CEN/TC 33 Secretariat

"Doors, windows, shutters, building hardware and curtain walling"

"Portes, fenêtres, fermetures, quincaillerie de bâtiment et façades rideaux"
"Türen, Tore, Fenster, Abschlüsse, Baubeschläge und Vorhangfassaden"

CEN/TC 33 N 3699

2018-12-13

prEN 1627, Pedestrian dooserts, windows, curtain walling, grilles and shutters – Burglar resistance _ Requirements and classification

WI 0033499

Action:	For information
Source:	CEN/TC 33/WG 7
Comments:	Draft sent to CCMC on 2018-12-05 for the CEN Enquiry.
	Start CEN Enquiry on 2019-03-21 until 2019-06-13

Your correspondent : Nathalie GIRARDOT
ligne directe : +33 (0)1 41 62 86 70
nathalie.girardot@afnor.org

Secretary : Élisabeth DERCHÉ
ligne directe : +33 (0)1 41 62 81 45
elisabeth.derche@afnor.org

CEN/TC 33

prEN 1627:2018

CEN/TC 33

Secretariat: AFNOR

Pedestrian doorsets, windows, curtain walling, grilles and shutters — Burglar resistance — Requirements and classification

Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse — Einbruchhemmung — Anforderungen und Klassifizierung

Blocs-portes pour piétons, fenêtres, façades rideaux, grilles et fermetures — Résistance à l'effraction — Prescriptions et classification

ICS:

Descriptors:

Document type: European Standard
Document subtype:
Document stage:
Document language: E

Contents

Page

European foreword

This document (*prEN 1627:2018*) has been prepared by Technical Committee CEN/TC 33 “Doors, windows, shutters, building hardware and curtain walling”, the secretariat of which is held by AFNOR.

This document is currently submitted to the CEN Enquiry.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by *Month Year,* and conflicting national standards shall be withdrawn at the latest by *Month Year*.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN 1627:2011.

Significant changes in this revision are:

a) Normative references updated

b) Scope includes electromechanical hardware products

c) Clause 6 - Building hardware re-written

d) New clause 8.2 – Non-lockable hardware

e) Clause 12 - Marking added

f) Annex B deleted

g) Annex E - Mechatronic and electronic security systems added

This European Standard is one of a series of standards for burglar resistant pedestrian doorsets, windows, curtain walling, grilles and shutters. The other standards in the series are:

- prEN 1628:2018, Pedestrian doorsets, windows, curtain walling, grilles and shutters — Burglar resistance — Test method for the determination of resistance under static loading;

- prEN 1629:2018, Pedestrian doorsets, windows, curtain walling, grilles and shutters — Burglar resistance — Test method for the determination of resistance under dynamic loading;

- prEN 1630:2018, Pedestrian doorsets, windows, curtain walling, grilles and shutters — Burglar resistance — Test method for the determination of resistance to manual burglary attempts.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

1 Scope

This European Standard specifies requirements and classification systems for burglar resistant characteristics of pedestrian doorsets, windows, curtain walling, grilles and shutters. It is applicable to the following means of opening: Turning, tilting, folding, turn-tilting, top or bottom hung, sliding (horizontally and vertically), pivoted (horizontally and vertically) and rolling as well as fixed constructions. It also covers products that include items such as letter plates or ventilation grilles. It specifies requirements for the burglar resistance of a construction product (as defined in 3.1 of this standard).

NOTE 1 The elements of curtain walling have to be assigned to group 1 to 4 product depending on their design.

Mechatronic and electronic security systems are included in Annex E.

This European Standard does not directly cover the resistance of locks and cylinders to attack with picking tools. It also does not cover precast concrete elements. Hardware is a component on the products and cannot be classified as such according to this standard.

This European Standard does not apply to doors, gates and barriers, intended for installation in areas in the reach of persons, and for which the main intended uses are giving safe access for goods and vehicles accompanied or driven by persons in industrial, commercial or residential premises, as covered by EN 13241.

NOTE 2 Construction products that can be reached or driven through by vehicles should be protected by appropriate measures such as barriers, extensible ramps, etc.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 356:1999, *Glass in building — Security glazing — Testing and classification of resistance against manual attack*

EN 1303:2015, *Building hardware — Cylinders for locks — Requirements and test methods*

prEN 1628:2018[1], *Pedestrian doorsets, windows, curtain walling, grilles and shutters — Burglar resistance — Test method for the determination of resistance under static loading*

prEN 1629:2018[2], *Pedestrian doorsets, windows, curtain walling, grilles and shutters — Burglar resistance — Test method for the determination of resistance under dynamic loading*

prEN 1630:2018[3], *Pedestrian doorsets, windows, curtain walling, grilles and shutters — Burglar resistance — Test method for the determination of resistance to manual burglary attempts*

EN 1906:2012, *Building hardware — Lever handles and knob furniture — Requirements and test methods*

[1] Under preparation. Stage at the time of publication: prEN 1628:2018

[2] Under preparation. Stage at the time of publication: prEN 1629:2018

[3] Under preparation. Stage at the time of publication: prEN 1630:2018

EN 12209:2016, *Building hardware —Mechanically operated locks and locking plates — Requirements and test methods*

EN 12519:2018, *Windows and pedestrian doors — Terminology*

EN 13126-3:2011*, Building hardware - Hardware for windows and door-height windows - Requirements and test methods - Part 3: Handles, primarily for TiltandTurn, Tilt-First and Turn-Only hardware*

EN 14846:2008*, Building hardware - Locks and latches - Electromechanically operated locks and striking plates - Requirements and test methods*

EN 15684:2012*, Building hardware - Mechatronic cylinders - Requirements and test methods*

prEN 15685:2018[4]*, Building hardware - Mechanically operated locks and locking plates - Requirements and test methods*

ISO 1000:1992, *SI units and recommendations for the use of their multiples and of certain other units*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 12519:2018 and in ISO 1000:1992 and the following apply.

3.1
burglar resistance
property of pedestrian doorsets, windows, curtain walling, grilles and shutters to resist attempts at forced entry using physical force and with the aid of predefined tools into the protected room or area

3.2
burglar resistant product
complete, functioning element that, when built in and fastened or fastened and secured, has the function of resisting forced entry through the application of physical force assisted by predefined tools

3.3
Group 1 product
product that has a solid and rigid leaf and/or opening element. If the product incorporates an opening element, the principal movement to open is turning of the element

NOTE to entry Examples of Group 1 products are hinged or pivoted windows and doorsets or fixed windows. Fixed constructions are also defined as a Group 1 product.

3.4
Group 2 product
product that has a solid and rigid leaf or opening element and the principal movement to open is sliding. Fixed elements of these products are tested in accordance with Group 1 products.

NOTE to entry Examples of Group 2 products are sliding doorsets and sliding windows.

[4] Under preparation. Stage at the time of publication: prEN 15685

3.5
Group 3 product
product that has a leaf or opening element constructed from a number of rigid elements joined together such that the elements may move relative to each other

NOTE to entry An example of a Group 3 product is a roller shutter.

3.6
Group 4 product
product with one or more openings (excluding letter plates) through which gap gauge B (25 mm) can pass

NOTE An example of a Group 4 product is a grille.

3.7
resistance class (RC)
level of resistance that the product provides against burglary attempts

3.8
attack side
side of the test specimen defined by the applicant as the side exposed to attack

3.9
non-attack side
side of the test specimen defined by the applicant as the side not exposed to attack

3.10
roller shutter
shutter, the curtain of which consists of movable, interconnected rigid elements, and travels over a roller in order to open/close

3.11
roller grille
component that can be moved vertically or horizontally in front of the opening to be secured and that can also be removed

NOTE to entry The individual grille bars are movably interconnected with each other. The grille curtain travels over a roller in order to open.

3.12
closed condition
condition defined and described by the manufacturer or applicant in which the tested element meets the burglar resistant requirements

NOTE to entry EN 12519:2018 defines closed, fastened, latched, locked and secured.

3.14
resistance time
working time of the test person carrying out the manual burglary test

NOTE to enty The resistance time includes times of less than 5 s each for tool changes, e.g. exchanging a screwdriver for a crowbar.

3.15
infilling
glazing or panel of any material or combination of materials which are used to fill an aperture in a window or doorset that can be replaced, and which are typically retained by glazing beads

4 Resistance classification

Each construction product conforming to this standard shall be classified according to one of seven resistance classes, depending on the level of burglar resistance offered by the product.

NOTE The resistance classes correspond to known methods of attack currently used by burglars as described in Annex B, Table B.1.

A system or family of products shall be classified using the approach described in Annex C.

The test specimen shall be in the closed conditions defined by the manufacturer.

A product offering burglar resistance at more than one closed condition can be tested, assessed and classified at each condition.

In the documentation accompanying the product, the resistance class shall be given as per the following examples:

- Burglar resistant window EN 1627 RC 1 N
- Burglar resistant window EN 1627 RC 3
- Burglar resistant door EN 1627 RC 2.

The procedure for testing and classification shall be carried out as described in Annex D.

For the purpose of historic data, products classified under EN 1627:2018 are assumed to meet the same classes of this standard.

5 Glazed infillings

The glazing infilling shall meet the minimum requirements in Table 1. When several panes of glass are used in a product, e.g. insulating glass units, then at least one pane shall meet the resistance class as shown in Table 1. On a product classified to EN 1627, the pane can be replaced with the same or higher resistance class of glazed infill if the retention system remains identical to that tested.

Table 1 — Minimum requirements for glazed infilling

Resistance class for product	Resistance class of pane according to EN 356:1999
RC 1 N	No requirements*
RC 2 N	No requirements*
RC 2	P4 A
RC 3	P5 A
RC 4	P6 B
RC 5	P7 B
RC 6	P8 B
* National provision may be followed.	

NOTE 1 The use of furniture that requires a removable key or tool to effect unlocking might be required when using glazing with a resistance class lower than P4A.

On elements equipped with emergency exit devices or panic exit devices, the glazing or the infilling shall prohibit operating the device to gain an accessible opening by penetrating the infilling with the relevant tools. This vulnerability shall be examined according to prEN 1630:2018 clause 6.3.1.

NOTE 2 Glazing according to EN 356:1999 with special or reinforced inlays may be necessary.

6 Building hardware

6.1 General

Performance evaluation of hardware fitted on pedestrian door sets, windows, curtain walling, grilles and shutters subject to this standard shall be carried out according to the rules defined in this Clause 6.

6.2 Key related security

Requirements

For all resistance classes, hardware components lockable with a key shall fulfil key related security requirements according to Table 2A.

Table 2A — Key related security

Hardware component standard	Requirement	RC 1 N	RC 2	RC 3	RC 4	RC 5	RC 6
EN 1303:2015 cylinder for lock	Digit 7	4	4	5	6	6	6
EN 15684:2012 Mechatronic cylinder	Digit 5[a] or Digit 6[a]	E	E	E[b]	F	F	F
		D	E	E[b]	F	F	F
EN 12209:2016 Mechanical lockcase	Digit 8 key identification (lever lock)	B	B	B	D	E	E
prEN 15685:2018 Multipoint locks (under process)	Digit 8 Mechanical keys	B	B	B	D	E	E
EN 14846:2008 (under revision)	Digit 11 (EN 12209:2016)	B	B	B	D	E	E
EN 13126-3:2011 Key operated lockable window handle	Digit 7 – 2nd part of digit 7 extension for locking mechanism	2[c]/2	2[c]/2	2/2	2/3	2/3	2/3

[a] The specified grades may alternatively be achieved by the mechanical (digit 5) or electronic (digit 6) key related security. Mechatronic cylinders do not need to have a mechanical lockwork (EN 15684:2012, digit 5, Grade A). In this case grade A in digit 6 of EN 15684:2012 fulfils the requirement.

[b] Mechatronic cylinder with mechanical codes shall have a minimum number of 6 movable detainers (digit 7 level 5 of EN 1303:2015).

[c] Grade 1 only if two or more handles are used on a single sash.

Application to windows

For handles on windows it may be possible to actuate the handle indirectly from the attack side by actuating the transmission rod by e. g. one of the locking cams. Therefore, either lockable window handles in accordance with the requirements of Table 2A or alternatively other hardware components to provide protection against this kind of attack shall be used.

Lockable window handles

- Key-operated lockable window handles: In the case of using window handles with a key operated locking mechanism the requirements of Table 2A are applicable to the window handle opposite to the attack side (digit 7: 2/2 or 2/3 in accordance with EN 13126-3:2011).
- Non-key-operated lockable window handles: In the case of using window handles with a non-key operated locking mechanism (for example PTO 'push to open'), the requirements in accordance with EN 13126-3:2011, digit 7: 2/1 shall be met.

For RC 1 N: In the case of using Non-key-operated lockable window handles, a test on the window handle in accordance with clause 8 and 6.3.1 of prEN 1630:2018 shall be carried out on the window with tool set A1. The resistance time shall be 3 minutes and the acceptance criterion shall be 'no accessible opening'.

For RC 2/RC 2 N up to RC 6: In the case of using Non-key-operated lockable window handles, a test in accordance with 6.3.1 of prEN 1630:2018 shall be done with the appropriate tool set and resistance time

Non-lockable window handles

In the case of using window handles without any locking mechanism, other components with an appropriate locking function should be used. In this case generally a test in accordance with clause 8 in EN 1627 and clause 6.3.1 in prEN 1630:2018 shall be carried out.

