BS ISO 16609:2012

BSI Standards Publication

Financial services — Requirements for message authentication using symmetric techniques

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of ISO 16609:2012. It supersedes BS ISO 16609:2004 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/12, Financial services.

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.

ISBN 978 0 580 72179 3

ICS 35.240.40

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 31 March 2012.

Amendments issued since publication

Date	Text affected

BS ISO 16609:2012

INTERNATIONAL STANDARD

ISO 16609

Second edition
2012-03-15

Financial services — Requirements for message authentication using symmetric techniques

Services financiers — Exigences pour l'authentification des messages utilisant des techniques symétriques

Reference number
ISO 16609:2012(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member 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 shall not be held responsible for identifying any or all such patent rights.

ISO 16609 was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Financial services, security*.

This second edition cancels and replaces the first edition (ISO 16609:2004), which has been technically revised.

Introduction

A MAC (message authentication code) is a data field used to verify the authenticity of a message, generated by the sender of the message and transmitted together with it. The MAC enables an intended recipient to detect whether the message has been altered. While non-keyed message integrity methods, e.g. checksums, only protect against accidental alteration of the message, MACs additionally protect against deliberate alteration since the adversary would not have access to the key used to generate the MAC.

This International Standard has been prepared so that institutions involved in financial services activities wishing to implement message authentication can do so in a manner that is secure and facilitates interoperability between separate implementations.

This International Standard identifies ciphers, hash functions and algorithms from ISO 9797 (all parts) that are specifically approved for secure banking purposes.

INTERNATIONAL STANDARD ISO 16609:2012(E)

Financial services — Requirements for message authentication using symmetric techniques

1 Scope

This International Standard specifies procedures, independent of the transmission process, for protecting the integrity of transmitted banking messages and for verifying that a message has originated from an authorized source. A list of block ciphers approved for the calculation of a message authentication code (MAC) is also provided. The authentication methods it defines are applicable to messages formatted and transmitted both as coded character sets and as binary data.

This International Standard is designed for use with symmetric algorithms where both sender and receiver use the same key. It does not specify methods for establishing the shared key, nor does it provide for encipherment for the protection of messages against unauthorized disclosure. Its application will not protect the user against internal fraud perpetrated by the sender or the receiver, nor against forgery of a MAC by the receiver.

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.

ISO/IEC 9797-1:2011, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

ISO/IEC 9797-2, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 2: Mechanisms using a hash-function*

ISO 11568-1, *Banking — Key management (retail) — Part 1: Principles*

ISO 11568-2, *Financial services — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle*

3 Terms and definitions

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

3.1
algorithm
specified mathematical process for computation or set of rules which, if followed, will give a prescribed result

3.2
authentication
process used between a sender and a receiver to ensure data integrity and provide data origin authentication

3.3
authentication algorithm
algorithm used, together with an authentication key and one or more authentication elements, for authentication

3.4
authentication element
message element that is to be protected by authentication

3.5
authentication key
cryptographic key used for authentication

3.6
beneficiary
ultimate party to be credited or paid as a result of a transfer

NOTE There can be more than one beneficiary.

3.7
block cipher
algorithm for computing a function which maps a fixed-length string of bits and a secret key to another string of bits with the same fixed length

3.8
checksum
fixed-length string of bits calculated from a message of arbitrary length, such that it is unlikely that a change of one or more bits in the message will produce the same string of bits, thereby aiding detection of accidental modification

3.9
cryptoperiod
defined period of time during which a specific cryptographic key is authorized for use or during which the cryptographic keys in a given system may remain in effect

3.10
data integrity
property pertaining to data that has not been altered or destroyed in an unauthorized manner

3.11
DMC
date MAC computed
date on which the sender computed the MAC (message authentication code)

NOTE The DMC can be used to synchronize the authentication process through selection of the proper key.

