PD ISO/TS 12812-3:2017

BSI Standards Publication

Core banking — Mobile financial services

Part 3: Financial application lifecycle management

bsi.

National foreword

This Published Document is the UK implementation of ISO/TS 12812-3:2017.

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.

Published by BSI Standards Limited 2017

ISBN 978 0 580 82719 8
ICS 03.060

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

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 April 2017.

Amendments/corrigenda issued since publication

Date	Text affected

TECHNICAL SPECIFICATION

ISO/TS 12812-3

First edition
2017-03

Core banking — Mobile financial services —

Part 3: Financial application lifecycle management

Opérations bancaires de base — Services financiers mobiles —
Partie 3: Gestion du cycle de vie des applications financières

Reference number
ISO/TS 12812-3:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 68, *Financial Services*, Subcommittee SC 7, *Core Banking*.

A list of all the parts in the ISO 12812 series can be found on the ISO website.

Introduction

The use of mobile devices to conduct financial services (i.e. payments and banking) is occurring following the steady rise of the number of customers using the Internet for these services. As an evolving market, mobile financial services are being developed and implemented on various bases throughout the different regions of the world and also among the various providers of such services. In these conditions, the purpose of the ISO 12812 series is to facilitate and promote interoperability, security and quality of mobile financial services while making sure that stakeholders in the services can benefit from the evolution, and service providers remain as commercially free and competitive as possible to design their own implementations in pursuing their own business strategies. This document addresses the interoperability only at the technical layer by considering the impact of new components and/or interfaces induced by the introduction of a mobile device in financial services. The intentions of the ISO 12812 series are:

a) to advance interoperability of mobile financial services globally by defining requirements based on a common terminology and basic principles for the design and operation of mobile financial services;

b) to define technical components and their interfaces, as well as roles that may be performed by different actors in addition to mobile financial service providers (e.g. mobile network operators, trusted service managers). These components and their interfaces, as well as roles, are defined according to identified use cases. Future use cases may be considered during the maintenance of the ISO 12812 series;

c) to identify existing standards on which mobile financial services should be based, as well as possible gaps.

Standardization effort in this area is beneficial for a sound development of the mobile financial services market because it will:

— facilitate and promote interoperability between the different components or functions building mobile financial services;

— build a safe environment so that consumers and merchants can trust the service and allow the mobile financial service providers to manage their risks;

— promote consumer protection mechanisms including fair contract terms, rules on transparency of charges, clarification of liability, complaints mechanisms and dispute resolution;

— enable the consumer to choose from different providers of devices or mobile financial services including the possibility to contract with several mobile financial service providers for services on the same device;

— enable the consumer to transfer a mobile financial service from one device to another one (portability);

— promote a consistent consumer experience among various mobile financial services and mobile financial service providers with easy-to-use interfaces.

To achieve these objectives, each part of the ISO 12812 series will specify the necessary technical mechanisms and, when relevant, refer to existing relevant standards as appropriate.

The ISO 12812 series provides a framework flexible enough to accommodate new mobile device technologies, as well as to allow various business models. At the same time, it enables compliance with applicable regulations including data privacy, protection of personally-identifiable data, consumer protection, anti-money laundering and prevention of financial crime.

It is not the intention of the ISO 12812 series to duplicate or to seek to replace any existing standard in the area of mobile financial services (e.g. communication protocols, mobile devices). It is also not the intention of the ISO 12812 series to drive technology to any specific application or to restrict

the development of future technologies or solutions. Messages and data elements to be exchanged at the interfaces between the different components or actors of the system are already specified (e.g. ISO 20022, ISO 8583 (all parts)].

The ISO 12812 series recognizes the need for unbanked or under-banked consumers to access mobile financial services. It also recognizes that these services may be provided by diverse types of institutions in accordance with the applicable regulation(s).

