

Contents

Introduction.....3

1 Scope6

2 Normative references7

3 Definitions and abbreviations7

3.1 Definitions7

3.2 Abbreviations10

4 Equipment attributes10

4.1 General10

4.2 Functionality11

5 CIE construction11

6 Security grade11

7 Environmental performance11

7.1 Requirements11

7.2 Environmental and EMC tests11

8 Functional requirements12

8.1 Inputs12

8.2 Outputs13

8.3 Operation13

8.4 Processing18

8.5 Indication19

8.6 Notification outputs20

8.7 Tamper security (detection/protection)21

8.8 Interconnections23

8.9 Timing24

8.10 Event recording24

8.11 Power supply25

9 Product documentation25

9.1 Installation and maintenance25

9.2 Operating instructions26

10 Marking and labelling26

11 Tests26

11.1 Test conditions27

11.2 Test procedures28

11.3 Reduced functional test28

11.4 Functional tests29

11.5 Access level40

11.6 Authorization requirements41

11.7 Operational tests46

11.8 Tamper security tests56

11.9 Substitution tests59

11.10 Testing of I&HAS timing performance59

11.11 Testing for interconnections60

11.12 Event log61

11.13 Marking and documentation62

11.14 Environmental and EMC tests63

Annex A (informative) Interconnection types65

Annex B (informative) Summary of timing requirements67

Annex C (normative) Use of non-I&HAS interface68

Annex D (informative) Summary of function cross references	69
Figures	
Figure A.1 – Specific wired interconnections	65
Figure A.2 – Non-specific wired interconnections	65
Figure A.3 – Wire-free interconnections	66
Tables	
Table 1 – Recognition of additional fault conditions	12
Table 2 – Recognition of biometric keys	15
Table 3 – Time intervals for methods of authorization used in combination	15
Table 4 – Detection of repeated invalid authorization attempts	16
Table 5 – Monitoring of processing	19
Table 6 – Indications supplementary to those of EN 50131-1	20
Table 7 – Tamper protection	22
Table 8 – Tamper detection	22
Table 9 – Tool dimension for tamper detection	23
Table 10 – Removal from mounting	23
Table 11 – Additional events to be included in event log	24
Table 12 – Reduced functional test	29
Table 13 – Tests of the processing of intruder signals or messages	30
Table 14 – Tests of the processing of hold-up signals or messages	32
Table 15 – Tests of the processing of tamper signal or messages	33
Table 16 – Test of processing of fault signals or messages	35
Table 17 – Test of processing of masking signals or messages	37
Table 18 – Test of processing of reduction of range signals or messages	38
Table 19 – Test of CIE processing in the presence of non-I&HAS inputs	40
Table 20 – Test of the access to the functions and controls	41
Table 21 – Test for disabling user input device by invalid keys	45
Table 22 – Test for generation of tamper by invalid keys	46
Table 23 – Test of setting procedure	47
Table 24 – Test of prevention of setting and overriding of prevention of setting procedure	48
Table 25 – Test for unsetting procedure	50
Table 26 – Test of setting and/or unsetting automatically at pre-determined times	52
Table 27 – Inhibit and isolate functions	53
Table 28 – Verification of test functions	54
Table 29 – Test of CIE process monitoring	55
Table 30 – Test of availability of indications	56
Table 31 – Test of event log	62
Table 32 – Environmental and EMC tests	64
Table B.1 – Timing table	67
Table C.1 – Conditions for use of non-I&HAS interface for control and indicating purposes	68
Table D.1 – Cross references	69
Bibliography	73