3.12
data origin authentication
corroboration that the source of data received is as claimed

3.13
encipherment
(reversible) transformation of data by a cryptographic algorithm with a cryptographic key in order to produce ciphertext, i.e. to hide the information content of the data

3.14
identifier for authentication key
IDA
field that identifies the key to be used in authenticating the message

3.15
MAC
message authentication code
fixed-length string of bits used to verify the authenticity of a message, generated by the sender of the message, transmitted together with the message, and verified by the receiver of the message

3.16
MAC algorithm
keyed cryptographic algorithm that produces a fixed-length string of bits (the MAC) from a message of arbitrary length, such that it is not feasible to compute the MAC without knowledge of the key

3.17
message element
contiguous group of bytes designated for a specific purpose

3.18
MID
message identifier
systems trace audit number (deprecated)
field used uniquely to identify a financial message or transaction (e.g. sending bank's transaction reference) within a given context (e.g. DMC)

NOTE In ISO 8583, the MID was referred to as the systems trace audit number (STAN), which it supersedes.

3.19
message text
information conveyed or transmitted between sender and receiver, excluding header and trailer information used for transmission purposes

3.20
receiver
party intended to receive the message

3.21
sender
party responsible for, and authorized to, send a message

3.22
value date
date on which funds are to be at the disposal of the beneficiary

4 Protection

4.1 Protection of authentication keys

Authentication keys are secret cryptographic keys that have been previously established by the sender and receiver and which are used by the authentication algorithm. Keys shall be managed in accordance with ISO 11568-1 and ISO 11568-2.

4.2 Authentication elements

The MAC calculation shall include those message elements, as agreed between sender and receiver, which require protection against fraudulent alteration.

Subject to bilateral agreement, the MAC calculation may also cover data elements not transmitted in the message (e.g. padding bits or data computable by both parties from information already shared).

The choice of data to be included in the MAC will depend on the specific application. When the following elements appear in a message, they should be included in the calculation of the MAC:

a) transaction amount;

b) currency;

c) identifier for authentication key (IDA);

d) identification of payer and beneficiary and/or, if appropriate, their payment agent's value date;

e) message identifier;

f) date and time;

g) indication as to the disposition of the transaction.

NOTE Integrity protection applies only to the selected authentication elements. Other parts of the message can be subject to undetected alterations. It is important that users ensure the integrity of data presentation.

4.3 Detection of duplication, loss or sequence errors

A mechanism should be implemented to detect duplication or loss, or messages arriving out of sequence. Without recourse to further message exchanges, the recipient may only detect the replay of a previous transaction if able to identify transactions uniquely, and should then check that such unique identifying information has not already occurred. To detect sequence errors, messages should be identifiable as being in a sequence. Furthermore, in order to detect loss, transactions should be identifiable as being in a defined sequence, predictable by the recipient. These conditions are achieved by involving in the MAC computation some elements (i.e. message elements or key elements) that are unique to the transaction and that relate it uniquely to the previous transaction. This may be achieved in one of the following ways.

a) Include in the MAC calculation a unique transaction reference that does not repeat within the lifetime of the system. To detect loss, the reference would need to change in a defined sequence that is known by the recipient who calculates this value and compares it to the received value.

EXAMPLE The reference will include sender ID, recipient ID, key ID and transaction number, where the transaction number increases by one for each transaction.

b) Include in the MAC calculation a MID, i.e. a value that does not repeat before either

   — the change of date, i.e. DMC (usable if the date is included in MAC elements), or

   — the expiration of the cryptoperiod of the key used for authentication.

   The MID may consist of a unique sending bank's transaction reference number in a fixed format message as a message identifier. A method of protection is described in Annex A. The MID may either contain the DMC or be a separate field. To simplify detection of loss, the MID could increase in a defined sequence.

c) Use a unique key per transaction where the key of one transaction is derived from that of the previous transaction (see ISO 11568-2).

d) Combine the above techniques.

5 Procedures for message authentication

5.1 MAC generation

The sender of a message shall generate a MAC by processing in an agreed order (e.g. the sequence in which they appear in the message) those authentication elements of the transmitted message that are to be protected by an approved authentication mechanism (see 4.2). The mechanism shall be activated by means of an authentication key, which is a secret between the two correspondents. This process creates the MAC, which shall then be included with the original message text.

5.2 MAC placement

The MAC shall be either

a) placed in the message, in an additional field specified for the transport of the MAC, or

b) appended to the data portion of the message, if there is no specified MAC field.

Where the field allocated has a length, for transport, greater than the MAC length, the MAC shall be positioned by left-justifying it within the field.

