LPCB®

Loss Prevention Standard

LPS 1650: Issue 1.1

Requirements and testing procedures for the LPCB approval and listing of 'theft resistant' electronic products

This standard specifies requirements for grading the 'theft resistance' of information and communication equipment (ICT) and consumer electronics equipment based on the tools and time required by a criminal to overcome:

(i) Denial of service technologies such as pin codes, passwords and biometrics.
(ii) Asset marking devices.
(iii) Physical restraining devices either incorporated into the design of the product or supplied with the product.
(iv) Alarm detection/signalling equipment incorporate into the design of the product and/or supplied with the product.

bre

CONTENTS **PAGE**

PARTICIPATING ORGANISATIONS

This standard was approved by the LPC Fire and Security Board and Expert Group G. The following organisations participated in the preparation of this standard:-

Association of British Insurers
Association of Building Engineers
Association of Chief Police Officers
Association for Specialist Fire Protection
British Automatic Fire Sprinkler Association
British Fire Protection Systems Association
British Security Industry Association
British Education Communication and Technology Agency
BT
Cabinet Office (Observers)
Chief Fire Officers Association
Department for Education and Skills
Door & Hardware Federation
Electrical Contractors Association
European Fire Sprinkler Network
Health & Safety Executive
Home Office
Loss Prevention Certification Board
Metronet
Post Office
Risk Engineering Data Exchange Group
Royal and Sun Alliance
Royal Institution of Chartered Surveyors
Special Services Group
TPS Consult

REVISION OF LOSS PREVENTION STANDARDS

Loss Prevention Standards will be revised by issue of revised editions or amendments. Details will be posted on our website at www.redbooklive.com

Technical or other changes which affect the requirements for the approval or certification of the product or service will result in a new issue. Minor or administrative changes (e.g. corrections of spelling and typographical errors, changes to address and copyright details, the addition of notes for clarification etc.) may be made as amendments. (See amendments table on page 29)

The issue number will be given in decimal format with the integer part giving the issue number and the fractional part giving the number of amendments (e.g. Issue 3.2 indicates that the document is at Issue 3 with 2 amendments).

USERS OF LOSS PREVENTION STANDARDS SHOULD ENSURE THAT THEY POSSESS THE LATEST ISSUE AND ALL AMENDMENTS.

FOREWORD

This standard identifies the evaluation and/or testing practices undertaken by LPCB for the purposes of approval and listing of products and services. LPCB listing and approval of products and services is based on evidence acceptable to LPCB:-

- that the product or service meets the standard
- that the manufacturer or service provider has staff, processes and systems in place to ensure that the product or service delivered meets the standard

and on:-

- periodic audits of the manufacturer or service provider including testing as appropriate
- compliance with the contract for LPCB listing and approval including agreement to rectify faults as appropriate

This Document should be read in conjunction with Scheme Document SD137.

NOTES

Compliance with this LPS does not of itself confer immunity from legal obligations. Users of LPSs should ensure that they possess the latest issue and all amendments.

LPCB welcomes comments of a technical or editorial nature and these should be addressed to "the Technical Director" at enquiries@breglobal.co.uk.

The BRE Trust, a registered charity, owns BRE and BRE Global. BRE Global and LPCB (part of BRE Global) test, assess, certificate and list products and services within the fire and security sectors. For further information on our services please contact BRE Global, Watford, Herts. WD25 9XX or e-mail to enquiries@breglobal.co.uk

Listed products and services appear in the LPCB "List of Approved Products and Services" which may be viewed on our website: www.redbooklive.com or by downloading the LPCB Red Book App from the App Store (for iPhone and iPad), from Google Play (for Android devices) or from the Windows Store (for Windows 8 Phones and Tablets from 2014).

1 SCOPE

This standard describes tests for classifying the 'theft resistance' of information and communication technology (ICT) equipment and consumer electronics products. This includes:

- In-car entertainment systems
- DVD players and writers
- Health care equipment
- Laptops
- Mobile telephones
- MP3 players
- PDA's
- Personal computers
- Projectors and wipe boards
- Printers
- Satellite navigation devices
- Televisions and screens

The requirements and tests within this standard permit assessment of the product's resistance to the following, as appropriate to the 'anti-theft' technologies built into and/or supplied with the product:

i) Overcoming denial of service technologies to enable the product to be used.
ii) Removing visible traceability to the owner, provided by overt asset marking technologies, without causing visible damage to the product.
iii) Removing covert traceability to the owner, provided by covert asset marking technologies or electronic displays, without visible damage to the product.
iv) Overcoming anchoring technologies supplied with the product such that the item can be removed to a remote location.
v) Preventing alarm/sensing technologies signalling the attempted removal of the product.

Whilst this standard does not specify any one particular design of 'anti-theft' technology it includes requirements for the performance of the following types built into and/or supplied with information and communication technology (ICT) and consumer electronics products:

- Denial of service technologies, such as pin codes, removable coded panels, biometrics, RFID proximity devices and key switches.
- Asset marking devices.
- Anchoring devices.
- Detection and alarm equipment.

Requirements relating to database registers to which asset marking devices shall be linked are described in LPS 1224[1] '*Requirements for Secure Database Registers'*.

Requirements relating to overt asset marking technologies are described in LPS 1225[2] '*Requirements for the LPCB Approval and Listing of Asset Marking Systems'.*

Requirements relating to anchoring devices used to secure computers, projectors and other ICT products are described in LPS 1214[3] '*Specification for testing and classifying physical protection devices for personal computers and similar equipment*'.

This standard does not cover the following 'anti-theft' techniques:

- Unique colours (e.g. the provision of orange coloured products for the education sector).

