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

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

3.10
external authentication
process by which a mobile payment application authenticates an entity

3.11
information security management system
part of the overall management system, based on a business risk approach, used to establish, implement, operate, monitor, review, maintain and improve information security

3.12
mobile device integrity
absence of unauthorized or unintended changes in the hardware, firmware and software of a mobile device

3.13
personalization
process of storing on the mobile device the user application data required to execute an MFS

3.14
point-to-point encryption
data encrypted between two nodes, where at least one of the two nodes is neither the source nor the final recipient of the data

3.15
protection profile
set of security requirements that are specified with the aim of countering identified threats in a particular environment

3.16
pseudo-anonymity
security traits whereby the true identity of the person (e.g. payer, payee) is masked

3.17
rooting
manipulation by which the user of a mobile device gains access to privileged operating system administration rights

3.18
secure element provider security domain
confined physical and/or logical unit within the secure element where a security policy under the control of the secure element provider is applied

3.19
security controls
management, operational and technical controls (i.e. safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information

3.20
security encapsulation
layered security where one protocol (e.g. PIN encryption) is embedded inside another (e.g. SSL,TLS)

3.21
sensitive data
data which is required to be protected by security controls for a given MFS

EXAMPLE Authentication credentials, payment and banking credentials, cryptographic keys.

3.22
session key
temporary cryptographic key used to protect data for the current session only

3.23
time stamp
security mechanism providing the digital proof that an electronic document or message was created or signed before a certain time

3.24
trusted mobile device
mobile device that has been certified to conform to certain industry practices that can support a known risk profile (e.g. generation of electronic signatures)

3.25
unlinkability
security property of a protocol that protect it against an unauthorized party being able to link two executions of the protocol to a specific mobile device

4 Abbreviated terms

AES	Advanced Encryption Standard
AML	Anti-Money Laundering
CBC	Cipher Block Chaining
CC	Common Criteria
CSP	Critical Security Parameters
CVV	Card Verification Value
ECC	Elliptic Curve Cryptography
GCM	Gallois Counter Mode
HCE	Host Card Emulation
HMAC	Keyed-Hash Message Authentication Code
HSM	Hardware Security Module
IMSI	International Mobile Subscriber Identity
ISMS	Information Security Management system
KEK	Key Encryption Key
MAC	Message Authentication Code
MFS	Mobile Financial Service
MFSP	Mobile Financial Service Provider
OEM	Original Equipment Manufacturer
OS	Operating System
OSI	Open System Interconnection
OTA	Over the Air
PCD	Proximity Coupling Device

PCI-DSS	Payment Cared Industry Data Security Standard
PET	Privacy Enhancing Technology
PEF	Privacy Enhancing Feature
PII	Personally Identifiable Information
PIN	Personal Identification Number
RSA	Rivest Shamir Adleman
RNG	Random Number Generator
SE	Secure Element
SMS	Short Message Service
SMSC	Short Message Service Center
SSL	Secure Sockets Layer
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TSM	Trusted Service Manager
USSD	Unstructured Supplementary Service Data
UVM	User Verification Method

5 Summary of the technical nature of the clauses

Table 1 describes the technical nature of the clauses, classified as requirement, recommendation or descriptive material.

Table 1 — Classification of the technical nature of the clauses

Clause	Title	Descriptive	Requirements	Recommendations
Clause 6 Security management considerations				
6.2 Three-layer model to manage security for mobile financial services				
6.2.1	Process layer		X	
6.2.2	Application layer		X	
6.2.3	Infrastructure layer		X	
Clause 7 Security principles and minimum requirements for mobile financial services				
7.1	Security architecture aspects to be considered			X
7.2 Mobile financial services hardening techniques				
7.2.2	Mobile device hardening techniques overview	X		
7.2.3	Wireless networks hardening techniques overview	X		
7.2.4	Secure remote management of mobile device components using OTA		X	
7.2.5	Mobile financial applications hardening techniques	X		

Table 1 *(continued)*

Clause	Title	Descriptive	Requirements	Recommendations
7.2.6	Platform security services	X		
7.2.7	Application-level security services for mobile financial applications			X
7.2.8	Application management security services			X
7.3 Minimum set of security requirements for mobile financial services				
7.3.2	Remote mobile financial services access requirements		X	
7.3.3	Transaction processing requirements		X	
7.3.4	Protection of sensitive data		X	
7.3.5	Mobile device requirements		X	
7.3.6	Customer education			X
7.4 Minimum set of security requirements for mobile application management				
7.4.1	Customer enrolment and provisioning requirements		X	
7.4.2	Key management		X	
7.4.3	Mobile financial service provider and trusted service manager exchanges		X	
7.4.4	Application downloading		X	
7.4.5	Application deactivation		X	
7.5	Summary: Requirements for security services for mobile financial applications and data	X		
Clause 8 Security requirements for cryptographic components used for MFS				
8.1 Mobile device secure environments				
8.1.1	Mobile device requirements for MFS		X	
8.1.2	Software based secure environment		X	
8.1.3	Trusted Execution Environment (TEE)		X	
8.1.4	Secure element requirements		X	
8.1.5	Secure element requirements for digital signature service		X	
8.2 Security requirements for cryptographic modules used for MFS				
8.2.1	List of requirements for cryptographic hardware modules		X	
8.2.2	Requirements for cryptographic software modules		X	
Clause 9 Security evaluation and certification aspects				
9.1	General recommendation			X
9.2 Common security evaluation requirements				
9.3	Security evaluation of the TEE		X	
9.4 Security evaluation and certification of secure elements				
9.5 Security evaluation of cryptographic hardware and software modules				
Clause 10 Security requirements for mobile proximate payments				
10.2 Common security requirements				
10.2.1	Integrity of sensitive data and applications at rest		X	
10.2.2	Authentication		X	
10.2.3	Data protection at rest		X	

Table 1 *(continued)*

Clause	Title	Descriptive	Requirements	Recommendations
Clause 11 Security requirements for mobile remote payments				
11.2 Security requirements				
11.2.1	Authentication		X	
11.2.2	Proof of consent		X	
11.2.3	Payment gateway processing requirements		X	
Clause 12 Security requirements for mobile banking				
12.2	Authentication considerations	X		
12.3	Security requirements		X	
Clause 13 Electronic money security properties				
13.2	Anonymity requirements		X	
13.3	Security requirements		X	
Clause 14 Data protection requirements				
14.1	General considerations and legal framework for compliance			X
14.2	Requirements and recommendations for data protection			
14.2.1	Requirements		X	
14.2.2	Recommendations for data protection			X
14.3	Privacy assessment			X
Annex A Risk analysis guidelines		X		
Annex B Mobile financial system implementation of Know-Your-Customer requirements		X		
Annex C Cryptographic mechanisms for mobile financial services				X
Annex D Vulnerabilities and attacks on mobile financial services		X		

6 Security management considerations

6.1 General

Clause 6 establishes a framework for the management of the security of MFS. MFSPs are very sensitive to the possibility of a loss of reputation and therefore strive to ensure that MFS are secure for their customers. Thus, all MFSPs take care of managing their customer relationships and maintaining the integrity and security of their MFS lest they suffer reputational, monetary, and legal damages that can result from data compromise and fraud.

NOTE Refer to Annex A for further details on risk analysis.

It is thus fundamental to establish a security policy for the MFS program in which

— roles and responsibilities are assigned,

— security issues are governed and incentive exists to implement and maintain security best practices,

— transactions are secured and reliable,

— privacy is ensured, and

— security management systems of the involved parties are comparable and credible.

One of the objectives of this document is to provide implementers, with both requirements and recommendations to establish a security policy for the MFS related operations. According to ISO 12812-1:2017, Clause 5, the objective of the standard is technical interoperability. This document provides with references to ISO cryptographic standards, whose implementation facilitates the interoperability of protocols and applications for MFS.

6.2 Three-layer model to manage security for mobile financial services

This document establishes a generic model for security management to reduce the potential risk associated with MFS. This model is based on the implementation of security controls on three different functional layers required to provide MFS, namely the (1) process layer, the (2) application layer and (3) the infrastructure layer. MFSPs are responsible to identify and mitigate the specific risks associated with each layer.

— The process layer is made up of the organization and associated policies designed by the MFS program and implemented by the MFSP in order to minimize the risks during the MFS.

— The application layer refers to the distributed software under the direct control of the MFSP or of its partners embedded in the different processing computers and communication links required to initiate and process MFS (e.g. an application stored in the secure environment of the mobile device, a kernel in a point-of-interaction).

— The infrastructure layer is made up of the computing and networking facilities generating, storing, processing or transporting MFS data (e.g. a mobile device, a wireless network, databases, cryptographic modules).

Figure 1 describes the three layers of the generic model and provides examples of security standards that implementers may find useful for the design of the security architecture for MFS.

