

PUBLICLY AVAILABLE SPECIFICATION

Internet safety – Access control systems for the protection of children online – Specification

ICS 35.040; 35.080



NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW



Documents
Document Sharing Hub

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© BSI 3 April 2008

ISBN 978 0 580 49979 1

Amendments issued since publication

Amd. no.	Date	Text affected
-----------------	-------------	----------------------

Contents

Foreword *ii*

Introduction *1*

1	Scope	<i>2</i>
2	Terms and definitions	<i>3</i>
3	Abbreviations	<i>6</i>
4	Internet-based content	<i>7</i>
5	Internet-based communications	<i>8</i>
6	Security of settings	<i>10</i>
7	Installation and implementation – including initial configuration	<i>10</i>
8	Configuration	<i>12</i>
9	Maintenance	<i>12</i>
10	Uninstall/removal	<i>13</i>
11	System support	<i>14</i>
12	Product description and user documentation	<i>14</i>
13	User education materials	<i>17</i>
14	Conformity declaration	<i>18</i>

Annexes

Annex A (normative)	Overview of the test laboratory process	<i>19</i>
Annex B (normative)	Categories of inappropriate content	<i>20</i>
Annex C (normative)	Criteria to be used for checking compliance against Clause 4: Internet-based content	<i>23</i>
Annex D (normative)	Criteria to be used for checking compliance against Clause 5: Internet-based communications	<i>25</i>
Annex E (normative)	Categories of Internet-based communication services	<i>26</i>
Annex F (normative)	Criteria to be used for checking compliance against Clause 6: Security of settings	<i>26</i>
Annex G (normative)	Criteria to be used for checking compliance against Clause 7: Installation	<i>27</i>
Annex H (normative)	Criteria to be used for checking compliance against Clause 8: Configuration	<i>28</i>
Annex I (normative)	Criteria to be used for checking compliance against Clause 9: Maintenance	<i>29</i>
Annex J (normative)	Criteria to be used for checking compliance against Clause 10: Uninstall/removal	<i>30</i>
Annex K (normative)	Criteria to be used for checking compliance against Clause 11: System support	<i>30</i>
Annex L (normative)	Criteria to be used for checking compliance against Clause 12: Product description and user documentation	<i>31</i>
	Bibliography	<i>33</i>

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, pages 1 to 33 and a back cover.

Foreword

This Publicly Available Specification (PAS) has been prepared by The British Standards Institution (BSI) in consultation with the Home Office and Ofcom and associated groups to provide a specification for access control systems for the protection of children online.

Acknowledgement is given to the following organizations that were involved in the development of this specification:

Becta

Borderware Technology

BSI Product Services

Child Exploitation and Online Protection Centre (CEOP)

Cyberpatrol from SurfControl

The Home Office

The Home Secretary's Task Force on Child Protection on the Internet

Intertek Research and Performance Testing

Microsoft

Mobile Broadband Group

NCH

Ofcom (Office of Communications)

The Children's Charities

In this Publicly Available Specification, the word "shall" indicates a requirement. The word "should" indicates a recommendation. Paragraphs marked "NOTE" are for guidance in understanding or clarifying the associated requirement.

This PAS has been prepared and published by BSI, which retains its ownership and copyright. BSI reserves the right to withdraw or amend this PAS on receipt of authoritative advice that it is appropriate to do so. This Publicly Available Specification will be reviewed at intervals not exceeding two years and any amendments arising from the review will be published in an amended Publicly Available Specification and publicized in *Update Standards*. Feedback on this Publicly Available Specification and future work will be gratefully received. This specification is not intended to restrict new developments in design and materials.

This Publicly Available Specification is not to be regarded as a British Standard. It will be withdrawn if its content is published in, or as, a British Standard.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a Publicly Available Specification does not in itself confer immunity from legal obligations.

Introduction

The Home Secretary's Task Force for Child Protection on the Internet was created in 2001. Its aim is to make the UK the safest place in the world for children to use the Internet and to help protect children across the world from abuse fuelled by criminal misuse of new technologies. The Task Force brings together representatives from law enforcement agencies, child protection organizations, the Internet industry, Government and representatives from opposition parties.