Note: This is because such provisions rely on it not being legitimately possible to obtain such products outside the sector/customer for which it was intended. As this is often outside direct control of manufacturers, particularly in the longer term, it is not possible to confirm the ongoing effectiveness of such technologies.

- Designs specific to particular customers, e.g. designs of in-car entertainment systems to suit particular dashboards.

Note also;

Replication or replacement of components, other than those included within the attack tool kits, are not taken into account. This is because it is not necessarily possible to determine a criminal's ability to acquire the necessary components/materials.

The durability of the products and associated components are outside the scope of this standard, as is resistance to attack techniques using tools other than those specified within this standard.

The product installation and operating instructions are assessed to determine the product's likely vulnerability to attack when installed and used in accordance with those instructions.

Although this standard specifies that the product instructions shall include hazard data, such data is only reviewed to ensure the safety of the laboratory staff evaluating the product's performance. The authenticity of such data is not assessed.

2 DEFINITIONS

2.1 Alarm / sensing technologies

Devices that are either built into the product or supplied with the product that trigger a built in sounder to sound and/or send an alarm signal to a nominated alarm control and indicating panel and/or activate the denial of service technology when the product is subjected to unauthorised attempts of removal.

Note: Where a Police presence is required in response to intruder alarm events the intruder alarm system must comply with ACPO requirements.*

Alarm devices that are to be linked to building intruder alarm systems shall not prevent the system meeting the requirements of EN 50131-1:2006[4] '*Alarm systems - Intrusion and hold-up systems - Part 1: System requirements*' at the intended security grade or environmental classification, as implemented by PD6662:2004[5] '*Scheme for the application of European Standards for intruder and hold-up alarm systems'* in the United Kingdom.

For more details of the ACPO requirements please refer to 'Police Response to Security Systems' available on the ACPO website: www.acpo.police.uk.

* ACPO is the Association of Chief Police Officers of England, Wales and Northern Ireland.

2.2 Anchoring devices

Devices that attach the product to defined structures, such as desks, building envelopes or vehicles.

Note: When selecting suitable mounting substrates, it is important to consider whether it is possible to easily overcome or remove the substrate in order to remove the product. Manufacturers of security products should therefore define suitable substrates within the installation/user instructions they supply with the product.

2.3 'Anti-theft' technologies

Physical items and/or software incorporated in a product to deter theft by:

i) Preventing the unauthorised use of the product.
ii) Visibly identifying the product's owner, via a third party database approved to LPS 1224[1].
iii) Covertly identifying the product's owner, via a third party database approved to LPS 1224[1].
iv) Preventing the unauthorised removal of the product.

2.4 Asset identification code

Series of at least four alphabetic and/or numeric characters incorporated on an asset marking device.

2.5 Asset marking devices

Methods of securely marking or tagging a product with information unique to that product so that the product can be traced to its owner via a nominated secure database register.

2.6 Asset marking systems

Asset marking systems comprise of one or more asset marking device (either overt or overt and covert) and a secure database register used to provide traceability of a marked asset to the legal owner.

2.7 Attack test

For the purposes of evaluating attack resistance, an attempt at overcoming the "anti-theft" technologies incorporated in a product using mechanical tools, electrical tools and electronic equipment is made to:

i) Enable the product to be used by unauthorised persons.

ii) Remove or destroy information placed on or contained within the product that identifies the owner directly or via a secure database register.

2.8 Covert asset marking devices

Asset marking devices that, when applied to the product:

i) Are secure and hidden from direct view.
ii) Cannot be read with the unaided eye, assuming normal vision and average* lighting conditions.

Examples of covert asset marking devices include RFID transponders, microdot and chemical trace marking devices.

* Average lighting conditions are considered to be those of a light intensity of between 1000 - 2000 lux.

2.9 Denial of service technologies

Physical devices and/or software designed to prevent unauthorised use of the product. Examples of denial of service technologies include PIN codes, removable coded panels, biometric sensors, coded wireless keys and mechanical key switches.

2.10 Fully cured state

This is the state when any adhesive or chemical used to attach or mark the product, is fully cured. That is, the fully cured state occurs when a maximum bond / permanent mark is achieved.

2.11 Overt asset marking devices

Asset marking devices that, when applied to the product:

i) Are secure.
ii) Are visible.
iii) Can be read with the unaided eye, assuming average* lighting conditions.

Examples of overt asset marking devices include adhesive labels, chemical or laser etching and embossing.

* Average lighting conditions are considered to be those of a light intensity of between 1000 - 2000 lux.

2.12 Resistance rating

Numeric indication of the attack resistance provided by the "anti-theft" technology incorporated in a product.

2.13 Secure database register

A system of recording the legal ownership of an asset using the unique asset identification code present on the marking device that is applied to the asset.

2.14 Total test time

The maximum duration of an individual manual intervention attack test. It is the accrued sum of the:

i) working time;
ii) rest time of an operative for wellbeing and safety reasons;
iii) time taken to change tools or exchange defective expendable tool elements; and inspection time called by the project leader.

2.15 Working time (resistance time)

The time of an individual attack test in which tools are used to attempt to weaken the security of the theft resistance.

The working time includes the duration of any treatments applied during manual intervention attack tests in an attempt to remove or damage the integrity of "anti-theft" technologies.

The working time excludes:

i) rest time of an operative for wellbeing and safety reasons;
ii) time to change tools or exchange defective expendable tool elements; and inspection time called by the project leader.