TECHNICAL SPECIFICATION **ISO/TS 12812-3:2017(E)**

Core banking — Mobile financial services —

Part 3:
Financial application lifecycle management

1 Scope

This document specifies the interoperable lifecycle management of applications used in mobile financial services. As defined in ISO 12812-1, an application is a set of software modules and/or data needed to provide functionality for a mobile financial service.

This document deals with different types of applications which is the term used to cover authentication, banking and payment applications, as well as credentials.

Clause 5 describes the basic principles required, or to be considered, for the application lifecycle management.

Because several implementations are possible with impacts on the lifecycle, this document describes the different architectures for the location of the application and the impacts of the different scenarios regarding the issuance of the secure element when present (see Clause 6), the different roles for the management of the application lifecycle and the domains of responsibilities (see Clause 7). It also specifies functions and processes in the application lifecycle management (see Clause 8) and describes scenarios of service models and roles of actors (see Clause 9).

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 12812–1, *Core banking — Mobile financial services — Part 1: General framework*

ISO/TS 12812–2, *Core banking — Mobile financial services — Part 2: Security and data protection for mobile financial services*

ISO/TS 12812–4, *Core banking — Mobile financial services — Part 4: Mobile payments-to-person*

ISO/TS 12812–5, *Core banking — Mobile financial services — Part 1: Mobile payments to business*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 12812-1 and ISO/TS 12812-2 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1
service management roles
set of roles that enable the lifecycle management of the application

4 Abbreviated terms

API	Application Program Interface
IBAN	International Bank Account Number
MFS	Mobile Financial Service
MFSP	Mobile Financial Service Provider
MNO	Mobile Network Operator
MSISDN	Mobile Station International Subscriber Directory Number (the mobile phone number)
NFC	Near Field Communication
OTA	Over The Air
PAN	Primary Account Number
SD Card	Secure Digital Card
SE	Secure Element
SLA	Service Level Agreement
SMS	Short Message Service
STK	SIM Tool Kit
TEE	Trusted Execution Environment
TSM	Trusted Service Manager
UICC	Universal Integrated Circuit Card
USSD	Unstructured Supplementary Services Data

5 Basic principles for application lifecycle management

5.1 General

In order to facilitate a consistent customer experience and to enable interoperability, this clause establishes requirements that apply to and principles that should be considered by the different entities involved in the application lifecycle management.

5.2 Portability of MFSs

The customer shall be able to change the mobile device (provided that the mobile device is compliant with the MFS and enabled to support the application user interface). This requirement implies that an MFSP shall document its compatibility requirements for a mobile device and permit a customer to change the mobile device. This requirement also means that a customer shall be able to download a new application user interface.

When the application is hosted by the UICC, the customer shall be able to switch from one MNO to another while keeping the possibility to use the same application (provided that the relevant arrangements between actors have been set up). This requirement implies that an MFSP shall permit the customer to select any MNO that support the required functionalities for the MFS.

The principle of portability applies also to the other types of secure environments, when the application is hosted by these secure environments.

Additional requirements regarding portability are provided in ISO/TS 12812-4 and ISO/TS 12812-5.

5.3 Entities involved in the application lifecycle management

The entities involved in the application lifecycle management shall comply with functional and security requirements related to the MFS as specified in this document. The implementation of this requirement is under the responsibility of the MFSP.

5.4 Security and privacy

The requirements specified in this document enable the secure deployment and operation of applications by MFSPs.

All parties involved in application lifecycle management shall conform to the security requirements set forth in ISO/TS 12812-2.

Security requirements for applications and their execution environment shall be determined by the MFSP based on a risk analysis and assessment and address in particular the following items depending on the configuration:

a) secure environment such as SE, TEE, secured server;

b) application user interface (display and entry on the keyboard);

c) mobile device;

d) application and its lifecycle management;

e) key management for application lifecycle management.

5.5 Risk assessment

The MFSP shall document the risk assessments used to configure an MFS and retain such information; the assumption is that this documentation should be available if it is required by national regulatory bodies.

