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).

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.