For RC 1 N: a test on the window handle in accordance with clause 8 and 6.3.1 of prEN 1630:2018 shall be carried out on the building element with tool set A1. The resistance time shall be 3 minutes and the acceptance criterion shall be 'no accessible opening'. Additionally a test in accordance with Annex C of prEN 1628 shall be carried out if applicable.

For RC 2/RC 2 N up to RC 6: a test in accordance with clause 8 and 6.3.1 of prEN 1630:2018 shall be done with the appropriate tool set and resistance time.

6.3 Attack related security

Hardware components fitted on pedestrian doorsets, windows, curtain walling, grilles and shutters subject to this standard shall either:

- meet the requirements of prEN 1627:2018 Table 2B (see under 6.4) or
- be tested in accordance with 6.5 (prEN 1627:2018)

For RC 2/RC 2 N up to RC 6 the retention of the hardware shall be tested in accordance with prEN 1630:2018.

6.4 Hardware assessment according to their appropriate standard

Building hardware components shall fulfil the requirements of Table 2B, according to their appropriate specific standard.

The requirements of Table 2B are valid for those parts of the hardware components that are on the attack side of the pedestrian doorsets, windows, curtain walling, grilles and shutters defined by the applicant.

For RC 5 and RC 6 building element, building hardware components fulfilling Table 2B requirements shall additionally be subjected to the manual attack in an attempt to open the building element in accordance with sub clause 8 of prEN 1627:2018 and prEN 1630:2018.

Table 2B — Attack related security

Hardware component standard	Requirement	RC 1 N	RC 2 N	RC 2	RC 3	RC 4	RC 5	RC 6
EN 1303:2015 cylinder for lock	Digit 8	C	C	C	C	D	test according to prEN 1630:2018	
EN 1303:2015 cylinder for locks in combination with EN 1906:2012 lever handle with plug protection	Digit 8 of EN 1303:2015	A	A	A	A	B	test according to prEN 1630:2018	
	Digit 7 of EN 1303:2015	2	2	2	3	4	test according to prEN 1630:2018	
EN 15684:2012, Mechatronic cylinders	Digit 8	1	1	1	1	2	2 and test according to prEN 1630:2018	
EN 15684:2012 mechatronic cylinder in combination with EN 1906:2012 lever handle with plug protection	Digit 8 of EN 15684:2012	1	2	2	2	2	2 and test according to prEN 1630:2018	
	Digit 7 of EN 1906:2012	2	2	2	3	4	test according to prEN 1630:2018	
EN 1906:2012 Lever handles and knob furniture	Digit 7 Security	1	1	3	3	4	test according to prEN 1630:2018	
EN 12209:2016 Mechanically operated locks and locking plates prEN 15685:2018 Multipoint locks, latches and locking plates: *Classification based on one point*	Digit 7	3	3	3	4	7[a]	test according to prEN 1630:2018	
prEN 15685:2018 Multipoint locks, latches and locking plates: *Classification based on more than one points*	Digit 7	2	3	3	3	5	test according to prEN 1630:2018	
	Digit 9 Security for anti-separation point	2	3	3	3	5	test according to prEN 1630:2018	

Hardware component standard	Requirement	RC 1 N	RC 2 N	RC 2	RC 3	RC 4	RC 5	RC 6
EN 14846:2008, Electromechanically operated locks and striking plate	Digit 7 Security	3	3	3	4	7[b]	test according to prEN 1630:2018	
	Digit 9	2	2	2	2	3	3	
EN13126-3:2011 window handle (lockable)	Digit 7 1st part of digit 7: grade for resistance against twisting-off and forcing-off"	2[c]/2 2 [c] /1	2 [c] /2 2 [c] /1	2 [c] /2 2 [c] /1	2/2 2/1	2/3 2/1	2/3 2/1	

[a] A lock with security class 6 (digit 7) may be used if the drill resistance required in class 7 is provided by the door construction.

[b] A lock with security class 4 (digit 7) may be used if the drill resistance required in class 7 is provided by the door construction.

[c] Grade 1 Only if two or more handles are used on a single sash.

6.5 Assessment of hardware not fulfilling prEN 1627:2018 Table 2B requirements

6.5.1 General

When hardware components do not fulfil prEN 1627:2018 Table 2B, assessment of hardware capability will be made on the complete building element for class RC 2/RC 2 N up to RC 4 building element. The assessment is made on request of the applicant.

- the objective of the tests will be to test the performance of the hardware component only for the characteristics as required in Table 2B;
- Test of the component itself will be carried out with that component fitted on the complete building element;
- The failure requirement will be "accessible opening" of the building element according to prEN 1630:2018 clause 6.7;
- Tests will be done according to prEN 1630:2018 "test method for the determination of resistance to manual burglary attempts";
- Tests to be carried out and the tool set to be used for each component are defined in paragraph 6.5.2;
- The resistance time shall be in accordance with prEN 1627:- for the claimed RC

NOTE Each specific test may be perform on a new sample.

- Hardware interchangeability rules (prEN 1627:2018 Annex C) do not apply for hardware tested according to clause 6.5.

6.5.2 Additional test and tool set for hardware not complying with Table 2B

This paragraph describes for each hardware component the test to be carried out and the tool set to be used for hardware not complying with Table 2B.

The Table of paragraph 6.5.2 state:

- The list of tests to be done according to clause 6.5.1;
- Tools to be used for each test. Tools are identified by their number according to prEN 1630:2018;
- Tool set A1 can be used for all tests carried out according to clause 6.5.

6.5.2.1 Cylinder for lock

Table 2C — Cylinder for lock

Hardware component	Test	RC 2 N	RC 2	RC 3	RC 4
Cylinder for locks	Resistance to attack by drilling	Tool set A1 + Drilling machine 4.7 + drill bit 4.7.1	Tool set A1 + Drilling machine 4.7 + drill bit 4.7.1	Tool set A1 + Drilling machine 4.7 + drill bit 4.7.1	Tool set A1 + Drilling machine 4.7 + drill bit 4.7.1
	Resistance to attack by chisel	Tool set A1 + chisel 4.2 and 4.3 + hammer 4.1	Tool set A1 + chisel 4.2 and 4.3 + hammer 4.1	Tool set A1 + chisel 4.2 and 4.3 + hammer 4.1	Tool set A1 + chisel 4.2 and 4.3 + hammer 4.1
	Resistance to attack by twisting	Tool set A1+ tube 2.8+ wrench 2.2	Tool set A1+ tube 2.8+ wrench 2.2	Tool set A1+ tube 2.8+ wrench 2.2	Tool set A1+ tube 2.8+ wrench 2.2
	Resistance to attack by plug/cylinder extraction	Tool set A1+ prEN 1630:2018 Annex E [a)]	Tool set A1+ prEN 1630:2018 Annex E [a)]	Tool set A1+ prEN 1630:2018 Annex E [a)]	Tool set A1+ prEN 1630:2018 Annex E [b)]
	Torque resistance of plug/cylinder	Tool set A1+ screwdriver 1.3 and 1.2 +hammer 4.1	Tool set A1+ screwdriver 1.3 and 1.2 +hammer 4.1	Tool set A1+ screwdriver 1.3 and 1.2 +hammer 4.1	Tool set A1+ screwdriver 1.3 and 1.2 +hammer 4.1
Cylinder for locks in combination with lever handle with plug protection	When assessment is made according to two different standards, only use of Table 2B				
[a] EN 1303:2015 attack resistance grade C [b] EN 1303:2015 attack resistance grade D					

6.5.2.2 Mechatronic cylinder

Table 2D — Mechatronic cylinder

Hardware component	Test	RC 2 N	RC 2	RC 3	RC 4
Mechatronic cylinder	Resistance to attack by drilling	Tool set A1 + Drilling machine 4.7 + drill bit 4.7.1	Tool set A1 + Drilling machine 4.7 + drill bit 4.7.1	Tool set A1 + Drilling machine 4.7 + drill bit 4.7.1	Tool set A1 + Drilling machine 4.7 + drill bit 4.7.1
	Resistance to attack by chisel	Tool set A1 + chisel 4.2 and 4.3 + hammer 4.1	Tool set A1 + chisel 4.2 and 4.3 + hammer 4.1	Tool set A1 + chisel 4.2 and 4.3 + hammer 4.1	Tool set A1 + chisel 4.2 and 4.3 + hammer 4.1
	Resistance to attack by twisting	Tool set A1+ tube 2.8+ wrench 2.2	Tool set A1+ tube 2.8+ wrench 2.2	Tool set A1+ tube 2.8+ wrench 2.2	Tool set A1+ tube 2.8+ wrench 2.2
	Resistance to attack by plug/cylinder extraction	Tool set A1+ prEN 1630:2018 Annex E [a)]	Tool set A1+ prEN 1630:2018 Annex E [a)]	Tool set A1+ prEN 1630:2018 Annex E [a)]	Tool set A1+ prEN 1630:2018 Annex E [b)]
	Torque resistance of plug/cylinder	Tool set A1+ screwdriver 1.3 and 1.2 +hammer 4.1	Tool set A1+ screwdriver 1.3 and 1.2 +hammer 4.1	Tool set A1+ screwdriver 1.3 and 1.2 +hammer 4.1	Tool set A1+ screwdriver 1.3 and 1.2 +hammer 4.1
	Attacks by hits	EN 15684:2012 use of grade 1 tool	EN 15684:2012 use of grade 1 tool	EN 15684:2012 use of grade 1 tool	EN 15684:2012 use of grade 2 tool
	Attacks by vibrations	EN 15684:2012 use of grade 1 tool	EN 15684:2012 use of grade 1 tool	EN 15684:2012 use of grade 1 tool	EN 15684:2012 use of grade 2 tool
	Increase voltage attacks	EN 15684:2012 use of grade 1 tool	EN 15684:2012 use of grade 1 tool	EN 15684:2012 use of grade 1 tool	EN 15684:2012 use of grade 2 tool
	Electrostatic discharge attack	EN 15684:2012 use of grade 1 tool	EN 15684: 2012 use of grade 1 tool	EN 15684: 2012 use of grade 1 tool	EN 15684: 2012 use of grade 2 tool
	Magnetic field attack	EN 15684: 2012 use of grade 1 tool	EN 15684: 2012 use of grade 1 tool	EN 15684: 2012 use of grade 1 tool	EN 15684: 2012 use of grade 2 tool
Mechatronic cylinder in combination with lever handle with plug protection	When assessment is made according to two different standards, only use of Table 2B				
[a] EN 1303:2015 attack resistance grade C [b] EN 1303:2015 attack resistance grade D					

NOTE EN 15684:2012 use of grade 1 tool: tests according to EN 15684:2012 are manual tests, so for mechatronic cylinder that do not fulfill requirements of Table 2B, test according to clause 6.5 will be carried out with grade 1 tool of EN 15684:2012.

6.5.2.3 Lever handle and knob furniture

Table 2E — Lever handle and knob

Hardware component	Test	RC 2 N	RC 2	RC 3	RC 4
Lever handles and knob furniture	Plate strength	chisel 4.2 and 4.3 + hammer 4.1 + tool set A2	chisel 4.2 and 4.3 + hammer 4.1 + tool set A2	chisel 4.2 and 4.3 + hammer 4.1 + tool set A3	tool set A4
	Strength of fastening element	chisel 4.2 and 4.3 + hammer 4.1 + tool set A2	chisel 4.2 and 4.3 + hammer 4.1 + tool set A2	chisel 4.2 and 4.3 + hammer 4.1 + tool set A3	tool set A4
	Resistance to attack by drilling	chisel 4.2 and 4.3 + hammer 4.1 + tool set A2	chisel 4.2 and 4.3 + hammer 4.1 + tool set A2	chisel 4.2 and 4.3 + hammer 4.1 + tool set A3	tool set A4
	Resistance to attack by chisel	chisel 4.2 and 4.3 + hammer 4.1 + tool set A2	chisel 4.2 and 4.3 + hammer 4.1 + tool set A2	chisel 4.2 and 4.3 + hammer 4.1 + tool set A3	tool set A4
	Additional requirement for the strength of plug protection plate (if fitted)	Tool set A1+ prEN 1630:2018 Annex E a)	Tool set A1+ prEN 1630:2018 Annex E a)	Tool set A1+ prEN 1630:2018 Annex E a)	Tool set A1+ prEN 1630:2018 Annex E b)

[a] EN 1303:2015 attack resistance grade C
[b] EN 1303:2015 attack resistance grade D

6.5.2.4 Single point lock

Table 2F — Single point lock

Hardware component	Test	RC 2 N	RC 2	RC 3	RC 4
Mechanically operated single point locks and locking plates	Torque resistance of lockable follower	Test of lock to complete access of the building element with the given grade tool set	Test of lock to complete access of the building element with the given grade tool set	Test of lock to complete access of the building element with the given grade tool set	Test of lock to complete access of the building element with the given grade tool set
	Side load on dead bolt/ drilling of dead bolt	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test
	Dead bolt projection	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test

Hardware component	Test	RC 2 N	RC 2	RC 3	RC 4
	End load on dead bolt	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test
	Resistance to pulling on hook bolt	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test	checked during prEN 1630:2018test
	Resistance to disengaging on hook bolt	checked during prEN 1630:2018 test	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test
	Resistance to forcing locating devices on sliding doors	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test
	Resistance to end load on box protected locking plates	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test
	Resistance to side load on locking plates	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test
	Resistance to pulling on locking plates	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test
	Resistance to lifting forces on locking plates	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test

NOTE Checked during prEN 1630:2018, this means that for component not complying with Table 2B, its performance will be assessed during the manual burglary attack according to prEN 1630:2018 clause 8.