5.3 MAC verification

On receipt of the message, the receiver shall compute a reference MAC using the authentication elements, an identical authentication key and an identical algorithm. Authenticity of the content of the authentication elements and the message source shall be considered to have been confirmed when the receiver's computed reference MAC agrees with that received with the message text.

A received MAC is not included in the algorithm computation.

The process of generating the MAC is sensitive to the sequence in which the authentication elements are processed (i.e. a change in the sequence of authentication elements after the MAC is generated will result in a failure to authenticate).

5.4 Approved authentication mechanisms based on ISO/IEC 9797

5.4.1 General

The MAC algorithm shall be one of those specified in ISO/IEC 9797-1 or ISO/IEC 9797-2.

5.4.2 Approved authentication mechanisms based on ISO/IEC 9797

ISO/IEC 9797-1 specifies six MAC algorithms that use a secret key and an n-bit block cipher to calculate an m-bit MAC, and which are based upon the cipher block chaining (CBC) mode of operation of a block cipher.

— MAC Algorithm 1 is a simple CBC-MAC using a single key.

— MAC Algorithm 2 is a variant on Algorithm 1, with an additional final transformation using a second key.

— MAC Algorithm 3 is a variant on Algorithm 1, ending with two additional transformations, the penultimate transformation uses a second key and the final transformation uses the first key.

— MAC Algorithm 4 is a variant on Algorithm 2, with an additional initial transformation using the second key.

— MAC Algorithm 5 is commonly known as CMAC.

— MAC Algorithm 6 uses two parallel instances of Algorithm 4, and combines the two results with a bit-wise exclusive-OR operation, while doubling the MAC algorithm key length.

The following table shows the authentication mechanisms based on ISO/IEC 9797-1 approved for the generation of MACs for financial services.

Table 1 — Approved algorithms from ISO/IEC 9797-1

ISO/IEC 9797-1 algorithm	ISO/IEC 18033-3 cipher	Key length (bits)	Padding method	MAC length (bits)	Applicable uses
1	AES	128, 192, 256	1	32-128	The length of the message needs to be known to the receiver in order to prevent message forgeries.
3	DEA	112	1	32-64	The length of the message needs to be known to the receiver in order to prevent message forgeries, backward-compatible with ANSI X9.19 and ISO 9807.
1	TDEA	112,168	1	32-64	The length of the message needs to be known to the receiver in order to prevent message forgeries, backward-compatible with ANSI X9.9, ISO 8730 and ISO 8731 (all parts).

Table 1 *(continued)*

ISO/IEC 9797-1 algorithm	ISO/IEC 18033-3 cipher	Key length (bits)	Padding method	MAC length (bits)	Applicable uses
1	TDEA	112,168	3	32-64	The message length is needed prior to starting MAC calculation.
1	AES	128, 192, 256	3	32-128	
3	DEA	112	3	32-64	
1	TDEA	112,168	2	32-64	The recipient need not have prior knowledge of the message length.
1	AES	128, 192, 256	2	32-128	
3	DEA	112	2	32-64	
5 (CMAC)	AES	128, 192, 256	4	32-128	
5 (CMAC)	TDEA	112,168	4	32-64	
Consideration should be given to the selection of MAC length. Short MAC lengths increase the likelihood of successful collision attacks, while full-length MACs calculated over single blocks are potentially susceptible to key recovery attacks if a large number of MACs can be calculated. See ISO/TR 14742 and ISO/IEC 9797-1 for additional information. The security analysis in ISO 9797-1:2011, Annex C provides implementation recommendations for protecting against forgery and key recovery attacks. If Algorithm 1 is used, then steps should be taken to prevent XOR forgery attacks as described in ISO 9797-1:2011, Annex C. An adequate precaution is to use Padding Method 3. If Algorithm 3 is used, then the number of MACs generated using the same key should be restricted. In order not to reduce the lifetime of the MAC-generating device, the use of session keys is recommended. Trivial forgery: if Padding Method 1 is used, then an adversary can typically add to, or delete from, the data string a number of trailing “0” bits without changing the MAC. This implies that Padding Method 1 should only be used in environments where the length of the data string is known to the parties beforehand, or where data strings with a different number of trailing “0” bits have the same semantics.					

