BRITISH STANDARD

BS ISO/IEC
14888-1:2008

Information technology — Security techniques — Digital signatures with appendix —

Part 1: General

ICS 35.040

BSI
British Standards

National foreword

This British Standard is the UK implementation of ISO/IEC 14888-1:2008. It supersedes BS ISO/IEC 14888-1:1998 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT — Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

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

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 May 2008

ISBN 978 0 580 54258 9

Amendments/corrigenda issued since publication

Date	Comments

BS ISO/IEC 14888-1:2008

INTERNATIONAL STANDARD

ISO/IEC 14888-1

Second edition
2008-04-15

Information technology — Security techniques — Digital signatures with appendix —

Part 1: General

Technologies de l'information — Techniques de sécurité — Signatures numériques avec appendice —

Partie 1: Généralités

Reference number
ISO/IEC 14888-1:2008(E)

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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

ISO/IEC 14888-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 14888-1:1998), which has been technically revised.

ISO/IEC 14888 consists of the following parts, under the general title *Information technology — Security techniques — Digital signatures with appendix*:

— *Part 1: General*

— *Part 2: Integer factorization based mechanisms*

— *Part 3: Discrete logarithm based mechanisms*

Introduction

Digital signature mechanisms are asymmetric cryptographic techniques which can be used to provide entity authentication, data origin authentication, data integrity and non-repudiation services. There are two types of digital signature mechanisms:

— When the verification process needs the message as part of the input, the mechanism is called a "signature mechanism with appendix". A hash-function is used in the calculation of the appendix.

— When the verification process reveals all or part of the message, the mechanism is called a "signature mechanism giving message recovery". A hash-function is also used in the generation and verification of these signatures.

Signature mechanisms with appendix are specified in ISO/IEC 14888. Signature mechanisms giving message recovery are specified in ISO/IEC 9796. Hash-functions are specified in ISO/IEC 10118.

blank

Information technology — Security techniques — Digital signatures with appendix —

Part 1: General

1 Scope

ISO/IEC 14888 specifies several digital signature mechanisms with appendix for messages of arbitrary length.

This part of ISO/IEC 14888 contains general principles and requirements for digital signatures with appendix. It also contains definitions and symbols which are used in all parts of ISO/IEC 14888.

Various means are available to obtain a reliable copy of the public verification key, e.g., a public key certificate. Techniques for managing keys and certificates are outside the scope of ISO/IEC 14888. For further information, see ISO/IEC 9594-8 [4], ISO/IEC 11770-3 [3] and ISO/IEC 15945 [5].

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.

None.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
appendix
string of bits formed by the signature and an optional text field

3.2
collision-resistant hash-function
hash-function satisfying the following property: it is computationally infeasible to find any two distinct inputs which map to the same output

NOTE Computational feasibility depends on the specific security requirements and environment.

[ISO/IEC 10118-1]

3.3
data element
integer, bit string, set of integers or set of bit strings

3.4
domain
set of entities operating under a single security policy

EXAMPLES public key certificates created by a single authority or by a set of authorities using the same security policy

3.5
domain parameter
data element which is common to and known by or accessible to all entities within the domain

3.6
hash-code
string of bits which is the output of a hash-function

[ISO/IEC 10118-1]

3.7
hash-function
function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties:

— for a given output, it is computationally infeasible to find an input which maps to this output;

— for a given input, it is computationally infeasible to find a second input which maps to the same output

NOTE 1 Computational feasibility depends on the specific security requirements and environment.

NOTE 2 This definition of hash-function is referred to as one-way hash-function.

[ISO/IEC 10118-1]

3.8
identification data
sequence of data elements, including the distinguishing identifier for an entity, assigned to an entity and used to identify it

NOTE The identification data may additionally contain data elements such as identifier of the signature process, identifier of the signature key, validity period of the signature key, restrictions on key usage, associated security policy parameters, key serial number, or domain parameters.

