NPIA
National Policing
Improvement Agency

Mobile Biometric Identification for Policing:

Performance Specification and Accuracy Evaluation

Geoff Whitaker
CTO – Biometrics
NPIA

Presentation for NIST IBPC 2010

NPIA
National Policing
Improvement Agency

What is the NPIA?

National Policing Improvement Agency

'….to support the police service in reducing crime, maintaining order, bringing criminals to justice and protecting and reassuring the public'

– NPIA provides leadership and expertise to the police service in areas including:
  - information and communications technology
  - support to information and intelligence sharing
  - core police processes – 'Best Practice'
  - managing change and recruiting, developing and deploying people.

What is the NPIA?

- Police National Computer
- IDENT1 – National Finger and Palm print service
- DNA Database
- IMPACT – Sharing of intelligence data across forces
- Fixed Network Infrastructure
- Identity and Access Management (IAM)
- Mobile Information Programme (MIP)

Project Lantern - Objectives

- To evaluate the feasibility and likely benefits of providing the UK police service with a real time mobile biometric ID capability
  - Searching against the full police national fingerprint collection on IDENT1

- 3 year field trial involving 300 mobile fingerprint devices

- Aims:
  - To help determine the user requirements for mobile ID
  - To establish a baseline for performance, based on 2 finger mobile searches
    - Operational performance testing conducted using 500 police volunteers
    - 1:Many searches launched against the entire UK police national database on IDENT1 (8M records)

Mobile ID

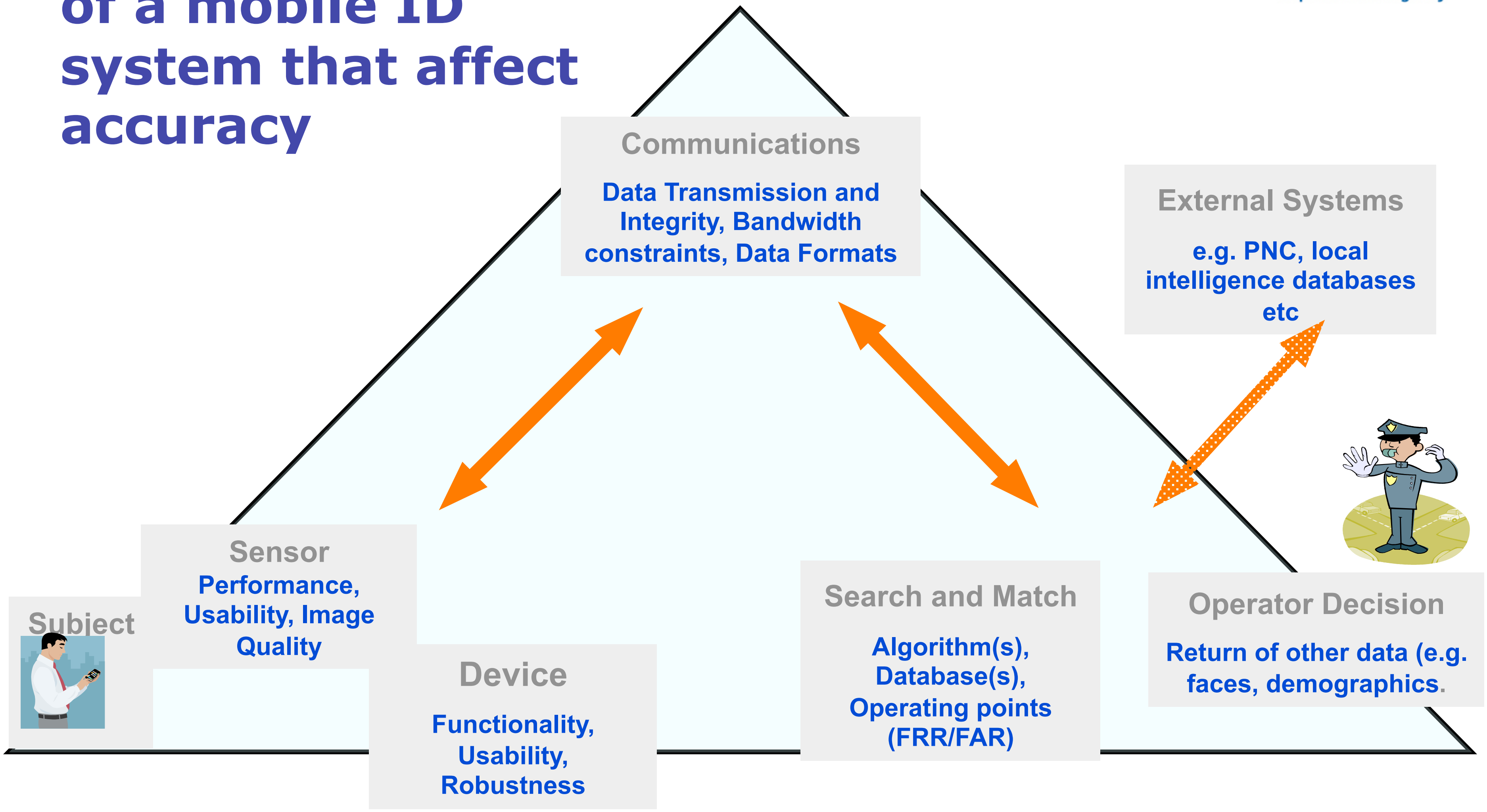
- Aim - to build on the success of the Lantern trial and to procure and deliver a full national mobile biometric identification capability for the UK police
- Initially based on fingerprints, but allowing for other modalities in the future
- Aligned with NPIA strategy for Police Information Systems (ISIS)
- Aligned with future for vision for mobile police applications
  - Integration with NPIA's Mobile Information Programme
    - ~30,000 Blackberries and PDAs already deployed