The Task Force's work to date includes the development of models of good practice for providers of Internet chat, instant messaging, web-based services and search services, guidance on the moderation of interactive services, and is currently developing good practice guidance for providers of social networks and user-generated content services. The Task Force also contributed to the development of codes of practice for new forms of content on mobile phones and passive location services and worked on public awareness campaigns and guidance for young people, and their parents and carers, for using the Internet and related technologies safely. In addition to the above, the Task Force recommended the creation of the Child Exploitation and Online Protection Centre (CEOP).

Recognizing the role of parents and carers in developing a safe Internet environment, a subgroup of the Task Force was created in 2003 to specifically consider rating, filtering and monitoring products (access control systems) for use in the home.

At this time numerous commercial products were emerging, but there were concerns over their quality and effectiveness. Additionally, there was no permanent, independent source of evaluation for such products, meaning that parents/carers often faced difficulties in understanding the many issues, and in finding reliable products which met their requirements.

In 2004, the subgroup coordinated a short-term project to produce a guide for parents on available options for managing their children's use of the Internet. Longer-term aims included the development of a solution for keeping parents informed of the risks, and suitable products and services for managing them, which could also keep pace with technological changes. The subgroup decided to develop a third-party conformity certification scheme against which access control systems could be tested, providing impartial advice to parents on product features, capabilities, ease of use and confidence in their quality.

This Publicly Available Specification has been developed primarily for use by software developers working with access control systems. It sets out the minimum performance requirements for the access control systems to obtain a third-party conformity certification. An overview of the laboratory procedures is given in Annex A.

It must be recognized however, that no access control system can be effective 100% of the time and that, despite rigorous controls, there may still be occasions when inappropriate materials may be accessed. In such instances, providing education on the issues, and developing strategies for protecting themselves, is essential in helping children and young people become safe and discriminating users of Internet-based content and services.

This Publicly Available Specification is primarily aimed at the development of access control systems for use in the consumer market in the UK. It covers both those products installed locally (i.e. by a parent/carer on a home computer) and remotely managed products/services (i.e. those products or services offered by Internet Service Providers).

The development of this Publicly Available Specification has been jointly sponsored by the Home Office and Ofcom.

1 Scope

This Publicly Available Specification specifies requirements for products, services, tools and other systems that allow UK adult Internet users to easily control children's access to inappropriate Internet-based content and services.

It specifies requirements on:

- a) ease of installation, configuration and use;
- b) effectiveness;
- c) minimum features;
- d) ease of updating;
- e) quality of instructions;
- f) consumer communications and support.

By using a certified product or service, parents/carers will have confidence in the ability of the access control system to:

- a) block inappropriate content (see Clause 4);
- b) block communications via Internet-based services that are inappropriate (see Clause 5);
- c) prevent unauthorized users from changing or disabling the access control settings (see Clause 6);
- d) provide an appropriate level of protection (as specified by this PAS) upon implementation/installation either through the use of default settings or configuration in accordance with user documentation (see Clause 7);
- e) configure the product or service where such a capability is offered (see Clause 8);
- f) remain up to date (within the terms of any licensing or subscription requirements) (see Clause 9).

Furthermore, where the access control system can be installed, parents/carers will have confidence in their ability to uninstall/remove the product or service (see Clause 10).

By using a certified product or service, parents/carers will:

- a) have confidence in the ability to obtain suitable system support should they encounter problems with implementing, maintaining or installing/removing the access control system (see Clause 11);
- b) have confidence in the level and quality of information they will receive in the product description and user documentation provided with the product or service and will have confidence in the quality of the instructions to enable them to effectively install and configure the access control system to an effective level of protection (see Clause 12);
- c) have access to user education materials providing information and links to information that enable parents/carers and children to stay informed of the issues and risks of using the Internet (see Clause 13).

2 Terms and definitions

For the purposes of this Publicly Available Specification, the following terms and definitions apply.

2.1 access control system

software product or service, including user documentation, designed to provide safeguards against inappropriate content and contact when using the Internet and/or related technologies through a process of filtering and blocking

NOTE Although this term is primarily used within this PAS to describe software used on a computer, access control systems can apply to any type of communications device providing access to Internet-based content and services, such as mobile phones, handheld devices and Internet-enabled games consoles.

