

DIN CEN/TS 18212-5:2026-08 (E)

Personal identification - Requirements for biometric products - Part 5: Face biometrics; English version CEN/TS 18212-5:2026

Contents

Page

European foreword	6
Introduction	7
1 Scope	9
2 Normative references	9
3 Terms and definitions	10
3.1 Terms	10
3.2 Symbols and parameters	12
4 Symbols and abbreviations	18
5 General concepts	19
6 Common resources for the face biometrics evaluations	20
6.1 Overview	20
6.2 Test crew	20
6.3 Capture devices	21
6.3.1 Overall specifications	21
6.3.2 Embedded capture devices	22
6.3.3 Changeable / exchangeable / removable capture devices	22
6.4 Background, scenarios and SETTINGS	22
6.5 Biometric reference data	23
6.6 Tools for improving impartiality and consistency of results	24
6.6.1 Reference application (REF_APP)	24
6.6.2 Toolboxes	24
6.7 Levels of assurance (LoA)	24
7 Phase 2: TOE performance evaluation	26
7.1 Overview	26
7.2 Common requirements for Phase 2 tests	26
7.2.1 Test crew	27
7.2.2 SETTINGS	27
7.2.3 Equipment and materials	27
7.2.4 TRIALS	27
7.2.5 ATTEMPTS	29
7.2.6 Data to be included in the ETR	29
7.3 Technology evaluation	30
7.3.1 Overview	30
7.3.2 Test T2-1-1: Technology evaluation	30
7.3.3 Test T2-1-2: Limited-size scenario evaluation	32
7.4 SETTING variation tests	34
7.4.1 Test T2-2-1: Check correct behaviour under different backgrounds	34
7.4.2 Test T2-2-2: Check correct behaviour under different capture devices	35
7.4.3 Test T2-2-3: Check correct behaviour under different reference data	36
7.5 SUBJECT variation tests	37
7.5.1 Test T2-3-1: Differentiation among lookalikes	37
7.6 Extended tests	39
7.6.1 Overview	39
7.6.2 Extended SETTING variation tests - Test T2x-2-1: Variations of lighting conditions	39
7.6.3 Extended SUBJECT variation tests	40

8	Phase 3: Vulnerability assessment	45
8.1	Overview	45
8.2	Common requirements for Phase 3 tests	46
8.2.1	Overview	46
8.2.2	Test crew	47
8.2.3	SETTINGS	48
8.2.4	Equipment and materials	48
8.2.5	ATTEMPTs	49
8.2.6	TRIALs	49
8.2.7	Minimum attack potential calculation	51
8.2.8	Data to be included in the ETR	52
8.3	Test T3-1-1: Pre-evaluation of TOE robustness against vulnerabilities	53
8.3.1	Description	54
8.3.2	Equipment and materials	55
8.3.3	TRIALs	55
8.3.4	ATTEMPTs	55
8.3.5	Minimum attack potential calculation	56
8.3.6	Data to be included in the ETR	56
8.4	Enrolment-based attacks	56
8.4.1	Test T3-2-1: Attack to the biometric reference storage	56
8.4.2	Test T3-2-2: Use of morphing techniques during enrolment	56
8.5	Attacks during recognition process	59
8.5.1	Test T3-3-1: Still images as PAIs	59
8.5.2	Test T3-3-2: Videos as PAIs	60
8.5.3	Test T3-3-3: Low-cost masks as PAIs	62
8.5.4	Test T3-3-4: Advanced masks as PAIs	65
8.5.5	Test T3-3-5: Make-up-based attacks	68
8.5.6	Test T3-3-6: Biometric data injection attacks	70
Annex A	(normative) AP1: Remote identity verification using videoconferencing tools and pre-issued documents, with human supervision before final decision	71
A.1	Introduction	71
A.2	TOE description	71
A.3	Evaluation type target	74
A.4	Levels of assurance	74
A.5	Phase 1: Interoperability requirements	75
A.6	Phase 2: TOE performance evaluation	75
A.6.1	Overall requirements	75
A.6.2	T2-1-1: Technology evaluation	76
A.6.3	T2-1-2: Limited-size scenario evaluation	77
A.6.4	T2-2-1: Check correct behaviour under different backgrounds	77
A.6.5	T2-2-2: Check correct behaviour under different capture devices	77
A.6.6	T2-2-3: Check correct behaviour under different reference data	77
A.6.7	T2x-2-1: Variations of lighting conditions	77
A.6.8	T2x-3-1: Variations of facial expression	78
A.6.9	T2x-3-2: Variation of face orientation towards the TOE	78
A.6.10	T2x-3-3: BONAFIDE_SUBJECT aesthetic appearance variations	79
A.7	Phase 3: Vulnerability assessment	80
A.7.1	Overall requirements	80
A.7.2	T3-1-1: Pre-evaluation of TOE robustness against vulnerabilities	81
A.7.3	T3-3-2: Videos as PAIs	81
A.7.4	T3-3-3: Low-cost masks as PAIs	82
A.7.5	T3-3-4: Advanced masks as PAIs	82
A.7.6	T3-3-5: Make-up based attacks	83
A.7.7	T3-3-6: Biometric data injection attacks	83
A.8	Overall assessment criteria	84
Annex B	(normative) AP2: Face recognition for the on-boarding of credentials in an Identity Digital Wallet (DIW)	85
B.1	Introduction	85
B.2	TOE description	85
B.3	Evaluation type target	87
B.4	Levels of assurance	87
B.5	Phase 1: Interoperability requirements	88