Mobile ID - Accuracy

- Use Cases and accuracy
  - 1:N Identity Checks
    - » National / Local searches
  - 1:1 Identity Checks
    - » Verify claimed ID
  - 1:N Watchlist searches
    - » National / Local / On-Device ?
  - 1:1 Verification from Documents
    - » ID Cards / Passport / Drivers Licence etc
  - 1:N Crime Scene Marks (Latents) searches
    - » Submission of crime scene latents
    - » Searching against the unsolved latents database
- NIST Mobile ID Best Practice
    - » – SAP Levels and Risk Profiles
- Modalities
    - » Finger (primary modality)
    - » Face (possible use in the future)
    - » Others ??

NPIA
National Policing
Improvement Agency

Major components of a mobile ID system that affect accuracy



Communications

Data Transmission and Integrity, Bandwidth constraints, Data Formats

External Systems

e.g. PNC, local intelligence databases etc

Subject

Sensor

Performance, Usability, Image Quality

Device

Functionality, Usability, Robustness

Search and Match

Algorithm(s), Database(s), Operating points (FRR/FAR)

Operator Decision

Return of other data (e.g. faces, demographics.

Performance Trade Offs

- At the Device
  - Sensor Type and Size – Optical / Capacitive, App F / PIV, 1, 2 or 4 finger capture
  - Total number of fingers to be captured / total time taken to capture
  - FTA rates / image quality thresholds
  - On device image processing / feature extraction
  - Integration with existing mobile devices (Blackberry, PDA)
  - Ergonomics / Usability / Training issues
- Network / Bandwidth issues
  - Number of fingers to be transmitted, Images v Templates
  - Data security overheads
  - Compression ratio and image formats
  - Data exchange formats (ANSI NIST XML?)
  - Tetra / GPRS
- Back End searching
  - Size and content of database
  - Number of fingers to be searched
  - Back end image processing / feature extraction
  - Search approach – binning / filters etc
  - Matching thresholds – single / multiple / variable
- External Systems
  - Use of 'additional' data to improve operational accuracy
  - Impact on response times
- Operator Decision
  - Presentation of results (e.g. display type and size)
  - Empirical data (name, DoB, Sex) / 'enriched' data from other systems

Accuracy Requirements

- 1:N Identity Checks – National searches
  - User Requirements:
    - To search a subject’s fingerprints against records of all subjects associated with the UK Master Reference Set of Identities (currently approx 8M subjects)
    - To do this with no drop in accuracy compared to Lantern
    - To capture a subject’s biometric data in no more than 2 ‘actions’
    - To enable the operator to correctly identify a subject (whose biometric template is present in the target database) with an accuracy of at least x%
    - To return an incorrect response (when the subject is NOT present in the target database) in no more than y% of all searches
    - To complete all of the above within a 2 minute time frame

NPIA
National Policing Improvement Agency

Accuracy Evaluation – When and How ?