6.5.2.5 Multipoint lock

Table 2G — Multipoint lock

Hardware component	Test	RC 2 N	RC 2	RC 3	RC 4
Multipoint locks, latches and locking plates: *Classified based on one point.*	torque resistance of lockable follower	Test of lock to complete access of the building element with the given grade tool set	Test of lock to complete access of the building element with the given grade tool set	Test of lock to complete access of the building element with the given grade tool set	Test of lock to complete access of the building element with the given grade tool set
	side load of locking point/ drilling of locking point	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test
	locking point bolt projection	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test
	disengaging force without box protected locking plate	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test

Hardware component	Test	RC 2 N	RC 2	RC 3	RC 4
	disengaging force with box protected locking plate	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test
	Strong key attack on lever locks	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test
	Resistance to force on box protected locking plates	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test
	Resistance to side load on locking plate	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test
	Anti-separation point bolt projection	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test
	Resistance to disengaging force of the anti-separation point	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test
	Resistance to pulling of anti-separation point	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test
	Resistance to forcing of anti-lifting device for sliding door	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test
	Resistance to pulling on locking plate for the anti-separation point	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018 test	checked during prEN 1630:2018test
	Resistance to lifting force on locking plate	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test	checked during prEN 1630:2018test

6.5.2.6 Electromechanically operated lock and striking plate

Table 2H — Electromechanically operated lock and striking plate

Hardware component	Test	RC 2 N	RC 2	RC 3	RC 4
Electro-mechanically operated locks and striking plates	Side load on dead bolt/ drilling of dead bolt	checked during prEN 1630: 2018 test	checked during prEN 1630: 2018 test	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test
	Dead bolt projection	checked during prEN 1630: 2018 test	checked during prEN 1630: 2018 test	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test
	End load on dead bolt	checked during prEN 1630: 2018 test	checked during prEN 1630: 2018 test	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test
	Resistance to pulling on hook/claw bolt	checked during prEN 1630: 2018 test	checked during prEN 1630: 2018 test	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test
	Resistance to disengaging on hook/claw bolt	checked during prEN 1630: 2018 test	checked during prEN 1630: 2018 test	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test
	Resistance to forcing locating devices on sliding doors	checked during prEN 1630: 2018 test	checked during prEN 1630: 2018 test	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test
	Resistance to pulling off of knob on bore locks	checked during prEN 1630: 2018 test	checked during prEN 1630: 2018 test	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test
	Resistance to side load on locking plates	checked during prEN 1630: 2018 test	checked during prEN 1630: 2018 test	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test
	Resistance to pulling on locking plates	checked during prEN 1630: 2018 test	checked during prEN 1630: 2018 test	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test
	Resistance to lifting forces on locking plates	checked during prEN 1630: 2018 test	checked during prEN 1630: 2018 test	checked during prEN 1630:2018 test	checked during prEN 1630:2018 test
	Voltage drop requirements	Table 2B requirements shall be fulfilled. No extra test according to prEN 1627:2018 clause6.5	Table 2B requirements shall be fulfilled. No extra test according to prEN 1627:2018 clause6.5	Table 2B requirements shall be fulfilled. No extra test according to prEN 1627:2018 clause6.5	Table 2B requirements shall be fulfilled. No extra test according to prEN 1627:2018 clause6.5

Hardware component	Test	RC 2 N	RC 2	RC 3	RC 4
	Protection against the effect of cutting cable	Table 2B requirements shall be fulfilled. No extra test according to prEN 1627:2018 clause 6.5	Table 2B requirements shall be fulfilled. No extra test according to prEN 1627:2018 clause 6.5	Table 2B requirements shall be fulfilled. No extra test according to prEN 1627:2018 clause 6.5	Table 2B requirements shall be fulfilled. No extra test according to prEN 1627:2018 clause 6.5
	Protection against the effect of wire manipulation	Table 2B requirements shall be fulfilled. No extra test according to prEN 1627:2018 clause 6.5	Table 2B requirements shall be fulfilled. No extra test according to prEN 1627:2018 clause 6.5	Table 2B requirements shall be fulfilled. No extra test according to prEN 1627:2018 clause 6.5	Table 2B requirements shall be fulfilled. No extra test according to prEN 1627:2018 clause 6.5
	Resistance to electromagnetic manipulation	Table 2B requirements shall be fulfilled. No extra test according to prEN 1627:2018 clause 6.5	Table 2B requirements shall be fulfilled. No extra test according to prEN 1627:2018 clause 6.5	Table 2B requirements shall be fulfilled. No extra test according to prEN 1627:2018 clause 6.5	Table 2B requirements shall be fulfilled. No extra test according to prEN 1627:2018 clause 6.5
	Resistance to electrostatic discharge	Table 2B requirements shall be fulfilled. No extra test according to prEN 1627:2018 clause 6.5	Table 2B requirements shall be fulfilled. No extra test according to prEN 1627:2018 clause 6.5	Table 2B requirements shall be fulfilled. No extra test according to prEN 1627:2018 clause 6.5	Table 2B requirements shall be fulfilled. No extra test according to prEN 1627:2018 clause 6.5
	Resistance to electrostatic manipulation	Table 2B requirements shall be fulfilled. No extra test according to prEN 1627:2018 clause 6.5	Table 2B requirements shall be fulfilled. No extra test according to prEN 1627:2018 clause 6.5	Table 2B requirements shall be fulfilled. No extra test according to prEN 1627:2018 clause 6.5	Table 2B requirements shall be fulfilled. No extra test according to prEN 1627:2018 clause 6.5

6.5.2.7 Lockable window handle

Lockable window handle not complying with EN 13126-3:2011:

- For RC 1 N: a test on the window handle in accordance with 6.3.1 of prEN 1630:2018 shall be carried out on the window with tool set A1. The resistance time shall be 3 minutes and the acceptance criterion shall be 'no accessible opening'.

- For RC 2/RC 2 N up to RC 6: a test in accordance with 6.3.1 of prEN 1630:2018 shall be done with the appropriate tool set and resistance time.

The aim of the test is to explore if the handle can be operated indirectly from the attack side by either actuating the transmission rods or by penetrating the element.

7 Mechanical strength

7.1 Static loading

When tested in accordance with prEN 1628:2018 using the loads detailed in Tables 3, 4 and 5 as appropriate, the test specimen shall not exhibit failure at the resistance class claimed.

The loading tests shall be conducted in the sequence detailed in the relevant test method.

Table 3 — Static loading of Group 1 and Group 2 products

	Gap gauge	Pressure pad	**Resistance class (RC)**			
			1, 2	**3**	**4**	**5, 6**
			Test Load	Test Load	Test Load	Test Load
Loading points	Type	Type	kN	kN	kN	kN
F1 Corner of infilling	B	1	3	6	10	15
F2 Leaf and casement corners	B	1 or 2	1,5	3	6	10
F3 Locking Points	A	1 or 2	3	6	10	15
F3.a Group 1[a] and 2[b] products Locking Points (additional loadings)	A	-	1,5	-	-	-

[a] Group 1 products only in resistance class 1

[b] Group 2 products only in resistance classes 1 and 2

Table 4 — Static loading of Group 3 products

	Resistance class (RC)											
	1, 2			**3**			**4**			**5, 6**		
	Test load	Limiting value	Pressure pad	Test load	Limiting value	Pressure pad	Test load	Limiting value	Pressure pad	Test load	Limiting value	Pressure pad
Loading points	kN	mm	Type	kN	mm	Type	kN	Mm	Type	kN	mm	Type
F1.1 Guide rail deflection test	3	30°[a]	4	6	30°[a]	4	10	30°[a]	4	15	30°[a]	4
F3 Curtain lift test	3	C[c]	1 or 2	6	C[c]	1 or 2	10	C[c]	1 or 2	15	C[c]	1 or 2
F2 Lath engagement test	1,5	10	1 or 2	3	10	1 or 2	6	10	1 or 2	10	10	1 or 2
F1 Static test on guide rail and curtain	3	10[b]	3	6	10[b]	3	10	10[b]	3	15	10[b]	3

[a] Maximum allowable deflection of the loaded leg of the guide rail is 30°. The determination of the angle is described in prEN 1628:2018**.**

[b] Minimum depth of penetration under static load.

[c] Checked by means of gap gauge type C, prEN 1628:2018, Figure A.14

Table 5 — Static loading of Group 4 products

	Resistance class (RC)											
	1, 2			**3**			**4**			**5, 6**		
Loading points	Test Load kN	Gap gauge mm	Pressure pad Type	Test Load kN	Gap gauge mm	Pressure pad Type	Test Load kN	Gap gauge mm	Pressure pad Type	Test Load kN	Gap gauge mm	Pressure pad Type
F2.1 Between two fixing points	1,5	C	5	3	C	5	6	C	5	10	C	5
F2.2 Loading between two junction points	1,5	C	5	3	C	5	6	C	5	10	C	5
F3 Locking points	3	C	1 or 2	6	C	1 or 2	10	C	1 or 2	15	C	1 or 2
F3.1 Fixing point between grille and masonry	3	C	5	6	C	5	10	C	5	15	C	5
F1 Static test on guide rail and curtain or two adjacent grille bars at a junction point	3	C	5	6	C	5	10	C	5	15	C	5
F1.1 Guide rail deflection test load	3	30°[a]	4	6	30°[a]	4	10	30°[a]	4	15	30°[a]	4
F3.2 Curtain lift test	3	C	1 or 2	6	C	1 or 2	10	C	1 or 2	15	C	1 or 2
F2.3 Drawing the grille curtain out of the guide rail	1,5	C	1 or 2	3	C	1 or 2	6	C	1 or 2	10	C	1 or 2

[a] Maximum allowable deflection of the loaded leg of the guide rail is 30°. The determination of the angle is described in prEN 1628:2018.

NOTE Gap gauge type C can be found in prEN 1628:2018, Figure A.14.

7.2 Dynamic loading in resistance classes 1, 2 and 3

When tested in accordance with prEN 1629:2018 using the mass and drop height given in Table 6, the test specimen shall not fail at the resistance class claimed. The centre of the test specimen and infillings shall be subjected to three impacts and all other impact points shall be subjected to one impact as detailed in prEN 1629:2018, Figures A.21 to A.29.

Table 6 — Drop height for dynamic test

Resistance class (RC)	**Mass of the impactor** kg	**Drop height** mm
1	50	450
2	50	450
3	50	750
4 - 6	no dynamic test is required	

8 Manual burglary attempts

8.1 General

When tested in accordance with prEN 1630:2018 using the tool sets and times specified in Table 7, the test specimen shall not fail at the resistance class claimed. For construction products of resistance class 1 no manual test will be carried out.

Table 7 — Tool sets and resistance time

Resistance class (RC)	**Tool set (see prEN 1630:2018, Clause 7)**	**Resistance time** min	**Maximum total test time** min
1	A1	–	–
2	A2	3	15
3	A3	5	20
4	A4	10	30
5	A5	15	40
6	A6	20	50
For RC 1 N products:2018no manual burglary attempt will be performed. A1 toolset is only intended for the preparation of the test sample.			

NOTE The maximum total test time is the sum of resistance time, rest time, tool change time and observation time (see definitions in prEN 1630:2018).

8.2 Non key operated hardware

For construction products without key operated hardware (e.g. panic exit device, knob cylinder, non-lockable window handle) on the non-attack side, entry might be gained by penetrating the product (including infillings of glass) and operating the hardware. This vulnerability shall be explored and tested in all resistance classes.

For RC 1 N: a test in accordance with 6.3.1 of prEN 1630:2018 shall be carried out on the building element with tool set A1. The resistance time shall be 3 minutes and the acceptance criterion shall be 'no accessible opening'.

For RC 2/RC 2 N up to RC 6: a test in accordance with 6.3.1 of prEN 1630:2018 shall be done with the appropriate tool set and resistance time.

9 Classification report

A classification report shall be provided and shall contain the following, minimum information:

a) classification report reference (number and date);

b) details of the applicant;

c) product description;

d) product name;

e) dimensions;

f) details of the attack side;

g) declared closing condition(s)

h) glazing details (thickness) and classification;

i) details of the hardware, including unique component reference(s);

j) reference to installation instructions;

k) the resistance class for each declared closing condition according to this standard;

l) reference to this standard and its date;

m) field of application where required, see Annex C.

The classification report shall also contain either:

a) Where it is applicable all the information required by the test reports in prEN 1628:2018, prEN 1629:2018and prEN 1630:2018;

or

b) reference to the relevant test reports.

10 Installation

Installation shall be carried out in accordance with the installation instructions provided by the manufacturer. Annex A gives recommendations for the contents of the manufacturer's installation instructions.

11 Test specimens

For RC 1 N products one test specimen is required. All tests shall be conducted on this specimen.

