TECHNICAL SPECIFICATION

ISO/TS 12812-2

First edition
2017-03

Core banking — Mobile financial services —

Part 2: **Security and data protection for mobile financial services**

Opérations bancaires de base — Services financiers mobiles —

Partie 2: Sécurité et protection des données pour les services financiers mobiles

Reference number
ISO/TS 12812-2:2017(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 ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **2**
4 Abbreviated terms **4**
5 Summary of the technical nature of the clauses **5**
6 Security management considerations **7**
6.1 General 7
6.2 Three-layer model to manage security for mobile financial services 8
6.2.1 Process layer 9
6.2.2 Application layer 10
6.2.3 Infrastructure layer 10
7 Security principles and minimum requirements for mobile financial services **11**
7.1 Security architecture aspects to be considered 11
7.2 Mobile financial services hardening techniques overview 13
7.2.1 General 13
7.2.2 Mobile device hardening techniques overview 13
7.2.3 Wireless networks hardening techniques overview 13
7.2.4 Secure remote management of mobile device components using OTA 14
7.2.5 Mobile financial applications hardening techniques 14
7.2.6 Platform security services 15
7.2.7 Application level security services for mobile financial applications 16
7.2.8 Application management security services 17
7.3 Minimum set of security requirements for mobile financial services 17
7.3.1 General 17
7.3.2 Remote MFS access requirements 17
7.3.3 Transaction processing requirements 18
7.3.4 Protection of sensitive data 19
7.3.5 Mobile device requirements 20
7.3.6 Customer education 20
7.4 Minimum set of security requirements for mobile application management 21
7.4.1 Customer enrolment and provisioning requirements 21
7.4.2 Key management 21
7.4.3 Mobile financial service provider and trusted service manager exchanges 22
7.4.4 Application downloading 22
7.4.5 Application deactivation 22
7.5 Summary: Requirements for security services for mobile financial services 22
8 Security requirements for cryptographic components used for MFS **23**
8.1 Mobile device secure environments 23
8.1.1 Mobile Device requirements for MFS 23
8.1.2 Software-based secure environment 24
8.1.3 Trusted execution environment (TEE) 24
8.1.4 Secure element requirements 26
8.1.5 Secure element requirements for digital signature services 28
8.2 Security requirements for cryptographic modules used for MFS 30
8.2.1 General 30
8.2.2 List of requirements for cryptographic hardware modules 30
8.2.3 Requirements for cryptographic software modules 31
9 Security evaluation and certification aspects **31**
9.1 General recommendation 31

9.2 Cryptographic modules ... 31
9.3 Software modules ... 32
9.4 Interoperability of security certifications ... 32
9.5 Guidance for TEE security evaluation and certification ... 33

10 Security requirements for mobile proximate payments ... 33
10.1 General ... 33
10.2 Common security requirements ... 34
10.2.1 Integrity of sensitive data and applications at rest ... 34
10.2.2 Authentication ... 34
10.2.3 Data protection in transit ... 34

11 Security requirements for mobile remote payments ... 34
11.1 General ... 34
11.2 Security requirements ... 35
11.2.1 Authentication ... 35
11.2.2 Proof of consent ... 35
11.2.3 Payment gateway processing requirements ... 35

12 Security requirements for mobile banking ... 35
12.1 General ... 35
12.2 Authentication considerations ... 36
12.3 Security requirements ... 37

13 Electronic money ... 37
13.1 General ... 37
13.2 Anonymity requirements ... 37
13.3 Security requirements ... 37

14 Data protection requirements ... 38
14.1 General considerations and legal framework for compliance ... 38
14.2 Requirements and recommendations for data protection ... 39
14.2.1 Requirements ... 39
14.2.2 Recommendations for data protection ... 39
14.3 Privacy assessment ... 39

Annex A (informative) **Risk analysis guidelines ... 40**

Annex B (informative) **Mobile financial system implementation of Know-Your-Customer requirements ... 45**

Annex C (informative) **Cryptographic mechanisms for mobile financial services ... 46**

Annex D (informative) **Vulnerabilities and attacks on mobile financial services ... 51**

Bibliography ... 55

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

ISO 12812 is made up of ISO 12812-1, an International Standard, and ISO/TS 12812-2 to ISO/TS 12812-4, published as Technical Specifications addressing interoperable and secure systems for the provision, operation and management of Mobile Financial Services (MFS).

This document is intended to assist MFS developers and MFS providers (MFSPs) to evaluate and select security mechanisms for an MFS to be managed according to a pre-established security policy. It is also important for users of MFS to understand how security requirements and considerations come into play in the mobile environment.

Security is a central requirement for any MFS. Institutions increasingly seek to mitigate the risk of fraud in order to protect their customers and hence their own business. Security objectives focus on risk mitigation of identified threats against the integrity and confidentiality of data. Any sustainable MFS business model relies on security and fraud prevention. Consequently, the MFSP needs to define the confidentiality and availability of data prior to implementing any MFS.

Mobile technology has security-specific concerns due to the proliferation and ease of availability of mobile devices and the observed hacking of mobile applications. The experience with traditional card payments is different than that with the mobile device and the wireless channel and requires that risks and controls be reassessed and re-implemented where necessary. Hence, MFSPs require a common understanding of the risks faced by the ecosystem and the suitability of existing security standards (architecture, devices and mechanisms) to address them. This document assumes that when the MFSP is deciding on the security policy to be implemented, the principle of proportionality applies. In other words, security countermeasures should be proportional to the potential risk of financial and reputational damage of a particular MFS.