5.6 Support of multiple applications and multiple MFSPs

The mobile device shall support the provisioning of multiple applications, as well as applications from multiple MFSPs. The MFSP shall allow the customer to be able to manage these applications (subscription and removal) inasmuch as the mobile device supports appropriate mechanisms allowing the customer to select applications and establish an order of priority.

5.7 User Interface and branding

The customers need to have access to a user friendly and consistent mechanism through their mobile device to select applications. A data structure should be used to represent the application in this user interface. This data structure should contain at least the name of the MFSP, the application name and brands/logos.

5.8 Customer relationship management

Point(s) of contact for the customer shall be clearly defined by the MFSP and any other entities participating in the MFS, with an agreement on their respective roles (for example, in case of loss, theft or questions/support).

5.9 Common APIs

To ensure interoperability of application management processes, entities involved in the application lifecycle management (MFSPs, MNOs, TSM, etc.) should use common APIs between their respective service management information systems.

5.10 Terms of service

The MFSP shall provide to the customer a document for terms of service including rights and obligations to both parties in relation with the application lifecycle management and in relation with applicable regulations.

In that purpose, the Terms of Service document shall address at least the following points:

a) maintenance of applications (embedded or downloaded) to enable customers to gain access to updates, new features, and security patches;

b) a process for an MFSP to terminate an application, including when a business decision has been made not to provide the application after a certain date;

c) a process to enable the customer to remove an application at their discretion;

d) articulation of rights or options a customer has regarding the different steps of the application lifecycle;

e) articulation of rights or options a customer has regarding access to data on past activity;

6 Location of the application

6.1 General

An application is a set of program modules (application software) and/or data (application data) needed to provide functionality for a mobile financial service. The application software and/or application data, including credentials, may be located, accessed and processed either in a mobile device or on a server.

When in a mobile device, the application may be located inside or outside a secure environment. When the application is located on a secured server, the user shall be able to access it through the mobile device. Credentials may be used with an authentication application located in a secure environment.

The user interface enables the customer to interact with the mobile device (see ISO 12812-1) and when applicable, the user interface application is an important feature to be considered in the application lifecycle management (e.g. activation, update).

6.2 Different types of secure environments

Possible secure environments include secure elements (UICC, embedded and removable), trusted execution environment, secured server and software with supplementary security controls. The roles and responsibilities of entities involved in the application lifecycle management are closely related to the type of secure environment (see Clause 9).

This document does not preclude architectures with more than one secure element residing inside the mobile device. In that case, an interoperable mechanism (e.g. API) should be implemented in order to grant access to the different secure elements and their hosted applications (software and/or data).

6.3 Scenarios for mobile proximate payments

For mobile proximate payment, the application may be located in a secure environment of the mobile device (e.g. in a SE hosted in the mobile device) for efficient and secure transactions. However, this document recognizes that the application may be located on a remote secured server.

6.4 Scenarios for mobile remote payments

6.4.1 General

Three scenarios are possible for mobile remote payment: the use of payment credentials or the use of an application or a combination thereof.

6.4.2 Payment credentials

Payment credentials (e.g. PAN, IBAN), which are considered to an application under this document, may be stored securely in the mobile device inside or outside a secure environment or on a remote server. They may be stored, accessed and managed through a mobile wallet.

The storage of payment credentials enables the customer to avoid having to manually enter these data at the time of the transaction. The access to the payment credentials shall be under the control of the customer.

Aliases may be used for the retrieval of payment credentials when located in a server. Examples of aliases include mobile phone number (MSISDN) and e-mail address. Aliases require the enrolment of the customer and the use of a directory to link the alias with the payment credentials.

Payment credentials are static data and may be used with an authentication application located in a secure environment where the authentication application generates dynamic authentication data.

Payment credentials can also be tokenized and stored or accessed on a remote server. Tokenization is the process of replacing payment credentials with values (called payment tokens) that resemble the payment credentials but with less sensitivity.

6.4.3 Application

The application(s) involved in an MFS include(s) authentication functionalities and generation of dynamic transaction data. When the application(s) is/are located on a remote server, the MFSP may require that the credentials of the user be present in the mobile device.