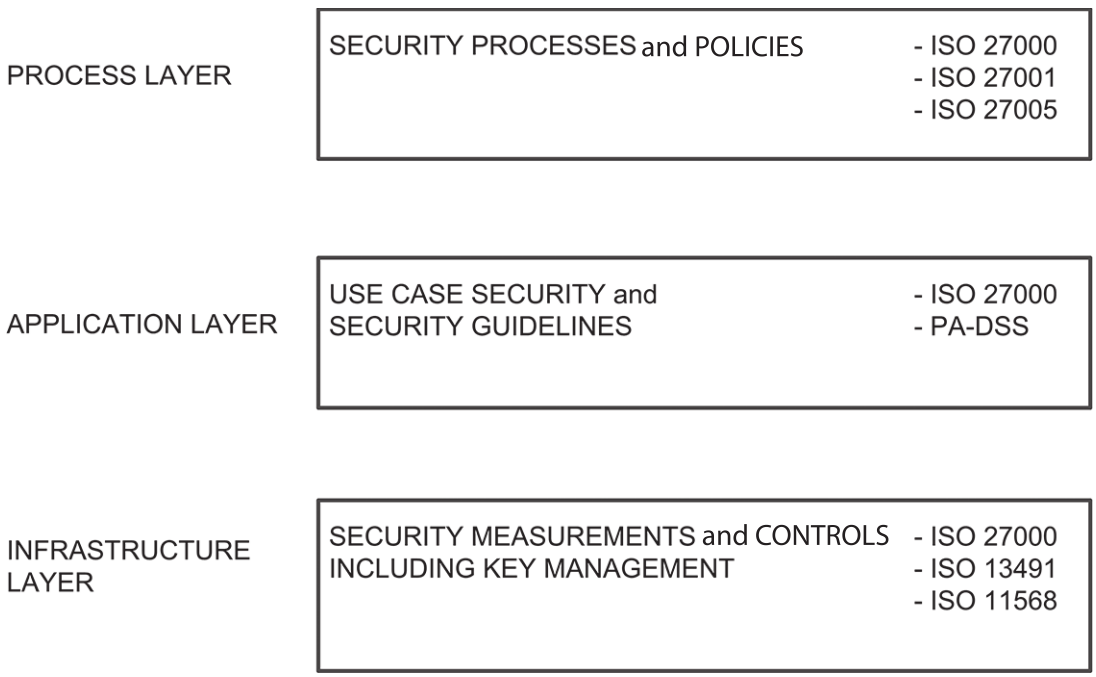

Figure 1 — Three-layer approach

Depending on the results of the risk assessment, further risk-driven measurements should be implemented in addition to the best practices aligned with the security requirements. Similarly, the attack surface can be effectively analysed and the appropriate countermeasures can be put in place, if the specific implementation vectors are known.

Implementers may wish to reference available resources in determining how to architect and implement their security measures. Among such resources are the FFIEC IT Examination Handbook, the NIST Guidelines (often used by various payment system participants) and the PCI-DSS

The Open System Interconnection seven-layer model (ISO/IEC 7498-1) may be mapped in to the Application and Infrastructure Layers described in 6.2.3 and 6.2.3.

6.2.1 Process layer

At the process (operational) layer, every party in the MFS program that provides or contributes to the provision of MFS shall have an information security management system (ISMS) in place consisting of a defined set of policies, processes, and systems to manage risks to information assets. In some instances, other than as a consumer, entities that consume MFS information (e.g. cloud providers) also shall have an information security management system in place. The respective party shall provide information on its ISMS upon request to anyone for whom that information is relevant (e.g. auditors, contractual partners), or in appropriate situations, even to customers. Any party who is required to have an ISMS shall periodically review (e.g. annually) and update it so that it is current.

The ISMS shall contain at least methods and procedures to monitor and manage relevant risks identified by the party and shall assign the appropriate resources and responsibilities to mitigate these risks.

Every participating party except a consumer shall define their responsibilities and the valuable assets to protect in their sphere of responsibility.

The minimum set of control objectives that shall be managed and documented by every participating party, except a consumer, are

— a security policy,

— the organization of information security (e.g. a hierarchical IT structure, a tiered secure management structure),

— an asset management plan, including access controls, and

— where appropriate, the party has human resource security and related training in place.

Depending on their supplied services, additional control objectives should be part of the information security management system, including but not limited to the following:

— physical and environmental security;

— communications and operations management;

— access control;

— information systems acquisition, development and maintenance;

— information security incident management;

— business continuity management;

— conformity or compliance mechanism(s).

Although the MFSP has the ultimate responsibility for achieving and maintaining security, if some services are outsourced or delivered through other contractual partners of the MFSP, some or part of any area of responsibility may be delegated to those other entities, even though the ultimate responsibility remains with the MFSP. The MFSP shall monitor its vendors and/or agents with whom it has outsourced any security requirements, to verify the existence of the security service level periodically to ensure the security issues are being handled in conformance with the requirements of this document.

Some implementers may find it useful refer to ISO 27001, which defines ISMS. It should be noted, however, that this document was not developed specifically for use by the financial services industry.

6.2.2 Application layer

At the application layer, software components shall comply with the information requirements outlined in this document.

The threats and risks related to a particular MFS can be described depending on the devices used, expected customer behaviour, attack patterns and application environments.

The risk assessment can then be conducted and the security measures can be evaluated following the use cases. This applies to the roles and responsibilities of each party in an MFS including the MFSP, customers and third parties. The wireless network, which provides the infrastructure layer (see 6.2.3), is not usually under the direct control of the MFSP. Different wireless protocols can be used to connect the mobile device to a processing infrastructure. This connection is performed through a mobile telecommunication network or an Internet connection, provided by an MNO or a third entity.

As a minimum, MFSPs shall identify, document, assess and mitigate the impact of specific threats for applications associated with the following attack patterns:

— unauthorized access to payment application and data (e.g. key disclosure, code breaking);

— misuse of applicative data generated during the MFS (e.g. relay/replay attacks, skimming, sniffing);

— prevent the access to the application by the legitimate user (e.g. denial of service);

— interception and capture of authentication data (e.g. mobile code);

— installation of rogue applications in the mobile device that may facilitate any of the above.

Specific security control objectives shall be set out to protect the customer and the MFSP from risks resulting from potential successful attacks. Such control objectives apply to

— authentication of applications,

— access control of applications,

— application maintenance, and

— application life cycle control.

6.2.3 Infrastructure layer

At the infrastructure layer, the software, network management, operating systems, firmware and hardware components shall comply with the information security requirements set forth in this document.

The choice of the security controls and performance measurement to be put in place depends primarily on the technical solution and the MFS program environment. In the infrastructure required to secure MFS, cryptographic devices and key management processes constitute central components. ISO 13491 (all parts) and ISO 11568 are largely used by the financial industry for implementation purposes.

Depending on the results of the risk assessment associated with the threats to the infrastructure, further risk driven measures should be implemented in addition to the best practices aligned with the security requirements. Similarly, the risks associated with the attack surface for the overall infrastructure can be analysed if the vectors are known enabling to design proportionate security controls.

A minimum set of control objectives for the infrastructure necessary to deliver the MFS, includes

— physical and environmental security,

— access control to databases,

— capacity management,

— business continuity management, and

— information security incident management.

7 Security principles and minimum requirements for mobile financial services

7.1 Security architecture aspects to be considered

Within the three-layer model described in 6.2, MFS and related applications are deployed over a wireless network, provided that security requirements defined by the MFSP can be fulfilled over that channel. Each of 7.2 to 7.4 are tied to and shall operate within the model; 7.5 summarizes the requirements of the earlier subclauses.

The security architecture is a design of how security controls are positioned and used to counter threats against mobile financial applications and sensitive data and how these relate to the overall mobile financial system architecture. Sensitive data include data used to carry out fraud, data used to initiate a mobile payment, data used for authentication purposes and any other data that if modified would compromise the security and/or privacy of the transaction.

This security architecture is intended to enable the MFS system to achieve a series of security objectives as set forth by the security policy of the system. These objectives depend on the nature of the MFS offered by the system. However, there exist significant objectives shared between different MFS, such as

— achieving a level of protection when executing a mobile application with a mobile device, equivalent to those applicable to other personal devices (e.g. corporate laptops),

— protecting MFS transactions with an appropriate and effective level of security at least equivalent to the one provided by legacy infrastructures,

— preserving user privacy,

— offering a trustworthy user interface for high-risk financial services, including features such as:

  a) what you see is what you sign;

  b) integrity and confidentiality of entered UVM data;

  c) secure service for application activation/selection;

— implementing effective countermeasures against open network threats (e.g. denial of service, phishing, spamming),

— preventing money laundering and other financial crimes, and

— complying with requirements imposed by regulations associated with the MFS related transactions.

Even if cryptography is an important tool to protect mobile financial assets, secure system design encompasses many other aspects, especially the correct implementation of the cryptographic mechanisms, the evaluation of the attack patterns and the secure storage of the cryptographic keys. Thus, the security architecture depends on the level of security of the devices able to establish secure communication links. A platform able to store multiple applications, whose life cycle may be managed in an independent way, raises specific concerns that are addressed in Clause 8.

The MFSP may also take into consideration, the non-technical requirements with special emphasis on the liability allocation decided as a result of the business model(s) supported and the risks identified.

The protection of an MFS transaction brings specific challenges, which are discussed here to provide additional guidance to MFSPs.

— **The complexity and heterogeneous nature of MFS systems**

MFS infrastructures are complex information systems. Access points and interfaces to the system are multiple and under the control of different stakeholders/customers, and the range of mobile devices capabilities available is high (and increasing). Therefore, it makes it difficult to monitor how each stakeholder is conforming to the requirements of the standard.

— **The threats posed by wireless and Internet connections**

The expansion of a broad-based mobile ecosystem has led to the use of new technologies (e.g. cloud computing) using open communication networks. An MFSP should maintain the security of transactions when using these emerging technologies, especially where there may be an unsecured channel or network (e.g. wireless or other unsecured network, Internet) and considering that MFS applications may be loaded in the secure environment of the mobile device over the air.

