



IBPC 2012 MARCH 5-9 2012 GAITHERSBURG MD

COMMON CRITERIA AND BIOMETRIC PERFORMANCE TESTING



Belen Fernandez-Saavedra, Raul Sanchez-Reillo,
Judith Liu-Jimenez, Inmaculada Tomeo-Reyes

 – CARLOS III UNIVERSITY OF MADRID

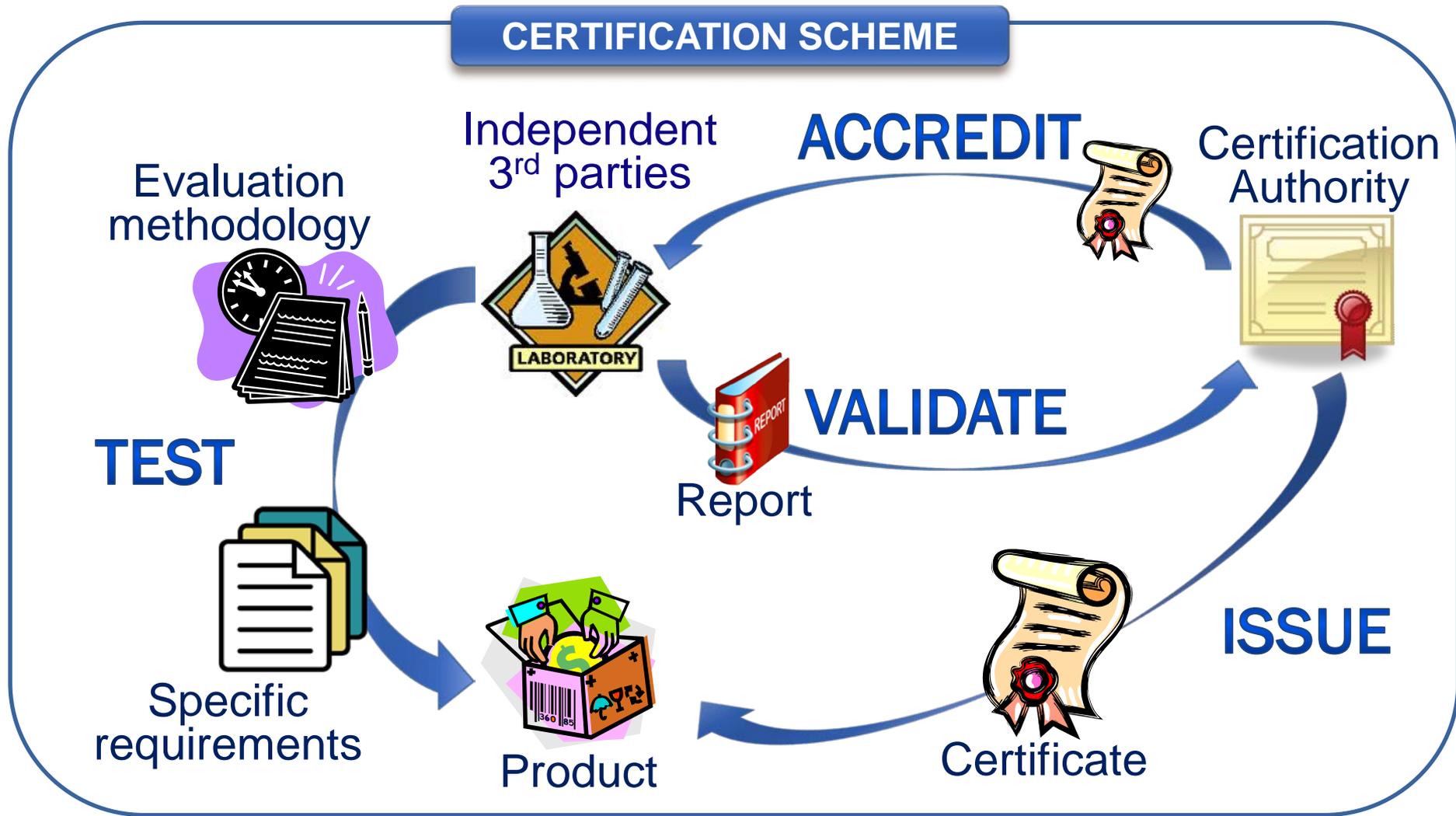


OUTLINE

- General evaluation process
- Biometric system evaluation process
 - Approaches for testing biometric systems
- Common Criteria & CEM
- Specific guidelines
 - Interpretation of a general biometric schema
 - CC testing activities involved in biometric performance testing
- Conclusions