3 REQUIREMENTS

3.1 Design requirements

3.1.1 Mandatory requirements

The product shall incorporate:

i) At least one denial of service technology meeting the requirements of Clause 3.2.
ii) Warning labels meeting the requirements of Clause 3.3.
iii) Product installation and user instructions describing how the product is to be used in order to achieve the designated performance to this standard. Refer to the requirements of Clause 3.8.

3.1.2 Options with requirements

The product may include the following options. Where options are provided and claimed to be a security related feature of enhancement, the option shall meet the requirements of this standard:

i) Overt asset marking. The overt asset marking device shall be placed in a secure, visible location on the product and shall meet the requirements of Clause 3.4.
ii) Covert asset marking. The covert asset marking device shall be hidden on or within the product and shall meet the requirements of Clause 3.5.

iii) Alarm/signalling technologies. The attempted opening and the attempted removal of the product shall be detected and notified. Alarm/signalling technologies shall meet the requirements of Clause 3.6.

iv) Anchoring devices. Anchoring devices supplied with the product shall meet the requirements of Clause 3.7.

3.2 Denial of service technology

The denial of service technology shall prevent unauthorised use of the product.

The means to prevent unauthorised use shall be an integral part of the product and shall be activated automatically either each time the product is used or upon disconnection or removal of the product. It shall be appropriate for use and shall not cause intentional injury or harm.

Note: The type of products included within the scope of this standard are varied and in the context of the above clause the terms 'disconnection' and 'removal' shall include, but need not be limited to, the disconnection of the product from an electrical power source and/or the removal of the product from a base station or cradle required for normal operation in the service environment.

Legitimate use shall require one or more action by the user to enable normal operation, for example; the entry of a PIN code and/or the use of an electronic key.

The product can be fitted with more than one denial of service technology.

The denial of service technology shall resist attack in accordance with the times and tool sets of the categories prescribed in Table 1. Compliance shall be demonstrated by application of the tests as described in Clause 5.5.

Table 1 Resistance rating requirements for attack testing denial of service technologies

Resistance rating classification	Equipment category (Clause 7)	Maximum working time (minutes)	Maximum test duration (minutes)
1	A	0.5	0.5
2	B	1	1
3	B	3	3
4	C	5	5
5	C	10	20
6	D	15	30
7	D	30	60
8	E	60	120

Refer to Clause 7 of this standard for a description of the tool categories.

User instructions supplied with the product shall contain information clearly stating how the denial of service technology shall be used to maximise the security of the product

and safeguard its operation from illegitimate users, for example; describe how to store securely electronic keys or removable fascia panels etc.

The product manufacturer and/or supplier shall have in place procedures for issuing spare and/or replacement PIN codes or parts such as electronic keys, fascia panels etc. The procedure shall permit the confirmation that the spare and/or replacement items are being supplied to the legitimate owner and ensure the integrity of the security features of the product are maintained.

Instructions shall be supplied to the user clearly stating how to obtain spare and/or replacement PIN codes or parts.

3.3 Warning labels

The product and its packaging shall incorporate visible warning that the product incorporates anti-theft technology and meets the requirements of this standard.

Note: To avoid the use of multiple labels, where an overt asset marking device is fitted to the product it may also incorporate such a warning.

The warning label shall resist removal from the product for at least 30 seconds when an attempt is made to remove it using only manual dexterity, i.e. without the aid of any tool.

Note: This equates to class 1 resistance to removal as defined within LPS 1225[2].

The warning label shall remain visible and securely attached to the product following exposure to the climatic conditioning of Clause 5.10.

In addition to labelling the product, each product shall be supplied with at least one warning label that owners can place in a visible location near the product to warn thieves that the product incorporates anti-theft technology. (e.g. on a door leading into the building/room where the product is located or on a window).

Note: If the product is approved by LPCB, the warning label can include the LPCB certification mark, certification number, number of this standard (i.e. LPS 1650) and, if desirable, the resistance rating achieved by the product.

3.4 Overt asset marking

When fitted to the product in accordance with the manufacturer's/supplier's fitting instructions, the overt asset marking device shall meet the requirements of at least security classification 1+1, defined in LPS 1225[2].

The overt marking shall provide traceability to the product owner via the link to a secure database register that meets the requirements of LPS 1224[1].

The asset identification code shall uniquely identify the marked product and be capable of being transferred should the owner relocate, sell, pass on or cancel ownership of the product.

Where asset marking is provided, registration forms and registration instructions in accordance with Clause 3.9 shall be supplied with the product.

The asset marking label shall remain visible and securely attached to the product following exposure to the climatic conditioning of Clause 5.10.

3.5 Covert asset marking devices

If covert asset marking devices are fitted to the product, such devices shall:

i) Be securely fastened to or incorporated into the product during manufacture.
ii) Remain hidden until revealed using detection apparatus specified by the product manufacturer/supplier.
iii) Not adversely affect the operation of the marked product.
iv) Allow the identity of the legal owner to be traced via a secure database register using the defined detection apparatus.

Where the option is provided, the product shall incorporate one or more of the established convert asset marking devices listed below, (alternative types of device are permitted provided the same level of security performance can be demonstrated);

3.5.1 Microdot marking devices

Microdot marking devices shall meet the requirements of LPS 1269[6] 'Requirements for the LPCB approval and listing of 'microdot' asset marking devices'.

3.5.2 Chemical trace marking systems

Chemical trace marking systems shall meet the requirements of LPS 1251[7] 'Requirements for the LPCB approval and listing of chemical trace asset marking systems'.

3.5.3 Electronically coded marking systems

Electronically coded marking systems shall, when read using a reader of a type defined by the product manufacturer, provide traceability to the owner via the nominated database.