— **The different levels of involvement and control of the stakeholders during both the MFS development and the system operation**

In traditional payment card systems, almost all components are controlled/managed by the financial institutions. In MFS systems, the components are supplied, owned and controlled by a variety of stakeholders. These stakeholders have different practices in terms of security that are the result of their main business activities.

— **The threats involving the identification of MFS users and servers**

The lack of common and robust identification and authentication procedures for users and servers enables impersonation and fraud, especially for mobile payments-to-persons transactions. These threats may be mitigated by the implementation of appropriate Know-Your-Customer (KYC; see Annex B) rules to comply with local laws for the prevention of money laundering and financial crime.

— **The confidentiality, integrity and availability of exchanged information**

Messages containing payment data sent to the mobile device (e.g. for authentication and/or notification purposes) related to MFS transactions may constitute a valuable digital asset, needing to be protected in terms of integrity, confidentiality and availability.

— **Secure Environments and the mobile devices are shared and open platforms**

Part of the security architecture of the system will be supported by the mobile device which shall include at least one security environment (e.g. SE, TEE, supplemental software subject to risk analysis). Mobile financial applications issued by different MFSP are likely to coexist on the same mobile device, use common resources and share the same secure environment. From the security standpoint, this has multiple consequences.

a) The provisioning of a new MFS application should be transparent to applications possibly present on the mobile device. The new application should not induce any security breach to the other applications during the provisioning, storage, and/or execution phases.

b) Stakeholders involved in the downloading process should protect exchanged data with the appropriate cryptographic mechanisms, in order to

— protect the integrity of the application when loaded over the air, and

— protect against the simultaneous loading of malicious software.

c) The security of an application should be evaluated and certified on the platform on which the application will be provisioned.

Annex D describes common security threats observed for MFS related activities: mobile proximate payments, mobile remote payments and mobile banking. However, information security issues need to be examined individually for each MFS.

7.2 Mobile financial services hardening techniques overview

7.2.1 General

7.2 describes different hardening techniques for components, devices and networks required for MFS, operating in the application and/or infrastructure layers.

— 7.2.2 and 7.2.3 refer to components of the infrastructure that are not necessary under the control of the MFSP and can therefore be considered as untrusted from the MFSP prospective: mobile device and wireless networks.

— 7.2.4 to 7.2.7 refer to hardening techniques for applications and MFS data used by the MFSP to minimize the risks.

7.2.2 Mobile device hardening techniques overview

The mobile device usually includes a user interface and a secure environment for the execution of the mobile financial service. Mobile devices may be able to initiate some forms of mobile financial transactions without an SE, provided the MFSP has issued an alternative form of security control. In addition, the mobile device may contribute to the implementation of functionalities in benefit of the mobile financial services such as: (1) support of different UVMs; (2) user interfaces for payer application selection and consent; and (3) remote block of the mobile device if it is lost or stolen.

As far as the security is concerned, the mobile device may be viewed as a vulnerable component. Therefore, there is a need for isolation and security principles to be utilized by application developers so that any specific issue with the operating system of a mobile device is addressed. Detailed requirements for secure environments of the mobile device are set forth in Clause 8.

7.2.3 Wireless networks hardening techniques overview

Wireless networks comply with different standard security requirements, which include implementation options.

NOTE Various standards bodies have adopted existing standards that can be useful to implementers of the infrastructure layer for MFS (e.g. IEEE, IUT-T, Bluetooth, WAP, ETSI).

A mobile device can be configured to operate on different networks using different protocols. Some of these networks may not be implemented in a safe environment. Therefore, this document assumes that the wireless communication channel is unsecure. The main security controls in the interaction between the application in the mobile device and the MFSP shall be transparent (i.e. invisible) to the wireless communication channel. They typically include

— the confidentiality and integrity protection of data and mobile application at rest and during transmission,

— the non-repudiation of transactions authorized by the user,

— the protection against replay attacks, and

— different authentication mechanisms for the user, the MFS application and the remote server facilities of the MFSP.

7.2.4 Secure remote management of mobile device components using OTA

7.2.4.1 OTA technology description

Over-The-Air (OTA) is a technology used to communicate with, download applications to, and manage devices such as UICCs and other secure environments across all wireless networks, including mobile networks and Wi-Fi.

OTA is based on client/server architecture where at one end there is an operator or its agent back-end system (e.g. customer service, billing system, application server) and at the other end there is a component embedded in a mobile device.

OTA manages and delivers connectivity to each mobile device and its secure environment, regardless of the channel (SMS, http or both) or network technology is used. The information exchange is protected by using a secure end-to-end communication link from the MFSP Trusted Service Manager (TSM) to the secure environment. The end-to-end security is achieved using cryptographic keys shared between the TSM and the secure environment.

In order to implement the OTA technology, the following components are used:

— a back-end system to send requests to the target mobile device component;

— an OTA gateway to process these requests;

— an SMSC server to transport requests over a bearer (e.g. the SMS bearer);

— a mobile device to receive the requests and transmit them to the secure environment in the mobile device;

— a secure environment to receive and execute the request;

— a TSM in a role similar to a card personalization system.

7.2.4.2 Trusted service manager on OTA

The TSM play a critical role to provide and manage MFS applications, using the following functionalities:

— interface between MFSP, MNO and for some scenarios the manufacturer of the mobile device (usually referred to as the Original Equipment Manufacturer or OEM);

— end-to-end security for provisioning to secure environment of the mobile device;

— application lifecycle management including activation and deactivation of MFS on mobile devices;

— management of keys from the MFSP, the MNO and the provider of secure environment.

7.2.4.3 Security requirements

The TSM shall use a secure OTA communication channel to avoid the possibility of intercepting sensitive data as it is transmitted over the air. In particular, the integrity and the confidentiality of the applications to be personalized in the secure environment shall be protected during their transmission over the OTA channel. For security requirements applicable to the key management to secure the OTA channel, refer to 7.4.

7.2.5 Mobile financial applications hardening techniques

The following security services are available to MFS client applications in order to secure a transaction which is performed through vulnerable components and networks out of the control of the MFSP:

— **Platform** security services (see 7.2.6) are those provided by the mobile device itself to be shared by all the applications and do not necessary require cryptographic mechanisms. They include services to

a) protect and filter suspicious data (e.g. whitelisting, anti-virus),

b) protect the mobile financial application during its execution,

c) deactivate the components used during the transaction (e.g. an NFC module), and

d) protect the MFS applications in case the mobile device is lost or stolen.

— **Application level** security services (see 7.2.7) are provided by the MFSP using the cryptographic resources (e.g. cryptographic libraries) offered by both a tamper-resistant component (e.g. a SE) where the application is resident and another remote cryptographic component as a Hardware Security Module (HSM). These services protect the application and application data both in rest and in transit.

— **Application management** (see 7.2.8) security services are activated during operations related to the lifecycle management of the application according to ISO/TS 12812-3.

7.2.6 Platform security services

The MFSP shall use the following platform security measures provided by the mobile device as a baseline for the security management of MFS.

— Protection against malware

The mobile device has the ability to execute all types of applications which extends to viruses and malware. Remote MFS often rely on software-based security which is susceptible to many threats.

The innovation pace of the technology (great heterogeneity on underlying computing platforms and operating systems evolving rapidly, making difficult a fit-in-all single antivirus solution, multiplicity of modes of communication) and the way the mobile device is used (permanent connection to open networks) make the mobile device more vulnerable to attacks compared with other personal computer devices. Stakeholders such as mobile device manufacturers or OS providers should include mobile security software (e.g. mobile antivirus) as part of the default suite of applications loaded onto new mobile devices.

— Secure Environment for application execution

The creation of a secure environment for the execution of the mobile financial application is based on two principles:

a) isolation of the application in one or more secure computing environments, over the mobile device itself (SE, TEE, mobile OS security controls);

b) securing the user interface by the creation of a trusted channel between the input/output peripherals of the mobile device and the secure computing environment.

— Deactivation of proximate interfaces

The mobile device OS may feature functionalities to deactivate the communication interface for proximate payments, when no external active communication protocol is detected and/or offering in the user interface the possibility to cut-off the communication link between the secure element and the external radiofrequency module. The consumer has full control over when to enable an interface for the transaction, leaving it largely disabled when the mobile device is not used for proximate payments. Otherwise, payment data could be read out by an attacker and be used for instance during a relay attack (Annex D).

— Remote deactivation of the mobile device

In case of a customer reporting that the mobile device has been stolen or lost, the MFSP should be in a position to remotely deactivate all of its resident mobile financial applications on that mobile device, using specific messages. The risk of financial losses is also reduced by the fact that the loss of the mobile device is quickly reported.

7.2.7 Application level security services for mobile financial applications

7.2.7.1 General

This clause focuses on security mechanisms at the application level. These mechanisms use cryptographic algorithms and keys to achieve different levels of protection on the data exchanged during the MFS. MFS application data are to be protected during their personalization, storage and use in the mobile device. In particular

— mechanisms are needed to ensure that no sensitive payment data and personal data are accessed or modified by an authorized party through any communication interface of the mobile device, and

— clear text sensitive payment and personal data are to be stored and managed in an appropriate secure environment.

Often, the execution of a mobile financial application will require the security services provided by several protocols, mechanism known as security encapsulation. For example,

— the first protocol may support access control to the mobile financial service, for instance, by using an external authentication mechanism and the exchange of data necessary to generate a session key, and

— a second protocol might provide a service of confidentiality for the exchanged messages, using the agreed session key/s, as well as a service of integrity of the exchanged information. These protocols might also protect against other types of attacks that are intrinsic to wireless channels (e.g. contactless skimming, replay and eavesdropping; see Annex D).