3.9
key pair
pair consisting of a signature key and a verification key, i.e.,

— a set of data elements that shall be totally or partially kept secret, to be used only by the signer;

— a set of data elements that can be totally made public, to be used by any verifier

3.10
message
string of bits of any length

3.11
parameter
integer, bit string or hash-function

3.12
signature
one or more data elements resulting from the signature process

3.13
signature key
set of private data elements specific to an entity and usable only by this entity in the signature process

NOTE Sometimes called a private signature key in other standards, e.g. ISO/IEC 9796-2, ISO/IEC 9796-3 and ISO/IEC 9798-3.

3.14
signature process
process which takes as inputs the message, the signature key and the domain parameters, and which gives as output the signature

3.15
signed message
set of data elements consisting of the signature, the part of the message which cannot be recovered from the signature, and an optional text field

NOTE In the context of this part of ISO/IEC 14888, the entire message is included in the signed message and no part of the message is recovered from the signature.

3.16
verification key
set of public data elements which is mathematically related to an entity's signature key and which is used by the verifier in the verification process

NOTE Sometimes called a public verification key in other standards, e.g. ISO/IEC 9796-2, ISO/IEC 9796-3 and ISO/IEC 9798-3.

3.17
verification process
process which takes as input the signed message, the verification key and the domain parameters, and which gives as output the result of the signature verification: valid or invalid

4 Symbols, conventions, and legend for figures

4.1 Symbols

Throughout all parts of ISO/IEC 14888 the following symbols are used.

H hash-code

K randomizer

M message

R first part of a signature

NOTE First part of a signature R is alternatively called a witness.

$\overline{R}$ recomputed first part of a signature

S second part of a signature

X signature key

Y verification key

Z set of domain parameters

Σ signature

$A \bmod N$ the unique integer B from 0 to $N-1$ so that N divides $A-B$

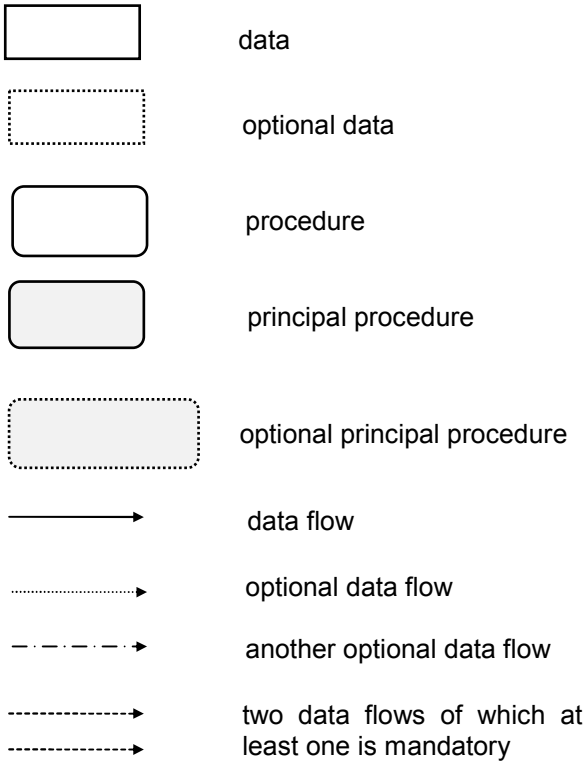
$A \equiv B \pmod{N}$ Integer A is congruent to integer B modulo N, i.e. $(A-B) \bmod N = 0$.

4.2 Coding convention

All integers in all parts of ISO/IEC 14888 are written with the most significant digit (or bit, or byte) in the leftmost position.

4.3 Legend for figures

The following legend for figures is used in all parts of ISO/IEC 14888.



5 General

The mechanisms specified in ISO/IEC 14888 are based upon asymmetric cryptographic techniques. Every asymmetric digital signature mechanism involves three basic operations.

— A process for generating pairs of keys, where each pair consists of a signature key and the corresponding verification key.

— A process using the signature key called the signature process.

- When, for a given message and signature key, the probability of obtaining the same signature twice is negligible, the operation is probabilistic.

- When, for a given message and signature key, all the signatures are identical, the operation is deterministic.

— A process using the verification key called the verification process.