The electronically coded marking device shall be unique to the product and shall not be visible even when the product is disassembled. The electronic code can reside within the circuitry of the product or can be held within a 'stand-alone' transponder (e.g. RFID tag) hidden inside the product.

Stand-alone transponders shall not be visible when the product is assembled but viewed with any user detachable covers or panels removed.

Using the means specified by the product manufacturer/supplier, it shall be possible to find and read the electronically coded mark within a maximum time duration of 2 minutes. The means of identification may comprise portable apparatus that can be electrically connected to the product or a wire free 'scanner' type device.

If the electronically coded mark can be located without the use of the specified reader, it shall not be possible to erase or remove the electronically coded mark without leaving the product permanently inoperable, or without leaving obvious signs of visible damage that would significantly reduce the re-saleable value of the product. Compliance with this requirement shall be demonstrated by conducting the tests of Clause 5.7.3.

The electronically coded mark shall, when read using the defined identification means, continue to provide traceability to the legitimate owner of the product via the secure database, after exposure to the climatic conditioning tests of Clause 5.10.

3.6 Alarm / signalling technologies

If alarm / signalling technologies are incorporated into or supplied with the product, such technologies shall:

i) Detect the removal of the product from the legitimate location before the product or detection means can be prevented from signalling an alarm condition.
ii) Detect the opening of any part of the product enclosure not normally accessible to the user before the product or detection means can be prevented from signalling an alarm condition. (Applicable only to those products or parts thereof that can be opened).

The alarm shall be signalled by an audible warning and/or by the transmission of a signal or message to a remote location.

It shall not be possible to silence the audible warning by forcible means within 1 minute without creating obvious signs of visible damage or leaving the product operable in.

Nor shall it be possible to terminate the transmission of an alarm signal or message by forcible means before the complete alarm signal or message has been sent, without creating obvious signs of visible damage or leaving the product operable in.

Where provision is made to connect the product's alarm sensor(s) to a building alarm system, the connection of the product shall be in accordance with the requirements of EN 50131-1[4] as implemented in the United Kingdom. Connection to the building alarm system shall not prevent that alarm system from meeting the intended security grade or environmental classification.

Note: Compliance with the environmental classification shall be demonstrated by evidence of compliance with the requirements of EN 50130-5:1998[8] 'Alarm systems - Part 5: Environmental test methods'.

Where a Police presence is required in response to intruder alarm events, the intruder alarm system must comply with the ACPO requirements as implemented by the guidance of DD 243:2004[9] '*Installation and configuration of intruder alarm systems designed to generate confirmed alarm conditions - Code of practice*'. Connection of the

product to the building security system shall not prevent compliance with these requirements.

3.7 Anchoring devices

Anchoring devices supplied with the product shall meet the requirements of at least security classification I defined in LPS 1214[3], when installed in accordance with the instructions supplied with the product.

3.8 Product instructions

The following information shall be included in the instructions that are supplied with the product:

i) Recommendations for secure installation, including wiring and networking, if appropriate.
ii) User instructions confirming how the security technologies shall be used to achieve the claimed security performance to this standard. This should also include the following, as appropriate to the security technologies incorporated in the product:
   - Recommendations for the appropriate secure storage of PIN codes, removable operating panels, keys etc.
   - Recommendations for maintaining network security.

iii) Security performance ratings achieved by the product and any ancillary security devices supplied with the product to this standard.
iv) The LPCB approval number of the secure database register(s) to which the asset marking device(s) are linked (if provided).
v) Recommendations for recording and safe storage of the record of the asset marking device's unique code.
vi) The procedure to be followed by the owner of the product when registering, transferring or cancelling ownership of the product on the associated secure database register.
vii) The procedure to be followed in the case of theft or loss of the marked asset.
viii) Recommendations where to place the warning labels.
ix) The procedure to follow when ordering replacements items, in particular PIN codes or electronic keys.

Where asset marking is provided, but the asset marking devices are not fitted to the product during manufacture, the devices can be supplied with the product.

However the product instructions must include detailed instructions for affixing the marking device to the product such that the marking device will provide the claimed level of resistance to removal/eradication to LPS 1225[2].

The instructions provided with the asset marking devices shall therefore include:

i) Details of where to place the asset marking device(s) on the product in order to achieve the advertised resistance to attack.
ii) Confirmation of the time taken for the mark to reach the fully cured state after being affixed to the product.
iii) Guidance on how the marked product / treated area should be protected while the mark cures.
iv) Appropriate hazard data that establishes COSHH requirements.

3.9 Asset registration forms and registration instructions

Where asset marking is provided, the following forms shall be supplied with the product:

i) Form for registering the ownership of the product on the associated secure database register(s) to which the asset marking devices are linked.
ii) Form for notifying the secure database register(s) of change of details.
iii) Form for notifying the secure database register(s) of change of ownership.

If the manufacturer also provides the option to register the product on the secure database register via the world-wide web:

i) The product instructions shall contain details of how to register the product via the world-wide web.
ii) With the exception of a signature, the online registration forms shall require at least the same level of information to be entered by the owner as is needed for offline registration.
iii) the online register shall require the owner to use a password of at least 8 characters made up of at least one numeric character and one letter and either one change in case or one symbol.

4 SUBMISSION REQUIREMENTS FOR LPCB APPROVAL

4.1 Information to be supplied by the applicant

4.1.1 General

Prior to examination and testing, the applicant shall provide comprehensive information about the product to be evaluated. All documents shall be dated and given a reference number and issue description. If the applicant is not the product manufacturer, then the application must be accompanied by written permission from the manufacturer for testing to be undertaken.