6.5 Scenarios for mobile banking

Several scenarios may be considered for mobile banking. A customer may be able to access mobile banking services:

a) via the Internet browser of the mobile device;

b) through a mobile banking application located in the mobile device; in this scenario, the customer has previously downloaded the application from the website of its financial institution or from an application store;

c) through the use of SMS, unstructured supplementary service data (USSD), SIM Tool Kit (STK) or other available mobile access channel.

An authentication application located in a secure environment with appropriate security controls may be used in order for the financial institution to grant the customer the access to the mobile banking service.

7 Service management roles

7.1 General

As several entities may be involved in the management of an MFS, the service management shall be executed through Service Level Agreements between these entities. Due to the complexity of the service management when a secure element is present, Clause 7 specifically focuses on these configurations.

When applications are located in a secure element, domains of responsibilities and technical roles of the entities providing the service management (such as MFSP or SE provider) shall be defined precisely in order for the MFS to be delivered as smooth as possible to the customer. This is based on the principle that responsibility areas cannot be shared by actors. This approach will avoid issues and conflicts between the MFSP, which has the ultimate responsibility for the security of the MFS, and entities providing the service management.

There may be several active MFSPs and SE providers (e.g. MNOs) and different models may exist in order for the service management roles to be agreed upon commercially and executed by actors through SLAs. Commercial relationships between an MFSP and an SE provider may be managed either directly by them on a bilateral basis or indirectly by one or several TSMs. A combination of both models is also possible. There should be a consistent level of customer protection between the different models with equivalent access to dispute resolution mechanisms.

For the management of the processes, the appropriate SLAs between the stakeholders shall be established. They should cover customer relationship management, scalability, operational aspects such as technical processes, security, fraud reporting and incident management.

In order to ensure interoperability between the different entities, providing the service management a common API should be defined between the SE providers and the TSMs on one side, and the TSMs and the MFSPs on the other side.

NOTE An example of API supporting secure messaging has been specified in Reference [1].

For the specific case of UICC used as secure element for mobile proximate payment (and in particular for contactless payment), the service management of application has been widely developed in Reference [5] and may be considered by the entities providing the service management. This document defines and clarifies roles and responsibilities of the actors on the service management. For example, the domains of responsibility of the MNO (as an SE provider) are to manage the UICC lifecycle and security framework. The domain of responsibility of the MFSP is to manage the application. Both actors are responsible for the customer lifecycle and the support of customers in their own areas. The service management of application for other types of SE may be found in Reference [7].

7.2 MFSP domain roles

This subclause lists the MFSP domain roles that may be encountered depending on the scenario implemented (see Clause 9):

a) development of application;

b) development of application user interface;

c) application approval;

d) data preparation (personalization data);

e) mfsp security domain key management (logical and physical secure storage and delivery);

f) download and installation of application;

g) download of application user interface;

h) personalization of application;

i) activation of application;

j) OTA management of the application;

k) MFSP hotline/customer relationship management;

l) management of customer lifecycle events.

NOTE An example of detailed roles is provided in Reference [5].

7.3 SE provider domain roles

This subclause identifies SE provider domain roles that may be encountered depending on the scenario implemented (see Clause 9):

a) SE security policy definition;

b) SE certification and mobile device verification (standards and interoperability);

c) management of the list of MFSP(s) applications stored on the SE;

d) creation of the MFSP supplemental security domain;

e) management of the SE memory;

f) contractual and technical pre-controls: eligibility management;

g) SE provider or third-party hotline/customer relationship management;

h) management of customer lifecycle events.

NOTE An example of detailed roles is provided in Reference [5].

8 Application lifecycle: functions and processes

8.1 General

Functions for application lifecycle management are triggered by one or several possible situations and require actions from the MNO and/or the MFSP and/or a third party (TSM). In some cases, actions may be required from the customer. The protocols used to execute the functions for application lifecycle management will typically encompass acknowledgement/confirmation of the actions. 8.2 provide a non-exhaustive list of functions.