1 During the Competitive Dialogue Process

Paper based assessment, Reference site visits etc

2 At BAFO to differentiate between final proposals

Evaluation benchmark of multiple proposals

3 At ‘Go Live’ as part of system assurance

Operational end-to-end benchmark of chosen solution

4 Throughout the life of the contract

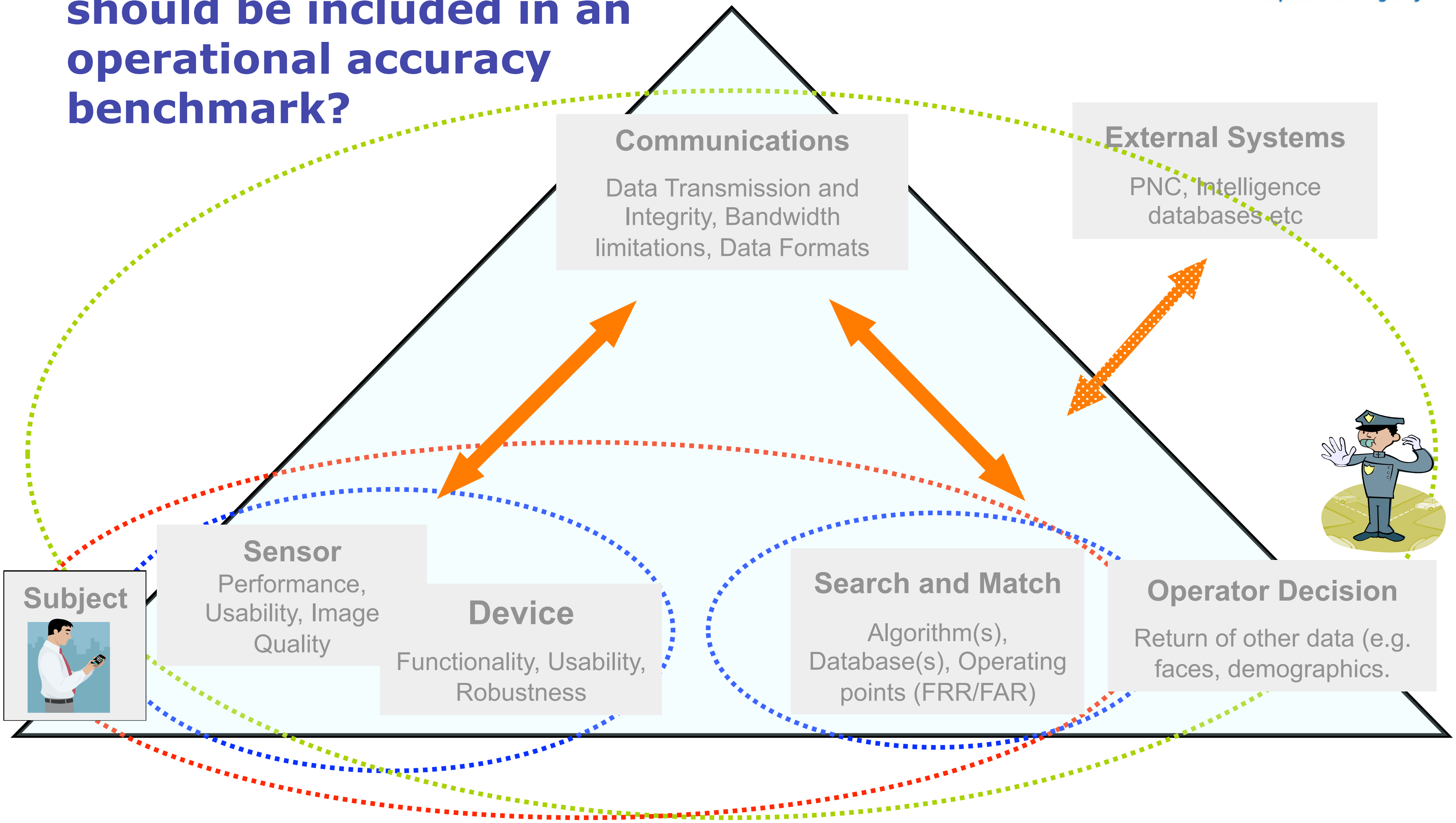
Effective use of MIS data and benchmarking for accuracy assurance