7.2.7.2 Security properties featured by mobile financial applications

The security services of the system provide various security properties for application data and transactions generated by applications. Amongst such properties are

a) user authentication,

b) confidentiality of sensitive data at rest, in transit and during execution to ensure that data can only be accessed by authorized parties,

c) integrity of data at rest, in transit and during execution maintained by using message authentication codes, and

d) non-repudiation when a message conveys a confirmation by the user.

The MFS may also use additional safeguards (e.g. time out) which are not based on cryptographic mechanisms.

7.2.7.3 Point-to-point encryption

Pont-to-point encryption is a special case of application-level encryption, where encryption is applied selectively within the processing chain of a MFS application. It defines a cryptographic process for data encryption between any two communicating nodes during the payment processing:

a) original data is encrypted at the point of capture;

b) data is decrypted only when it is needed by specific processing nodes that have no choice but to access the original data.

Point-to-Point encryption requires a strict control on the keys needed to decrypt data, to ensure that only authorized nodes may gain access to the original data.

7.2.7.4 End-to-end security

End-to-end security, similar to end-to-end encryption, defines a cryptographic process for data encryption at the source of confidential data, so that the corresponding decryption only occurs at the final destination of the message. In this case, a given message is to be encrypted in the secure environment using for instance a shared key with a remote Hardware Security Module (HSM), under control of the MFSP. HSMs are widely used to manage and protect cryptographic keys and to support secure processing in order to achieve the cryptographic protection required when data are encrypted by remote MFS.

Regardless of the fact that the message may transit through vulnerable networks, if properly implemented, end-to-end encryption protects data against eavesdropping and brute force attacks.

NOTE Point-to-point encryption between the source and the final recipient corresponds to end-to-end security.

7.2.8 Application management security services

These security services are intended to protect application-level assets throughout the lifecycle of the MFS application. Management operations provide applications with confidentiality and authenticity, during their personalization, ensuring that mobile applications are only downloaded from trusted sources.

Security requirements for application management are set forth in 7.4.

7.3 Minimum set of security requirements for mobile financial services

7.3.1 General

The minimum requirements for MFS apply to the MFSPs who may implement them with the support of MFS schemes and other MFS vendors/suppliers.

NOTE The term “session” refers in this subclause refers to a process opened with a successful connection with a MFSP with the purpose to run one or more transactions.

7.3.2 Remote MFS access requirements

The requirements in this subclause and 7.4 apply differently to the three different access mechanisms to remote MFS.

7.3.2.1 For MFS accessed through a mobile browser, the security considerations closely resemble those applicable to financial services accessed through a traditional desktop personal computer (PC). The MFSP shall provide means for the customer to verify the authenticity of the website at the time of access (e.g. by using Extended Validation certificates or similar mechanisms).

7.3.2.2 For MFS accessed through a dedicated functionality on the mobile device (e.g. a MFS application), the relevant requirements set forth in this subclause and 7.4 shall apply. In particular, the MFSP shall provide means for the customer to verify the authenticity of the mobile financial application (e.g. use of software signing, out-of-band communication).

7.3.2.3 For MFS provided using the MNO’s channels (e.g. SMS, USSD) without a specific mobile financial application previously downloaded onto the customer’s mobile device, the relevant requirements set out in this subclause shall apply.

7.3.3 Transaction processing requirements

7.3.3.1 Customer and MFS data authentication

7.3.3.1.1 A customer authentication mechanism shall exist to ensure that only the legitimate account holder is authorized to carry out financial transactions.

7.3.3.1.2 The MFSP shall provide the customer with a UVM (e.g. a mobile code) to prove his/her presence during the MFS transaction.

7.3.3.1.3 Prior to providing a new customer with authentication credentials, an MFSP shall proceed during the enrolment to a KYC verification according to applicable regulation (see Annex B).

7.3.3.1.4 Customer authentication may have various strengths (strong or basic). The level of strength corresponding to strong customer authentication refers to an authentication procedure implemented by the MFS provider or its agent which complies with the three following conditions:

a) the successful verification shall consist of at least two personal independent authenticators from the security prospective, meaning that the compromise of one of the authenticators does not compromise the other;

b) at least one of the authenticators shall be dynamic with perfect forward secrecy, non-reusable and not replicable;

c) at least one of the authenticators shall be a UVM.

7.3.3.1.5 The verification process shall be designed in a way that the authenticators remain confidential:

a) if biometrics is used as a UVM, the security controls required in ISO 19092 shall be met;

b) if the PIN code is used as a UVM, the PIN shall be managed according to ISO 9564 (all parts);

c) if a mobile code is used as a UVM, the mobile code shall be encrypted.

The term strong authentication may have a legal definition under individual national laws.

Basic Customer Authentication is either a one factor authentication or an authentication based exclusively on static data.

7.3.3.1.6 Additionally, the MFS application shall be protected (e.g. by the use of encryption, MAC, HMAC, digital signature), recognizing that there are various degrees based on the security of the operating system or security of where the application is stored (e.g. SE, TEE, or in software with supplementary security controls). Both aspects contribute to a level of security assurance originating from a customer authentication. Other factors (e.g. device identification, analysis of spending patterns) may contribute as well.

7.3.3.1.7 The level of security assurance shall be taken into account when determining the types and/or levels of transactions and environments to be permitted. This includes allowing only low-value transactions or transfers between accounts owned by the same individual, for example, when a low-assurance authentication has taken place, while, on the other hand, allowing higher-value transactions when a high level of assurance has been achieved.

7.3.3.1.8 It is important for the MFSP to take into account that, whereas a mobile device might be a second channel for payments initiated from a PC or with a chip card, when a transaction is initiated from a mobile device, that mobile device may now be the same channel. In this situation, then, the MFSP shall implement second-channel security mechanisms using a different device (e.g. a tablet, a second mobile

device) so that the mobile device cannot inadvertently serve as both the first and the second channel. Thus, for example, in this case SMS shall not be used to communicate a one-time-password.

7.3.3.1.9 Mechanisms such as timing out customer authentications (i.e. requiring a new authentication after a session has lasted a certain time since the last successful authentication) and limiting the allowable number of retries in case of unsuccessful authentications should be utilized by the MFS provider

7.3.3.1.10 The MFSP shall use mechanisms to authenticate the MFS application.

7.3.3.2 Transaction monitoring

7.3.3.2.1 The MFS provider shall use security mechanisms that mitigate or protect against brute force attacks (e.g. exhaustion attacks on UVM) and other attacks that fit known fraud patterns.

7.3.3.2.2 Prior to providing a customer with mobile financial services, an MFSP should set limits applying to those services, (e.g. a maximum amount for each individual payment or a cumulative amount over a certain period of time) and should inform customers accordingly.

7.3.3.2.3 An MFS provider shall, to the extent it has the physical capabilities, log significant events, including

a) failure to authenticate;

b) failure to validate a message;

c) data required for solving the repudiation of a payment;

d) start of session;

e) end of session.

7.3.3.2.4 Sensitive data shall not be logged. Other error conditions may be logged.

7.3.4 Protection of sensitive data

7.3.4.1 General

7.3.4.1.1 An MFSP shall employ security mechanisms that prevent unauthorized access to sensitive data at rest or in transit.

7.3.4.1.2 A trusted user interface may be used in order to limit the exposure to malware masquerading as a legitimate mobile financial application or customer authentication prompt.

7.3.4.1.3 The strength of the sensitive data protection provided should be taken into account when considering what types and/or levels of transactions are permissible, and which kinds of data can be stored on the mobile device or in a secured server.

7.3.4.2 Data protection during storage

7.3.4.2.1 The confidentiality and integrity of sensitive data shall be protected on the mobile device. Sensitive data shall be stored in the secure environment of a mobile device, and it shall be encrypted and its integrity shall be cryptographically protected. The cryptographic algorithms used shall be among those specified in Annex C.

7.3.4.2.2 The integrity and authenticity of public keys used for MFS generated using recognized standards (see Annex C) shall be protected using digital certificates.

7.3.4.3 Data protection during transmission

7.3.4.3.1 If the MFS application is not residing in a secure environment, then other effective security measures be taken to limit the exposure of the customer account in case of a compromise. Such measures may include the use of one time tokens or the use of mobile device only for authentication purposes. PIN data shall be entered and transmitted only in conformance with ISO 9564 (all parts). In these cases, no sensitive data shall be stored in the mobile device and the authentication mechanism is not vulnerable to a compromise of the mobile device.

NOTE Code obfuscation is not considered sufficient on its own.

7.3.4.3.2 Sensitive data shall be encrypted when transmitted between any two points in the transaction processing. Similar to PIN translation, to avoid exposure of keys and sensitive data, cryptographic hardware is required for decryption, or only non-sensitive data is allowed. Sensitive data should be authenticated and it shall be protected against substitution and modification. When these data correspond to an application to be downloaded, then in addition, the requirements set out in 7.4 shall apply.

7.3.5 Mobile device requirements

7.3.5.1 An MFSP shall use security mechanisms that protect the mobile financial application from unauthorized modification and/or substitution. These mechanisms should include device security checks that verify patch and versions of the operating system, detect malware or rooting (so-called "jail-breaking" of device).

7.3.5.2 MFS implementations shall provide countermeasures against threats arising from the use of mobile device input and output interfaces, including NFC, Bluetooth and 2D barcode scanning.