Each phase of the lifecycle (subscription, installation, usage and termination) is carried out by the execution of the processes listed in 8.3. A process may be covered by functions described in 8.2.

8.2 Functions

a) Eligibility request: The MFSP requests an eligibility report from the MNO or a third party to ascertain that the customer's mobile device is technically capable of hosting the application and operating the related MFS.

b) Installation of application.

c) Installation of application user interface.

d) Personalization and activation.

e) Update of application parameters.

f) Deletion of application.

g) Deletion of application user interface.

h) Blocking of application.

i) Unblocking of application.

j) Blocking of mobile network connectivity.

k) Unblocking of mobile network connectivity.

l) Audit of application.

m) Audit of secure environment.

8.3 Processes

a) Subscription

   1) Subscription to MFS

   2) Renewal of MFS

   3) Eligibility check

b) Installation

   1) Install application

   2) Install application user interface

c) Usage

   1) Audit application

   2) Update application parameters

   3) Change SE if applicable

   4) Change mobile number

   5) Change mobile device

   6) Loss/theft of mobile device

   7) Recovery of mobile device

   8) New mobile device after loss/theft

   9) Change MNO

   10) Temporary mobile services suspension

   11) Resume mobile services

   12) Temporary application suspension

   13) Resume application

   14) Customer relationship management

d) Termination

   1) Mobile service termination by customer

   2) Mobile service termination by MNO

   3) Application termination by customer

   4) Application termination by the MFSP

NOTE Details and mapping between processes and functions are more precisely specified in Reference [5] for UICC being used as a secure element.

9 Scenarios for service models

9.1 General

The services associated to the lifecycle management of the applications depend on the use and type of secure environment as defined in ISO 12812-1 and subject to requirements described in ISO/TS 12812-2.

The type of the secure environment has an impact on the roles and responsibilities of the various stakeholders.

When the secure environment is covered by an SE, several options could be chosen to install the application on the secure element, such as remotely via OTA using, for example, SMS and data channel or preloaded in the factory before the supply.

Whatever the scenario, the MFSP is responsible for the issuance and lifecycle management of the application.

9.2 Scenario 1: UICC

In this scenario, the secure environment is the UICC which is provided by the MNO.

In this scenario, the application lifecycle management services may be provided by one or several TSMs according to the agreements between MNOs and MFSPs.

A TSM may provide following services:

a) technical services: OTA-services, provisioning and application lifecycle event;

b) commercial services:

   1) procuring space for applications on the UICC on behalf of the MFSP;

   2) providing space for applications on the UICC on behalf of the MNO.

NOTE Reference [5] and Reference [1] provide guidance for this scenario.

9.3 Scenario 2: Embedded secure element

In this scenario, the secure environment is an embedded SE in a mobile.

The embedded secure element may be provided by the mobile device manufacturer or a third party to the mobile device manufacturer who acts as the SE provider from the point of view of the MFSP.

The mobile device usually includes a UICC for the mobile subscription.

A TSM may provide the following services:

a) technical services: OTA-services, provisioning and application lifecycle event;

b) commercial services:

   1) procuring space for applications on the embedded SE on behalf of the MFSP;

   2) providing space for applications on the embedded SE on behalf of the mobile device manufacturer.

This scenario requires a specific application in the mobile device to provide connectivity between the SE and the provisioning service possibly using API services. This application can be downloaded over the air or be pre-installed.

9.4 Scenario 3: Secure micro SD card

9.4.1 General

In this scenario, the secure environment is a secure element with the format of a secure micro SD card (a micro SD card with the features of a secure element). The secure micro SD card is a removable component provided by either the MFSP or a third party.

The mobile device usually includes a UICC for the mobile communication service subscription.

NOTE Micro SD cards are not supported by all mobile devices.