The verification of a digital signature requires the signer's verification key. It is thus essential for a verifier to be able to associate the correct verification key with the signer, or more precisely, with (parts of) the signer's identification data. If this association is somehow inherent in the verification key itself, the scheme is said to be "identity-based". If not, the association between the correct verification key with the signer's identification data shall be provided by a certificate for the verification key. The scheme is then said to be "certificate-based".

6 General model

A digital signature mechanism with appendix is defined by the specification of the following processes:

— key generation process;

— signature process;

— verification process.

In the signature process, the signer computes a digital signature for a given message. The signature, together with an optional text field, forms the appendix, which is appended to the message to form the signed message.

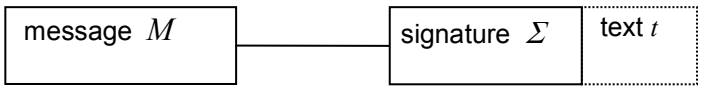


Figure 1 — Signed message

Depending on the application, there are different ways of forming the appendix and associating it with the message. The general requirement is that the verifier is able to relate the correct signature to the message.

For successful verification it is also essential that, prior to the verification process, the verifier is able to associate the correct verification key with the signature. The optional text field can be used for transmitting the signer's identification data or an authenticated copy of the signer's verification key to the verifier. In some cases the signer's identification data may need to be part of the message M, so that it is protected by the signature.

A digital signature mechanism shall satisfy the following requirements:

— Given only the verification key and not the signature key it is computationally infeasible to produce any message and a valid signature for this message.

— The signatures produced by a signer can neither be used for producing any new message and a valid signature for this message nor for recovering the signature key.

— It is computationally infeasible, even for the signer, to find two different messages with the same signature.

NOTE Computational feasibility depends on the specific security requirements and environment.

7 Options for binding signature mechanism and hash-function

Use of the signature schemes specified in this standard requires the selection of a collision-resistant hash-function. There shall be a binding between the signature mechanism and the hash-function in use. Without such a binding, an adversary might claim the use of a weak hash-function (and not the actual one) and thereby forge the signature.

There are various ways to accomplish this binding. The following options are listed in order of increasing risk.

a) Require a particular hash-function when using a particular signature mechanism. The verification process shall exclusively use that particular hash-function;

b) Allow a set of hash-functions and explicitly indicate the hash-function in use in the certificate domain parameters. Inside the certificate domain, the verification process shall exclusively use the hash-function indicated in the certificate. Outside the certificate domain, there is a risk arising from certification authorities (CAs) that may not adhere to the user's policy. If, for example, an external CA creates a certificate permitting other hash-functions, then signature forgery problems may arise. In such a case a misled verifier may be in dispute with the CA that produced the other certificate;

c) Allow a set of hash-functions and indicate the hash-function in use by some other method, e.g., an indication in the message or a bilateral agreement. The verification process shall exclusively use the hash-function indicated by the other method. However, there is a risk that an adversary may forge a signature using another hash-function.

NOTE The 'other method' referred to in item c) immediately above could be in the form of a hash-function identifier which explicitly indicates in a signature in the form of hash-token, a concatenation of a hash-code and a hash-function identifier. If the hash-function identifier is included in this way then an attacker cannot fraudulently reuse an existing signature with a different message, even when the verifier could be persuaded to accept signatures created using a hash-function sufficiently weak that pre-images can be found. However, as discussed in detail in [1] (see also Annex A), using the weak hash-function, an attacker can still find a valid signed message by randomly generating signatures containing the identifier of the weak hash-function.

The user of a digital signature mechanism should conduct a risk assessment considering the costs and benefits of the various alternative means of accomplishing the required binding. This assessment should include an assessment of the cost associated with the possibility of a bogus signature being produced.

8 Key generation

The key generation process of a digital signature mechanism consists of the following two procedures:

— generating domain parameters,

— generating signature key and verification key.

The first procedure is executed once when the domain is set up. The second procedure is executed for each signer within the domain and the outputs are the signature key X and the verification key Y. For a specific set of domain parameters, a value of X, which is different with overwhelming probability from values used previously, shall be used.