2.2 blocking

prevention of access to content or services in its entirety (e.g. chat)

2.3 certification body

third-party body contracted to provide certification to a customer

2.4 chat

real time communication between two or more users over the Internet in virtual meeting places or chat rooms (see also 2.13)

2.5 communication

any process where data (such as messages, files or administration information) is conveyed between computer systems

2.6 content

any material, such as text, images, sound, animation or video, which can be accessed or received using the Internet

2.7 email

system of sending messages (which may include text, images, sound, animation or video) over the Internet for immediate or later retrieval

2.8 end user

person who is protected by the access control system

NOTE It is anticipated that in most instances the end user will be a child, young person or vulnerable adult, but if the access control system or system software allows for multiple user accounts to be created it could be any person using the computer/device.

2.9 filtering

selective blocking of content (e.g. web pages) against specified criteria

2.10 hate material

material which promotes hatred and intolerance (see also **2.25** and **B.3**)

2.11 inappropriate content

material which, while not illegal, may not be considered suitable for a particular person

NOTE The content covered by this definition are listed in Annex B.

2.12 inexperienced user

person who has basic IT skills considered to include a basic knowledge of navigating an operating system, system desktop (user interface) and running productivity tools, but includes little to no experience of configuring system changes for both hardware and software

NOTE It is assumed that the parent/carer is an inexperienced user (see 2.19).

2.13 instant message

collaborative messaging system which allows communication and sharing of files in real time over the Internet (see also chat), usually one-to-one

2.14 Internet

global interconnected network of networked computers, providing an infrastructure through which applications such as web browsing, email, chat and instant messaging operate

2.15 Internet Service Provider

provider of Internet services such as Internet connectivity and web site hosting

2.16 manufacturer

organization which develops the access control system

2.17 newsgroup

area categorized by its subject on Usenet, where users can post or read comments about that subject

2.18 overblocking

prevention of access to acceptable content as a result of the controls imposed by an access control system

2.19 parent/carer

person who authorizes the implementation and configuration of the access control system

NOTE 1 It is anticipated that in most instances the local administrator will be a parent (or other responsible adult) who wishes to provide access controls on a computer or other Internet-enabled device within the home setting.

NOTE 2 It is assumed that the parent/carer is an inexperienced user (see 2.12).

2.20 post, posting

process of contributing to a forum or newsgroup or publishing comments or other material, typically on a website which is viewable by others

2.21 product description

readily accessible information stating the properties of the access control system

NOTE The product description can help potential consumers evaluate the suitability of the product before purchasing it.

2.22 product packaging

physical wrapping of a software product, or point of download for software products downloaded from the Internet

2.23 product/service type A

access control system providing default settings enabling parents/carers to provide defined levels of end user protection

2.24 product/service type B

access control system requiring full configuration of the access control settings thereby providing the parent/carer with the ability to configure access control system to provide user defined levels of end user protection

2.25 racist material

material which promotes hatred and intolerance on the basis of race (see also **2.10** and **B.3**)

2.26 software product

set of computer programs, procedures, and possibly associated documentation and data

2.27 system support provider

organization that provides technical support to consumers and parents/carers of the access control system

NOTE 1 This will not necessarily be the manufacturer of the product.

NOTE 2 System support may be provided via various means such as email, Internet-based forms, or telephone.

NOTE 3 It is not anticipated that end users seek support from system support providers.

2.28 system support

act of maintaining the access control system and its user documentation in a functional state

2.29 Usenet

collection of user-submitted notes, messages and binary files on various subjects that are posted to servers on a worldwide network

NOTE Users post to these newsgroups which are then distributed to other Usenet servers connected to the Internet.

2.30 user documentation

complete set of documents, available in print or electronic form, that provides information on the installation, configuration, use and maintenance of the access control system

2.31 user education material

material intended for use by both parents/carers and those for whom they are responsible that explains the purpose, function and limitations of access control systems

2.32 virus

program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down

2.33 web-based chat

system that allows two or more logged-in users to take part in a synchronous, text-based communication, typed in real-time, across the Internet

2.34 webcam

real time camera whose images can be accessed using Internet browser applications, instant messaging applications, video calling applications either continuously or at regular intervals dependent on application

2.35 web forum

online discussion group

NOTE Online services and bulletin board services provide a variety of forums, in which participants with common interests can exchange open messages.

