirements	Identify subject using one or more biometric modalities	Verify subject identity using one or more biometric modalities	Verify [the validity of] documentation and its ownership	Create, enroll, and augment biometric and/or available biographic data into the selected *on-site* database(s)	Create, enroll, and augment biometric and/or available biographic data into the selected *central* database(s)	Present data from database to the requestor for investigative purposes	Conduct a biometric search against a system and/or database
	Protect mission sensitive information	Permit authorized agent(s) to manage operation of the mobile device	Design shall not jeopardize agent safety	Properly function in targeted operating ambient environment(s)	Properly function in targeted architectural environment(s)	Monitor and indicate the status of transactions and designated conditions	Detect and prevent device malfunctions and errors

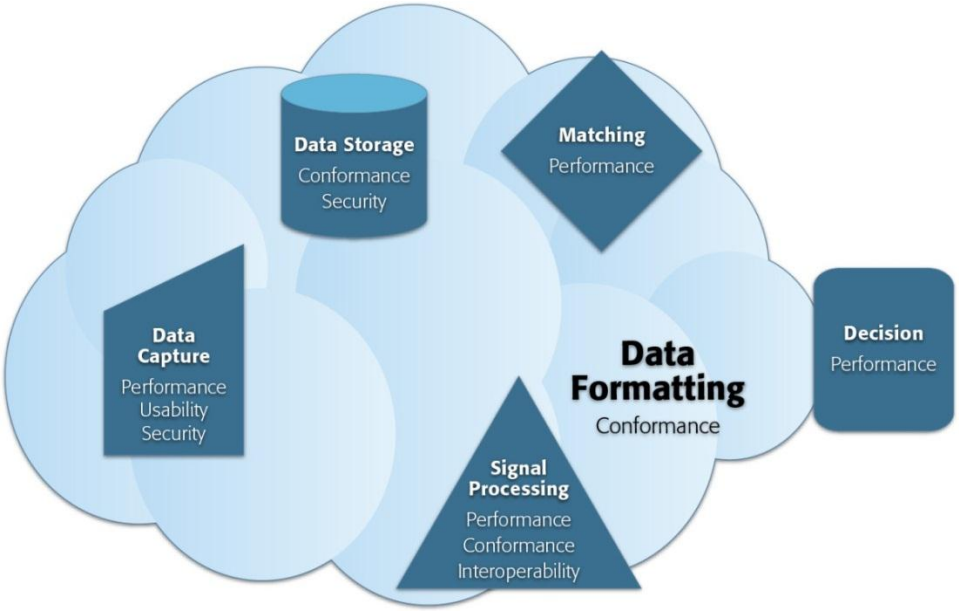
Key
Derived from Documents
Derived from Scenarios, Appendix D Requirements, or Other Requirements
Created by Team

Linkage of the Taxonomy to the Test Framework



Test Framework Overview

- Currently only houses ***component-level*** tests for the ***biometric subsystem***
- Organization based on general biometric model subsystems
  - Data Input
  - Signal Processing
  - Data Storage
  - Matching
  - Decision
- New subsystem
  - Data Formatting
- Types of testing based on existing test programs and reports



Structure of the Test Framework

- Each subsystem has 3 components
  - Framework
    - Structure for user interaction
    - Relationship between products tested vs. tests passed
  - Description
    - Description of the purpose of each test
    - Breakdown of test structure within the repository
  - Methods
    - Breakdown of test methods for each test
    - Where applicable, metric(s) and threshold(s) are specified

Test Framework Organization & Navigation

Example :: Appendix F

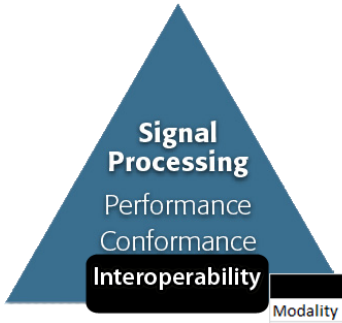
	Fingerprint															
	Imager - Sensor															
	Performance															
	Appendix F								PIV							
Method	1	2.1	2.2	3	4	5.1	5.2	5.3	1	2.1	2.2	3	4	5.1	5.2	5.3
Product A	x	x	x	x	x	x	x	x								
Product B									x	x	x	x	x	x	x	x