7.3.5.3 Mechanisms to protect MFS shall take into account the potential vulnerability of the connection between the mobile device and servers.

7.3.5.4 The aggregate strength of the security mechanisms provided by customer authentication, data protection mobile device security and application security should be taken into account when determining which transactions are permissible and which kinds of data can be stored in the mobile device. MFS that supports exclusively lower-value transactions requiring no storage of sensitive data may require less security than MFS that can be used for higher-value transactions or store sensitive customer data.

7.3.6 Customer education

An MFSP should ensure that the prior information supplied to the customer contains specific details relating to the MFS. These should include, as appropriate:

— clear information on any requirements in terms of customer equipment, software or other necessary tools (e.g. compatible Operating Systems/versions/mobile device);

— guidelines for the proper and secure use of credentials;

— a detailed description of the procedure for the customer to submit and authorize a transaction and/or obtain information, including the consequences of each action;

— guidelines for the proper and secure use of all hardware and software provided to the customer;

— the procedures to follow in the event of loss or theft of the credentials or the customer's hardware or software for logging in or carrying out transactions;

— the procedures to follow if an abuse is detected or suspected;

— a description of the responsibilities and liabilities of the MFSP and the customer respectively with regard to the use of the MFS.

7.4 Minimum set of security requirements for mobile application management

7.4.1 Customer enrolment and provisioning requirements

7.4.1.1 For any enrolment, the customer shall be authenticated by the MFSP. This authentication should use multiple factors and/or channels providing independent security assurance in the sense that a compromise of one factor (e.g. a compromised password) or one channel (e.g. malware on a device) is unlikely to coincide with a compromise of another factor or channel.

7.4.1.2 Mobile financial applications shall be bound, at the time of installation, to the particular mobile device, and at the time of activation, shall be associated with a unique authenticated customer and/or other persons of his/her choice. Accordingly, the application shall be used exclusively for transactions by that customer and/or other persons of his/her choice.

7.4.1.3 The MFSP shall provide means for the customer, to verify the successful installation and personalization of any downloaded mobile financial application.

7.4.1.4 The MFSP shall manage a directory of all the MFS provided by the mobile device.

7.4.2 Key management

7.4.2.1 The MFSP or its agent shall operate a key management system to derive unique keys specific to secure environments or mobile devices.

7.4.2.2 All keys used for mobile financial data encryption/decryption shall be generated using a random or pseudo-random generator certified against recognized standards.

7.4.2.3 The personalization of keys shall incorporate a validation mechanism to verify that the keys were effectively personalized for the device they were intended to and that these keys are authentic.

7.4.2.4 The MFSP shall document the procedures used to secure the administration of the cryptographic keys used by the components of the mobile system, during the personalization and in-field operation of the component.

7.4.2.5 The MFSP shall use encryption algorithms to secure data transmission over OTA.

NOTE Refer to Annex C for guidance.

7.4.2.6 Cryptographic keys shall be transported securely using exclusively Key Exchange Keys (KEK) with high entropy, meaning, having at least the entropy of the key being transported.

7.4.2.7 In-clear components of cryptographic keys to be used by the mobile system shall be stored in a tamper resistant security module and/or, where applicable, in a device using a tamper evident mechanism.

NOTE Implementers can find guidance on security requirements for HSM in PCI-SCC technical specifications.

7.4.3 Mobile financial service provider and trusted service manager exchanges

7.4.3.1 All applications provided by the MFSP to the TSM shall be stored in an encrypted form with integrity protection.

7.4.3.2 Once encrypted, the TSM shall not allow any MFS application or other sensitive data to be decrypted except for the purpose to re-encrypt them with a device-specific key before sending them to an end user device, or transmitting them in the payment processing system.

7.4.4 Application downloading

7.4.4.1 The MFSP shall ensure end-to-end encryption between the TSM and the mobile device.

7.4.4.2 Mobile financial applications shall only be provisioned after the establishment of a secure channel between the mobile device and the distributor of the application.

7.4.4.3 The secure channel shall protect the integrity of the MFS application throughout the downloading process.

7.4.4.4 The MFSP shall provide the means to authenticate the application downloaded.

7.4.5 Application deactivation

7.4.5.1 The MFSP shall provide means for the customer to deactivate, partially or completely, the mobile financial application.

7.4.5.2 When compromised or upon customer request, the MFSP shall provide the means to remotely deactivate, partially or completely, the mobile financial application

7.5 Summary: Requirements for security services for mobile financial services

Security Service	Implementation Mechanisms	Clause
Confidentiality protection of data at rest	— encrypt application data stored in MFSP, TSM and mobile device — store data in a tamper resistant module in-the-clear or encrypted using key material located in the tamper resistant component	7.2.5 7.3.4.2 If stored in an SE: 8.1.4
Confidentiality protection of data in transit	apply transport encryption (e.g. TLS) and encryption of sensitive data in messages exchanged	7.2.7.3
Integrity protection of data at rest	by means of an application of digital signature data stored on mobile device or tamper resistant component with key material located in tamper resistant component	7.2.5 7.3.4.2
Integrity protection of data in transit	Use encryption mechanisms for transport encryption which also provide integrity protection (e.g. AES with GCM) or sign messages exchanged. Refer to C.3 for relevant ISO standards providing a detailed description of these cryptographic mechanisms.	7.3.3.2 7.3.4.1 7.3.4.3
Integrity protection of application during provisioning	sign messages exchanged	7.4

Security Service	Implementation Mechanisms	Clause
Integrity protection of application at rest	validate the application signature client side using key material located on the tamper resistant component	7.2.5 7.3.4.1 7.3.4.2
Integrity protection of application during execution	isolated environment for execution	7.3.5 Executed in TEE: 8.1.3 Executed in SE: 8.1.4
Non-repudiation of transactions approved by the user	sign transaction data after customer authentication	7.3.3.1 8.1.5
Authenticity (integrity and origin authentication) of mobile data or application	Data origin authentication using e.g. Message Authentication Codes (MAC), Hash-based Message Authentication Codes (HMAC) or Digital Signature. Refer to C.3 for relevant ISO standards providing a detailed description of these cryptographic mechanisms.	7.4

8 Security requirements for cryptographic components used for MFS

8.1 Mobile device secure environments

8.1.1 Mobile Device requirements for MFS

This document considers the mobile device as a potentially vulnerable environment. The following clauses focus on security requirements for secure environments in mobile devices, understood as desired properties that enhance the integrity of mobile financial applications. This document assumes that operating systems of mobile devices pose security risks, specially where they execute MFS applications owned by a third party.

A mobile device compliant with this document shall support appropriate security services which may include one or more of the following:

a) to ensure the secure execution of the mobile financial applications;

b) to identify and authenticate the legitimate user of the mobile financial application;

c) to provide secure communication interfaces;

d) to support appropriate security controls for storing the mobile financial applications;

e) to encrypt sensitive data where required by the MFS;

f) to provide the customer with mechanisms for managing the available mobile financial applications, including when relevant, secure enrolment, application installation, application activation, listing of available applications and their secure selection;

g) to provide either an authorization request to an MFSP or the data needed to build this authorization request (i.e. when the authorization is requested by the POI);

h) to support optional functionalities such as the generation and verification of mobile digital signatures or other security services offered by the MFSP.

In particular, a mobile device shall implement at least one secure environment for the storage and/or the execution of mobile payment applications.

This document identifies five security levels for secure environments. They may be combined:

— Two levels are purely software security solutions:

  L1: Software Security Controls: Rely usually on code obfuscation or diversification and generic operating system security architecture;

  L2: Trusted Execution Environment (TEE) as pure software solution.

— L3 secure environment uses extended hardware

  L3: Trusted Execution Environment (TEE) with specific hardware support (e.g. by managing dedicated execution contexts).

— L4 and L5 secure environments require specific secure certified hardware for storage and execution purposes:

  L4: Secure Element (SE);

  L5: Secure Element and Trusted Execution Environment (SE + TEE) usually designed to provide a Trusted User Interface.

Neither the implementation of the TEE nor of the SE is mandatory. However, if the MFSP decides to use them, then compliance with 8.1.3 and 8.1.4 respectively is required.

8.1.2 Software-based secure environment

8.1.2.1 Definition and core functionalities

Software based secure environment refers to pure software used to protect MFS data and run applications using the mobile device OS resources. The technology Host Card Emulation (HCE) used for mobile proximate payments is an example of software-based secure environment.

8.1.2.2 Security requirements

8.1.2.2.1 Static MFS sensitive data shall not be stored in a software secure environment, unless these data are protected by a TEE.

8.1.2.2.2 Code and data stored in software secure environment shall be protected using specific methods such as code obfuscation and white box cryptography.

8.1.2.2.3 Transactions initiated from a software secure environment shall make use of a payment token instead of the real payment account identifier.

8.1.3 Trusted execution environment (TEE)

8.1.3.1 Definition and core functionalities

The trusted execution environment (TEE) is a protected environment that runs a secure operating system in the main processor of a mobile device. The TEE includes key-storage and management functionalities, which shall conform to ISO 11568. It also includes secure storage, which can be used to store transaction logs and authentication credentials in a private area.

Generally, the TEE

— implements an isolated computing resource in the mobile device,

— takes control over mobile vulnerable resources, particularly peripherals,

— provides security properties to the executing mobile financial application so that the application is immune to malicious software threats, and

— complements the security execution environment offered by an SE, including the provision of any encryption functionality that the MFSP requires by

a) all sensitive mobile financial application code should be executed in this isolated and protected environment, and

b) sensitive data stored in this area should be encrypted.