GENERAL EVALUATION PROCESS





BIOMETRIC SYSTEMS EVALUATION PROCESS

- A global certification scheme does not exist yet
 - First step towards a global scheme: NVLAP in US
- Importance of testing biometric systems
 - Biometric systems are conceived for:
 - × Operating at critical scenarios: border control, banking, ...
 - × Handle sensitive information
- Two approaches for testing biometric systems



1ST APPROACH

- According to national or international standards
 - ISO/IEC JTC1
 - × SC37: Biometric standards
 - ★ ISO/IEC 19795 Biometric performance testing and reporting
 - × SC27: Security standards
 - ★ ISO/IEC 19792 Security evaluation for biometrics
- Disadvantages
 - Only specific requirements which are included in the standard are assessed



2ND APPROACH

- According to other certification schemes
 - Common Criteria for Information Technology Security Evaluation (CC)
 - × Certificates internationally recognized
 - × Overall evaluation process
 - × Common Evaluation Methodology (CEM)
- Disadvantages
 - General evaluation framework and testing methodology
 - × Not totally adapted to biometric products



COMMON CRITERIA & CEM

- More exhaustive evaluation: 2nd approach
- Specific guidelines for biometric systems are necessary
 - This problem is not recent:
 - × 2001: Biometric Technology Security Evaluation under CC (BTSE)
 - × 2002: Biometric Evaluation Methodology Supplement (BEM)
 - × 2009: ISO/IEC 19792
 - BTSE and BEM documents need to be:
 - × Updated to the current version of CC
 - × Expanded for covering ISO/IEC 19795 requirements
 - ISO/IEC 19792:
 - × Does not provide a fully detailed methodology (Requirements of ISO/IEC 19795-2 are not addressed)
 - × Does not provide a relation between the defined requirements and CEM



NEW GUIDELINES

- New guidelines for applying CC to biometric products
 - Based on previous works: BTSE, BEM and ISO/IEC 19792
 - Consider current versions of CC and ISO/IEC 19795
 - Provide a relation between additional biometric testing requirements and CEM working units
 - Only cover biometric performance testing and the analysis of those threats that are counteracted by it (i.e. impersonation and disguise)
 - × For covering the analysis of the rest of vulnerabilities it is necessary a formal methodology which has not been specified yet

- Contents
 - Interpretation of a general biometric system
 - × Functional specification
 - × TOE Design
 - CC testing activities involved in biometric performance testing
 - × Guidance documents (AGD)
 - × Tests (ATE)



INTERPRETATION OF A GENERAL BIOMETRIC SYSTEM

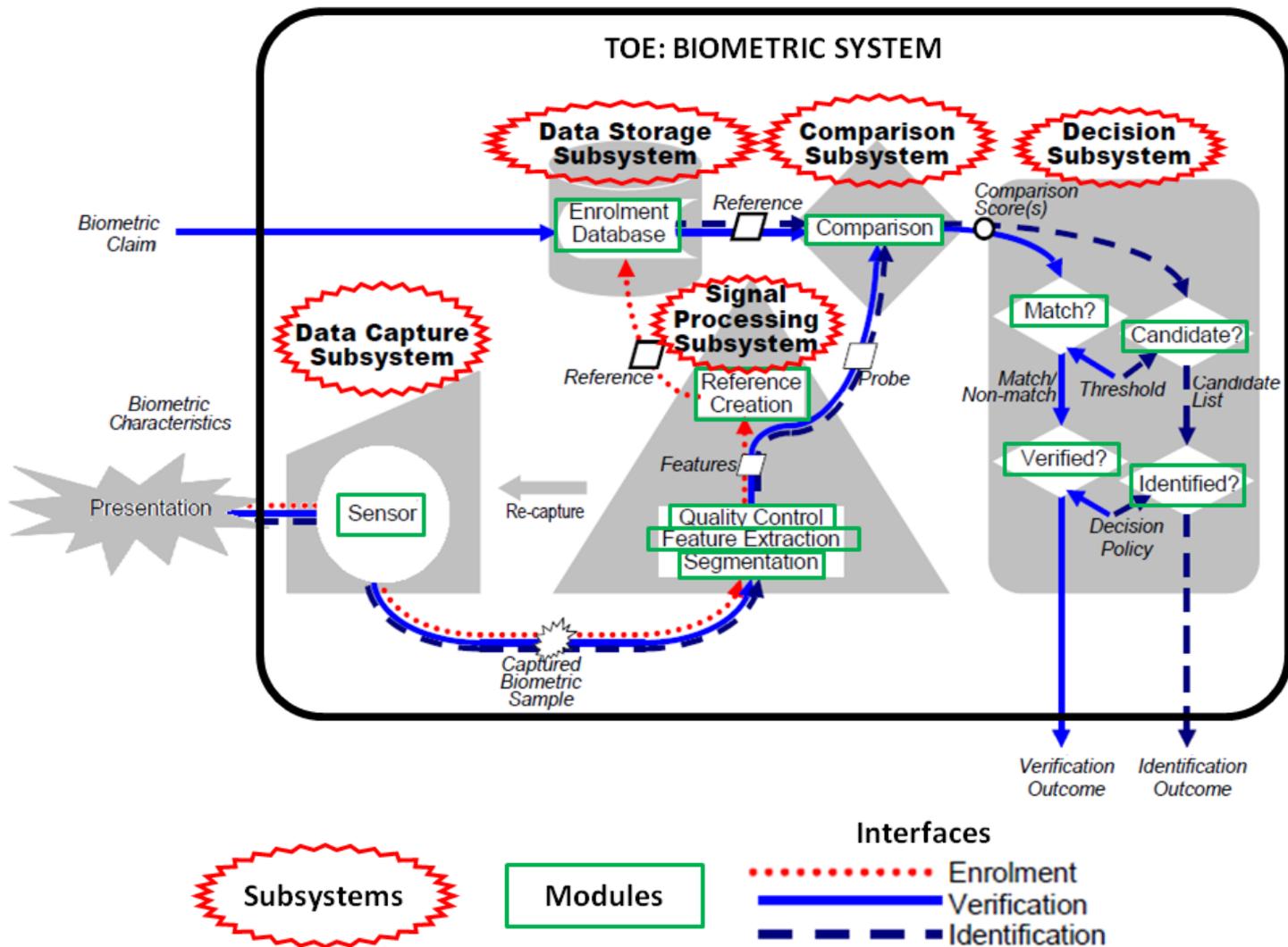
- Interpretation of a general biometric schema from a CC point of view
 - TOE (Target of evaluation)
 - × General biometric system established by ISO/IEC SC37 in the Standing Document SD11
 - Security objectives:
 - × Authenticate/Identify users correctly
 - × Fulfil specific error rates
 - TSF (TOE Security Functionality)
 - × Combination of hardware and software that are involved in the enrolment and verification/identification functions