Test category	HW/SW	Component	Modality	Test	Description
Performance	Hardware	Imager - Sensor	Fingerprint	Appendix F - Test Procedures for Verifying the IAFIS Image Quality Requirements for Fingerprint Scanners and Printers	This assesses the performance of fingerprint image scanners and printers to ensure the meet the specification laid out in FBI Electronic Biometic Transmission Sepecification (EBTS) Appendix F

Test	Method	Description	Metric	Threshold
App F	1	A linear, least squares regression is run between the step-averaged target reflectance or transmission values and the corresponding step-averaged scanner output gray-levels. The deviation of each step-averaged scanner output step gray-level from the linear, least squares regression line of best fit is noted.	Gray-Levels	Within 7.65 gray-levels of a linear, least squares regression line

Test Framework Organization & Navigation

Example :: MINEX



Interoperability										
Modality	Fingerprint									
Component	Template Generator									
Test	MINEX					Ongoing MINEX				
Method	1	2	3	4	5	1	2	3	4	5
Product A	x	x	x	x	x					
Product B	x	x	x	x	x	x	x	x	x	x
Product C						x	x	x	x	x

Signal Processing					
Test Category	HW/SW	Component	Modality	Test	Description
Interoperability	Software	Template Generator	Fingerprint	MINEX 04	The MINEX04 test was created to assess the interoperability of the INCITS 378 fingerprint minutiae template as well as compare the performance of the template with proprietary (image based) implementations.
	Software	Template Generator	Fingerprint	On-going MINEX	This test follows the same approach of the MINEX04 test. This test continues to evaluate template generators and matchers submitted to NIST for use in biometrically-enabled PIV readers.
	Software	Template Generator	Iris	IREX I	The IREX I test was created in cooperation with the iris recognition industry to develop and test standard image formats and test their interoperability. This results of this test provided insight to ISO/IEC JTC!/SC37 biometric data interchange format standard for iris image data (ISO/IEC 19794-6)

Test	Method	Description	Metric	Threshold
MINEX	1	Each matcher was tested by matching enrollment templates versus its own authentication templates for the MIN:A, MIN:B and their own proprietary templates.		
	2	Scenario 1		
	2.1	The enrollment template is prepared by vendor X to be used in the later verification transaction.		
	2.2	The verification template is then prepared by vendor Y.		
	2.3	The enrollment template prepared by vendor X and the verification template prepared by vendor Y are then matched using vendor Y's matching algorithm.	FNMR at specific FMR value	FMR = 0.01: mean FNMR <= 0.0098

Prototype Repository

- Place for storage of the test framework information and mobile biometric device requirements.

- Provides methods of user interaction and navigation through information
- Role-based access
  - Acquisition Personnel
  - Testing Laboratories
  - Vendors and Manufacturers