MFS are initiated from a mobile device which is able to support different wireless communication protocols for different modes of operation. The mobile device can leverage various technologies to deliver MFS, including but not limited to near-field communications in conjunction with the presence of an appropriate secure environment (e.g. SE, TEE, software with supplementary security controls) resident in the mobile device or accessible from a remote/cloud-based back-office. Both types of technology offer different methods for securing financial data, financial applications, and personal data. In order to define security requirements for MFS, this document differentiates between:

- **a proximate mode of operation**, appropriate for various forms of payments where the mobile device directly communicates with another mobile device (i.e. a payee’s mobile device) or a payment terminal located at a merchant. Proximate payments are defined as those occurring where the payer and the payee are physically present in the same location (see ISO 12812-1).
- **a mobile remote mode of operation**, where the mobile device uses a mobile communication network which enable MFS to operate where the payer and the payee are not physically located in the same place (see ISO 12812-1). In remote mode, the wireless communication channel is established according to a specific set of standard protocols (e.g. GSM, CDMA, WiFi) which includes authentication procedures to grant access to the network services. A second authentication process of the mobile financial application enables the connection with the corresponding peer application in a remote platform.

This document analyses the various security issues that may arise from the choice of platform and technologies for the operation of MFS. This document also identifies various mobile malware vulnerabilities (e.g. worms, viruses, trojans) specific to mobile devices.

ISO/TS 12812-2 objectives include

a) defining the minimum security requirements, recommendations and guidelines as appropriate,

b) facilitating a generic security framework for the provision and execution of MFS with sufficient flexibility to accommodate different security policies,

c) establishing a generic model for managing security of MFS,

d) providing references for implementers to use in evaluating risks of MFS, and

e) identifying security management practices for the operation of MFS, including reference to specific national legal requirements to combat criminal activities (e.g. anti-money laundering) and to enhance data security through the use of proven cryptographic methods.

This document is structured as follows.

Clause 5 categorizes the technical content of the clauses of the document as types of materials: descriptive, recommendations or requirements.

Clause 6 introduces the concept of security management, addressing all different aspects of MFS security including risk management. Insight into risk analysis is found in Annex A.

Clause 7 describes the minimum set of security requirements for MFS, starting with challenges and technologies for a secure mobile application system design.

Clause 8 sets out requirements for those components specifically designed to create a secure environment in the mobile device, as well as cryptographic modules used for MFS transaction processing.

Clause 9 provides insight and sets out requirements for secure evaluation and certification methods.

Clause 10 through Clause 12 discuss more in depth the concepts outlined in Clause 7, by providing further requirements for security services needed to balance the vulnerabilities and threats of different wireless networks both in proximate and remote modes.

Clause 13 is specific to electronic money security requirements.

Clause 14 provides information relevant for selecting countermeasures to mitigate the legal risks of infringement of data protection laws.

Annex A focus on risk analysis including principles to establish a security management program for MFS.

Annex B provides insight into regulatory constraints that are taken into account when designing and/or operating an MFS.

Annex C is a list of ISO recommended cryptographic standards and implementations to design the security services set out in this document.

Annex D elaborates on vulnerabilities and threats for different communication channels used for MFS.

For additional information on the security of mobile payments, please refer to the Bibliography.

Core banking — Mobile financial services —

Part 2:
Security and data protection for mobile financial services

1 Scope

This document describes and specifies a framework for the management of the security of MFS. It includes

- a generic model for the design of the security policy,
- a minimum set of security requirements,
- recommended cryptographic protocols and mechanisms for mobile device authentication, financial message secure exchange and external authentication, including the following:
  a) point-to-point aspects to consider for MFS;
  b) end-to-end aspects to consider;
  c) security certification aspects;
  d) generation of mobile digital signatures;
- interoperability issues for the secure certification of MFS,
- recommendations for the protection of sensitive data,
- guidelines for the implementation of national laws and regulations (e.g. anti-money laundering and combating the funding of terrorism (AML/CFT), and
- security management considerations.

In order to avoid the duplication of standardization work already performed by other organizations, this document will reference other International Standards as required. In this respect, users of this document are directed to materials developed and published by ISO/TC 68/SC 2 and ISO/IEC JTC 1/SC 27.

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 9564 (all parts), *Financial services — Personal Identification Number (PIN) management and security*

ISO 11568, *Financial services — Key management (retail)*

ISO 12812-1, *Core banking — Mobile financial services — Part 1: General framework*

ISO/TS 12812-3, *Core banking — Mobile financial services — Part 3: Financial application lifecycle management*

ISO 13491 (all parts), *Financial services — Secure cryptographic devices (retail)*

ISO 19092, *Financial services — Biometrics — Security framework*

ISO 22307, *Financial services — Privacy impact assessment*

ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*

ISO/IEC 29192 (all parts), *Information technology — Security techniques — Lightweight cryptography*

3 Terms and definitions

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

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

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

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

3.1
application isolation
security property of the operating system whereby applications are isolated from one another both during execution and in terms of data they store and/or access

3.2
attack pattern
abstracted approach utilized to attack an MFS asset

3.3
attack potential
measurement of the effort to be expended in attacking an MFS asset, expressed in terms of an attacker's expertise, resources and motivation

3.4
attack surface
set of attack points that an attacker can use in order to enter or capture data in an information system

3.5
certificate revocation list
signed data structure containing a time-stamped list of revoked certificates implemented in public key infrastructures

3.6
common criteria
security evaluation methodology for Information Technology components standardized by ISO/IEC 15408

3.7
cryptographic module
set of hardware, software and/or firmware that implements approved security functions

3.8
data breach
loss of control, compromise, unauthorized disclosure, unauthorized acquisition or access where persons other than the legitimate ones have access to personally identifiable information (PII) or any other sensitive information (e.g. authentication data, keys)

3.9
end-to-end security
data encrypted at the source so that only the final recipient has access to the data