Thief Resistant Electronic Door Locking Devices

DHF TS 621:2018

Including corrigendum 1

Technical guide: Thief Resistant Electronic Door Locking Devices TS 621:2018

Contents

List of figures

List of tables

This Technical Specification DHF TS 621:2018 and includes corrigendum 1, replaces DHF TS 621:2011 Thief Resistant Electromechanically Operated Lock Assemblies, which is now withdrawn.

Introduction

This Technical Specification was prepared by the Door & Hardware Federation (**dhf**) in response to a market requirement for third party certification of residential thief resistant electronic door locking devices. It is hoped that it may in due course be replaced by a British standard (BS) or a publicly available specification (PAS); if and when this occurs, this specification will be withdrawn.

Although it is possible for lock manufacturers to test their own products to this specification, users are recommended to consider the benefits of third party certification against this specification

This specification incorporates requirements from BS EN 14846:2008, BS EN 1303:2015, BS 3621:2017 amendment 1, and PAS 3621:2011

Amongst the requirements of BS 3621:2017 which are referenced in this specification is an assessment for general vulnerability. To this is added a requirement for an assessment of a locks electromechanical vulnerability, specified herein in Annex A. These assessments are essential to simulate a criminal attack as accurately as possible.

Also referenced in this specification is the BS 3621:2017 requirement for the qualifications and experience of personnel undertaking these assessments.

Suitability of the application

Doors and frames to which electronic door locking devices conforming to this Technical Specification are attached should be of adequate strength and should be designed to resist criminal attack.

1: Scope

This Technical Specification describes performance requirements and test methods for the following electronic door locking devices (including the lock interface, credentials, striking plate, fixing screws, fitting instructions, and where appropriate, cylinder and protective furniture):

- Electronic escutcheon (an escutcheon that drives a mechanical single or multipoint lock)
- Electronic multipoint lock (a multipoint lock that contains the electronic components required for it to operate)
- Electronic single point lock (a single point lock that contains the electronic components required for it to operate)
- Electronic cylinder (an electronic cylinder that drives a mechanical lock case)

This specification covers electronic door locking devices which are used in doors, window doors and entrance doors in residential and similar buildings.

Because functional differences such as key egress, keyless egress and dual mode operation can be determined electromechanically, all variants are covered in this one document.

Please see figure 1 for a pictorial representation of the components covered within the scope of this document.

2: Referenced documents

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

BS EN 1303:2015
Building hardware - Cylinders for locks – Requirements and test methods

BS EN 12209:2016
Building hardware – Locks and latches - Mechanically operated locks, latches and locking plates – Requirements and test methods

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

PAS 24:2016
Enhanced security performance requirements for door assemblies – Single and double leaf, hinged external door assemblies to dwellings

PAS 3621:2017
Thief resistant multipoint lock assemblies – key egress

prEN 16867:2016
Building hardware – Mechatronic door furniture

BS EN 15684:2012
Building Hardware – Mechatronic cylinders

3: Definitions

For the purpose of this Technical Specification, the terms and definitions given in BS EN 14846, BS EN 12209, BS EN 1303, PAS 24, PAS 3621, prEN 16867 and the following apply:

3.1 Lock

Mechanism that secures the door in the closed position (see Fig.1)

3.2 Lock interface

Unit that communicates with the lock to change the lock status (see Fig.1)

3.3 Credential

Element or unit that communicates with the lock interface (see Fig.1)

3.4 Electronic escutcheon

Electronic door furniture connected to the lock mechanism containing a lever handle

3.5 Active devices

Electronic equipment which introduces net energy in order to communicate with other equipment (e.g. mobile phone or router)

3.6 PAN (Personal Area Network)

An interconnection of information technology devices typically operating within a residential property

3.7 Communication protocol

A system of rules that allow two or more active devices to transmit information (usually via radio)

4: Lock and lock interface

4.1 General

Lock and lock interface shall comply with BS EN 14846 or pr EN 16867 to the following minimum classification:

For Electronic Single Point and Electronic Multipoint Locks

BS EN 14846

1	M (see 4.2)	4	0	-	H	7 or 5 (see 4.3)	1	3

For Electronic Escutcheons

prEN 16867

1	6	-	0	0	4	A	0	0

Sections 4.1.5 (product information requirements) and section 8 (marking) of pr EN 16867 should be ignored as these are covered within Section 8 of this document.