For RC 2/RC 2 N to RC 6 products a minimum of two test specimens are recommended. In such case the static load test according to prEN 1628:2018, the dynamic load test according to prEN 1629:2018 and the pre-test according to prEN 1630:2018 may be conducted on the first specimen. The main manual test may be carried out on the second specimen. At the discretion of the manufacturer all tests may be carried out on a single specimen.

More specimens may be required, if a range (e.g. opening direction, sizes, hardware, infills etc) of products is to be tested.

12 Marking

Products classified according to this standard shall as a minimum be marked with:

- Resistance class according to EN 1627 (including edition)
- Type designation or similar
- Name of the manufacturer or similar

The marking shall be supplied with the product on at least one of the following:

- On any suitable part of the product itself, providing the visibility is ensured when the leaves, casements or sashes are opened;
- on an attached label;
- on its packaging;
- on the accompanying commercial document(s) (e.g. a delivery note) or the manufacturers published technical specification(s).

NOTE If any of the information above is included in other markings it is not necessary to repeat it.

Annex A
(informative)

Recommendations for the contents of the manufacturer's installation instructions

The manufacturer's installation instructions should contain the following information:

a) Typical details of structural openings into which the product can be installed.

b) Details regarding fixing points as well as a precise description of the fixing components.

c) Details of points requiring particularly rigid fixing e.g. in the vicinity of locks and hinges.

d) Details of the compression resistance of packing in the cavity between the wall and the frame, e.g. in the vicinity of locks and hinges.

e) Details of the gaps to be maintained between moving and fixed parts.

f) Details, where appropriate, regarding the maximum permissible projection of the lock cylinder outside the external lock shield plate.

g) Other details as far as they influence the burglar resistant properties of the test specimen.

h) Details of the closing condition and or conditions that meet the requirements for the resistance class claimed.

Additional information regarding roller shutters and roller grilles:

i) Fixing type and maximum distance between fixings in the guide rail.

j) Minimum penetration depth of the shutter curtain into the guide rail.

k) Type and fixings of anti-lift device, if necessary.

l) Information about protection to the roller shutter box.

Annex B
(informative)
Resistance classes – Classification according to EN 1627

B.1 Introduction

It has taken several years and many lively debates by the member states representatives to agree the method of classifying burglar resistance construction products according to EN 1627. During these discussions the attack methods employed by the burglar (modus operandi) and crime statistics from National sources have been taken into consideration. Also a series of development tests has been carried out and commonly available tools have been grouped into kits for use in the various classes detailed in this Standard.

The issue of reproducibility and repeatability of the manual attack test has been raised by a number of the member states. To address these issues the overall assessment has been enhanced by the further development of the static load test, and the manual attack, now excluded from class 1. The combination of the three test methods, static loading, dynamic loading and manual attack has given rise to an assessment procedure that is more robust and covers that relevant elements relative to each of the classes and therefore the anticipate burglar.

Observations in a number of the member states have concluded that the move from the more traditional level lock towards cylinder-operated locks resulted in an increase in the number of burglaries employing drill attacks on cylinders. This, in turn, gave rise to a significant increase in the use of drill resistant cylinders with a consequence that the occurrences of drill-based attacks have all but disappeared. It is this experience that has led to the requirement for drill resistance cylinders according to EN 1303:2015 and has allowed the creation of tool kits in the lower classes that do not include drills.

The various classes detailed in this standard are intended to cover the opportunist or casual burglar as well as the more experience and professional.

Whilst this standard includes a number of classes the difference between each consecutive class varies. The most significant step is that between classes 3 and 4. This reflects the two distinct groups of burglars recognised in this standard and is discussed in the following paragraphs.

See also Annex E, Table E.1 for further descriptions of anticipated methods and attempts to gaining entry.

B.2 Resistance classes 1 to 3

Classes 1, 2 and 3 are intended to address the levels of attack normal associated with the casual or opportunist burglar. It is believed that these attacks are the result of an opportunity presenting itself with no particular regard to the likely reward that success may bring. The level of force used in not excessive and the tools used are more likely to be common hand tools and levers.

Burglaries covered by these classes are likely to avoid noise and unnecessary risk. As risk is associated with time, the period spent attempting to gain entry is limited and varies with the classes. Likewise, the level of resistance encountered during the attack is a factor. High levels of resistance often resulting in aborted attack.

B.3 Resistance classes 4 to 6

Resistance classes 4, 5 and 6 are associated with the more experienced and professional type burglar with a more focused aim and knowledge of the likely reward that success may bring. These attacks are general planned with knowledge of the construction products to be defeated. Noise is not an issue and time is less of a concern. The tools used often include powerful, single operator power tools with a high likelihood that organised crime is involved.

Table B.1 — Anticipated method and attempts to gaining entry

Resistance class	Anticipated method and attempts to gaining entry
1	The casual burglar attempts to gain entry using small simple tools and physical violence e.g. kicking, shoulder charging, lifting up, tearing out. The burglar typically attempts to take advantage of opportunities, has no specific information on the level of resistance offered by the construction product and is concerned with both time and noise. No specific knowledge of the likely rewards is anticipated and the level of risk the burglar is willing to take is low.
2	The casual burglar additionally attempts to gain entry using simple tools e.g. screwdriver, pliers, wedge and in the case or grilles and exposed hinges the use of small handsaws. Mechanical drilling tools are not associated with this level of burglar as a result of the use of drill resistant cylinders. The burglar typically attempts to take advantage of opportunities, has little knowledge of the likely level of resistance and is concerned with both time and noise. No specific knowledge of the likely rewards is anticipated and the level of risk the burglar is willing to take is low.
3	The burglar attempts to gain entry using a crowbar, an additional screwdriver and hand tools such as a small hammer, pin punches and a mechanical drilling tool. With the use of the crowbar the burglar has the opportunity to apply increased forces. With the drilling tool the burglar is able to attack vulnerable locking devices. The burglar typically attempts to take advantage of opportunities, has some knowledge of the likely level of resistance and is concerned with both time and noise. No specific knowledge of the likely rewards is anticipated and level of risk the burglar is willing to take is medium.
4	The practised burglar uses in addition, a heavy hammer, axe, chisels and a portable battery powered drill. The heavy hammer, axe and drill give the burglar an increased number of attack methods. The burglar anticipates a reasonable reward and is likely to be resolute in his efforts to gain entry. He is also less concerned with the level of noise he produces and is prepared to take a greater risk.
5	The experienced burglar uses in addition electric tools e.g. drills, jig- and sabre saw, and an angle grinder with a disc of max. 125 mm diameter. The use of the angle grinder further expands the range of attack methods likely to be successful. The burglar anticipates a reasonable reward, is resolute in his efforts to gain entry and is well organised. He also has little concerned for the level of noise he generates and is prepared to take a high level of risk.
6	The experienced burglar uses in addition spalling hammer, powerful electric tools, e.g. drills, jig- and sabre saw, and an angle grinder with a disc of max. 230 mm diameter. The tools are capable of being operated by a single person, have a high level of performance and are potentially very effective. The burglar anticipates a good level of reward, is resolute in his efforts to gain entry and is very well organised. He also has no concerned for the level of noise he generates and is prepared to take a high level of risk.

Annex C
(normative)

Field of application

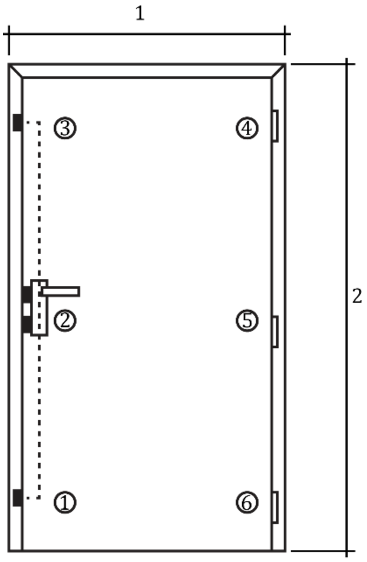
C.1 Dimensions

The classification of a product is valid only for sizes determined in accordance with this annex.

If a system or family of products are to be assessed then a range of test specimens shall be required. The number of test specimens shall depend upon the size of the system of family to be covered. For sample sizes outside the extrapolation rules detailed below, a full technical justification shall be provided.

The following extrapolations for sizes other than those tested shall be permissible without a statement provided that no written limitation is made in the test report.

Increases above those below are permissible with an expert statement.

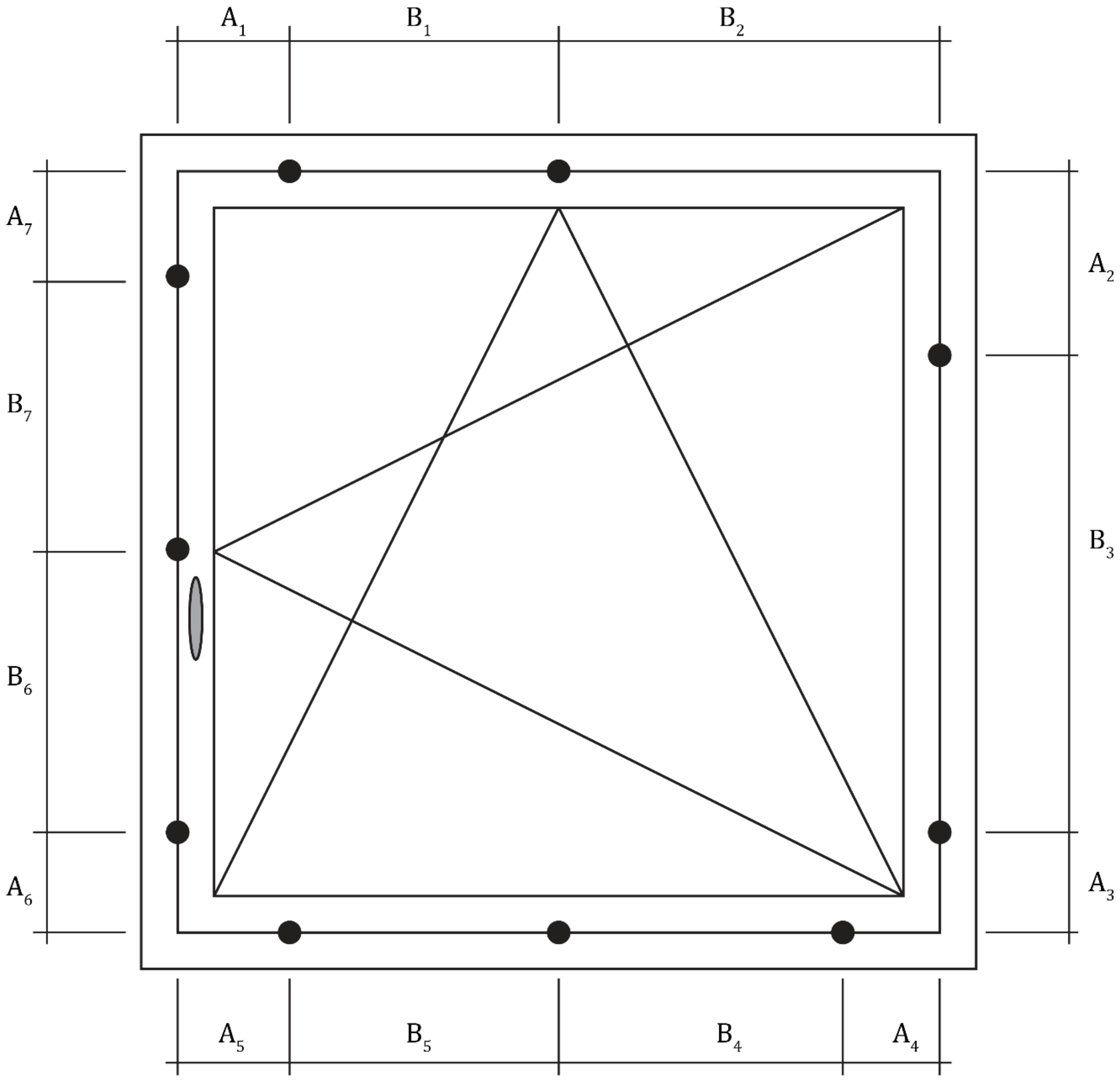


Key

1	Width +10%, -50%
2	Height +10%, -50%
① to ⑥	Locking points

Additionally for doorsets: The number of locking points may be reduced only if the distances between the locking points are not greater than on the tested size.

Figure C.1 — Extrapolation rules for doorsets

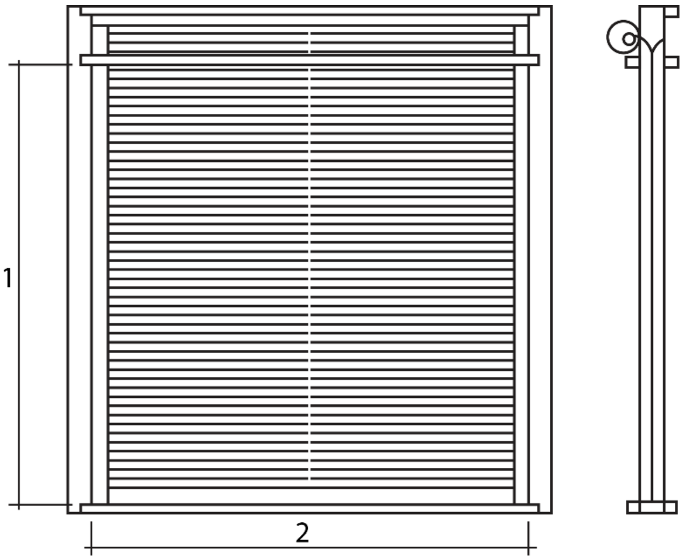


Key

$A_1 \ldots A_7$	+ 5%, - 20%
$B_1 \ldots B_7$	+ 5%, - 30%
area	± 25%

Figure C.2 — Extrapolation rules for windows

Additionally, for windows: The number of locking points may be reduced only if the distances between the locking points are not greater than on the tested size.



