Biometric Performance Testing
Methodology Standards

Michael Thieme, Vice President
IBG, A Novetta Solutions Company
Overview

- Published standards
- In-development ISO/IEC standards
  - Scope and status
Published 19795 Standards

- **19795 series: Biometric performance testing and reporting**
  - 19795-1: *Principles and framework*
    - Key terms, concepts, and metrics for subsequent performance testing standards
  - 19795-2: *Biometric testing methodologies for technology and scenario evaluation*
    - Offline testing of algorithms and lab testing of end to end systems
  - 19795-3: *Modality-specific testing (technical report)*
    - Testing considerations specific to fingerprint, face, iris, voice, vascular, etc.
  - 19795-4: *Interoperability performance testing*
    - Used in NIST MINEX and IREX testing
  - 19795-5: *Access control scenario and grading scheme*
    - Only performance testing standard to enumerate specific performance rates (e.g. FMR, FNMR, enrollment rates, transaction times)
  - 19795-6: *Testing methodologies for operational evaluation*
    - Testing live systems with real users, introduces “acceptance rate” metric
  - 19795-7: *Testing of on-card biometric comparison algorithms*
    - Used in PIV fingerprint testing
ISO/IEC 29120-1: Test Reports

Scope
- Establishes machine readable records for documenting output of a biometric test
- Supports documentary reporting requirements of some parts of ISO/IEC 19795
- Includes mechanism to protect the integrity of the test report
- Provides trusted test information (date, lab, accreditation body, manner of testing, conformance, test size, accuracy)

Status
- Mature draft (DIS)

ISO/IEC 29120-2: Test Input Data

Scope
- Establishes a mark-up for corpora of archival sample data
- Supports research, development and calibration activities by allow tests to be executed repeatably

Status
- Stable draft (CD)
Level of Difficulty of Fingerprint Databases

- ISO/IEC 29198: Characterization and measurement of difficulty for fingerprint databases for technology evaluation

Scope
- Technical report
- Provides guidance on determining how “challenging” or “stressing” a fingerprint dataset is for recognition
- Considers common area, relative deformation, and relative sample quality
- Can be used to characterize and measure the relative difficulty levels of fingerprint datasets used in technology evaluation.

Status
- Near publication
Examiner-Assisted Biometric Applications

- **ISO/IEC 29189: Evaluation of examiner-assisted biometric applications**

- **Scope**
  - Technical report
  - Describes characteristics of examiner assisted biometric applications (e.g. AFIS / latent examiner application)
  - Contrast examiner-assisted and mainstream biometric applications
  - Discusses how system-level error rates incorporate examiner decisions

- **What is an “examiner”?**
  - a field expert in a given biometric modality
  - trained to use the system to an advanced degree of proficiency
  - authorized to override the biometric system’s decisions based on their own examination of the biometric samples and the results returned.

- **Status**
  - Mature draft (DTR)
Multi-Modal Biometric Implementations


- Scope
  - Defines multimodal-specific requirements for technology and scenario evaluation
  - Applicable when experimenter require insight into the multimodal “black box”
  - Can be used to compare different types of fusion (score, sample, etc.)

- Status
  - Mature draft (PDAM)

<table>
<thead>
<tr>
<th>Row</th>
<th>NUMBER OF MODALITY TRANSACTIONS PERFORMED</th>
<th>OVERALL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MATCH DECISIONS COMPLETED</td>
<td></td>
</tr>
<tr>
<td></td>
<td>N = 510</td>
<td>410</td>
</tr>
<tr>
<td>2</td>
<td>25.5%</td>
<td>20.5%</td>
</tr>
<tr>
<td>3</td>
<td>CORRECT MATCH (TRUE ACCEPT RATE)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>500 (gen)</td>
<td>400</td>
</tr>
<tr>
<td>4</td>
<td>50%</td>
<td>40%</td>
</tr>
<tr>
<td>5</td>
<td>FALSE MATCH</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10 (imp)</td>
<td>10</td>
</tr>
<tr>
<td>6</td>
<td>1%</td>
<td>1%</td>
</tr>
<tr>
<td>7</td>
<td>NO MATCH DECISION – FALSE REJECT</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>CORRECT NO MATCH DECISION</td>
<td></td>
</tr>
</tbody>
</table>
Environmental Influence in Biometric Systems

- **ISO/IEC 29197: Evaluation methodology for environmental influence in biometric systems**

- **Scope**
  - Specifies requirements for planning and execution of environmental evaluations for biometric systems based on scenario and operational evaluations
  - Specifies requirements for establishing a baseline performance in order to compare the influence of environmental parameters
  - Discusses controlled testing (e.g. in climactic chambers) to provide baseline measurements against which to compare environment-specific results

- **Status**
  - Mature draft (DIS)
Security and Usability in Biometric Applications

- **ISO/IEC 29156: Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics**

- **Scope**
  - Technical report
  - Provides guidance on specifying performance requirements for biometric authentication to achieve desired levels of security and usability
  - Guidance addresses issues such as
    - Biometric performance metrics that impact security and usability;
    - Comparing and quantifying the security and usability of biometrics and other authentication mechanisms, when used alone or in combination;
    - How to combine performance of individual authentication elements in order to meet an overall security and usability requirement;
    - Trade-offs between security and usability in applications using biometric recognition
    - Considerations in maintaining security and usability in biometric systems

- **Status**
  - Working draft
Presentation Attack Detection

- ISO/IEC 30107: Presentation attack detection
- Scope
  - Terms and definitions useful in the specification, characterization and evaluation of presentation attack detection methods
  - Common data format for conveying the type of approach used and the assessment of presentation attack in data formats
  - Principles and methods for performance assessment of presentation attack detection algorithms or mechanisms
  - Classification of known attacks types (in an informative annex)
- Status
  - Working draft
Template Protection Schemes

- ISO/IEC 30136: Template Protection Schemes
- Scope
  - Evaluation of accuracy, security, and privacy of biometric template protection implementations
  - Definitions, terminology, and metrics for stating the performance of such implementations
  - Requirements for the measurement and reporting of theoretical and operational accuracy of biometric template protection implementations
  - Guidance on measuring and reporting the revocability and renewability of templates
  - Guidance on the design of multiple biometric template protection systems for mitigating linkage attacks
- Status
  - Initial working draft stages