NOTE Validation of domain parameters and keys may be required. However, it is outside the scope of this standard.

9 Signature process

9.1 General

The following data elements are required for the signature process:

— domain parameters Z;

— signature key X;

— message M;

— hash-function identifier *hid* (optional);

— other text t (optional).

The hash-function identifier can be used for binding the signature mechanism and the hash-function, see Clause 7.

The signature process of a digital signature mechanism with appendix consists of the following procedures:

— computing signature;

— constructing appendix;

— constructing signed message.

9.2 Computing the signature

The inputs to this procedure are the message M, the signature key X and the domain parameter Z. The output of this step is the signature Σ consisting of the first part of signature R and, depending upon the mechanism, the second part of signature S, see Figure 2.

9.3 Constructing the appendix

The appendix is constructed from the signature and an optional text field, ***text***, as (Σ, t). The text field could include a certificate that cryptographically ties the verification key to the identification data of the signer.

NOTE Depending on the application, there are different ways of forming the appendix and appending it to the message. The general requirement is that the verifier is able to relate the correct signature to the message. For successful verification, it is also essential that prior to the verification process, the verifier is able to associate the correct verification key with the signature.

9.4 Constructing the signed message

The signed message consists of message M and the appendix, i.e., M, (Σ, t).

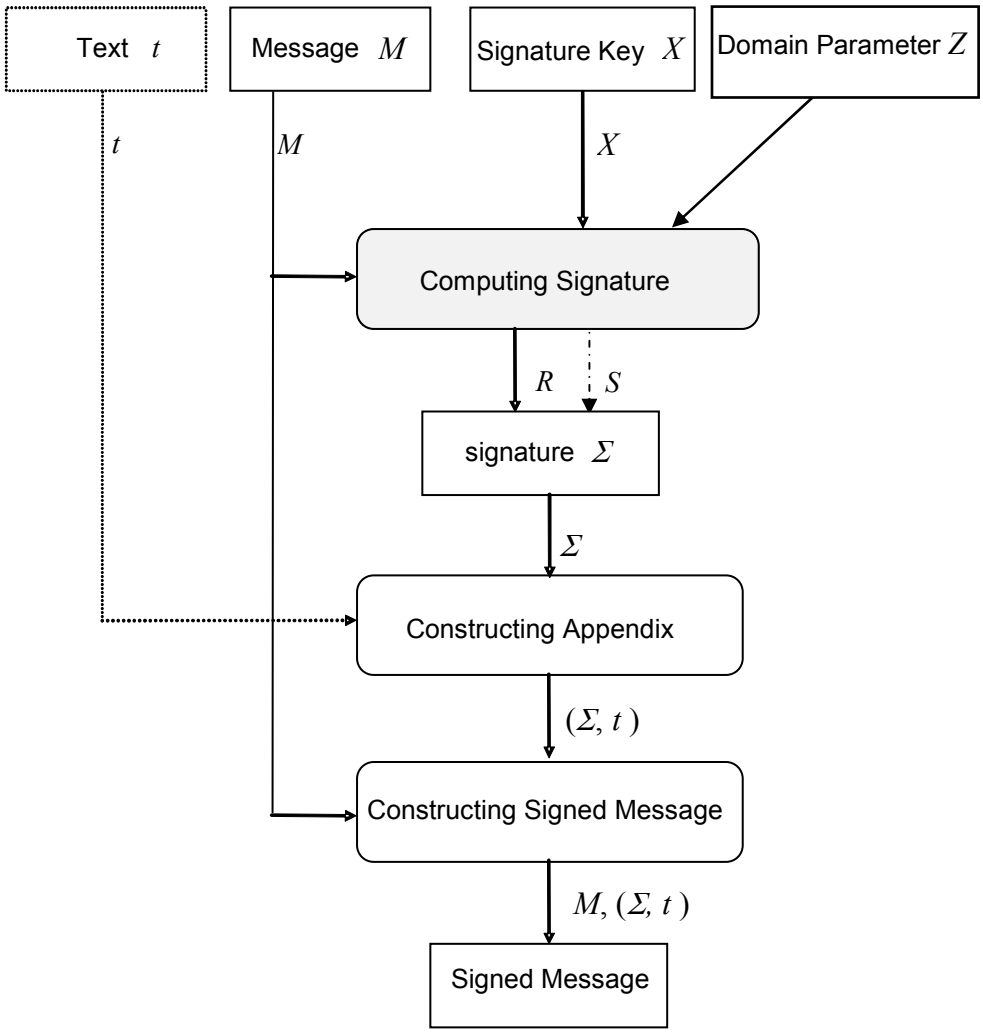


