

# ISO/IEC 19989-1:2020 (E)

## Information security — Criteria and methodology for security evaluation of biometric systems — Part 1: Framework

---

### Contents

	Foreword
	Introduction
1	Scope
2	Normative references
3	Terms and definitions
4	Symbols and abbreviated terms
5	General remarks
6	Vulnerabilities in biometric systems and security evaluation
6.1	Categorization of common vulnerabilities of biometric systems
6.2	Biometric system and presentation attack detection
6.3	Categorization of TOEs in relation to the type of evaluation
6.3.1	Biometric recognition performance evaluation
6.3.2	PAD evaluation
7	Extended security functional components to Class FPT: Protection of the TSF
7.1	General
7.2	Presentation attack detection (FPT_PAD)
7.2.1	Family behaviour
7.2.2	Component levelling
7.2.3	Management of FPT_PAD.1
7.2.4	Audit of FPT_PAD.1
7.2.5	FPT_PAD.1 Presentation attack detection
7.3	Biometric capture with presentation attack detection (FPT_BCP)
7.3.1	Family behaviour
7.3.2	Component levelling
7.3.3	Management of FPT_BCP.1
7.3.4	Management of FPT_BCP.2
7.3.5	Audit of FPT_BCP.1
7.3.6	Audit of FPT_BCP.2
7.3.7	FPT_BCP.1 Check of biometric samples for capture
7.3.8	FPT_BCP.2 Biometric capture with low failure rate
8	Extended security functional components to Class FIA: Identification and authentication
8.1	General
8.2	Enrolment of biometric reference (FIA_EBR)
8.2.1	Family behaviour
8.2.2	Component levelling
8.2.3	Management of FIA_EBR.1
8.2.4	Management of FIA_EBR.2
8.2.5	Audit of FIA_EBR.1
8.2.6	Audit of FIA_EBR.2
8.2.7	FIA_EBR.1 Check of biometric samples for enrolment
8.2.8	FIA_EBR.2 Biometric enrolment with low failure to enrol rate
8.3	Biometric verification (FIA_BVR)
8.3.1	Family behaviour
8.3.2	Component levelling

- 8.3.3 Management of FIA\_BVR.1
- 8.3.4 Management of FIA\_BVR.2
- 8.3.5 Management of FIA\_BVR.3
- 8.3.6 Management of FIA\_BVR.4
- 8.3.7 Audit of FIA\_BVR.1
- 8.3.8 Audit of FIA\_BVR.2
- 8.3.9 Audit of FIA\_BVR.3
- 8.3.10 Audit of FIA\_BVR.4
- 8.3.11 FIA\_BVR.1 Biometric verification with high performance
- 8.3.12 FIA\_BVR.2 Timing of user authentication with biometric verification
- 8.3.13 FIA\_BVR.3 User authentication with biometric verification before any action
- 8.3.14 FIA\_BVR.4 Biometric verification not accepting presentation attack instruments
- 8.4 Biometric identification (FIA\_BID)
  - 8.4.1 Family behaviour
  - 8.4.2 Component levelling
  - 8.4.3 Management of FIA\_BID.1
  - 8.4.4 Management of FIA\_BID.2
  - 8.4.5 Management of FIA\_BID.3
  - 8.4.6 Management of FIA\_BID.4
  - 8.4.7 Audit of FIA\_BID.1
  - 8.4.8 Audit of FIA\_BID.2
  - 8.4.9 Audit of FIA\_BID.3
  - 8.4.10 Audit of FIA\_BID.4
  - 8.4.11 FIA\_BID.1 Biometric identification with high performance
  - 8.4.12 FIA\_BID.2 Timing of biometric identification
  - 8.4.13 FIA\_BID.3 Biometric identification before any action
  - 8.4.14 FIA\_BID.4 Biometric identification not accepting presentation attack instruments
- 9 Supplementary activities to ISO/IEC 18045 on Class APE: Protection Profile evaluation
- 10 Supplementary activities to ISO/IEC 18045 on Class ASE: Security Target evaluation
- 11 Supplementary activities to ISO/IEC 18045 on Class ADV: Development
  - 11.1 Supplementary activities to security architecture ADV\_ARC
  - 11.2 Supplementary activities to functional specification ADV\_FSP
    - 11.2.1 Supplementary activities to evaluation of sub-activity ADV\_FSP.1
    - 11.2.2 Supplementary activities to evaluation of sub-activity ADV\_FSP.2
    - 11.2.3 Supplementary activities to Evaluation of sub-activity ADV\_FSP.3
    - 11.2.4 Supplementary activities to Evaluation of sub-activity ADV\_FSP.4
  - 11.3 Supplementary activities to TOE design ADV\_TDS
    - 11.3.1 Supplementary activities to evaluation of sub-activity ADV\_TDS.1
    - 11.3.2 Supplementary activities to evaluation of sub-activity ADV\_TDS.2
    - 11.3.3 Supplementary activities to evaluation of sub-activity ADV\_TDS.3
- 12 Supplementary activities to ISO/IEC 18045 on Class AGD: Guidance documents
  - 12.1 Supplementary activities to operational user guidance AGD\_OPE
  - 12.2 Supplementary activities to preparative procedures AGD\_PRE
- 13 Supplementary activities to ISO/IEC 18045 on Class ALC: Life-cycle support
  - 13.1 Supplementary activities to CM support ALC\_CMS
  - 13.2 Supplementary activities to Delivery ALC\_DEL
  - 13.3 Supplementary activities to flaw remediation ALC\_FLR
- 14 Supplementary activities to ISO/IEC 18045 on Class ATE: Tests
  - 14.1 Supplementary activities to functional tests ATE\_FUN
  - 14.2 Supplementary activities to independent testing ATE\_IND
    - 14.2.1 General
    - 14.2.2 Supplementary activities to evaluation of sub-activity ATE\_IND.1
    - 14.2.3 Supplementary activities to Evaluation of sub-activity ATE\_IND.2
- 15 Supplementary activities to ISO/IEC 18045 on Class AVA: Vulnerability assessment
  - 15.1 General
  - 15.2 Supplementary activities to vulnerability analysis AVA\_VAN
    - 15.2.1 Supplementary activities to evaluation of sub-activity AVA\_VAN.2