Accuracy Evaluation

- Drivers for Benchmarking:
  - To determine whether or not the technical solution
    - *Meets operational requirements*
    - *Delivers the performance claimed by the supplier*
  - To *quantify a baseline* for search accuracy to be maintained / improved on during the contract.
  - To *provide assurance* to the police service that the search accuracy meets their needs
  - To be able to *demonstrate* to the general public and media that the agency is addressing legitimate concerns over the accuracy of Mobile ID checks
  - To obtain operational data that can be used for *SLA* purposes

NPIA
National Policing Improvement Agency

Which components should be included in an operational accuracy benchmark?



Communications

Data Transmission and Integrity, Bandwidth limitations, Data Formats

External Systems

PNC, Intelligence databases etc

Subject

Sensor

Performance, Usability, Image Quality

Device

Functionality, Usability, Robustness

Search and Match

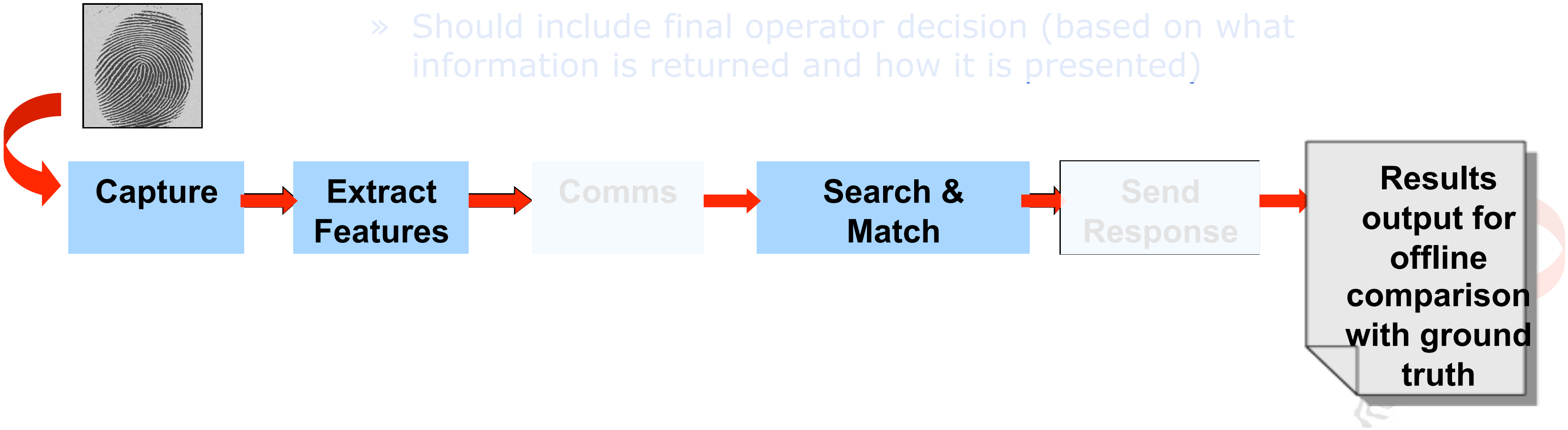
Algorithm(s), Database(s), Operating points (FRR/FAR)

Operator Decision

Return of other data (e.g. faces, demographics.

Operational Benchmarking

- A process for determining the expected *'end to end'* search accuracy of a system during operational use
- Encompasses:
  - » Capture process (including failures to acquire, finger sequence errors, human error etc)
  - » Image processing and feature extraction
  - » Data transmission between capture device and back-end (bandwidth constraints, data integrity)
  - » Searching and Matching (database penetration, thresholds, fusion etc)
  - » Should include final operator decision (based on what information is returned and how it is presented)