Key

1 Clear opening height

2 Width of specimen

Figure C.3 — Extrapolation rules for shutters and grilles

The following extrapolations for sizes other than those tested shall be permissible without a statement provided that no written limitation is made in the test report.

Permissible extrapolations without an expert statement: A reduction in width and/or height of up to 20 % is allowed. An increase in height of up to 50 % is allowed.

Greater changes in the clear opening height and width shall be supported by an expert statement.

C.2 Exchange of hardware elements

Exchange of hardware elements shall be permissible for cylinders and protective hardware on construction products in resistance classes 1 to 4 without any expert statement by the testing laboratory, if the means of installation and the length of fixing lugs of the protective hardware remain unchanged, and if evidence exists of conformity with the requirements of Tables 2A and 2B.

The exchange of lock cylinders on construction products in resistance classes 5 and 6 is permissible without an expert statement only, if the burglar resistant characteristics of the construction products are not impaired. This is the case, if the required protection of the lock cylinder by the protection shield (extended version), the cylinder with a cover or other measures have been taken into account during the test and have been recorded in the test report.

The exchange of floor and rebate seals is permissible in all classes if the burglar resistant characteristics of the construction products are not impaired.

Modifications are the responsibility of the applicant and any modification shall not reduce the tested burglar resistant characteristics of the product.

C.3 Other modifications

The following modifications require an expert statement written by the testing laboratory:

- change of infilling components, excluding infillings of glass when requirements in clause 5 are fulfilled;
- change of infilling geometry, including infillings of glass (especially for change of the infilling area and changes of the fixing elements, e.g. thicker infillings);
- change of the mode of opening provided that the security related hardware components (e.g. locks, hinges, hinge bolts, electric door opener, etc.) are retained;
- insertion of cable leads for electronic security devices and access controls;
- change of seals around infillings;
- installation of lippings and decorative elements;
- change in thickness of leaf;
- changes of profile design and profile cross section of framed constructions;
- changes to shutter profiles and guide rails;
- changes of structure and reduction of thickness of flat constructions;
- insertion of openings such as the slot for a letter box or ventilation openings;
- changes to shutter operating devices.

Annex D
(normative)

Procedure for testing and classification

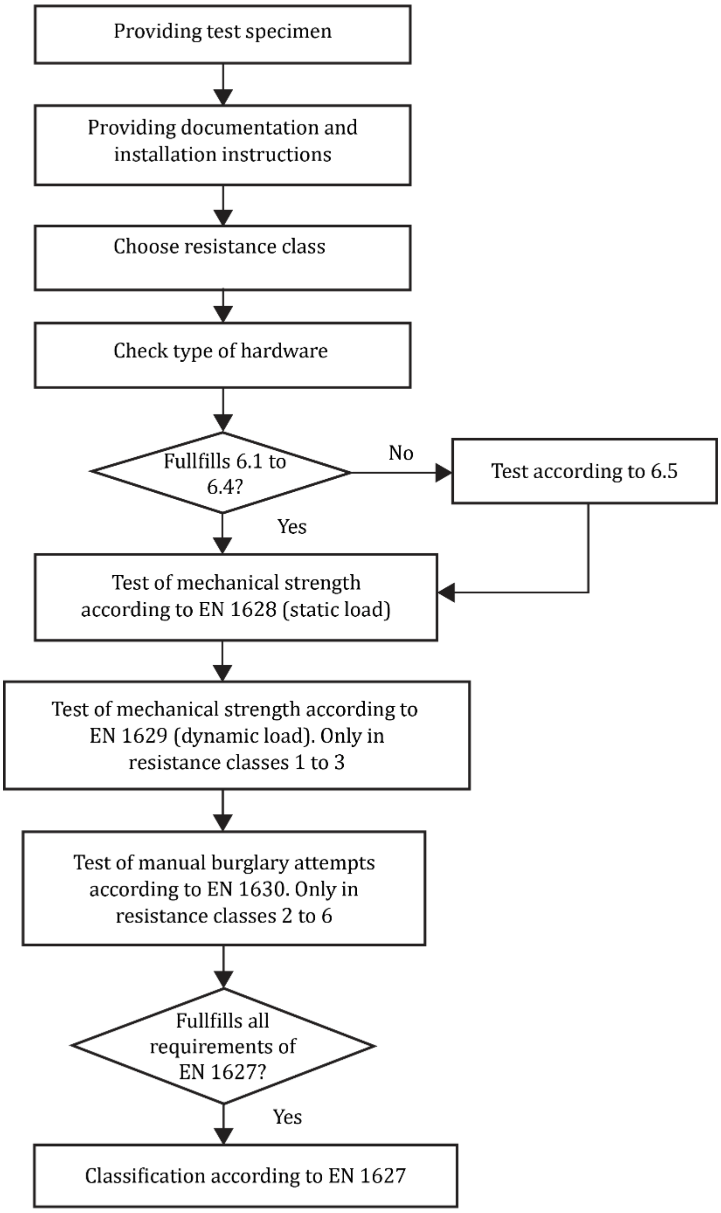

Providing test specimen
Providing documentation and installation instructions
Choose resistance class
Check type of hardware
Fullfills 6.1 to 6.4?
No
Test according to 6.5
Yes
Test of mechanical strength according to EN 1628 (static load)
Test of mechanical strength according to EN 1629 (dynamic load). Only in resistance classes 1 to 3
Test of manual burglary attempts according to EN 1630. Only in resistance classes 2 to 6
Fullfills all requirements of EN 1627?
Yes
Classification according to EN 1627

Figure D.1 — Testing and classification for burglar resisting elements

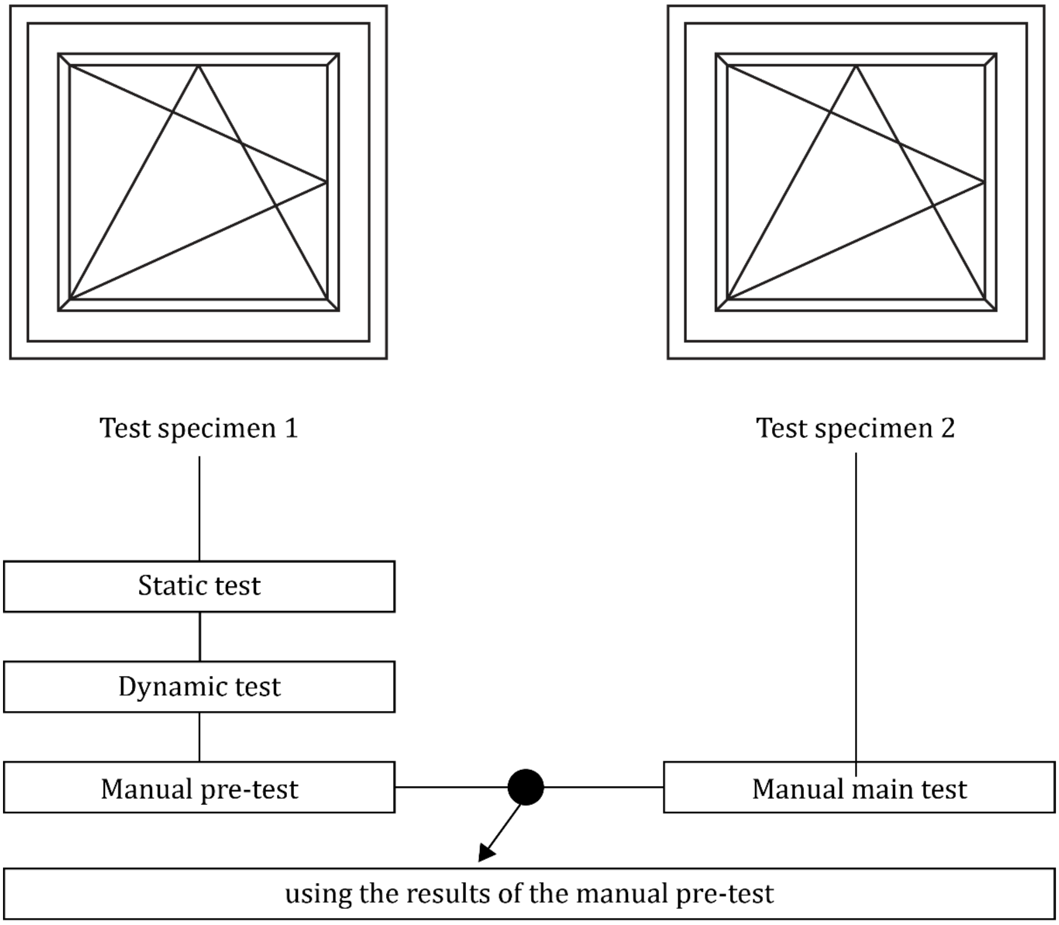


Figure D.2 — Test procedure according to EN 1627

Annex E
(normative)
Mechatronic and electronic security systems

This annex E describes and define in addition to the standard the requirements for electronic and mechatronic systems in addition to Table 2A and 2B (key related security and attack resistance).

E.1 Terms and definitions

E1.1
Electronic security system
Combination of different connected mechatronic and/or electronic security system components, credentials, cables, software, etc. to a coherent unit (assembly) to grant access

E1.2
Mechatronic/Electronic system components
Various units which are necessary to operate, control, process an electronic security system. This can be for example mechatronic cylinders, mechatronic door furniture, electronic locks, electronic striking plates, wall mounted readers, keypads

E1.3
Credential
Means for identification where the information for granting the access is stored e.g. ICC Card, Code, biometric, mobile device etc.

E1.4
Connection
The different electronic security system components can be linked through a cable, radio, data on card. This connection is used to transfer data, and for verifying the credentials

E1.5
Programming Unit
Device to create and modify credentials or to modify the master data of electronic security system components.

E1.6
False acceptance rate – FAR
Measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's FAR typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts. The FAR is normally expressed as a percentage, following the FAR definition this is the percentage of invalid inputs which are incorrectly accepted.

E1.7
FAR-1
FAR-1 (1/FAR) is the inverse of FAR

E1.8
Smart Device
portable communication device, typically smartphone, tablet or the like, on which an application is started. The device is used as a credential with a direct connection to the electronic security system component, typically using BLE – Bluetooth low energy, NFC - near field communication technology.

E1.9
ICC = Integrated Circuit Card
card, tag or device with an integrated circuit. Can be used with contact or contactless (RFID) active or passive. Examples: RFID, Smartcard

E1.10
access card
Card or tag, read only or read write, without integrated circuit, does not provide encryption. They can be used with contact or contactless. Examples: magnetic stripe, Wigand, barcode

E1.11
Browser-based application
An application that is basically no different than a specially programmed HTML page, which is recognized by the Smart Device and optimized for it.

E1.12
Native application
An application that has been programmed specifically for an operating system (such as iOS, Android, etc.) and is only executable on it.

E1.13
User code
is a user-selected character/letter sequence, which protects against the use of the application by unauthorized persons. This is another code than the unlocking code used by the smart devices. It is used as an additional security level.

E1.14
Secure Element
By linking to a hardware-integrated security module in the smart device (Secure Element), cryptographic procedures can be used to provide additional protection for sensitive data. This secure element can be realized in a SIM card, a micro-SD card or in an implemented chip in the smart device. A secure app can be used a secure element when the sensible data is encrypted in the app.

E1.15
Master
the central unit of the electronic security system or the web server for browser-based applications

E1.16
Obfuscation
practice of making something difficult to understand, for example programming code is written in a confused structure to protect intellectual property and prevent an attacker from reverse engineering a proprietary software program.