Figure 2 — Signature process

10 Verification process

The following data elements are required for the verification process:

— domain parameters Z;

— verification key Y;

— message M;

— signature Σ;

— identification data Id (optional);

— identifiers of the hash-functions in use hid, if not uniquely determined by other means (see Clause 7);

— other text t (optional).

The verification process takes as inputs, the message M, the domain parameter Z, the verification key Y, the signature Σ and depending upon the mechanism the identification data Id. The outputs of this process is a Boolean value *Yes* (*Accept*) or *No* (*Reject*) as shown in Figure 3. Computing verification function consists of one of the following combination of functions:

a) signature opening, hashing and comparing;

b) signature opening, representative recovery and checking the recovered representative;

c) retrieving witness, retrieving assignment, recomputing pre-signature, recomputing witness and verifying witness.

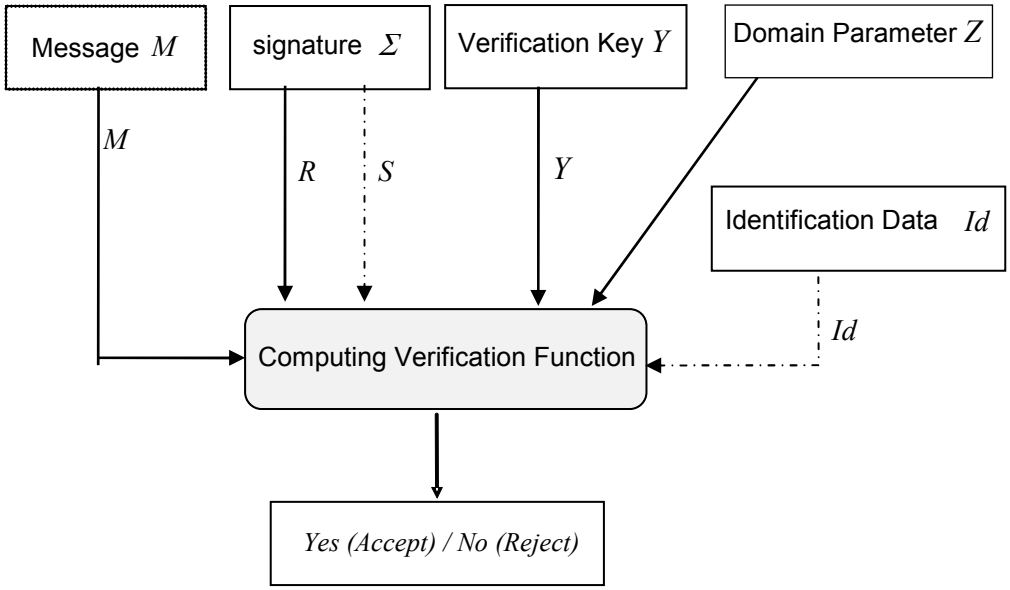


Figure 3 — Verification process

Annex A
(informative)

On hash-function identifiers

As specified in clause 7, users of signature schemes specified in this standard should select a collision resistant hash-function. It is important that the verifier has an unambiguous way of determining which hash-function was used to generate a signature, in order that the verification process can be carried out securely. If a malicious third party could persuade a verifier that a 'weak' hash-function had been used to generate a signature (e.g. a hash-function which lacks the one-way property), then this third party could persuade the verifier that a valid signature actually applies to a 'false' message.