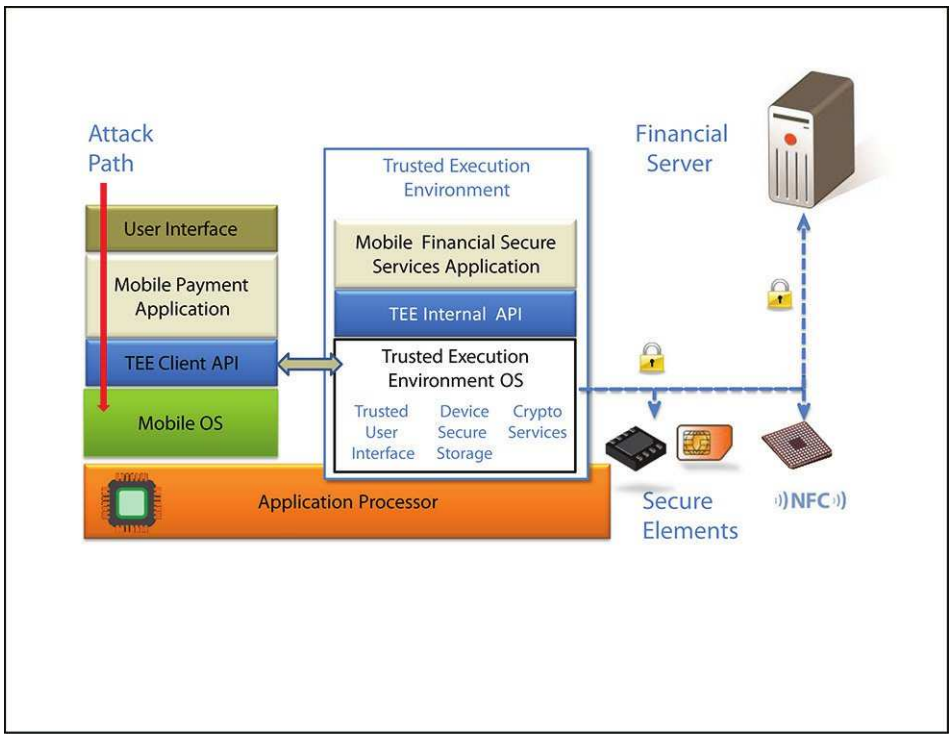

Figure 2 — Logical Interfaces for the integration of the TEE in mobile device architecture

The TEE includes cryptographic as well as key-storage and management functionalities. It also includes secure mass storage, which can be used to store transaction logs and authentication credentials in a private area.

8.1.3.2 Trusted user interface: TEE and secure element implementation

Depending on the use cases, the TEE provides a trade-off between the high flexibility and easy developments on the mobile operating system with a low level of security and the low flexibility and drastic constraints of development on a Secure Element with a high level of security.

The TEE is intended to complement the Secure Elements in the mobile device, jointly implementing a trusted user interface (TUI). This TUI provides a secure communication channel between the User Interface and a security environment either in the mobile device or in a remote server.

The TUI controls the screen and keyboard and/or touchpad, isolating them from the operating system, therefore ensuring the following security services.

— **Secure authentication**: protected entry of authentication credentials which can then be securely transferred through a private communication channel to a Secure Element, or to a server for online verification.

— **Non-repudiation**: critical transaction information is displayed on mobile device screen in such a way that it cannot be tampered with. Access controls to authenticate the legitimate user requires

the presence of a software module executing either on the mobile device or within the Secure Element itself.

The security properties of TEE implementations should be demonstrated through a security evaluation and certification process. 9.5 introduces guidance for TEE certification.

8.1.4 Secure element requirements

8.1.4.1 Hardware-level security

8.1.4.1.1 Secure elements shall provide storage and processing of sensitive data in a physically separated computing module. Confidential data shall also be protected against disclosure-attacks even if the attack causes the physical destruction of the SE.

8.1.4.1.2 Secure elements shall provide an isolated execution environment for MFS, meaning the ability to run application software in complete isolation from other code in the secure element itself or in another component in the mobile device.

8.1.4.1.3 Secure elements shall be designed with physical security mechanisms in order to have built-in tamper-resistance capabilities.

8.1.4.1.4 Secure elements shall verify the integrity and authenticity of firmware and software downloaded prior to installation, as well as provide a mechanism to validate the installed firmware or software versions (e.g. release numbers, dates).

8.1.4.1.5 Secure elements shall be able to dynamically authenticate themselves to the SE provider.

8.1.4.1.6 Secure elements shall be designed so that an attacker shall not be able to impersonate the secure element.

8.1.4.1.7 The production and personalisation of secure elements shall take place in an environment that prevents any of the following:

— compromising keys during personalisation;

— abusive or unauthorized personalisation;

— unauthorized upload of software and data;

— the theft of secure elements.

8.1.4.2 Protection and use of sensitive data

8.1.4.2.1 Protection of authentication data

8.1.4.2.1.1 The secure element shall implement a secure mechanism for the personalization of authentication data.

8.1.4.2.1.2 Secure elements shall support a security architecture made up of an SE provider security domain with its own authentication credentials and optionally supplemental security domains.

8.1.4.2.1.3 If any, supplemental security domains shall store independent authentication credentials.

8.1.4.2.1.4 Secure elements shall be designed to generate dynamic data for authentication.

8.1.4.2.1.5 Secure elements shall provide tamper-responsive mechanisms (e.g. zeroization) for stored authentication credential.

8.1.4.2.2 User verification data

8.1.4.2.2.1 Secure elements shall be able to store reference user verification data and make its comparison against the user entered data.

8.1.4.2.2.2 Secure elements shall support a mechanism so that the user verification data cannot be replayed.

8.1.4.2.3 Management and protection of cryptographic keys

8.1.4.2.3.1 The secure element provider shall implement a policy for the deployment, management and possibly the periodically change and renewal of cryptographic keys.

8.1.4.2.3.2 Cryptographic keys shall be exclusively used with cryptographic algorithms compliant with ISO standards by Annex C.

8.1.4.2.3.3 The secure element provider security domain shall store and manage cryptographic keys for the following:

— over-the-air secure provisioning;

— secure element content management;

— supplemental security domain creation and management.

8.1.4.2.3.4 The secure element provider security domain shall exclusively use specific keys for the secure transport of other cryptographic keys.

8.1.4.2.3.5 Supplementary security domains may rely on the secure element provider security domain key manager for loading applications or shall have their own key manager.

8.1.4.2.3.6 Secure elements shall provide identity-based authentication for usage of symmetric or asymmetric private keys.

8.1.4.2.3.7 Secure elements shall provide tamper-responsive mechanisms (e.g. zeroization) for stored cryptographic keys.

8.1.4.2.3.8 Secure elements should provide tamper-detection and zeroization of cryptographic keys.

8.1.4.2.3.9 Secure elements shall provide the mechanisms to detect and prevent any attempt to reuse zeroized cryptographic keys.

8.1.4.2.4 Application data integrity and secrecy

8.1.4.2.4.1 The secure element shall provide application's data secrecy and integrity both at rest and when processed.

8.1.4.2.4.2 MFS applications and other applications resident in the secure element shall be isolated by using a firewalling mechanism.

8.1.4.2.4.3 The secure element shall authenticate any application attempting to use the secure element.

8.1.4.2.4.4 Application data stored and/or processed by the secure element shall be protected against unauthorized manipulation.

8.1.4.2.4.5 When a secure domain or resident application uses a digital signature for data authentication and non-repudiation purposes, the requirements of 8.1.5 shall apply.

8.1.4.2.4.6 When protecting data in transit, the secure element shall use separate keys for confidentiality and integrity.

8.1.4.2.4.7 The encryption, decryption, verification and generation of authentication related data shall be processed inside the secure element.

8.1.4.2.5 Transaction logging

8.1.4.2.5.1 The data related to transactions processed by the secure element shall be logged.

8.1.4.2.5.2 The log processing shall be secured.

8.1.4.2.5.3 Stored log data shall be protected against unauthorized disclosure and manipulations and securely transmitted only to an authorized entity.

8.1.5 Secure element requirements for digital signature services

8.1.5.1 Rationale

Mobile digital signature is a functionality that might be needed when accessing MFS whose execution requires a non-repudiable proof of consent by the legitimate user. This subclause assumes that the communication between the user and the server may take place with both trusted ("agreed") and vulnerable mobile devices.

8.1.5.2 Trusted mobile device for digital signature generation

8.1.5.2.1 A trusted signature mobile device shall guarantee that the displayed information is included in the signed data.

8.1.5.2.2 A trusted signature mobile device shall guarantee the not-recording and not authorized disclosure of data entered by the customer.

8.1.5.2.3 A trusted signature mobile device shall pass an evaluation and certification procedure according to a protection profile [in accordance with ISO 15408 (all parts)] taking into account the nature of the financial services to be accessed and the environment in which it is operated.

8.1.5.3 Requirements applying to digital signatures generated by a mobile device

8.1.5.3.1 An application generating digital signatures resident in a secure element may be run in either exclusively trusted mobile devices or on a less secure mobile device, depending on the degree of security required by the MFSP.

8.1.5.3.2 A trusted mobile device shall authenticate to the signing secure element or to the external environment.

8.1.5.3.3 A signature produced by the application resident in a secure element using a trusted mobile device shall include the proof that the mobile device is authentic.