3 Abbreviations

For the purposes of this PAS, the following abbreviations apply.

3.1 FAQs

Frequently Asked Questions

3.2 FTP

File Transfer Protocol

3.3 FTPS over SSL

Secure File Transfer Protocol with SSL security

3.4 HTTP

Hyper Text Transfer Protocol

3.5 IRC

Internet Relay Chat

3.6 P2P

Peer to Peer

3.7 PIN

Personal Identification Number

3.8 SSL

Secure Socket Layout

3.9 VoIP

Voice over Internet Protocol

4 Internet-based content

4.1 General

For purposes of compliance manufacturers shall apply the mandatory requirements applicable to their specific product/service type (see 4.2.1 and 4.2.2).

NOTE The criteria used for checking compliance for products and services offered for third-party conformity testing under Clause 4 are listed in Annex C.

4.2 Mandatory requirements

4.2.1 Product/service type A – access control system providing default settings

For the purposes of compliance with PAS 74, 4.2.1 shall be supported by detailed user implementation/installation instructions to ensure the default settings of the access control system are implemented/installed in compliance with third-party conformity testing (see 12.2.3.2).

4.2.1.1 As a default, the access control system shall block inappropriate content.

NOTE For the purposes of this PAS, this is deemed to be content as defined by the categories listed in Annex B.

4.2.1.2 The access control system shall not overblock access to appropriate Internet-based content.

NOTE For the purposes of this PAS, overblocking is defined by the tests outlined in Annex C.

4.2.1.3 The access control system shall provide parents/carers with the ability to access all Internet-based content.

NOTE This should not override any mandatory filtering of illegal Internet content provided by the Internet Service Provider (ISP).

4.2.1.4 The access control system shall allow parents/carers to completely block access to Internet-based content.

4.2.1.5 The access control system shall provide the parent/carer with the ability to apply the default settings of the access control system to specified user accounts.

4.2.2 Product/service type B – access control system requiring full configuration of settings

4.2.2.1 For the purposes of compliance with PAS 74, 4.2.2 shall be supported by detailed user installation/configuration instructions to ensure the access control system can be configured to an appropriate level of protection in compliance with third-party conformity testing (see 12.2.3.3).

4.2.2.2 The access control system shall provide parents/carers with the ability to configure access control settings against specified system/device user accounts.

4.2.2.3 The access control system shall provide parents/carers with the ability to block inappropriate content.

NOTE For the purposes of this PAS, this is deemed to be content as defined by the categories listed in Annex B.

4.2.2.4 The access control system shall not overblock access to appropriate Internet-based content.

NOTE For the purposes of this PAS, overblocking is defined by the tests outlined in Annex C.

4.2.2.5 The access control system shall provide parents/carers with the ability to access all Internet-based content otherwise accessible through their Internet Service Provider.

NOTE This should not override any mandatory filtering of illegal Internet-based content provided by the Internet Service Provider (ISP).

4.2.2.6 The access control system shall provide parents/carers with the ability to completely block access to Internet-based content.

4.2.2.7 The access control system shall provide the parent/carer with the ability to configure the access control system to provide or deny access to Internet-based content following clear prompts and instructions as defined in Clause 12.

5 Internet-based communications

5.1 General

For purposes of compliance manufacturers shall apply the mandatory requirements applicable to their specific product/service type (see 5.2.1 and 5.2.2).

NOTE The criteria used for checking compliance for products and services offered for third-party conformity testing under Clause 5 are listed in Annex D.

5.2 Mandatory requirements

Where communication via Internet-based services is possible the following requirements shall be mandatory:

5.2.1 Product/service type A – access control system providing default settings

5.2.1.1 For the purposes of compliance with PAS 74, 5.2.1 shall be supported by detailed user implementation/installation instructions to ensure the default settings of the access control system are implemented/installed in compliance with third-party conformity testing (see 12.2.3.2).

5.2.1.2 The access control system shall block inappropriate Internet-based communication services as defined in Annex E.

5.2.1.3 Where the access control system offers the ability to configure individual user accounts, parents/carers shall have the ability to apply the default settings of the access control system to specified accounts.