9.4.2 Secure micro SD card provided by the MFSP

When the secure micro SD card attached to the mobile device is provided by the MFSP, a TSM may provide the following services on behalf of the MFSP:

a) Technical services: OTA-services, provisioning and application lifecycle event;

b) Commercial services: providing space for applications on the secure SD card.

9.4.3 Secure micro SD card provided by a third party

When the secure micro SD card attached to the mobile device is provided by a third party, a TSM may provide the following services:

a) Technical services: OTA-services, provisioning and application lifecycle event;

b) Commercial services:

   1) procuring space for applications on the secure SD card on behalf of the MFSP;

   2) providing space for applications on the secure SD card on behalf of the third party.

This scenario requires a specific application in the mobile device to provide connectivity between the SE and the provisioning service possibly using API services. This application can be downloaded using an OTA channel.

9.4.4 Secure micro SD card for contactless payment

There are two types of secure micro SD cards in a contactless payment perspective:

a) a secure micro SD card with NFC antenna that should be used only in a mobile device without NFC capabilities to avoid radio frequency issues and conflict;

b) a secure micro SD card without NFC antenna to be used in a mobile device with NFC capabilities.

9.5 Scenario 4: Trusted execution environment

In this scenario, the secure environment is the TEE.

A TSM may provide the following services:

a) Technical services: OTA-services, provisioning and application lifecycle event;

b) Commercial services:

   1) procuring space for applications on the TEE on behalf of the MFSP;

   2) providing space for applications on the TEE on behalf of the mobile device manufacturer.

This scenario requires a specific application in the mobile device to provide connectivity between the TEE and the provisioning service possibly using API services. This application can be downloaded over the air or be pre-installed.

9.6 Scenario 5: Mobile application located in the mobile device host

This scenario applies typically to application downloaded from an application store or directly from the MFSP website. The application is located in the mobile device host under the control of the operating system.

The application lifecycle management may be operated by the MFSP.

9.7 Scenario 6: Mobile application on a secured server

In this scenario, the application is remotely stored on a secured server which may be managed by the MFSP or a third party.

The application lifecycle management may be operated by the MFSP.

Bibliography

[1] GlobalPlatform System — *Messaging specification for management of mobile NFC services*. Version 1.1, February 2013

[2] EMV Mobile Contactless — EMV Profiles of GlobalPlatform UICC Configuration

[3] Contactless Mobile Payment EMV Application Activation User Interface

[4] EMV Contactless Specifications for Payment systems – Book B – Entry Point Specification

[5] EPC-GSMA – Mobile contactless payments service management roles – Requirements and specifications. Version 2.0, October 2010

[6] EPC – White paper – Mobile Payments. Version 4.0, October 2012

[7] EPC – Mobile contactless SEPA card payments – Interoperability Implementation Guidelines. Version 2.0, November 2011

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.

Copyright in BSI publications

All the content in BSI publications, including British Standards, is the property of and copyrighted by BSI or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use.

Save for the provisions below, you may not transfer, share or disseminate any portion of the standard to any other person. You may not adapt, distribute, commercially exploit, or publicly display the standard or any portion thereof in any manner whatsoever without BSI's prior written consent.

Storing and using standards

Standards purchased in soft copy format:

- A British Standard purchased in soft copy format is licensed to a sole named user for personal or internal company use only.
- The standard may be stored on more than 1 device provided that it is accessible by the sole named user only and that only 1 copy is accessed at any one time.
- A single paper copy may be printed for personal or internal company use only.

Standards purchased in hard copy format:

- A British Standard purchased in hard copy format is for personal or internal company use only.
- It may not be further reproduced – in any format – to create an additional copy. This includes scanning of the document.

If you need more than 1 copy of the document, or if you wish to share the document on an internal network, you can save money by choosing a subscription product (see 'Subscriptions').

Reproducing extracts

For permission to reproduce content from BSI publications contact the BSI Copyright & Licensing 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 subscriptions@bsigroup.com.

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.

Useful Contacts

Customer Services
Tel: +44 345 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 345 086 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 Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.