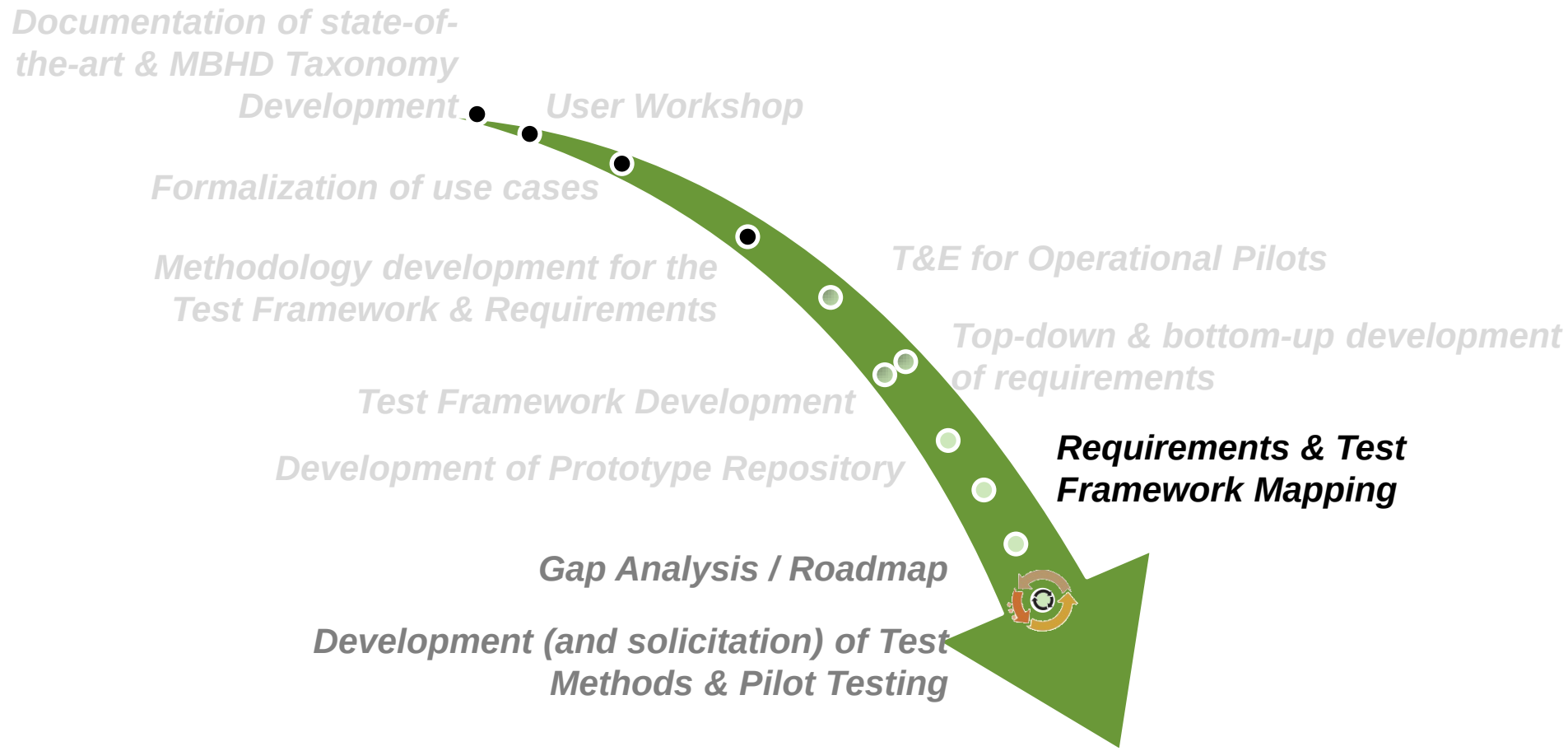
- Built using LabKey Software open-source framework*

*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.

Next Steps

- Integrate all levels of test integration to the test framework
  - Subsystem
  - System
  - System-of-Systems
- Map requirements to the test framework
  - Using metrics and thresholds
  - Maps to engineering space requirements (functional, performance, derived)