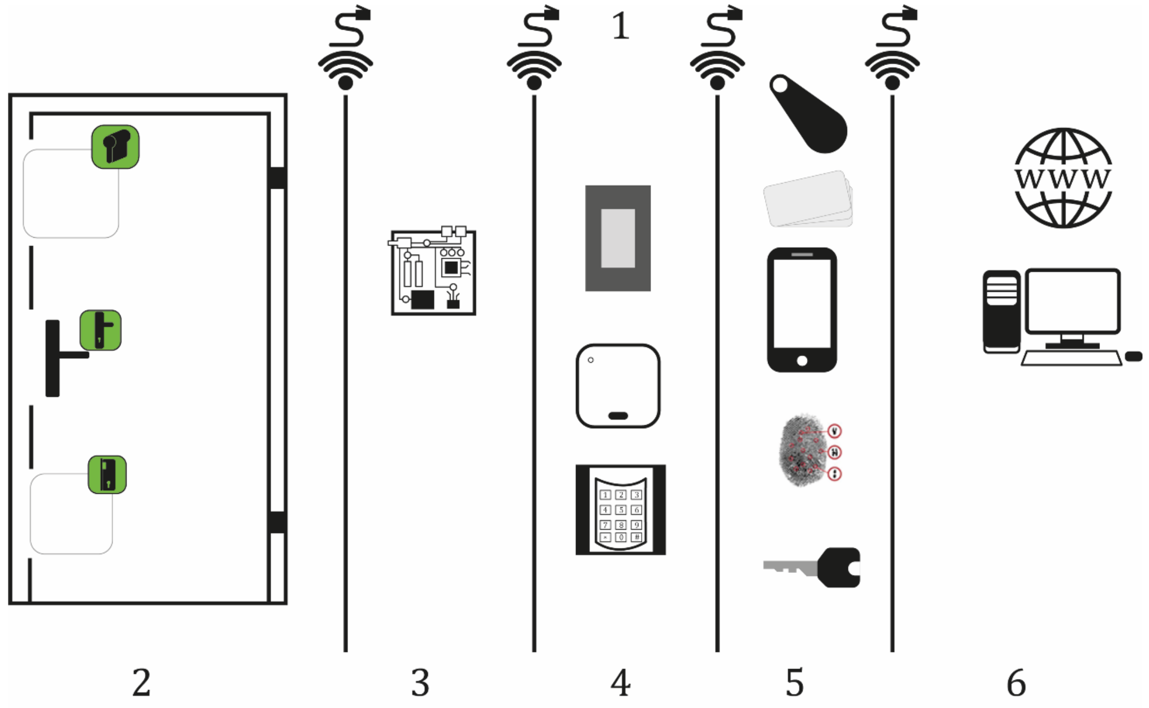
E.2 Introduction

In addition to the Table B.1 - Anticipated method and attempts to gaining entry - new forms of burglar methods and new burglar types were found without using any toolsets given in the existing standard for mechatronic and electronic security systems. The requirements and classification are in respect of the existing burglar resistance classes RC 1 N to RC 6.

The classification of the electronic security system shall be done in one of the six grades with Grade 1 being the lowest and Grade 6 the highest. This classification follows the principle of the existing classification RC 1 N to RC 5. The system security classification shall be defined for each Electronic system components for entry.

E.3 Electronic Security system

The electronic security systems can consist of different components as shown in Figure E.1. The door hardware is normally standardised by EN standards, like the mechatronic cylinder EN 15684:2012, the mechatronic door furniture by EN 16867 and the electrical operated lock and electrical striking plates by EN 14846:2008. Other components of the system like control unit, activator, input units like wall mounted readers or keypads, different credentials like mobile phone, biometric and the environment as software (local installed or cloud based must be taken in consideration in this annex. The components can be linked by different kind of connection like wired, radio based through different technologies or by the credential itself. The electronic security system can be a part of a smart home solution.



Key

1 Connection between the hardware can be cabled or wireless
2 Standardized hardware on the door
3 Other hardware on the door, not imperative: Control units and/or activators
4 Other hardware on the door, not imperative: Input units
5 Credentials
6 Environment (software, data and data storage)

Figure E.1 — Example of electronic security systems and components

NOTE Standardized hardware on the door as locking or unlocking device on the door element or door frame.

E.4 Resistance grade based on presumptive modus operandi

The various classes detailed in this standard are intended to cover the opportunist or casual burglar as well as the more experience and professional.

Different grades for components of an electronic security system can be used in the same installation as long as the functions provided by the electronic security system and credentials used fulfil at least the requirements of the highest security classification of access point(s) controlled by that system.

Table E.1 — Anticipated method and attempts to gaining entry

Resistance class	Anticipated method and attempts to gaining entry
1 low resistance	No methods known without using a tool or device to bypass an electronic security system
2 low to medium resistance	The casual or opportunistic burglar is expected to have little knowledge of electronic security systems and credentials and be restricted to a limited range of easily available tools. No knowledge of IT systems. The requirement of the physical security is to deter and delay burglars as shown in Table 2A. Assets have limited value and burglars in presence will probably give up the idea of attacking when confronted with minimum resistance
3 medium resistance	The casual or opportunistic burglar is expected to have certain knowledge of the functionality of electronic security system, credentials, IT technologies and the use of a general range of tools and portable instruments. The objective of the physical security and the electronical bypass is to deter, delay and detect unauthorized access attempts. The assets have higher value and burglars in presence will likely give up the idea of succeeding when they realize they may be detected.
4 medium to high resistance	The experienced and professional burglar is expected to be conversant with electronic security system and have a comprehensive range of tools and portable standard electronic equipment. The objective of the physical security is to deter, delay, detect and unauthorized access attempts. The assets have higher value and burglars in presence may not give up the idea of succeeding when they realize they may be detected
5 high resistance	The experienced and professional burglar is expected to have the ability or resources to plan the attack in detail and have a full range of equipment including means of substitution of components in the electronic security systems. The objective of the physical security is to deter, delay, detect and unauthorized access attempts. The assets have very high value and the burglar is going to erase all traces like tracking, etc.
6 Very high resistance	

E.5 Requirements of electronic security

In addition to the requirements and test methods in this standard, electronic security systems have to fulfil the following requirements.

E.5.1 Mechatronic security components

Mechatronic security components which are covered by the scope of one of the EN standards shall fulfil the requirements in the different standard and has be verified and tested. These components are applicable to use in their relation to Table 2A and 2B.

In addition, the following requirements shall be fulfilled in their level of assignment in their grade of security.

E.5.1.1 General

The electronic security system and its credentials for grade 1 to 6 shall be secure against code manipulations, brute force attacks, credential copying, code spying and code guessing regardless of the technique used.

The requirements for the credential related security vary with the different credential techniques used for the electronic security system. Table E.2 shows the requirements for ICC (e.g. radio frequency identification, active or passive), PIN code, magnetic stripe and biometric techniques.

If the method of obtaining access to the electronic security system does not fall into any of these categories, the credential related security grade shall be declared by analogy to the best comparable technique.

In the case where the electronic security system may be authorized by two or more of the techniques the grade for credential related security depends on whether these techniques may be used alternatively to gain access or these techniques are always used together to gain access. In the first case, the grade is the lower one of the grades of the individual techniques, in the latter case the grade is one grade higher than the highest grade of the individual technique, but not higher than the highest possible grade 4.

E.5.2 Credential related security

As the credential is the access key for all electronic system components the Table E.2 shows the minimum requirements for credentials in the burglar resistant classes 1 to 6.

Table E.2A — requirements for credential and hardware

Type of credential	**Requirements**	**Ref.**	**Grades**				
			1	**2**	**3**	**4**	**5 and 6**
ICC	Code variations/max number of auth. Codes	E.5.2.1.1	10.000	> 1.000.000	-	-	-
	Data Encryption Standard	E.5.2.1.2	No	yes	Communication encrypted with AES or 3DES; session keys,	Communication encrypted with AES or 3DES; session keys, unique key	Communication encrypted with AES or 3DES; session keys, unique key
	Encryption key length	E.5.2.1.3	No	>= 48 Bits	>=128 Bits	>=128 Bits	>=128 Bits
	Copy protection (anti-cloning)	E.5.2.1.4	No	Yes	Yes	yes	yes
Electronic PIN code	code variations/max number of auth. Codes	E.5.2.2.1	1.000	1.000	10.000	100.000	-
	Dead time after failed attempt	E.5.2.2.2	No	T = 6 h	T = 24 h	T = 240 h Scrambled key pad or unspyable input unit	-
	Protected visibility	E.5.2.2.3	No	yes	yes	yes	-
Access Cards	Code variations/max number of auth. codes	E.5.2.3.1	No	10.000	1.000.000	Not permitted	
	Copy protection	E.5.2.3.2	No	-	yes		
	Dead time after failed attempt	E.5.2.3.3	No	T = 6 h	T = 24 h		
Biometrics	False acceptance rate	E.5.2.4.1	100	1.000	10.000	-	-
	Alive detection	E.5.2.4.2	No	-	yes	-	-

[1] If applicable

[2] If technically reasonable optionally to E.5.2.5.12 and E.5.2.5.13

NOTE Grade 4 is not achievable for pure biometric system; Grade 3 and 4 are not achievable for pure PIN codes or access card

Table E.2B — requirements for credential and hardware, smart device applications

Type of credential	Requirements		Ref.	Grades				
				1	2	3	4	5 and 6
Smart devices and applications (apps) Native apps (N) and browser based apps (B)	Basic attack	firewall	E.5.2.5.1	No	Yes	Yes	Yes	Yes
		Web-Application-Firewall		No	Yes	Yes	Yes	Yes
		Virus protection	E.5.2.5.2	No	Yes	Yes	Yes	Yes
		User code	E.5.2.5.3	No	No	Yes	Yes	Yes
		Update Management	E.5.2.5.4	No	No	Yes	Yes	Yes
	Brute-Force-Attack	Time constant	E.5.2.5.5	No	No	Yes	Yes	Yes
		User code length	E.5.2.5.6	No	No	4 digits	6 digits	8 digits
		Complete blocking	E.5.2.5.7	No	No	No	No	Yes
	Reverse engineering	obfuscation	E.5.2.5.8	No	No	Standard	Standard	high
	loss of confidentiality on the transmission path	confidentiality on the transmission path	E.5.2.5.9	No	Yes	Yes	Yes	Yes
		Level of online communication	E.5.2.5.9.1	No	Basic	Basic	Medium	High
		Level of offline communication	E.5.2.5.9.2	No	Basic	Basic	Medium	High
	Keylogging	Individual keypad	E.5.2.5.10	No	No	No	Yes	No
		Scrambled individual keypad	E.5.2.5.11	No	No	No	No	Yes
	Loss of confidentiality on the smart device	Encrypted stored in the device	E.5.2.5.12	No	No	Yes	Yes	Yes
		protection of integrity	E.5.2.5.13	No	No	No	Yes 1)	Yes 1)
		Secure element	E.5.2.5.14	No	No	No	Yes 2)	Yes 2)
	Root-exploit	Prevention and Detection	E.5.2.5.15	No	No	Yes	Yes	Yes
Credential data sent through WLAN	Encryption		E.5.2.5.16	No	Yes	Yes	Yes	-
	Firewall		E. 5.2.5.17	No	Standard	Standard	Higher	Higher
	Update Management		E. 5.2.5.18	No	Yes	Yes	Yes	Yes

E.5.2.1 Requirements for ICC

E.5.2.1.1 Effective code variations

The effective code variations are all code variations possible by design divided by the maximum possible number of authorized codes on one hardware item of the electronic security system. It shall be at least the number according to Table E.2.

NOTE In the case where the unique ID of the ICC is used, this corresponds to the possible variations of the unique ID divided by the maximum possible number of authorized credentials.

E.5.2.1.2 Data Encryption Standard

In grade 2 the data on the ICC or the communication between ICC and hardware of the electronic security system shall be encrypted by any encryption algorithm. In grade 3 or higher the communication between the ICC and the hardware of the electronic security system shall be encrypted by the AES encryption method according to ISO/IEC 18033-3:2010

E.5.2.1.3 Encryption key length

The length of the encryption key in grade 2 shall be at least 48 Bits long.

In grade 3 or higher the encryption key shall be at least 128 Bits long. For each communication attempt (session) a new session key shall be created and used for the communication. Session keys and encryption keys shall never be broadcasted (challenge response technique). The encryption key shall be unique for each installation of electronic security system or, alternatively, shall be user configurable.

E.5.2.1.4 Copy protection (Anti-cloning)

In grade 2 or higher the credential shall be copy protected. It shall not be possible to copy an authorized credential using standard third-party equipment.

NOTE Standard third-party equipment are tools or devices which can be free purchased from every person on the market

E.5.2.2 Requirements for PIN Code

E.5.2.2.1 Effective code variations

The effective code variations are the possible code variations divided by the maximum number of possible authorized codes on one component of the electronic security system. It shall be at least the number according to Table E.2.

NOTE In the case of a 4-digit PIN code and a maximum number of 10 users, the effective code variations are 1000.

E.5.2.2.2 Dead time failed attempts

The electronic security system shall have the security feature that makes it impossible to try out all or a large portion of all possible codes within a reasonable time.

The dead time “T” results in the maximum number of codes of the unit divided by the read speed (the number of possible codes per hour), divided by the number of possible users and divided by 2.

E.5.2.2.3 Protected visibility

For components of electronic security systems grade 2, 3 and 4 the included angle over which code information may optically be observed shall be not more than 30° about the centre-line.

E.5.2.3 Requirements for Access Cards

E.5.2.3.1 Effective code variations

The effective code variations are all code variations possible by design divided by the maximum possible number of authorized codes on one components of the electronic security system. It shall be at least the number according to Table E.2

E.5.2.3.2 Copy protection

In grade 3 the credential shall be copy protected. It shall not be possible to copy an authorized credential using standard third-party equipment and standard magnetic card blanks.

NOTE Standard third-party equipment are tools or devices which can be free purchased from every person on the market.

E.5.2.3.3 Dead time failed attempts

The electronic security system shall have the security feature that makes it impossible to try out all or a large portion of all possible codes within a reasonable time.

The dead time "T" results in the maximum number of codes of the unit divided by the read speed (the number of possible codes per hour), divided by the number of possible users and divided by 2.