4.1.2 Data

The applicant shall supply the following detailed information relating to the product and hardware to be tested.

a) Manufacturing information:

   i) Name of manufacturer.
   ii) Place(s) of manufacture.
   iii) Relationship of applicant to manufacturer.
   iv) Company responsible for design and quality assurance.

b) General assembly drawings of the product and any ancillary device(s), for example, removable key pads, keys or other security devices forming part of the approved product/system.

c) A list of parts (Bill of Materials), including component datasheets covering each component source.

d) Specifications and drawings accurately detailing the construction of elements of the product/ancillary equipment likely to affect performance to this standard. These include, but are not restricted to:

   i) Circuit diagram(s).

   ii) PCB track layout drawings (all layers).

   iii) Casing materials (as this can affect the efficacy of asset marking devices applied to the casing).

   iv) Anchoring devices.

   v) Specifications for the construction of asset marking devices including:

      - Material specifications for any tags, plates or stickers incorporated in the system as described in LPS 1225[2].
      - Any adhesives, etching, curing or other chemical agents that affect the performance of the asset marking device.

e) Source code/logic data for elements of the product relating to the security performance of that product (e.g. security codes, splash screens etc). The exact content of the submission shall be agreed between the manufacturer and the test laboratory.

f) Installation and user instructions.

g) Confirmation of the secure database register to which the marking device(s) fitted to the product is linked and a copy of the service level agreement between the product manufacturer/applicant and the database operator.

h) Product registration and change of details forms.

i) Where applicable, evidence of compliance with electrical safety standards such as EN 60950-1:2006[10] (Incorporating Corrigenda Nos. 1and 2) *'Information technology equipment – Safety - Part 1: General requirements'* or EN 60065:2002[11] *'Audio, video and similar electronic apparatus. Safety requirements '*.

Note: As well as being a prerequisite of LPCB approval, this information is required to help ensure the safety of staff evaluating the product to this standard. It is the responsibility of the applicant to ensure products submitted for test are electrically safe.

j) The operating and storage climatic ranges (temperature and relative humidity).

k) Appropriate material hazard data sheets that adhere to the requirements of COSHH*.

l) Confirmation of the build status of the product, i.e. whether the product is a prototype or a sample from series production.

* Control Of Substances Hazardous to Health

4.2 Specimens to be supplied for testing

Subsequent to the LPCB's acceptance of an application for approval, the following shall be observed:

a) The applicant shall supply the agreed number of specimens.

b) If a prototype device is supplied for testing, approval will not be given until the drawings for subsequent series production have been examined and confirmed that they accord with the tested prototype or that any changes will not affect the theft resistance rating.

c) Additional components of some products may be requested for testing purposes.

d) When the product incorporates advances or changes in technology, then additional specimens or components may be requested for evaluation prior to the supply of the agreed specimens.

e) The number of specimens to be supplied for testing shall be specified by the laboratory and shall be dependent on the range and scope of the applications in which the products can be used.

All specimens shall be supplied complete with any associated ancillary devices (e.g. Security anchoring devices), instructions and asset registration and change of details documents.

In addition to the test specimens the following shall also be supplied by the applicant;

i) Items of support equipment needed to demonstrate correct functionality of the product and/or accessories intended for use with the product.

ii) Any equipment or apparatus needed to read information from the covert asset marking systems. For example, a wire free scanner device to read the electronically coded mark, or a microscope to read alpha dot marking.

5 TEST METHODS

5.1 Testing protocol

General laboratory procedures, confidential handling of specimens and information supplied by the applicant, event recording requirements and presentation of the test report shall be in accordance with the requirements specified in EN ISO/IEC 17025:2000[12] *'General requirements for the competence of testing and calibration laboratories'*.

5.2 General test conditions

The atmospheric conditions in the test laboratory shall be those specified in EN 60068 - 1:1994, IEC 60068-1:1988 [13] *'Environmental testing. General and guidance'*, Subclause 5.3.1, unless stated otherwise.

Temperature: 15 °C to 35 °C

Relative humidity: 25 % RH to 75 % RH

Air pressure: 86 kPa to 106 kPa

5.3 Examination

5.3.1 Data

All information and drawings supplied will be reviewed to ensure suitability for test, certification and end-user purposes.

5.3.2 Conformity between specimen and documentation

Prior to testing, the test specimen(s) shall be visually examined for conformity with the details supplied by the applicant. A lack of conformity identified at this stage or during testing will, unless promptly corrected, prevent the granting of approval.

5.3.3 Design requirements

The specimens, product instructions and other information supplied by the applicant shall be reviewed against the requirements laid down in this standard in order to assess general compliance with design requirements and potential weaknesses of the system that may be exploited.

5.4 Test objectives

The general objectives of the following series of tests are to confirm the resistance of the product to;

i) Removal and use by unauthorised persons after attacking using manual and electronic tools without creating obvious damage to the product that may significantly lower its re-sale value.

Where asset marking devices are fitted,

ii) Removal/destruction of asset marking devices, using manual and electronic tools, such that it is not possible to trace the owner of the product via the nominated secure database register(s).

5.5 Manual intervention attack of the denial of service technologies

Setup the denial of service technologies in accordance with the manufacturer's recommendations such that all the denial of service technologies are activated. Confirm correct operation of each technology against the description given in the instructions supplied with the product.

Examine the product and the accompanying documentation to establish how the denial of service technologies operate.

Identify each component associated with the denial of service means and conduct an assessment of each to list the potential methods by which the denial of service technology may be disabled or circumvented. The list may include but shall not be limited to; identifying factory reset functions, the use of reprogramming tools, re-wiring/modification of electronic circuitry, exposure to extreme climatic conditions and substitution of readily available components.