8.1.5.3.4 When the signing secure element is used to authenticate a mobile device and/or MFS, the user shall be provided with a proof of the authentic nature of the mobile device and/or MFS.

8.1.5.3.5 The use of the signing secure element in any mobile device shall not undermine the security of the trusted mobile device. For instance, the signing secure element should support two different authentication credentials in order to authorize the digital signature in an agreed or not-agreed terminal. The goal is not to compromise the first authentication credential used for highly sensitive applications, at the MFSP disposal because of the use of the signing secure element in a not-agreed and eventually tampered mobile device.

8.1.5.3.6 Time stamping servers shall be put in place under the responsibility of a time stamping provider. When the MFS requires a time-stamp, the digital signature produced by the signing secure element should include a proof of the identity of the time stamping server.

8.1.5.3.7 Digital signature algorithms to be supported by the signing secure element shall comply with ISO standards by Annex C.

8.1.5.3.8 Upon request by the trusted mobile device and according to the associated access rules, the signing secure element shall generate a pair of asymmetric keys, one private for digital signature purposes and the other public for the verification of the signature purposes.

8.1.5.3.9 The signing Secure Element shall authenticate two types of servers: those managing the certificate revocation lists (CRL), or online certificate status protocol (OCSP) services as alternative to CRL, and those providing time-stamping services.

8.1.5.3.10 Beyond the algorithms and formats required to support the above functionalities, the interactions between the mobile device and the signing secure elements shall conform to the relevant ISO standard (e.g. ISO/IEC 7816).

8.1.5.3.11 Signing secure element interoperability requires conformance with standards specifying a syntax for the interoperable processing of the transferred data. In particular, the syntax for digitally signed messages (including certificates) should be independent from the signature algorithm used.

NOTE W3C has specified an XML signature syntax and processing. European standardization organizations CEN and ETSI have developed a number of standards for electronic signature products. In the US, the X9 standard is X9.31, which is based on NIST FPS 186–2.

8.1.5.3.12 The signing secure element for financial applications shall be able to process public-key algorithms. The signing secure element shall also be able to support several applications, requiring a digital signature for authentication and non-repudiation purposes with special needs (counting, signature log). Each financial application in the signing secure element may have its own pair of keys and a specific digital certificate corresponding to that application.

8.1.5.3.13 The signing secure element shall support the two following methods for the generation of pair of asymmetric keys for the generation of digital signatures:

— generation by the secure element of the pair of keys and certification of the public key by the certification authority (CA);

— generation by the CA of the pair of keys, then personalization into the secure element of these keys along with the public-key certificate. This personalization process shall take place using a highly secure end-to-end channel, between the CA server and the signing secure element.

8.2 Security requirements for cryptographic modules used for MFS

8.2.1 General

MFS programs makes extensive use of cryptographic modules to protect messages, cryptographic keys and other sensitive data used by MFS. A cryptographic module is defined as the set of hardware, software, and/or firmware that implements approved security functions within the cryptographic boundary specified by ISO 19790 (including cryptographic algorithms and key generation).

The security of the MFS is largely dependent upon the security of these cryptographic modules.

Four standard security levels for cryptographic modules are defined in ISO/IEC 19790. Each security level offers an increase in security compared with the precedent one.

— Security Level 1 provides the lowest level of security with specific physical security mechanisms required and allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an unevaluated operating system.

— Security Level 2 enhances the security mechanisms of a Security Level 1 cryptographic module by adding the requirement for tamper-evidence and at a minimum, role-based authentication.

— Security Level 3 improves the lower security levels by requiring detective and preventive mechanisms to thwart an intruder from gaining access to any critical security parameters (CSP) such as symmetric key or asymmetric private keys, and authentication credentials. Authentication is increased by requiring identity-based (versus role-based) mechanisms. Further, separation of data ports for CSP from other types of information is also required.

— Security Level 4 provides the highest level requiring a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access. The detective and preventive mechanisms require zeroization of CPS.

Generally speaking, Security Level 1 is a software module running on a general-purpose computer. Security Level 2 can be a software module or a hardware module. Security Level 3 is a hardware module or might be a software module running on a dedicated-purpose computer which has formally been evaluated per the Common Criteria at an Evaluation Assurance Level (EAL) 3 or higher. Security Level 4 is always a special purpose hardware module. Most special purpose hardware security modules (HSM) are Security Level 3, but some are certified at Security Level 4 when operating in ISO/IEC 19790 mode. Type 1 cryptographic modules used by military and some government agencies are certified using a different formal evaluation process. Other cryptographic modules that are not formally certified as Type 1 or Type 2 are referred to as Type 3 modules.

8.2.2 List of requirements for cryptographic hardware modules

8.2.2.1 The hardware cryptographic module shall be designed for compliance with ISO/IEC 19790. In particular, the module shall be designed in such a way that any attempt to tamper with it shall destroy all stored cryptographic material.

8.2.2.2 The hardware cryptographic module shall at least implement one of the security functions as per ISO/IEC 19790:2012, Annex C. The MFSP may in addition specify a security function not included in Annex C but required by the MFS.

8.2.2.3 If the application is deleting keys, it shall make sure that the module is fully operational when a key is deleted. Otherwise, the deleted key might reappear when the module is recovered.

8.2.2.4 In addition to the requirements set out in ISO/IEC 19790, the MFSP may decide to have additional procedures and policies for high availability functionality of the services provided by the module. In particular, the MFSP shall implement and document a recovery policy in case of an outage.

8.2.2.5 The MFSP shall precise the nature of the cryptographic services, if any, that may still be provided by the cryptographic module in degraded mode of operation.

8.2.3 Requirements for cryptographic software modules

A software module can achieve an ISO/IEC 19790 Security Level 2 by supporting role-based authentication and providing a tamper-evidence mechanism. For software, this implies the detection that the executable (binary) code has been altered in some fashion, such that the module is no longer a legitimate copy of the original code. This is a type of malware vulnerability that while not necessarily preventable is detectable. Anti-virus products can detect, alert and quarantine modified software modules. Code signatures can be used to verify software prior to execution, periodic scans, or at the time of downloading newer code as part of an overall vulnerability lifecycle management system (VLMS).

Code signatures rely on cryptographic algorithms such as hashes, digital signatures or trusted time stamps. A single hash is insufficient to detect a code modification as collisions (the same hash value is derived from more than one string of binary bits) can occur. Secure hash (see Annex C) and/or the use of cryptographic keys can severely deter an intruder's ability to modify or create another software module that will generate an existing hash.

9 Security evaluation and certification aspects

9.1 General recommendation

Each component of mobile payment systems should undergo a security evaluation and certification process by an independent third party. The evaluation of physical components such as cryptographic modules can be largely carried out using standard procedures. Considering the strongest available adversaries and taking advantage of the latest cryptanalytic progresses during evaluations of cryptographic hardware appears important in view of the difficulty to fix security breaches.

This clause provides an overview of different security evaluation methodologies based on ISO standards that may be used for the certification of components required by the MFS.

9.2 Cryptographic modules

A cryptographic module is defined as the set of hardware, software, and/or firmware that implements approved security functions within the cryptographic boundary specified by ISO/IEC 19790 (including cryptographic algorithms and key generation). Four standard security levels for cryptographic modules are defined in ISO/IEC 19790. Each security level offers an increase in security compared with the precedent one.

— Security Level 1 provides the lowest level of security with specific physical security mechanisms required and allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an unevaluated operating system.

— Security Level 2 enhances the security mechanisms of a Security Level 1 cryptographic module by adding the requirement for tamper-evidence and at a minimum, role-based authentication.

— Security Level 3 improves the lower security levels by requiring detective and preventive mechanisms to thwart an intruder from gaining access to any critical security parameters (CSP) such as symmetric key or asymmetric private keys, and authentication credentials. Authentication is increased by requiring identity-based (versus role-based) mechanisms. Further, separation of data ports for CSP from other types of information is also required.

— Security Level 4 provides the highest level requiring a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access. The detective and preventive mechanisms require zeroization of CPS.

Generally speaking, Security Level 1 is a software module running on a general-purpose computer. Security Level 2 can be a software module or a hardware module. Security Level 3 is a hardware module or might be a software module running on a dedicated-purpose computer which has formally been evaluated per the Common Criteria at an Evaluation Assurance Level (EAL) 3 or higher. Security Level 4 is always a special purpose hardware module. Most special purpose hardware security modules (HSM) are Security Level 3, but some are certified at Security Level 4 when operating in ISO/IEC 19790 mode. Type 1 cryptographic modules used by military and some government agencies are certified using a different formal evaluation process. Other cryptographic modules that are not formally certified as Type 1 or Type 2 are referred to as Type 3 modules.

9.3 Software modules

A software module can achieve an ISO/IEC 19790 Security Level 2 by supporting role-based authentication and providing a tamper-evidence mechanism. For software this implies the detection that the executable (binary) code has been altered in some fashion, such that the module is no longer a legitimate copy of the original code. This is a type of malware vulnerability that while not necessarily preventable is detectable. Anti-virus products can detect, alert and quarantine modified software modules. Code signatures can be used to verify software prior to execution, periodic scans, or at the time of downloading newer code as part of an overall vulnerability lifecycle management system (VLMS).

Code signatures rely on cryptographic algorithms such as hashes, digital signatures or trusted time stamps. A single hash is insufficient to detect a code modification as collisions (the same hash value is derived from more than one string of binary bits) can occur. Secure hash (see Annex C) and/or the use of cryptographic keys can severely deter an intruder's ability to modify or create another software module that will generate an existing hash.