E.5.2.4 Requirement for Biometrics

E.5.2.4.1 False acceptance rate (FAR−1)

The analogy of effective code variations in biometric systems is the inverse of the false acceptance rate (FAR-1) divided by the maximum possible number of authorized templates on one components of the electronic security system. It shall be at least the number according to Table E.2.

E.5.2.4.2 Alive detection

In grades 3 the system hardware shall be able to detect whether the presented credential (fingerprint, hand vein image, iris image) comes from an alive human to prevent that artificially produced images may be successfully presented to the system hardware.

E.5.2.5 Requirement for Smart Devices

E.5.2.5.1 Firewall

The user of the application shall be informed in the documentation that, if technically possible, a firewall shall be used on the smart device and the master for secure operation. Furthermore, the operator is advised that the software of the firewall must be automatically and regularly updated by a suitable process.

If the master is reachable through a public network, the following requirements shall be obeyed: The user of the application must be informed in the documentation that, if technically possible, an application firewall must be used on the master for secure operation. Furthermore, the operator is advised that the software of the application firewall must be automatically and regularly updated by a suitable process.

E.5.2.5.2 Protection against Malware

The user of the application shall be informed in the documentation that the use of a suitable protection program against malware on the Smart Device, the Master and any essential server is required for safe operation. Furthermore, a regular check for malware and the automatic update of the signature database shall be recommended.

The user shall be informed that he has to ensure that in case of infection by malware programs, the virus detection of protection programs is documented and corrected by appropriate measures. If there is any suspicion that personal data has reached third parties, the operator must report this immediately in accordance with the legal requirements.

E.5.2.5.3 User Code

The application may only be started by authorized persons. The authorization must be verified by entering a user code or another equivalent identification (e.g. fingerprint). The user code is not the same as the lock code of the smart device.

The user should be advised of the importance of choosing a secure user and lock code in the documentation.

E.5.2.5.4 Update Management

The user of the application shall be informed in the documentation that it is necessary for safe operation always to use the current software and firmware version of the programs required for the safe and proper operation of the application on the smart device to the master and other essential server. This includes also the application itself and the respective operating systems of the existing hardware components.

There must be a software-based update management, which ensures that the application is always up to date. The application must check for updates each time it is started by the user (at least once a day for multiple starts) and inform the user as soon as an update is available (notification). The user then has a certain grace period, which is calculated from the time the knowledge is acquired by the application through the availability of an update and results in Table E.3 update management in order to carry out the update of the application. If this time is exceeded, the application may no longer be used (forced lock). If both Master and Smart Device are operating without an Internet connection, the forced lock request is not relevant.

NOTE The update management can also be realised by third party program e.g. App Store ®, Google play ® etc.

Table E.3 — requirements for update management

Grade	Notification	Forced app lock
1	-	-
2	-	-
3	immediate	-
4	Immediate	After 30 days
5 and 6	Immediate	After 7 days

E.5.2.5.5 Time constant

If a wrong user code has been entered, a time delay shall ensure that the next trial of entering is possible only after a certain time has elapsed. The time t is calculated depending on error trials n after t = 2n seconds.

E.5.2.5.6 User code length

The user code length shall have at minimum 4 digits in grade 3, 6 digits in grade 4 and 8 digits in grade 5 and 6. The user should be required automatically in regular intervals to change his user code.

E.5.2.5.7 Complete blocking

If five wrong user codes are entered consecutively, the starting of the application is to be blocked completely. The manufacturer shall foresee a suitable procedure by which a complete blocking may annihilated.

For annihilation of the complete blocking, a PUK may be polled for example. If a wrong PUK has been entered three times consecutively; all information concerning this application shall be deleted. The user of the application must be informed in the documentation of the complete deletion of the data.

E.5.2.5.8 Obfuscation

For native applications in grade 3 and 4 the source code shall be protected against reverse engineering using standard obfuscation mechanisms offered by the development system.

In grade 5 and 6 the native applications shall be protected against reverse engineering using standard by superior graded obfuscation mechanisms. The obfuscations procedure which is offered by the development system is not to be used exclusively.

E.5.2.5.9 Loss of confidentiality on the transmission path

The confidentiality and integrity of data transmitted over data networks shall be ensured. This shall be done by suitable methods and algorithms (e.g., https connections with current encryption techniques and use of checksum functions).

Https connections shall be made with at least a SHA-256 bit certificate signing algorithm. In order not to endanger the https connection, protocols with a version higher than TLS 1.0 shall be used. Outdated protocols like TLS 1.0 shall not be used.

The manufacturer shall list the procedures and algorithms used in the manufacturer's documentation. Certificates must be checked for validity. Only valid certificates shall be used.

For grade 4 or higher cloud based electronic security systems operated by the manufacturer or another third party, the operating organisation shall be certified according to ISO/IEC 27001 Information technology – Security techniques.

E.5.2.5.9.1 Online communication of the application

Is the application communicating through Https the certificate levels shall be used according to Table E.4. The key length symmetric and/or asymmetric shall be used.

Table E.4 — requirements for online communication of the application

Level	Certification class	Symmetric key length	Asymmetric key length
Basic	Domain Validation	≥ 1 024Bit	≥ 128 Bit
Medium	Organisational Validation	≥ 2 048Bit	≥ 256 Bit
High	Extended Validation	≥ 4 096 Bit	≥ 256 Bit

NOTE If the application defines the master and possibly other required servers and these cannot be changed and accessed through generally available browsers and furthermore the certificate of the trusted Certification Authority is integrated by the manufacturer and cannot be changed, self-issued certificates may also be used that are derived from this trusted Certification Authority. The requirement for key length and the algorithms used remain unaffected.

E.5.2.5.9.2 Offline communication of the application

If the master cannot be reached via a public network, the following levels in Table E.5 shall be used.

Table E.5 — requirements for offline communication of the application

Level	Certification class	Symmetric key length	Asymmetric key length
Basic	Signed by the certificate owner [a]	≥ 1 024Bit	≥ 128 Bit
Medium	Signed by the certificate owner [a]	≥ 2 048Bit	≥ 256 Bit
High	Signed by the certificate owner [a]	≥ 4 096 Bit	≥ 256 Bit
[a] Certificates signed by the manufacturer or signed by a process specified by the manufacturer must be authenticated by a suitable procedure during connection dialog. The certificate must arrive in a secure way in the client.			

E.5.2.5.10 Individual keypad

In order to ensure protection against spying out keypad inputs (key logging), the keypad as commonly offered for the model kits for the application development shall not be used. A keypad function shall be implemented by which the information of the keypad inputs is generated and processed only within the application. Instead, an own keypad shall be programmed so that inputs are not fed via interface from the operating system into the application.

E.5.2.5.11 Scrambled individual keypad

For a sufficient protection against spying out of keypad inputs (key logging) also for applications in grade 5 and 6, an individual keypad E.5.2.5.9 shall be used, which additionally scramble the alignment of the input buttons for each new input sequence (scrambled function).

E.5.2.5.12 Loss of confidentiality on the smart device – encrypted storage

The confidentiality of the data stored on the smart device for the relevant application shall be ensured. The manufacturer of the application shall ensure this by using specially protected memory areas or secure encryption of the data (e.g. AES).

NOTE The storage of data on the smart device should be based on the minimum principle.

The manufacturer must document the memory areas used and the encryption method used in the manufacturer documentation.

E.5.2.5.13 Loss of confidentiality on the smart device - protection of integrity

In grade 4 or hither the integrity of the application data stored or transferred on the smart device shall be ensured. This shall be done by using a suitable and current checksum function of the data. Non-integer data may not be processed by the application and must be discarded.

E.5.2.5.14 Loss of confidentiality on the smart device – secure element

The application data, if technically possible, shall be stored in a secure element. The manufacturer must inform the operator of the application in the operator documentation that the use of a secure element in the smart device offers greater security and recommends the use of a suitable smart device.

E.5.2.5.15 Root-Exploit – Prevention and Detection

The user of the application shall be informed in the documentation that, if technically possible, appropriate measures shall be taken to protect the smart device from root exploit and that it shall inform the manufacturer immediately upon discovery of an exploit whether a fixing software or firmware update is available.

The application shall reliably detect when the operator executes the application with administrative authorizations or obtains them during use. In this case, the application must be terminated immediately and secured against a restart.

E.5.2.5.16 Credential data sent through WLAN – Encryption

If the one of the hardware components of the electronic security system can be linked with WLAN the WLAN shall be encrypted. The level of encryption shall be WPA2 or higher. An End-to-End Encryption (E2EE) shall be the normal transmission path of data in the electronic security system.

The password for the WLAN shall have more than 48 characters composed of small letters, capitals, digits and special characters.

Also, the administrator password shall have more than 48 characters composed of small letters, capitals, digits and special characters.

The password shall be change in periodic intervals.

E.5.2.5.17 Credential data sent through WLAN – Firewall

The user of the electronic security system shall be informed in the documentation that a firewall shall be used for secure operation. The user is advised that the software of the firewall shall be automatically and regularly updated by a suitable process.

For grade 2 and 3 a standard commune used firewall is sufficient. For grade 4 or higher an own WLAN network with a higher level of firewall shall be used.

E.5.2.5.18 Credential data sent through WLAN – Update Management

The user of the electronic security system shall be informed in the documentation that it is necessary for safe operation always to use the current software and firmware version of the programs required for the safe and proper operation of the system. This includes the software itself and the respective operating systems of the existing hardware components.

There shall be a software-based update management, which ensures that the application is always up to date. The application shall check for updates in a periodic interval and inform the user when hardware components are updated through the WLAN network.

If a firmware update of hardware components is technically not possible over the WLAN network other update mechanism shall be used.

E.5.3 Cabling

If electronic security systems are linked with a cable the cabling shall fulfil the requirements E.5.3.1.

E.5.3.1 Cabling and power failure

All lockable electronic security system components shall accomplish the operation in working current. Especially mechatronic lockcases and mechatronic striking plates and cylinders or other components shall be in a lockable mode in current-free status.

Power failure or a breakdown shall not change the component to an accessible position from the attack side. In grade 5 and 6 cables shall have monitored connection between the components of an electronic security system to show manipulation.

NOTE It is recommended to use connecting cables without colour coding. All lines shall be in the same colour.

The connecting cables, strip connectors and the control unit (which activated the access permission) shall be installed on the non-attack side; see Figure E.2A and E.2B.

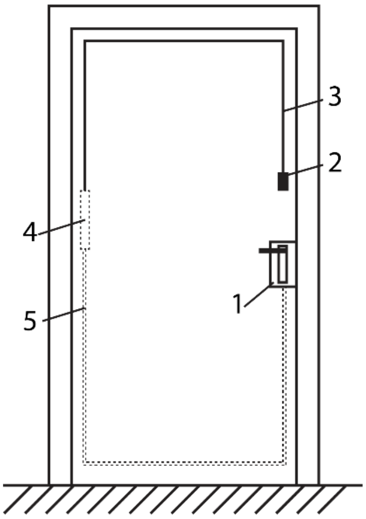


Figure E.2A - Door with control unit in the door leaf

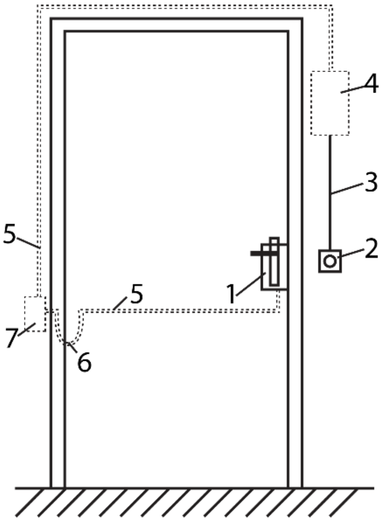


Figure E.2B - Door with separated control unit

Key

1 Mechatronic operated lock
2 input unit for credential
3 cable with encrypted signal to the control unit
4 control unit
5 cable to the lockable device, RC 5 to RC 6 monitored connection
6 cable access point for cables
7 junction box

NOTE The components no 4 - 7 shall be installed on the non-attack side

These components shall not be reachable during the manual attack according to prEN 1630:2018 in the relevant resistance class so that a manipulation e.g. stripping wires and fixing of a connector shall not be possible.

E.5.4 Hardware

The hardware components shall have a revision proved protocol for more than 1.000 authorized access attempts in grade 2 and 3 and more than 1.000 in total for authorized and unauthorized access attempts.

E.6 Test methods - procedures

E.6.1General

This annex doesn't require any specific tests for the electronical security system. Tests shall be done by the manufacturer or a third party to show particular test results and bring the manufacturer in the position to issue a specific manufacturer's declaration.

It is up to the tester together with the applicant to decide which requirements and test methods that are relevant to the technical design.

As an electronic security system can consist of many different credentials and hardware components the manufacturer shall clearly state for which grade the electronic security system is suited.

E.6.1.1 Credential test ICC

The ICC credentials have to be verified by a written manufacturer's declaration and/or test reports or technical specifications from third parties.

E.6.1.1.1 ICC - Code variations/maximum number of authentically codes

The code variations and maximum number of authentically codes shall conform to E.5.2.1.1.

The manufacturer has to present documents or mathematic formulas which conforms the values in Table E.2.

E.6.1.1.2 ICC - Data Encryption Standard

The data encryption standard shall conform to E.5.2.1.2.

Compliance is checked by a manufacturer's declaration which encryption methods are used.