FUNTIONAL SPECIFICATION: TSFIs

- Physical Interfaces:
 - TSFI.Biometric_characteristic: obtains a signal that contains the biometric characteristic of the user
- Logical Interfaces:
 - TSFI.Enrol: invokes the enrol function
 - TSFI.Verify / TSFI.Identify: invokes the verification/identification function
 - TSFI.Configure: invokes the configuration function

TOE DESIGN





CC TESTING ACTIVITIES

- AGD: Guidance Documents
 - AGD_PRE: Preparative procedures
 - AGD_OPE: Operational user guidance
- ATE: Tests
 - ATE_COV: Coverage
 - ATE_DPT: Depth
 - ATE_FUN: Functional tests
 - ATE_IND: Independent testing



AGD_PRE: PREPARATIVE PROCEDURES

- BTSE, BEM and ISO/IEC 19792
 - Include information about the influence of the environmental factors and the ways to minimize it
- New guidelines to AGD_PRE.1-2 should also address the inclusion of the following information:
 - Description of biometric system location
 - × Height and orientation
 - × Considering multiple locations: wall, turnstile, etc. (if necessary)
 - Description of user's interactions
 - × Specific workspace
 - Description of certain functions to adjust biometric capture sensor to the existing environmental factors
 - × E.g.: function to calibrate the illumination level



AGD_OPE: OPERATIONAL USER GUIDANCE (I)

- Two roles: Administrator and user
- User guides:
 - BTSE, BEM and ISO/IEC 19792
 - × Include guidance on the capture and enrolment processes and aspects such as privacy
 - New guidelines should also address the inclusion of the following information:
 - × Physical interface
 - ★ Influential factors at the capture process such as physical elements, behavioural aspects, etc. (AGD_OPE.1-2, 1-3 and 1-6)
 - ★ Feedback to users (AGD_OPE.1-2 and 1-4)
 - ★ Template adaptation (AGD_OPE.1-4)
 - × Logical interfaces
 - ★ Instructions to use the interfaces (AGD_OPE.1-1 and 1-2)
 - ★ Number of attempts, time limit, feedback (AGD_OPE.1-3 and 1-4)
 - ★ Enrolment process: Personal data and their handling (AGD_OPE.1-6)



AGD_OPE: OPERATIONAL USER GUIDANCE (II)