- 15.2.2 Supplementary activities to evaluation of sub-activity AVA\_VAN.3
- 15.2.3 Supplementary activities to evaluation of sub-activity AVA\_VAN.4

**Annex A (informative) Introduction to the basic concepts of ISO/IEC 15408**

- A.1 General
- A.2 Security functional requirements
- A.3 Security assurance requirements

**Annex B (normative) Class FPT: Protection of the TSF**

- B.1 Presentation attack detection (FPT\_PAD)
  - B.1.1 FPT\_PAD.1 Presentation attack detection
    - B.1.1.1 User application notes
    - B.1.1.2 Operations
      - B.1.1.2.1 Assignment
- B.2 Biometric capture with presentation attack detection (FPT\_BCP)
  - B.2.1 FPT\_BCP.1 Check of biometric samples for capture
    - B.2.1.1 User application notes
    - B.2.1.2 Operations — Assignment
  - B.2.2 FPT\_BCP.2 Biometric capture with low failure rate

**Annex C (normative) Class FIA: Identification and authentication**

- C.1 Enrolment of biometric reference (FIA\_EBR)
  - C.1.1 FIA\_EBR.1 Check of biometric samples for enrolment
    - C.1.1.1 User application notes
    - C.1.1.2 Operations — Assignment
  - C.1.2 FIA\_EBR.2 Biometric enrolment with low failure to enrol rate
- C.2 Biometric verification (FIA\_BVR)
  - C.2.1 FIA\_BVR.1 Biometric verification with high performance
    - C.2.1.1 Operations — Assignment
    - C.2.1.2 Operations — Selection
  - C.2.2 FIA\_BVR.2 Timing of the user authentication with biometric verification
    - C.2.2.1 Operations — Assignment
    - C.2.2.2 Operations — Selection
  - C.2.3 FIA\_BVR.3 User authentication with biometric verification before any action
    - C.2.3.1 Operations — Assignment
    - C.2.3.2 Operations — Selection
  - C.2.4 FIA\_BVR.4 Biometric verification not accepting presentation attack instruments
    - C.2.4.1 User application notes
    - C.2.4.2 Operations — Assignment
- C.3 Biometric identification (FIA\_BID)
  - C.3.1 FIA\_BID.1 Biometric identification with high performance
    - C.3.1.1 Operations — Assignment
    - C.3.1.2 Operations — Selection
  - C.3.2 FIA\_BID.2 Timing of the biometric identification
    - C.3.2.1 Operations — Assignment
    - C.3.2.2 Operations — Selection
  - C.3.3 FIA\_BID.3 Biometric identification before any action
    - C.3.3.1 Operations — Assignment
    - C.3.3.2 Operations — Selection
  - C.3.4 FIA\_BID.4 Biometric identification not accepting presentation attack instruments
    - C.3.4.1 User application notes
    - C.3.4.2 Operations — Assignment

**Annex D (informative) Background information on supplementary activities for PAD evaluation**

- D.1 Class APE: Protection Profile evaluation/Class ASE: Security Target evaluation
  - D.1.1 APE\_INT PP introduction/ASE\_INT ST introduction
  - D.1.2 APE\_SPD Security problem definition/ASE\_SPD Security problem definition
- D.2 Class ADV: Development
  - D.2.1 ADV\_ARC Security architecture
  - D.2.2 ADV\_FSP Functional specification
  - D.2.3 ADV\_IMP Implementation representation
  - D.2.4 ADV\_TDS TOE design
- D.3 Class AGD: Guidance documents
  - D.3.1 AGD\_OPE Operational user guidance

- D.3.2 AGD\_PRE Preparative procedures
- D.4 Class ALC: Life-cycle support
  - D.4.1 ALC\_CMS CM scope
  - D.4.2 ALC\_DEL Delivery
  - D.4.3 ALC\_FLR Flaw remediation
  - D.4.4 ALC\_TAT Tools and techniques
- D.5 Class ATE: Tests
  - D.5.1 ATE\_FUN Functional tests
  - D.5.2 ATE\_IND Independent testing
- D.6 Class AVA: Vulnerability assessment
  - D.6.1 AVA\_VAN Vulnerability analysis

**Annex E (informative) Other general vulnerabilities**

- E.1 General
- E.2 Two-channel attacks
- E.3 Feedback provided by TOEs

**Annex F (normative) Attack potential and TOE resistance**

- F.1 Calculating attack potential
  - F.1.1 General
    - F.1.2 Identification and exploitation of attacks
      - F.1.2.1 Identification of attacks
      - F.1.2.2 Exploitation of attacks
    - F.1.3 Factors to be considered
    - F.1.4 Calculation of attack potential
    - F.1.5 Rating of vulnerabilities and TOE resistance

Page count: 62