B.6	Phase 2: TOE performance evaluation	88
B.6.1	General requirements	89
B.6.2	T2-1-1: Technology evaluation	90
B.6.3	T2-1-2: Limited-size scenario evaluation	90
B.6.4	T2-2-1: Check correct behaviour under different backgrounds	90
B.6.5	T2-2-2: Check correct behaviour under different capture devices	91
B.6.6	T2-3-1: Differentiation among lookalikes	91
B.6.7	T2x-2-1: Variations of lighting conditions	92
B.6.8	T2x-3-1: Variations of facial expression	92
B.6.9	T2x-3-2: Variation of face orientation towards the TOE	93
B.6.10	T2x-3-3: BONAVIDE_SUBJECT aesthetic appearance variations	93
B.7	Phase 3: Vulnerability assessment	94
B.7.1	Overall requirements	94
B.7.2	T3-1-1: Pre-evaluation of TOE robustness against vulnerabilities	96
B.7.3	T3-2-1: Attack to the biometric reference storage	96
B.7.4	T3-2-2: Use of morphing techniques during enrolment	96
B.7.5	T3-3-2: Videos as PAIs	97
B.7.6	T3-3-3: Low-cost masks as PAIs	97
B.7.7	T3-3-4: Advanced masks as PAIs	98
B.7.8	T3-3-5: Make-up based attacks	99
B.7.9	T3-3-6: Biometric data injection attacks	100
B.8	Overall assessment criteria	100
Annex C	(normative) AP3: Face recognition for the on-boarded Digital Identity Digital Wallets (DIW)	101
C.1	Introduction	101
C.2	TOE description	101
C.3	Evaluation type target	102
C.4	Levels of assurance	102
C.5	Phase 1: Interoperability requirements	103
C.6	Phase 2: TOE performance evaluation	103
C.6.1	General requirements	103
C.6.2	T2-1-1: Technology evaluation	104
C.6.3	T2-1-2: Limited-size scenario evaluation	104
C.6.4	T2-2-1: Check correct behaviour under different backgrounds	104
C.6.5	T2-2-2: Check correct behaviour under different capture devices	105
C.6.6	T2x-2-1: Variations of lighting conditions	105
C.6.7	T2x-3-1: Variations of facial expression	105
C.6.8	T2x-3-2: Variation of face orientation towards the TOE	106
C.6.9	T2x-3-3: BONAVIDE_SUBJECT aesthetic appearance variations	106
C.7	Phase 3: Vulnerability assessment	107
C.7.1	General requirements	107
C.7.2	T3-1-1: Pre-evaluation of TOE robustness against vulnerabilities	109
C.7.3	T3-3-1: Still images as PAIs	109
C.7.4	T3-3-2: Videos as PAIs	109
C.7.5	T3-3-3: Low-cost masks as PAIs	109
C.7.6	T3-3-4: Advanced masks as PAIs	109
C.7.7	T3-3-5: Make-up based attacks	110
C.7.8	T3-3-6: Biometric data injection attacks	110
C.8	Overall assessment criteria	110
Annex D	(normative) AP4: Face biometrics under constrained and supervised recognition systems	111
Annex E	(normative) AP5: Presentation Attack Detection (PAD) systems	112
E.1	Introduction	112
E.2	TOE description	112
E.3	Evaluation type target	113
E.4	Levels of assurance	113

E.5	Phase 1: Interoperability requirements	113
E.6	Phase 2: TOE performance evaluation	113
E.6.1	General requirements	113
E.6.2	T2-1-1: Technology evaluation	114
E.6.3	T2-1-2: Limited-size scenario evaluation	114
E.6.4	T2-2-1: Check correct behaviour under different backgrounds	115
E.6.5	T2-2-2: Check correct behaviour under different capture devices	115
E.6.6	T2x-2-1: Variations of lighting conditions	115
E.7	Phase 3: Vulnerability assessment	115
E.7.1	General requirements	115
E.7.2	T3-1-1: Pre-evaluation of TOE robustness against vulnerabilities	116
E.7.3	T3-3-1: Still images as PAIs	117
E.7.4	T3-3-2: Videos as PAIs	117
E.7.5	T3-3-3: Low-cost masks as PAIs	117
E.7.6	T3-3-4: Advanced masks as PAIs	118
E.8	Overall assessment criteria	118
Annex F	(normative) AP6: Physical access control systems using face biometrics	119
F.1	Introduction	119
F.2	TOE description	119
F.3	Evaluation type target	121
F.4	Levels of assurance	121
F.5	Phase 1: Interoperability requirements	122
F.6	Phase 2: TOE performance evaluation	122
F.6.1	General requirements	122
F.6.2	T2-1-1: Technology evaluation	123
F.6.3	T2-1-2: Limited-size scenario evaluation	123
F.6.4	T2-2-1: Check correct behaviour under different backgrounds	123
F.6.5	T2x-2-1: Variations of lighting conditions	124
F.6.6	T2x-3-1: Variations in facial expressions	124
F.6.7	T2x-3-2: Variations in face orientation towards the TOE	125
F.6.8	T2x-3-3: BONAFIDE_SUBJECT aesthetic appearance variations	125
F.7	Phase 3: Vulnerability assessment	126
F.7.1	General requirements	126
F.7.2	T3-1-1: Pre-evaluation of TOE robustness against vulnerabilities	128
F.7.3	T3-2-2: Use of morphing techniques during enrolment	128
F.7.4	T3-3-1: Still images as PAIs	128
F.7.5	T3-3-2: Videos as PAIs	128
F.7.6	T3-3-3: Low-cost masks as PAIs	128
F.7.7	T3-3-4: Advanced masks as PAIs	129
F.7.8	T3-3-5: Make-up-based attacks	129
F.8	Overall assessment criteria	130
	Bibliography	131