ISO/IEC 14888 allows a "hash-token", a hash-function identifier concatenated to a hash-code, to specify a hash-function in use in every signature to accomplish the necessary binding. If the hash-function identifier is included in this way then an attacker cannot fraudulently reuse an existing signature with a different message, even when the verifier could be persuaded to accept signatures created using a hash-function sufficiently weak that pre-images can be found. This was thought to solve the problem referred to in the previous paragraph.

However, as discussed in detail in [1], even if a hash-function identifier is included in the signature in the form of a hash-token, other attacks are possible if a verifier can be persuaded that a 'weak' hash-function has been employed. By weak here we mean a hash-function which lacks the one way property, i.e. given a hash-code it is computationally feasible to find an input string which is mapped to this hash-code by the hash-function. (Note that it is precisely this type of weakness that first motivated the inclusion of a hash-function identifier in the signature in the form of hash-token).

The attacks described in [1] operate in the following two general ways.

a) In a case that the attacker has total control over the value of hash-token in a signature, the attacker can embed a hash-function identifier of a weak hash-function in a randomly generated signature. Then, the attacker inverts the weak hash-function and gets a message M. In this case, forging the signature may be possible even if the hash-function is only weak for some particular hash-value.

b) In a case that long hash-function identifier is allowed, the attacker generates a random signature and computes a message representative T, a bit string computed from a signature using a verification key. If one of T is formatted correctly as $T = Pad \,||\, HID \,||\, H,$ where Pad is a constant bit string, HID is random but syntactically correct hash-function identifier and H is a hash-code. Then, the attacker will invert the weak hash-function to get a message M from H. If the length of Pad is not enough long and the long HID is allowed, the odds of this happening is not negligible. Even in this case, however, the attacker has to convince the verifier to use the new randomly generated but syntactically correct hash-function identifier.

Given such a 'signature', the attacker now takes the hash-code embedded in the signature or in the recovered message representative and, using the fact that the hash-function is weak, discovers a message, which hashes to the desired hash-code. That is, the attacker can forge a new signature. Hence the concatenation of a hash-function identifier with a hash-code does not always avoid the need for the verifier to have a secure independent means of knowing which hash-function to use to verify the signature.

Most of digital signature schemes in ISO/IEC 14888 require to specify the hash-function in use in the domain parameter (as specified in Clause 7 a), or mechanisms themselves specify particular hash-functions (as specified in Clause 7 b). The user of a digital signature mechanism should conduct a risk assessment considering the costs and benefits of the various alternatives. This assessment includes the cost associated with the possibility of a bogus signature being produced.

Bibliography

[1] B. Kaliski, *On hash function firewalls in signature schemes*, in Proc. Cryptographers' Track RSA Conference 2002, B. Preneel, Ed, Lecture Notes in Computer Science, Vol. 2271, pp. 1-16, Berlin, Springer-Verlag, 2002

[2] ISO/IEC 9796 (all parts), *Information technology — Security techniques — Digital signature scheme giving message recovery*

[3] ISO/IEC 11770-3, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*

[4] ISO/IEC 9594-8:2001, *Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks*

[5] ISO/IEC 15945:2002, *Information technology — Security techniques — Specification of TTP services to support the application of digital signatures*

[6] ISO/IEC 10118 (all parts), *Information technology — Security techniques — Hash-functions*

BSI — British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Tel: +44 (0)20 8996 9000. Fax: +44 (0)20 8996 7400.

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: +44 (0)20 8996 9001. Fax: +44 (0)20 8996 7001. Email: orders@bsi-global.com. Standards are also available from the BSI website at http://www.bsi-global.com.

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library and its Technical Help to Exporters Service. Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre. Tel: +44 (0)20 8996 7111. Fax: +44 (0)20 8996 7048. Email: info@bsi-global.com.

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration. Tel: +44 (0)20 8996 7002. Fax: +44 (0)20 8996 7001. Email: membership@bsi-global.com.

Information regarding online access to British Standards via British Standards Online can be found at http://www.bsi-global.com/bsonline.

Further information about BSI is available on the BSI website at http://www.bsi-global.com.

Copyright

BSI
389 Chiswick High Road
London
W4 4AL