Methodology & Roadmap

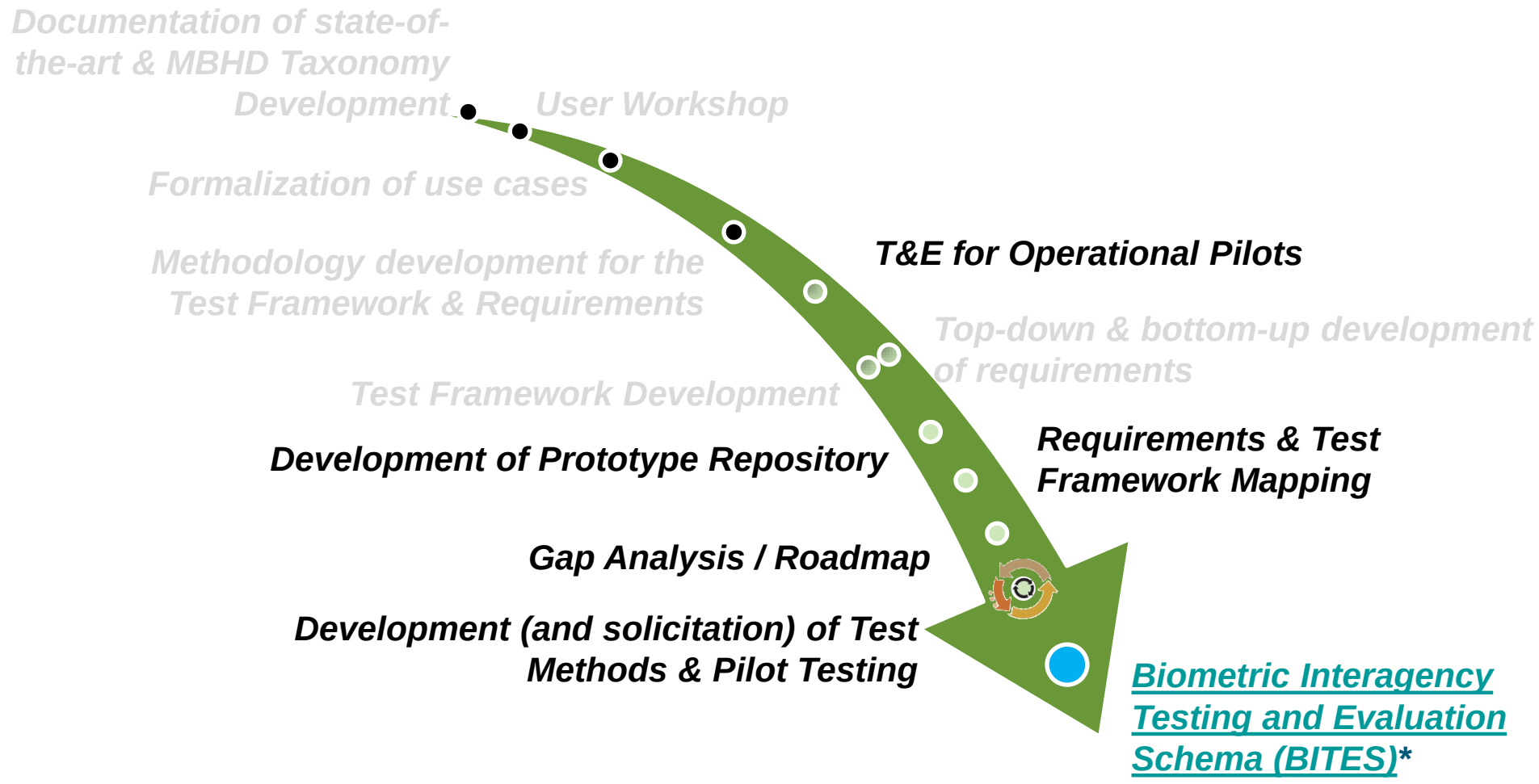


Requirements Traceability Matrix

ID	Functional Requirement	Condition	Requirement Source	Biometric Subsystem	Backward Traceability (corresponding customer requirements)	Forward Traceability (corresponding performance requirements)	Corresponding Test(s)
F1.1	The mobile device shall capture a single flat fingerprint image for use in identification				C1	P6, P7	
F1.2	The mobile device shall capture a single flat fingerprint image for identity verification				C2, C3, C9	P6, P7	
F1.3	The mobile device shall capture a single flat fingerprint image for enrollment in a fingerprint database				C4, C5	P6, P7	
F1.4	The mobile device shall capture a single flat fingerprint image for documentation				C4, C5	P6, P7	

ID	Performance Requirement	Condition	Source	Biometric Subsystem	Backward Traceability (corresponding functional requirements)	Forward Traceability (corresponding derived requirements)	Corresponding Test(s)
P6	The mobile device shall have a minimum FAP level of ____ as specified in the most current version of ANSI/NIST-ITL				F1.1, F1.2, F1.3, F1.4		
P7	The mobile device shall capture a single flat fingerprint in less than 3 seconds				F1.1, F1.2, F1.3, F1.5		

Next Steps



*For more information on BITES, see http://biometrics.nist.gov/cs_links/ibpc2012/presentations/Day3/333_Lazarick-Wolfhope_IBPC.pdf

Benefits

- Improved testing efficiency and thoroughness
  - Traceability between devices, requirements and test methods
- Uniformity of test methods to support sharing between agencies and programs
- Addresses challenges laid out in the NSTC National Biometrics Challenge Document
  - Repository of test methods and results
  - Lowers costs by reusing test procedures and certifications
  - Development of testing and evaluation methodologies
  - Development of frameworks for test data and results

Thank You For Your Attention

Questions?

Contact Information:

Patricia Wolfhope, DHS S&T	patricia.wolfhope@dhs.gov
Eric Kukula, PhD, Noblis	eric.kukula@noblis.org
Frank Shaw, Noblis	frank.shaw@noblis.org

Sponsor:

Homeland Security
Science and Technology

Noblis Team Members:

Eric Kukula, *Technical/Project Manager,*
Ann Breckenkamp, Emily Keener, George Kiebuzinski, Larry Nadel, PhD, Frank Shaw & Rachel Wallner

DHS S&T Team Members:

Patty Wolfhope, *DHS S&T Biometrics Transition Program Manager*
Ryan Bednar, Rick Lazarick & Brad Wing