The environmental resistance should only be carried out on components which are to be mounted on the external face of the door.

Section 4.2.5 of prEN 16867 should be disregarded.

For Electronic Cylinders

BS EN 15684:2012

1	6	-	0	3	E	F	2	2

4.2 Durability (2nd digit in BS EN 14846 classification) (Electronic Single Point and Multipoint Locks Only)

4.2.1 Non-standard test regimes

Where the durability test regime is not fully defined, a suitable test regime shall be devised in line with the principles of BS EN 12209 or PAS 3621, as appropriate

4.2.2 Locks designed to be used with a cylinder

Testing shall be performed on a lock assembly that includes the cylinder with which it is intended to be used

4.3 Security and drill resistance (7th digit in BS EN 14846) classification

4.3.1 Electronic Single point locks

BS EN 12209:2016 security grade 7 shall apply

4.3.2 **Electronic Multipoint locks**

PAS 3621:2011 requirements (security grade 5) shall apply

4.3.3 Electronic Escutcheon & Electronic Cylinder

The Electronic Escutcheon shall comply with the manipulation test in PAS 24:2016 and the TS 007:2014 + A1:2015 attack test

4.3.4 Locks designed to be used with a cylinder

Testing shall be performed on a lock assembly that includes the cylinder with which it is intended to be used

4.4 Resistance to dust and moisture

Lock elements exposed on the secure face of the door shall meet the ingress protection IP 55 rating when tested in accordance with BS EN 60529, subject to the variation that products covered by TS 621 may be either category 1 or category 2. The IP rating of X4 shall be sufficient if an electronic cylinder has a mechanical key override

4.5 Mechanical release of the lock from the inside face of the door

The device shall have a mechanical override on the inside face of the door to allow egress due to function failure or power loss

5: Credentials

Credentials used with electronic door locking devices conforming to this Technical Specification must comply with the relevant European Council Directives listed below:

- Radio Equipment Directive (RED) 2014/53/EU
- Electromagnetic Compatibility (EMC) Directive 2014/30/EU
- Low Voltage Directive (LVD) 2014/35/EU

ICCs, PIN Codes, Access Cards and Biometrics

Devices using ICCs, PIN Codes, Access Cards and Biometrics as Credentials should comply with prEN 16867 (Credential Related Security, grade B)

6: Vulnerability of radio frequency network

Objective

The objective of this test is to assess the Electronic Door Locking Device's resistance to attack through manipulation of a credential sent from an active device.

Please note that ICCs, PIN Code, Access Cards and Biometrics are covered in 5. Credentials section above and are outside the scope of tests within this section.

Procedure

Carry out the test from the exterior face of the door assembly with full knowledge of the sample's construction and hardware details.

Testing shall include declared and undeclared communication protocols or applications of the device.
The test lab should use its own equipment to carry out any communications that in normal use would be sent received by an active device.

Devices using any kind of PAN should be tested for vulnerabilities by a laboratory that is both a member of CREST and is UKAS accredited.

Part 1

Part 1 consists of attempting to manipulate a credential that would be communicated from an active device to the Electronic Door Locking Device, to allow the Electronic Door Locking Device to be made insecure. The total test time shall consist of attack time and rest time. During the rest time, the Electronic Door Locking Device should not be communicated with.

The total attack time shall not exceed 5 minutes. The total rest time shall not exceed 5 minutes.

Part 2

Part 2 consists of attempting to manipulate a credential that would be communicated from an active device to the Electronic Door Locking Device, to allow multiple Electronic Door Locking Devices to be made insecure. The total test time shall consist of initial attack time and subsequent attack time. The initial attack time should be used to find a vulnerability and create a process for replicating this. The subsequent attack time should be used to attack a separate Electronic Door Locking Device with the process devised during the initial attack time. The tester should have no access to any working credentials for the lock during the subsequent attack.