A programme of attack tests shall be determined from the above list.

Note: Manufacturers/applicants may choose to have each denial of service technology evaluated in isolation of others. In this case the report shall reflect the results achieved with each of the denial of service technologies activated.

Undertake the programme of series of attack tests using equipment of the appropriate category relative to the resistance rating expectation and in accordance with Table 1. Only one test operative may be used for each individual attack test.

Attack tests shall only be conducted on product specimens that have not been damaged by a previous test to the same target area.

During each individual attack test, the timing device used to measure test duration shall remain activated. The resolution of this device shall be at least 1 second. The timing device(s) used to record working time shall have a resolution of at least 0.01 second. At the conclusion of the test the aggregate working time shall be rounded to the next full second.

Each individual attack test shall be continued until one of the following occurs:

i) The objective of the attack test is achieved.
ii) The maximum test duration is exceeded.
iii) It is decided to abandon the test owing to ineffectiveness for classification purposes.

The product shall have met the requirements of a particular resistance rating if the denial of service technology cannot be disabled or circumvented in the allocated time without rendering the product operable in, or without creating visible damage to the product and/or ancillary equipment that can be clearly seen without disassembly of the product.

5.6 Manual intervention attack of overt asset marking devices

Where the product is fitted with overt asset marking, conduct a series of manual intervention attack tests on the marked product in accordance with the requirements defined in LPS 1225[2].

5.7 Manual intervention attack of covert asset marking devices

Where the product is fitted with covert asset marking, apply the appropriate attack test(s) described below;

5.7.1 Microdot marking devices

Conduct a series of manual intervention attack tests on the marked product in accordance with LPS 1269[6].

5.7.2 Chemical trace marking devices

Conduct a series of manual intervention attack tests on the marked product in accordance with LPS 1251[7].

5.7.3 Electronically coded marking systems

Conduct the tests as described below;

Visual identification

Using the specified reading apparatus (e.g. a scanner), and following the procedure recommended by the manufacturer, attempt to read the electronic code. The attempt shall be timed from the moment the test operator begins setting up the reading apparatus until the point when the electronic code is successfully read. The measurement shall not include the time taken to trace the owner via the database. The requirements of Clause 3.5.3 shall be met.

An attempt shall be made to locate the transponder or device containing the electronic code by a second test operator, with no prior knowledge of the position of the transponder or device and without the use of the specified reader.

Using the appropriate tools, disassemble the product in the normal way, i.e. as if conducting service maintenance, removing all parts of the enclosure. Examine the product and the dismantled parts to confirm that the electronically coded mark and/or transponder are not visible. The examination shall be performed by a person with normal vision, without magnification and under average lighting conditions having an intensity of between 1000 – 2000 lux.

Physical attack

If the position of the transponder or device containing the electronic code can be located by the second test operator, apply the following manual intervention attack tests.

These tests are intended to demonstrate that it is not possible to erase or remove the electronically coded mark without leaving obvious signs of visible damage or the product permanently inoperable.

a) Attempt to prevent the electronic code from being read by drilling the transponder or device containing the code using a tungsten carbide tipped drill bit of 0.5mm diameter.

   It shall not be possible to prevent the code being read after drilling through the device unless the product is also rendered operable in, or obvious signs of damage are created that are visible even when the product is fully assembled.

b) In an attempt to prevent the electronic code from being read, apply 3 positive and 3 negative polarity electrostatic discharge (ESD) pulses directly onto the transponder or device containing the electronic code. Alternatively, if the coded device cannot be reached, the ESD pulses shall be applied as close as possible to the device.

   The ESD pulses shall have the following characteristics:

Table 2 ESD pulse characteristics

Discharge voltage	Polarity	Type of Discharge	No. of discharges per point
15kV	+ve & -ve	Air contact	3

   The application of the ESD pulses shall not prevent the code being read, unless the product is also rendered operable in.

c) Attempt to remove the transponder or device containing the electronic code using tools from tool category B of Clause 7.

It shall not be possible to remove the transponder or device containing the electronic code without creating obvious signs of damage that remains clearly visible even when the product is fully assembled, or leaving the product operable in.

d) Expose the product including the electronically coded marking device to the extreme hot and cold temperatures of the climatic conditioning of Clause 5.11.

It shall not be possible to prevent the electronic code being read by applying extreme hot and cold temperatures without creating obvious signs of damage to the product or leaving the product inoperable.

5.8 Manual intervention attack of the anchoring devices

Install samples of the product and anchoring device in accordance with the instructions provided with the product.

Conduct a series of intervention attack tests in accordance with the requirements of LPS 1214[3].

5.9 Manual intervention attack of the alarm / signalling devices

Install the alarm/signalling device(s) in accordance with the instructions provided with the product and confirm correct operation.

Confirm that it is not possible to remove the product without triggering the alarm and/or signalling device(s).

Using the tools provided in tool category B of Clause 7 and within a time period of one minute, attempt to disable or circumvent the alarm and/or signalling device whilst the alarm is in the quiescent condition, i.e. active but not warning of an alarm condition.

The attempt to disable the alarm sensing devices or critical parts of the alarm circuitry by tampering shall include removing or probing the product's enclosure and/or applying suitable electrical stimuli.

Trigger an alarm condition and, within a time period of one minute using the tools provided in tool category B of Clause 7, attempt to stop the audible alarm and/or signalling device warning of an alarm condition.

The tool categories applied shall be selected either by making an assessment of the product and choosing the most appropriate tools, or by starting with Category A and progressively working through each additional category, until the alarm/signalling device can be compromised.