5.4.3 Approved authentication mechanisms based on ISO/IEC 9797-2

A MAC algorithm based on ISO/IEC 9797-2 shall be MAC Algorithm 2, commonly known as HMAC. As specified in ISO/IEC 9797-2, HMAC uses a secret key and a hash function (or its round function) with an n-bit result to calculate an m-bit MAC.

The following table shows the authentication mechanisms based on ISO/IEC 9797-2 approved for the generation of MACs for financial services.

Table 2 — Approved algorithms from ISO/IEC 9797-2

ISO/IEC 9797-2 algorithm	ISO/IEC 10118-3 hash function	Key length (bits)	Maximum MAC length (bits)
2 HMAC	RIPEMD-160	160-512	160
	SHA-1	160-512	160
	SHA-256	256-512	256
	SHA-384	384-1 024	384
	SHA-512	512-1 024	512
NOTE For the security of SHA-1, refer to ISO/TR 14742.			

The strength of the message authentication mechanism is dependent on the length, k, (in bits), and secrecy of the key, on the length, n, (in bits), of the hash function and its strength, on the length, m, (in bits), of the MAC, and on the specific algorithm. The probability of a successful guessing attack is the larger of the following:

$$\frac{1}{2^k} \text{ and } \frac{1}{2^m}$$

5.5 Implementation recommendations

One simple criterion for choosing between mechanisms in ISO/IEC 9797-1 and mechanisms in ISO/IEC 9797-2 is the availability of an implementation of the block cipher or hash function. As indicated in Table 1 and Table 2, other criteria will help the appropriate choice of parameters. A security comparison of all the MAC algorithms is provided in ISO/IEC 9797-1 and ISO/IEC 9797-2.

Annex A
(informative)

Protection against duplication and loss using MIDs

A.1 Purpose

Protection against duplication and loss can be accomplished, in accordance with predefined agreements, by using unique-per-transaction message elements, time-variant keys, or other methods. This annex describes methods for detecting duplication and loss of transmitted messages using MIDs in accordance with 4.3. Other methods, including variations of those described in this annex, may also be devised.

A.2 Protection against duplication

A.2.1 Duplicated messages

Duplicated messages can be detected if, under normal operation, the MID from a given sender does not repeat for a given date and a given key. The receiver should check the MID to ensure that it did not appear in a previous message. This check may be performed in one of the following ways.

a) If MIDs are sent in no predetermined order, the receiver may compare the received MID against a list of the MIDs received on that day.

b) If the MIDs for messages authenticated under a particular key are always sent in increasing order, the receiver need only check that the identifiers are strictly increasing.

Other methods, including variations on a) or b), may also be devised.

A.2.2 Multi-party operation

When more than two parties share a common key (multi-party operation), duplication can be detected if each party uses a mutually exclusive portion of the possible MIDs. The receiving party checks that the MID is in the proper range and has not already been received.

A.2.3 Including identities

When the identities of both the sending and receiving parties are included as authentication elements in each message, the receiving party need only check that it is the intended receiver and that the MID has not appeared previously in a message from the sending party. In this case, the entire range of MIDs may be used by each sending and receiving pair, and MIDs may repeat between different pairs.

A.3 Loss detection

Loss of a transmitted message can be detected if both the sending and receiving parties keep a list of all MIDs used at a given time. One party sends its list (via an authenticated message which has duplication protection) to the party wishing to detect any loss. A comparison of the two lists is then performed. Alternatively, if the MIDs are to be received in sequence, the receiver can detect a lost message as soon as an out-of-sequence MID is received. The last MID for a day can be sent to the loss detection party by way of an authenticated message which has duplication protection. Other methods, including variations of those just described, may also be devised.

If it is necessary to ensure that deletion of messages is detected quickly enough (i.e. that silence means that no messages were sent), then null messages or reconciliation messages may be requested or sent at appropriate times.

Annex B
(informative)

General tutorial information

The purpose of message authentication is to ensure that transaction messages are received exactly as originated by the legitimate originator. To accomplish this, message authentication detects both the fraudulent insertion of totally spurious transaction messages, and the fraudulent modification of otherwise legitimate transaction messages.