The total initial attack time shall not exceed 7 hours per communication protocol. The total subsequent attack time shall not exceed 5 minutes.

7: Vulnerability of device

Electronic door locking devices shall comply with the requirements of clause 6 of BS 3621:2017 Amendment 1, with the following modification:
In clause 6.1, the term "general vulnerability" shall be understood to include electromechanical vulnerability and "thief resistant lock assembly" shall be understood to include thief resistant electronic locking devices
Annexes A and B of BS 3621:2017 shall apply, with the following modifications and additions:

a) Annex A.5 shall be replaced by: "The assessment shall be carried out in two stages as follows: Electromechanical vulnerability assessment: Using the tools specified in Table 1 (of DHF TS 621:2018) the assessors shall attempt to render the device insecure using knowledge and skill, rather than excessive force, general vulnerability assessment: Using the tools specified in A.7 of BS 3621:2017 the assessors shall attempt to render the device insecure using manual dexterity and manipulative skills, rather than excessive force.

(NOTE: Should the assessor believe that it is possible to open the lock assembly using a tool that is not listed in either table, but which is readily available, this shall not, at that point, be recorded as a failure, but shall be reported to **dhf**)"

8: Marking and information to be supplied by the manufacturer

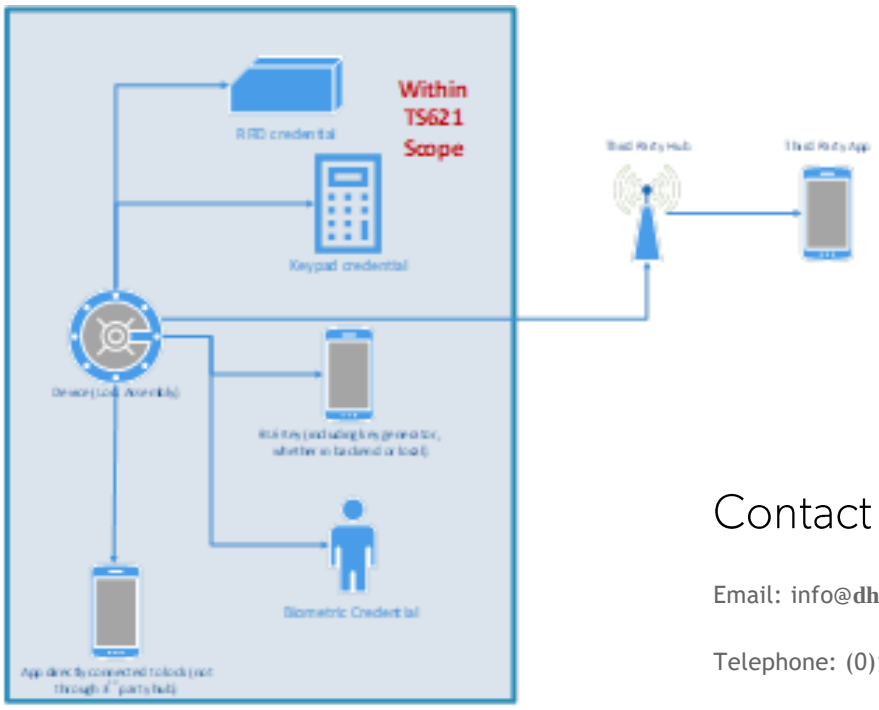
Locks shall comply with clauses 9 of BS 3621:2017 with the following modifications:

a) Clause 9.1 (d) of BS 3621:2017 shall be replaced by "the number and publication date of this specification, i.e. DHF TS 621:2018
b) Clause 9.1 (c) will not apply

Table 1

Item	Additional details
Engineers' pliers	Long and short nose
Side and face wire cutters	Large and small
Small magnet	1.2 tesla
Piezo-electric spark generator	
Freezing agent	0.5 litre can
Cigarette lighter	
Butane/Propane gas torch	
Knife	Max. blade dimensions – length 120mm, thickness 3mm
Scalpel	

Figure 1



Contact us for more information

Email: info@dhfonline.org.uk

Telephone: (0)1827 52337

Address: **dhf** 42 Heath Street, Tamworth, Staffordshire B79 7JH