Compliance shall have been demonstrated if;

i) It was not possible to remove the product without generating an alarm condition.
ii) The alarm/signalling device resisted the attack using the tools of Category B for a duration of one minute or the product displayed obvious signs of damage that may significantly affect the resale value.

5.10 Climatic conditioning

Confirm the product labelling and the overt asset marking associated with the security features remain legible and intact following exposure to the climatic conditions over the claimed operating and/or storage temperature and humidity range (whichever in the greater).

The tests shall be conducted generally in accordance with the procedures described in EN 60068-2-1:200714 'Environmental testing. Tests. Test A. Cold ', EN 60068-2-2:199315, IEC 60068-2-2:1974 'Environmental testing. Test methods. Tests B. Dry heat' and EN 60068-2-78:200116, IEC 60068-2-78:2001 'Environmental testing. Test methods. Test Cab. Damp heat, steady state'. The limit temperatures and relative humidity conditions shall be those of the ranges claimed by the product manufacturer and for a duration of 16hrs.

5.11 Extreme temperatures

Confirm that the security features of the product continue to provide theft resistance following the application of the dry heat and cold tests describe below. The product shall remain un-powered and free of any packaging throughout the conditioning.

5.11.1 Dry Heat

Test Ba: Dry heat for non heat-dissipating specimen with sudden change of temperature as prescribed by EN 60068-2-2[15] and held at +100°C* for 16hrs.

No intermediate measurements are made during the conditioning.

*Note * Care shall be exercised when applying the high temperature of the dry heat conditioning as some materials used in the construction of the product may not within stand high temperatures. For example some products may contain batteries that could explode. In some circumstances, and at the discretion of the test laboratory, the limit temperature can be reduced to +70°C.*

5.11.2 Cold

Test Aa: Cold for non heat-dissipating specimen with sudden change of temperature as prescribed by EN 60068-2-1[14] and held at -25°C for 16hrs.

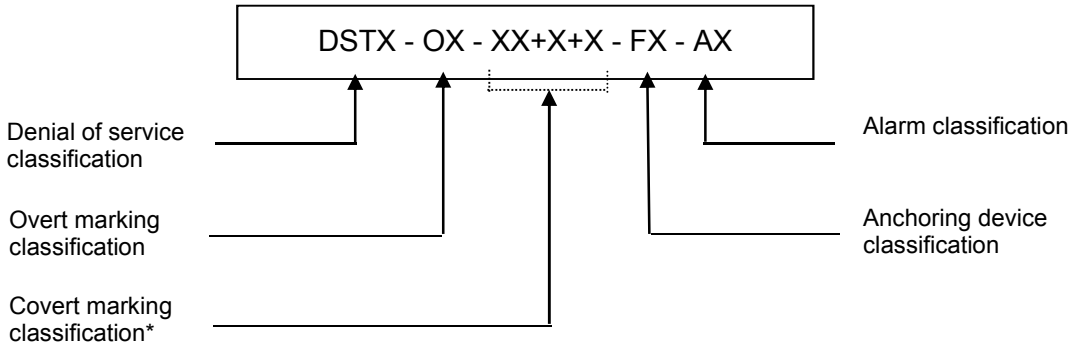
No intermediate measurements are made during the conditioning.

6 SECURITY PERFORMANCE RATING

The overall security performance rating is indicated by a series of security performance classifications, as illustrated by the examples in Table 3. The higher the numbers in each classification, the higher the security performance of the product tested, as described in Table 3.

To meet the minimum requirement of this standard, products must achieve at least one denial of service ('DST') classification.

The security performance rating may be displayed on the product, accompanying instructions and/or the packaging. When it is displayed it shall be of the following format:



The label of products meeting only some of the classification requirements need only display those ratings that apply.

With reference to Table 3 a typical label may appear as follows;

DST4 - O2 - M2+2+6 – FI - A3

Note * Where two or more convert marking technologies are provided the classification of each technology can be displayed as follows;

DST4 - O2 - M2+2+6 - FI - A3
E3+3+6

Table 3 Security performance classifications

Technology	Applicable Standards	Description	Example Rating
Denial of service technology	LPS 1650	The letters 'DST' followed by a number indicating the lowest resistance rating achieved by the combined set of "Denial of Service Technologies" incorporated within the product.	DST4
Overt asset marking	LPS 1225[2]	An 'O' followed by two numerals separated by a plus sign. The first numeral represents the resistance rating to erasure of traceability and the second numeral to complete removal / asset restoration.	O2+6
Covert asset marking technology	LPS 1269[6] LPS 1251[7] LPS 1650	A letter followed by three numerals separated by plus signs. The letter indicates the technology used: C = Chemical trace (forensic) marking system M = Microdot marking system E = Electronically coded marking system The first two numerals reflect the lowest resistance rating achieved by the warning label(s). The third numeral reflects the resistance to erasure/removal of the element needed to trace the legal owner, e.g. removal of chemical, microdots or destruction of RFID device.	M2+2+6
Anchoring device	LPS 1214[3]	Classifications I or II.	FI
Alarm	LPS 1650	The letter "A" followed by a number between 1 and 3 to indicate the performance of any detection and alarm technology built into the product.	A3

Table 4 Explanation of resistance rating classifications relating to denial of service technologies