- Administrator guides:
 - BTSE, BEM and ISO/IEC 19792
 - × Include information about the environmental controls
 - × Address considerations of decision thresholds
 - × Consider user behaviour and the need for users to be monitored or supervised
 - New guidelines should address the inclusion of similar information to user guides in addition to the following information:
 - × Physical interface
 - * Procedures for training users to present their biometric characteristics (AGD_OPE.1-2)
 - * Quality requirements to determine correct/incorrect presentations (AGD_OPE.1-3)
 - × Logical interfaces
 - * TSFI.Enrol:
 - Quality requirements to accept/reject acquired samples, if this decision is not automatically made (AGD_OPE.1-3)
 - How to manage personal and biometric data (AGD_OPE.1-6)
 - * TSFI.Verify/TSFI.Identify:
 - Procedures for training users to use these functions (AGD_OPE.1-2)
 - * TSFI.Configure:
 - How to manage security settings such as quality thresholds, maximum number of attempts, etc., considering also different operation modes (AGD_OPE.1-3 and 1-5)



ATE_COV: COVERAGE

- ISO/IEC 19792
 - Appropriate testing methodology ISO/IEC 19795 - 1
- New guidelines should also address the following:
 - Testing TSFIs previously mentioned (ATE_COV.2-1)
 - Testing several TSFIs at the same time (ATE_COV.2-2)
 - × Technology evaluations: TOE does not include the capture sensor
 - × Scenario evaluation: TOE includes the capture sensor
 - Testing procedures: test pre-requisites, test steps and expected results (ATE_COV.1-3)
 - × Data size or test crew size and user characteristics
 - × Environment similar to the operational environment
 - × Genuine and impostor attempts for testing TSFI.Verify and TSFI.Identify
 - × Testing order: e.g. TSFI.Enrol before TSFI.Verify/TSFI.Identify
 - × and all requirements specified at ISO/IEC 19795 Part 1 and Part 2



ATE_DPT: DEPTH

- Highly dependent of the TOE design and its architecture
- Additional guidelines should address that:
 - Technology evaluations are appropriate to analyse all the subsequent parts of a biometric system after the human-sensor interface (ISO/IEC 19795-2)



ATE_FUN: FUNCTIONAL TEST

- BTSE, BEM and ISO/IEC 19792
 - Carry out performance testing and obtain FNMR and FMR
 - Use proper and statistically representative data
 - Take care of collection procedures and environment
- New guidelines should address that evaluators must:
 - Check the following:
 - × If test documentation includes the mandatory information defined at ISO/IEC 19795 Part 1 and 2 for reporting (ATE_FUN.1-1)
 - × If test documentation specifies the type of performance evaluation and procedures for conducting it (ATE_FUN.1-2)
 - × Proper test configuration: biometric system settings and operational environment (ATE_FUN.1-3)
 - × If test procedures and the execution sequence are appropriate to obtain error rates (ATE_FUN.1-4)
 - × If test documentation includes the claimed error rates (ATE_FUN.1-5)
 - × The obtained error rates are consistent with the claimed error rates and the application of statistical methods to calculate them (ATE_FUN.1-6)
 - Report the testing effort including the type of performance evaluation, obtained performance metrics and most relevant details (ATE_FUN.1-7)



ATE_IND: INDEPENDENT TESTING

- BTSE, BEM and ISO/IEC 19792
 - Similar recommendations to functional test
- Join functional and independent testing activities in one biometric performance evaluation to reduce cost
 - e.g. PalmSecure SDK Version 24 Premium Fujitsu Limited
- New guidelines should address that evaluators must:
 - Check the following:
 - × Correct configuration, installation and operation of the biometric system (ATE_ID.1-1,1-2, 2-1 and 2-2)
 - × Correct application of the test plan by developers and consistent results (ATE_IND.2-3 to 2-5)
 - Plan and execute some tests in accordance to ISO/IEC 19795 (ATE_IND.1-3 to 1-5 and 2-6 to 2-8)
 - × Equivalent database/test crew
 - Record and report results and testing effort and check if the obtained error rates are consistent (ATE_IND.1-6 to 1-8 and 2-9 to 2-11)



CONCLUSIONS

- A global certification scheme for biometric systems does not exist yet
- Biometric systems can be tested using CC and CEM
- Specific guidelines to apply CC & CEM evaluation activities have been proposed
- These guidelines need to be completed
 - including particular procedures to analyse biometric vulnerabilities (Class AVA)
 - including other recommendations to apply CC evaluation activities (ADV and ALC) to biometric systems (if necessary)

IBPC 2012 MARCH 5-9 2012 GAITHERSBURG MD

THANK YOU FOR YOUR ATTENTION



B. Fernandez-Saavedra, R. Sanchez-Reillo,
J. Liu-Jimenez, I. Tomeo-Reyes

{mbfernan, rsreillo, jliu, itomeo}@ing.uc3m.es