Capture

Extract Features

Comms

Search & Match

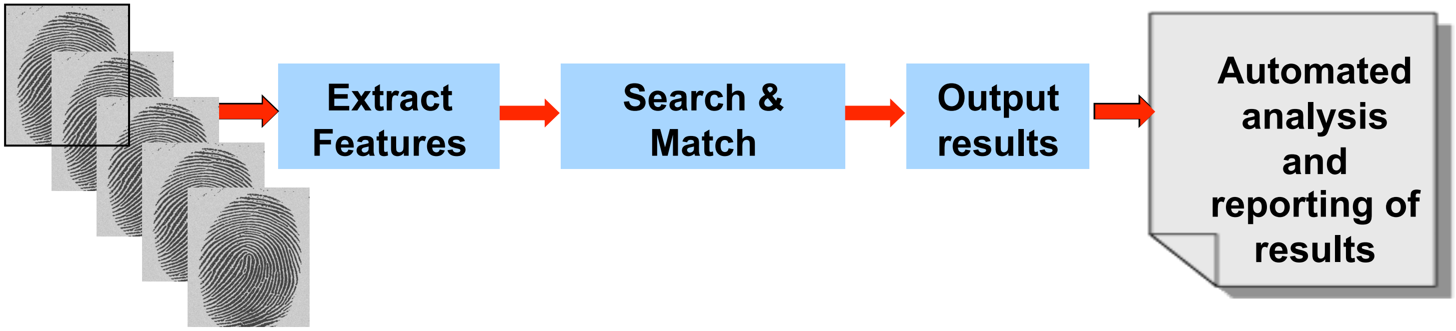
Send Response

Results output for offline comparison with ground truth

Ongoing Accuracy Assurance

- To ensure that the accuracy of the system is maintained
  - Following major releases / upgrades
  - Database growth
  - Deployment of new functionality

- Typically focuses on 'back-end' accuracy:
  - » One or more sets of enquiry data with known matches / non-matches
  - » Searches launched automatically on a regular basis and following major system changes
  - » Automated analysis and output of results



Extract Features

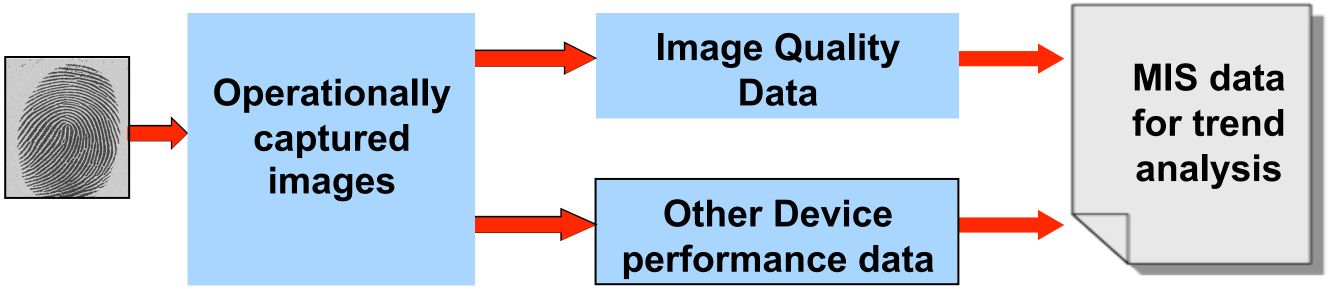
Search & Match

Output results

Automated analysis and reporting of results

Ongoing Accuracy Assurance

- What about the devices?
  - Image Quality has a major impact on accuracy:
    - » Sensor Size
    - » Sensor Certification
    - » FTA / FTE rates
    - » Image Quality measurement and thresholds
    - » Ease of Use / Capture Process Issues
  - Continual monitoring of sensor / device / user performance (e.g. image quality, FTA rate, data entry errors etc)
  - Effective processes to address problems identified at the capture stage
    - » Maintenance / repair / upgrade
    - » HCI design, Operator training



Operationally captured images

Image Quality Data

Other Device performance data

MIS data for trend analysis

Summary

For a biometric application such as Mobile ID, and using this type of procurement approach:

- Performance targets should not be too solution specific in the early phase of a project so as to allow for innovation by suppliers
- Performance targets are refined, and finally agreed by award of contract, along with the processes by which compliance will be established.
- Operational response times, system availability etc are relatively easy to measure on a live system; operational accuracy is not
- However, a benchmark can establish a baseline figure. Trends can then be identified and action taken when and where necessary
- Performance targets used within an SLA must be measurable and enforceable – this can be a challenge where operational accuracy is concerned

Thankyou

email – geoff.whitaker@npia.pnn.police.uk

Geoff Whitaker
CTO – Biometrics
NPIA

Presentation for NIST IBPC 2010