Resistance rating classification	Risk at which the classification and attack equipment is aimed
1	Opportunist attempt at overcoming denial of service technology prior to removing the product from a public area equipped with CCTV and with security staff in the vicinity, e.g. a busy school, university, office or retail premises during trading hours.
2 - 3	A situation in which an opportunist employs easily concealed common household or do-it-yourself items in order to overcome denial of service technology prior to removing the product from a public area. Alternatively, a situation where the tool kit may be employed in an attempt to overcome denial of service technology prior to taking the product from either: i) A manned environment such as a shop, warehouse or factory during working hours. ii) Unmanned premises whose structure and building components offer a lower level of physical security than that required by security rating classification 2 of LPS 1175[17] *'Requirements and testing procedures for the approval and listing of intruder resistant building components Strongpoints, Security Enclosures and free-standing barriers.'*
4 - 5	A situation where portable items are employed in an attempt to overcome denial of service technology either prior to or after removing the product from either: i) A sparsely-manned environment such as an automated warehouse or factory during working hours. ii) Premises whose structure and building components offer a lower level of physical security than that required by security rating classification 4 of LPS 1175[17].
6 - 7	A situation where an extensive tool kit provides a professional means of overcoming denial of service technology, generally following removal of the product from a location offering a lower level of physical security than that required by security rating classification 5 of LPS 1175[17].
8	An enhancement of the situation relevant to resistance rating 6-7.

Table 5 Rating classifications relating to alarm /signalling devices

Rating classification	Security Feature
1	On board detection and audible warning of an alarm condition
2	Alarm signalling capability to a remote location
3	On board detection and audible warning of an alarm condition combined with alarm signalling capability to a remote location

Each security feature shall resist attack for a minimum of 1 minute when assessed in accordance with Clause 5.9.

7 EQUIPMENT FOR DENIAL OF SERVICE ATTACK TESTS

The equipment manifest for the attack tests on denial of service technologies and the ascribed equipment category is as follows.

The equipment category selected for each security classification is defined in Table 1.

Equipment category A

Manual dexterity without the aid of any tool.

Equipment category B

The equipment included in category B is, for example, of the type commonly available in school laboratories.

- The tools specified in category B of LPS 1225[2] plus;
- Adjustable wrenches (various sizes)
- Socket set
- Programmable remote control (e.g. universal – 'One for All' type)
- Soldering iron + Solder sucker
- Computer with access to internet and code breaking freeware
- Oscilloscope (Digital storage - Dual channel <=20 MHz)
- Freezer spray
- Climatic conditioning chamber (-20°C to +40°C)
- Regulated power supply (0 to 48 v DC)

Equipment category C

The equipment included in category C is, for example, of the type available in electrical/electronic repair shops;

- The tools specified in equipment category B above plus category C of LPS 1225[2] plus;
- Security bit set
- Circuit/current tracer
- IC extraction tool
- Logic probe
- Multi-meter
- Circuit board magnifier or microscope
- Oscilloscope (Analogue or digital storage <=100 MHz)
- Phase meter
- Wireman tool set

Equipment category D

The equipment included in category D is, for example, of the type available in a manufacturing facility;

- The tools specified in equipment category C plus;
- Signal generator – (frequency)
- Surface mount chips and surface mount rework station
- Programmer (e.g. PROM, CPU etc.)

Equipment category E

The equipment included in category E is, for example, of the type available in an engineering design laboratory;

The tools specified in equipment category D above plus;

- ASIC design tools
- Circuit simulators
- Electronic design automation (EDA) tools (e.g. VHDL silicon design)
- ESD probe (≤ 15 kV)
- Logic analyser
- 4 channel Storage scope (<= 1GHz)
- Microprocessor programmer emulator
- Purpose built test equipment
- Spectrum analyser – frequency
- Waveform generator

8 PUBLICATIONS REFERRED TO

1. LPS 1224 Requirements for Secure Database Registers.
2. LPS 1225 Requirements for the LPCB Approval and Listing of Asset Marking Systems.
3. LPS 1214 Specification for testing and classifying physical protection devices for personal computers and similar equipment
4. EN 50131-1:2006 Alarm systems - Intrusion and hold-up systems - Part 1: System requirements.
5. PD6662:2004 Scheme for the application of European Standards for intruder and hold-up alarm systems
6. LPS 1269 Requirements for the LPCB approval and listing of 'microdot' asset marking devices.
7. LPS 1251 Requirements for the LPCB Approval and Listing of Chemical Trace Asset Marking Systems.
8. EN 50130-5:1998 Alarm systems - Part 5: Environmental test methods.
9. DD243:2004 Installation and configuration of intruder alarm systems designed to generate confirmed alarm conditions - Code of practice.
10. EN 60950-1:2006 *Incorporating Corrigenda Nos. 1and 2* Information technology equipment - Safety - Part 1: General requirements, (IEC 60950-1:2005, modified).
11. EN 60065:2002 Audio, video and similar electronic apparatus. Safety requirements.
12. EN ISO/IEC 17025:2005 General requirements for the competence of testing and calibration laboratories.
13. EN 60068-1: 1994, IEC 60068-1:1988 Environmental testing. General and guidance
14. EN 60068-2-1:2007 Environmental testing. Tests. Test A. Cold
15. EN 60068-2-2:1993, IEC 60068-2-2:1974 Environmental testing. Test methods. Tests B. Dry heat
16. EN 60068-2-78:2001, IEC 60068-2-78:2001 Environmental testing. Test methods. Test Cab. Damp heat, steady state
17. LPS 1175 Requirements and testing for the approval and listing of intruder resistant building components Strongpoints, Security Enclosures and free-standing barriers

Amendments Issued Since Publication

DOCUMENT NO.	AMENDMENT DETAILS	SIGNATURE	DATE
LPS 1650-1.1	1 New front cover 2 Title added to header 3 Notes amended on Page 4 4 Repagination 5 Update to copyright information	DC	Feb. 2014