E.6.1.1.3 ICC - encryption key length

The encryption key length shall conform to E.5.2.1.3.

Compliance is checked by a manufacturer's declaration or other relevant documents confirming the values in Table E.2

E.6.1.1.4 ICC - copy protection

The encryption key length shall conform to E.5.2.1.4.

Compliance is checked by a manufacturer's declaration.

E.6.1.2 Credential test pin code

Pin codes are also a kind of credential. Conformity is check in the clauses E.5.2.2.1 to E.5.2.2.2.

E.6.1.2.1 Pin code - Code variations/maximum number of authentically codes

The code variations and maximum number of authentically codes shall conform to E.5.2.2.1.

The manufacturer has to present documents or mathematic formulas which conforms the values in Table E.2.

E.6.1.2.2 Pin code - dead time after failed attempt

The dead time after failed attempt shall conform to E.5.2.2.2.

Compliance is checked by a manufacturer's declaration.

Scrambled keypads should be checked for alternative scrambling by the manufacturer.

E.6.1.2.3 Pin code – Protected visibility

The protected visibility shall conform to E.5.2.2.3.

Compliance is checked by evaluation of design.

E.6.1.3 Credential test – Access cards

Access cards e.g. cards with magnetic strip shall comply with clauses E.5.2.3.1 to E.5.2.3.2.

Access cards are not allowed to use in grade 4, 5 and 6.

E.6.1.3.1 Access cards – Code variations/maximum number of authentically codes

The code variations and maximum number of authentically codes shall conform to E.5.2.3.1.

The manufacturer has to present documents or mathematic formulas which conforms the values in Table E.2.

E.6.1.3.2 Access cards - copy protection

The encryption key length shall conform to E.5.2.3.2.

Compliance is checked by a manufacturer's declaration.

E.6.1.3.3 Access cards - dead time after failed attempt

The dead time after failed attempt shall conform to E.5.2.3.3.

Compliance is checked by a manufacturer's declaration.

E.6.1.4 Credential test – biometrics

Biometric based credentials shall comply with clauses E.5.2.4.1 to E.5.2.4.2.

NOTE Test for biometric are shown in various ISO/IEC standards. The requirements in this annex are the mail requirements for burglar resistance.

E.6.1.4.1 Biometrics – False acceptance rate

The false acceptance rate shall comply with E.5.2.4.1. The calculation to check the compliance has to be provided by the manufacturer.

Compliance is checked by a manufacturer's declaration.

E.6.1.4.2 Biometrics – Alive detection

The alive detection shall conform to E.5.2.4.2. Compliance is checked by a manufacturer's declaration and possible random test by the tester.

E.6.1.5 Credential test – Smart Device

Smart Devices shall comply with E.5.2.5.1 to E.5.2.5.15.

E.6.1.5.1 Smart Device – Firewall

It is checked according to E.5.2.5.1 whether the manufacturer in the operator documentation points out that for a safe operation of the application a firewall must be operated on the Smart Device or on the master and recommends appropriate measures for the automatic and regular updating of the firewall software.

Compliance is checked if the operator documentation contains a corresponding note on the operation of a firewall on the smart device or on the master and measures for automatic and regular updating.

It is checked whether the master can be reached through a public network. If this is the

case, it is checked whether the manufacturer indicates in the operator documentation that an application firewall must be operated on the master for safe operation of the application and recommends appropriate measures for automatic and regular updating of the application firewall software.

Compliance is checked if the operator documentation contains a corresponding note on the operation of the application firewall on the master and automatic updating measures.

E.6.1.5.2 Smart Device – Virus protection

It is checked whether the manufacturer indicates in the operator documentation according to E.5.2.5.2 that for a safe operation of the application a current protection program must be operated against malware on the smart device, the master and other servers and a regular check and automatically update of the signature database is recommended.

Compliance is checked if the operator documentation contains a corresponding note on the use of a protection program against malware on the smart device, the master and other servers and recommends a regular check and automatic update of the signature database.

It is checked whether the manufacturer indicates in the operator documentation according to E.5.2.5.2 that for a safe operation of the application, the operator must ensure that in case of an infection by malware the virus detection is documented by the protection program and by appropriate action is taken.

Compliance is checked, if the operator documentation contains a corresponding notification that the operator must ensure that in case of an infection by malware program the virus detection is documented by the protection program and remedied by suitable measures.

E.6.1.5.3 Smart Device – User code

It is checked whether the starting of the application requires the input of a user code according to E.5.2.5.3 or the authentication of another, equivalent identification feature (for example fingerprint).

Compliance is checked if a corresponding identification feature is requested when starting the application.

It is checked whether the operating instructions for the operator and/or user of the application contain an indication of the importance of selecting a secure user and lock code.

Compliance is checked if the instruction manual contains an appropriate note about the importance of choosing a safe user and lock code.

E.6.1.5.4 Smart Device – Update Management

It is checked whether the manufacturer indicates in the operator documentation that for safe operation the current software version of all programs required for the proper operation of the application must be used on the smart device, the master and any required server. The application itself and the respective operating systems of the mentioned hardware components must also be mentioned explicitly.

Compliance is checked if the operator documentation contains a corresponding note on the use of the current software version of all the software required for the secure operation of the application on the smart device, the master and possibly required server, as well as an indication of the current operating system versions of the mentioned hardware components and the application itself.

Compliance is checked whether the application searches for updates every time it is started (at least once a day) and informs the user as soon as an update is available.

Compliance is checked if a corresponding note informs the operator in the event of an update or if this functionality can be reconstructed on the basis of the source code.

It is checked whether the application can no longer be started, which has been exceeded since the knowledge of the application about the existence of an update as defined in E.5.2.5.4 Table E.3 waiting time.

Compliance is checked if the application cannot be started after the defined waiting time or if this functionality can be reconstructed using the source code.

E.6.1.5.5 Smart Device – Time constant

It is checked whether the next entry attempt is delayed by a time constant according to E.5.2.5.5 when entering an incorrect user code.

Compliance is checked if the next input attempt of the user code is delayed by the time (t) according to E.5.2.5.5 after previous error input.

E.6.1.5.6 Smart Device – User code length

It is checked whether the user manual for the user of the application contains an indication of the importance of selecting a secure user and lock code.

Compliance is checked if the operating instructions contain a note on the importance of selecting a safe user and lock code according to Table E.2.

In the operating instructions, the manufacturer must inform the operator or user about special password assignment of server access.

E.6.1.5.7 Smart Device – Complete blocking

It is checked whether after ten times incorrect entry of the user code according to E.5.2.5.7 the starting of the application is completely blocked.

Compliance is checked according to E.5.2.5.7 if, after the user code has been misprinted ten times, the starting of the application is blocked, or if this complete blocking is documented in the operator information.

It is checked whether the full lock can be deactivated by entering a PUK.

Compliance according to E.5.2.5.7 is checked, when after entering the correct PUK, the full blocking is deactivated, or if this is documented in the operator information.

It is checked whether all application-related information is deleted after three incorrect entries of the PUK.

Compliance according to E.5.2.5.7 is checked if the operator information contains a corresponding indication of complete deletion of the data after three incorrect entries of the PUK.

E.6.1.5.8 Smart Device – Obfuscation

It is checked whether the source code of the application is fundamentally obfuscated.

Compliance of E.5.2.5.8 is checked if the manufacturer indicates and confirms the type of obfuscation in its manufacturer's declaration. For Grade 3 and 4 a standard obfuscation is sufficient, for Grade 5 and 6 a higher obfuscation must be implemented and confirmed by the manufacturer of the application.

E.6.1.5.9 Smart Device – confidentiality on the transmission path

It will be checked whether the manufacturer uses suitable procedures for securing data when transmitting through data networks. (e.g. https: //) and meets the requirements in E.5.2.5.9 and that only valid certificates are used and accepted when transmitting data.

Compliance is checked if the manufacturer declaration lists the procedures and algorithms used to save and back up the data in the manufacturer's documentation and only confirms the use of valid certificates when transmitting data in the manufacturer's declaration. If necessary, this can also be confirmed by using several invalid certificates.

E.6.1.5.9.1 Smart Device –Level of online communication

It is checked whether the communication between Smart Device, Master and possibly further server is encrypted using a key length corresponding to Table E.4.

Compliance is checked if the manufacturer has documented the key lengths used in the manufacturer's declaration.

E.6.1.5.9.2 Smart Device –Level of offline communication

It is checked whether the communication between Smart Device, Master and possibly further server is encrypted using the key length of the corresponding grades according to Table E.5.

Compliance is checked if the manufacturer has documented the key length used in the manufacturer's declaration.

E.6.1.5.10 Smart Device –Individual keypad

It is checked whether in the application according to E.5.2.5.10 if the lock code on the smart device is missing, a manufacturer-specific individual keypad is effectively implemented.

Compliance is checked if based on the source code, it can be seen that a proprietary keypad is effectively implemented and adequately described in the user manual.

E.6.1.5.11 Smart Device –Scrambled individual keypad

It is checked whether a proprietary individual keyboard is effectively implemented in the application according to E.5.2.5.11 if the lock code on the smart device is missing. In addition, the arrangement of the input buttons should be scrambled with each call (scrambled function).

Compliance is checked if it is shown in the source code that a proprietary keypad function is effectively implemented, and the keypad has a scramble function.

E.6.1.5.12 Smart Device –Encrypted stored in the device

It is checked whether data is stored in specially secured storage areas or encrypted on the smart device and whether the encryption method used is listed in the manufacturer's documentation.

Compliance is checked if the manufacturer's documentation describes in detail the encryption method and the location of stored and secured data.

E.6.1.5.13 Smart Device – protection of integrity

It is checked whether checksums of the transmitted data are generated and checked by the application.

Compliance is checked if a change of several checksums of data to be processed is rejected by the application. The manufacturer must document this in writing in a separate test scenario.

E.6.1.5.14 Smart Device – Secure element

It is checked whether the secure element according to E.5.2.5.14 is used and the data is stored on the secure element and whether the manufacturer informs the user in the operator documentation about additional protection by a secure element and recommends the use of an appropriate smart device.

Compliance is checked if, based on the source code or in the manufacturer's declaration, the logic of the file system of the smart device can be reconstructed, that the data of the application is stored in a secure element and if there is also a corresponding note in the operator documentation.

E.6.1.5.15 Smart Device – Prevention and Detection

It is checked whether, according to E.5.2.5.15 the operator documentation contains a note that the operator must ensure that safe measures are taken to protect against exploits and that, as soon as the corresponding exploits become known, the user must be immediately informed if a corrective software update is available. If there is an update, he will be forced to install it.

Compliance is checked if a corresponding note is available in the operator and user documentation.

It is checked whether the application according to E.5.2.5.15 reliably detects that an operator has obtained administrative authorizations on the smart device. If this is the case, the further execution of the application must be stopped immediately.

Compliance is checked if execution of the application with administrative rights on the smart device terminates the application immediately and saves it against a restart.

E.6.1.6 WLAN – Encryption

It is checked whether if the user documentation according to E.5.2.5.16 refers to the protection of the WLAN in detail and the user documentation assumes the encryption of the network for safe operation.

Compliance is checked if the requirements are explicitly presented in the user documentation.

E.6.1.7 WLAN – Firewall

It is checked whether the manufacturer according to E.5.2.5.17 in the operator documentation points out that for a safe operation of the electronic security system linked through WLAN a firewall must be operated on the master and recommends appropriate measures for the automatic and regular updating of the firewall software.

Compliance is checked if the operator documentation contains a relevant note on the operation of a firewall on the master and measures for automatic and regular updating.

It is checked whether the master can be reached through a public network. If this is the case, it is checked whether the manufacturer informs in the operator documentation that measures are recommended for a safe operation of the electronic security system and that regular updating of the firewall software is essential.

Compliance is checked if the operator documentation contains a corresponding note on the operation of the firewall and that a periodic update of the firewall is essential.

E.6.1.8 WLAN – Update Management

It is checked whether the manufacturer according to E.5.2.5.18 the operator documentation has to point out that for safe operation only the current firmware and software version installed on all hardware components of the Electronic Security System has to be used. The application itself and the respective operating systems of the hardware components must also be mentioned explicitly.

Compliance is checked if the operator documentation contains a corresponding note on the use of the current firmware and software version of all hardware components required for the safe operation of the application, as well as an indication of the use of the current operating system versions of the hardware components and the application itself.

E.6.1.8.1 Cabling and power failure

The manufacturer must indicate in his installation instructions in accordance with E.5.3.1 of wired electronic security systems how secure cabling must be provided. The connection diagrams and wiring types are to be described in the manufacturer's documentation.

Compliance is checked if the manufacturer's documentation and the installation instructions provide a corresponding note.

E.6.1.8.2 Hardware

The hardware components according to E.5.3.2 shall have a revision proved protocol for more than 1.000 access attempts. These access attempts are stored normally in the electronic security system hardware and can be read out.

Compliance is checked if the manufacturer's documentation and the operator documentation indicate how and in what way the access attempts can be read out.

Bibliography

[1] EN 13241, *Industrial, commercial, garage doors and gates — Product standard, performance characteristics*

[2] EN ISO 6508-1, *Metallic materials — Rockwell hardness test — Part 1: Test method (ISO 6508-1:2016)*