Message authentication differs from message encipherment in that the latter does not inherently protect against modified transactions, whereas the former not only provides this protection, but provides it on the cleartext message, allowing the message to be comprehended, processed and journalled while still protected. Message authentication is needed to thwart “active wiretapping” and related fraud threats. These are relatively sophisticated threats in which transaction data are modified or inserted in real time, perhaps via a microcomputer system inserted into a communications line. For example, assume that a criminal cuts the communications line from an automatic teller machine (ATM) (which does not use any form of message authentication) to its host, and inserts a microcomputer system in series with this line. To the host, this system “looks” like an idle ATM. To the ATM, this system “looks” like the host. This fraudulently inserted system is programmed to intercept and discard every request-for-cash message originated by the ATM, and to send in response the approval indication. Thus, the criminal can readily “drain” the ATM of cash, yet no account will be debited in the process.

Message authentication thwarts active wiretapping fraud scenarios by appending a message authentication code, or MAC, to each of the transaction messages. This code consists of a number of check digits, which are analogous to a parity check or cyclic redundancy check, except that they are generated via a cryptographic process. The MAC is generated by the originator of the message and is based on the entire message, or upon critical elements of the message, according to prior agreement between the originator and the recipient. (Elements not included in the message but known to both originator and recipient can, by predefined agreement such as this, be included in the MAC computation.) The MAC is included in the transmitted message, then verified by the recipient who holds the same secret key used in the generation process.

Should anyone attempt to modify the protected message elements between the time the MAC is generated and the time it is checked, his/her attempt would be detected. Without knowledge of the secret key, he/she would be unable to generate the correct MAC for the modified message. Similarly, no one can successfully introduce a spurious message because, without the secret key, the proper MAC for this message cannot be generated.

For message authentication to be effective, it is important to ensure the secrecy of the cryptographic key. Preferably, a unique key is used by each communicating pair so that, should the key be compromised, this only jeopardizes the transactions between the two parties and limits accountability to those two parties.

Although message authentication can detect spurious and modified transaction messages, it cannot inherently detect the fraudulent replay of a previously valid message nor the loss of a message. See Annex A for a discussion of these issues.

Message authentication cannot protect against errors in, nor subversion of, the message processing that takes place before the MAC is generated or after it has been verified. For example, it cannot protect against a dishonest merchant that modifies its terminal to indicate one value of the transaction to the customer, while causing the customer’s account to be debited (and the merchant’s account to be credited) by a higher value.

Message authentication can be used effectively by some participants in a retail electronic funds transfer (EFT) system, even if not used by all. Should an institution decide not to implement message authentication, but later become the victim of an active wiretapping fraud scenario, this institution could be made liable for the fraud loss since transaction journals, etc. would indicate where the transaction was fraudulently modified. Thus, each institution participating in the retail EFT system should estimate the implementation cost for message authentication, and the fraud cost for no message authentication, and make its decision accordingly.

Bibliography

[1] ISO 8583, *Financial transaction card originated messages — Interchange message specifications*[1)]

[2] ISO 8730, *Banking — Requirements for message authentication (wholesale)*[2)]

[3] ISO 8731 (all parts), *Banking — Approved algorithms for message authentication*[3)]

[4] ISO 9797-3, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 3: Mechanisms using a universal hash-function*

[5] ISO 9807, *Banking and related financial services — Requirements for message authentication (retail)*[4)]

[6] ISO/TR 14742, *Financial services — Recommendations on cryptographic algorithms and their use*

[7] ISO/IEC 10118-3, *Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions*

[8] ISO/IEC 18033-3, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

[9] ANSI X9.9:1986, *Financial institution message authentication codes (MAC) (wholesale)*[5)]

[10] ANSI X9.19:1996, *Financial institution retail message authentication*[6)]

1) Withdrawn and replaced by ISO 8583-1 and ISO 18245.

2) Withdrawn and replaced by ISO 16609:2004.

3) Withdrawn and replaced by ISO 16609:2004.

4) Withdrawn and replaced by ISO 16609:2004.

5) Withdrawn.

6) Withdrawn.

ICS 35.240.40

Price based on 10 pages

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™