9.4 Interoperability of security certifications

The certification of mobile financial applications raises several interoperability issues with regards the mutual recognition of the security certificates issued by different certification bodies. Mobile financial applications should be built on certified platforms.

In this clause, the term platform refers to a hardware and software device, within a mobile device made up of a certified integrated circuit, hosting

— an operating system,

— an interpreter or virtual machine, and

— one or more mobile financial applications.

This document differentiates between the two following scenarios.

— When the platform has been issued by an institution which is responsible of the certification of both the platform and the applications, legacy certification process can be used. In that case, the security evaluation and certification methodologies used, for example, by traditional payment cards are to be adapted.

— When the platform has been issued by a third party, responsible for the platform certification, and according to the system rules, an institution wants to download its own application in this platform, using a mechanism according to ISO/TS 12812-3. In this case, several interfaces for interoperability are involved.

  In this scenario, from the financial industry prospective, the problem is the degree of trust offered by a platform which is issued by a third party (e.g. a MNO), to execute a mobile financial application owned typically by a financial institution.

A second great difference with the traditional card certification relies on the fact that the mobile financial applications may be downloaded in the SE after the issuance of the SE. In this case, a given application can be downloaded over several platforms from the same or different vendors.

— This application has in turn been certified over a platform, which in a general case is different from the target platform in a system and using a given security evaluation methodology. Because at the time, the application has been certified.

  a) The application provider ignores in which platform it will be downloaded and executed.

  b) The possible vulnerabilities of the application if resident in another platform.

  c) The possible vulnerabilities of the platform revealed.

In a generic case, these platforms have been evaluated by different security laboratories, not necessary using the same methodology.

The following scenarios can be differentiated for certification.

— When both the platform and the applications are owned by the institution, the certification process is similar to the one for a mono or multi-applicative payment card.

— When the platform is owned by a third party, and the application is owned by an institution, the scope of the certification includes the platform personalized with at least one mobile financial application.

One concrete example is the security evaluation and certification of a Secure Element for mobile financial applications. Once a mobile application has been certified over a platform (SE) provided by vendor A using a security methodology of a Laboratory A, it would be rational to reuse part of these evaluation result if the same application is to be executed over a platform (SE manufactured by vendor B).

This case leads to the need to harmonize the security and functional properties of those platforms that are suitable for the storage and execution of a given application. The provider of an SE therefore will dispose of a series of mobile financial applications and has also provisioned secure elements from different certified hardware tamper resistant platforms offered by different vendors. The application vendor will not need to certify its application with all certified platforms.

9.5 Guidance for TEE security evaluation and certification

Any TEE implementation should be capable of providing evidence of its “trusted” capacity through an evaluation of the product in order to determine its security properties.

Greater assurance results from a greater evaluation effort, through a broader scope, a greater attention to fine details or a more formal evaluation process.

— If the Common Criteria (CC, ISO/IEC 15408) methodology is selected by the MFS, the assurance level should be equivalent to the assurance package defined as EAL2+ extended AVA_VAN.2 in the CC methodology

— In case FIPS 140-2 is preferred, the security evaluation should conform to at least FIPS 140-2 Level 3 or better assurance.

10 Security requirements for mobile proximate payments

10.1 General

The secure implementation of mobile proximate payments requires the mobile device to implement a security architecture, isolating trusted and untrusted components for sensitive data storage and processing purposes and preventing the unauthorized activation of the mobile device (e.g. activating

the NFC module). Requirements in this clause are divided into those common to proximate payment and those specific to a contactless implementation.

10.2 Common security requirements

10.2.1 Integrity of sensitive data and applications at rest

10.2.1.1 Mobile devices shall notify the user when the mobile proximate payment interface of the mobile device is active.

10.2.1.2 Mobile devices shall implement a mechanism to prevent unauthorized capture of data when the payment application is at rest (e.g. deactivating the communication interface for proximate payments of the mobile device).

10.2.1.3 Sensitive data used for proximate payments shall be stored and processed exclusively in an isolated secure environment.

10.2.2 Authentication

10.2.2.1 The MFSP shall employ a dynamic authentication element for each mobile proximate payment transaction.

10.2.2.2 The mobile proximate application shall support at least one UVM based on the knowledge of a mobile code. When required, the mobile code shall be entered by the customer and verified.

10.2.2.3 The MFSP shall configure parameters managing the risk of the transaction (e.g. amount max of the transaction without requiring an UVM to be entered) and in particular the conditions making the user verification necessary.

10.2.2.4 If a mobile code is used as UVM, it shall be protected using the appropriate requirements such as those defined in ISO 9564-2.

10.2.3 Data protection in transit

10.2.3.1 The establishment of a secure channel for a proximate mobile payment is not mandatory. If implemented, the secure channel shall only be established upon the successful authentication of the mobile device application.

10.2.3.2 Cryptographic mechanisms shall be designed to optimize the security/transaction time ratio.

10.2.3.3 For low risk and fast transactions, standard lightweight cryptography compliant with ISO/IEC 29192 (all parts) may be considered. ISO/IEC 29192 (all parts) shall be implemented in such a way that no attacker should be able to recover the session key of an eavesdropped encrypted transaction.

11 Security requirements for mobile remote payments

11.1 General

This clause sets forth additional requirements in order to achieve two security objectives:

— to reduce fraud;

— to avoid repudiation of legitimate approved remote transactions.

11.2 Security requirements

11.2.1 Authentication

11.2.1.1 The MFSP shall implement at least one dynamic customer authentication for each mobile remote payment transaction.

11.2.1.2 The authentication mechanisms to be used shall be proportionate to the risk assessed for a particular mobile remote payment.

11.2.1.3 The acquiring entity shall provide mechanisms for the authentication of the payment gateway by the mobile device (e.g. by the mobile financial application).

11.2.1.4 If a mobile code is used as UVM, it shall be protected using the appropriate requirements such as those defined in ISO 9564-2.

11.2.2 Proof of consent

11.2.2.1 The remote mobile payment service provider shall provide the payer the technical means (e.g. cryptographic based) required to generate a non-forgeable evidence of the user consent on the payment terms, when the payment exceeds a certain amount. This mechanism shall also be provided to the enrolled retailers accepting the mobile remote payments.

11.2.2.2 The MFSP shall provide the payer with a proof that the remote payment has taken place or shall notify the payer that the authorization has been denied.

11.2.2.3 A message proving the user consent for a mobile remote payment transaction shall not be forgeable nor reusable.

11.2.2.4 The MFSP shall authorize the mobile remote transaction.

11.2.3 Payment gateway processing requirements

11.2.3.1 The payment gateway shall support the risk parameters of the acceptor of the transaction.

11.2.3.2 The payment gateway and the MFSP shall guarantee the integrity of authentication and transaction data.

11.2.3.3 The MFSP shall authenticate the payment gateway.

NOTE If a card payment instrument is used for the mobile remote payment, the MFSP is the acquirer of the transaction.

12 Security requirements for mobile banking

12.1 General

Access to mobile banking services requires at least the three following conditions:

— the customer has registered for this particular service (enrolment);

— the customer is to be authenticated;

— the mobile device is connected to a server controlled by the Financial Institution.

12.2 Authentication considerations

It is commonly accepted that at least a two-factor authentication process is needed for a robust process.

Authentication levels of assurance refer to the pre-established levels of confidence in the verification of the claimed identity. These levels are defined in terms of severity of loss, either financial or in the bank reputation that could occur from fraud during the authentication process. Any level of confidence involves specific technologies and processes for authentication factors integrated in a security system operated by the financial institution itself or by a third party. The security system is built upon a security policy as a result of the financial institution analysis in terms of system threats, incurred potential losses and associated cost for countermeasures.

A good security system is one where the security requirements are aligned with the financial motivations of those liable if the system fails. High-risk mobile banking applications should require at least, integrity and authenticity of the sensitive messages exchanged. This means that a secure channel is to be established before the transaction takes place. In addition, and due to legal constraints, confidentiality and non-repudiation services to protect the financial institution and the customer may be supported.

Because a successful entity authentication opens the door to banking services, it is assumed that security attacks will likely target the authentication processes. Therefore, the Security Policy of the system has to carefully address the authentication issues to minimize threats including:

— Authentication credentials: Static credentials are weaker than one-time credentials, and a hardware authentication token is better than a software one;

— Authentication protocols: A protocol known to be secure against man-in-the-middle attacks is a basic requirement for remote banking. A proof of security for the protocol provides additional guarantees against certain attacks;

— Entities to be authenticated (e.g. mutual authentication and/or multi-factor user authentication): User, mobile device, mobile financial application and financial institution server;

— Hardware Authentication Token: A dedicated tamper resistant device able to store cryptographic keys is able for instance to execute a mutual authentication protocol with a bank server;

— Authentication Environment: It may be secure, using for instance a certified card reader or unsecure;

— Authentication Data Carrier: Between the entity being authenticated and the server providing authentication and/or granting access to mobile banking services;

— Authentication Data and their strength against manipulation by an attacker: It is important to assess the risk associated with the compromise of cryptographic keys or with undue practices for the verification of authentication data;

— Authentication Infrastructure integrating front-end servers, authentication and mobile banking servers and different databases;

— Lifecycle management of authentication-related information.

The order in which the authentication of the entities is executed has an impact on the risk level faced by the financial institution and the customer. If the first stage for the transaction is the Authentication of the financial institution, it may be followed by the establishment of a secure channel between the client and the authenticated financial institution. While customer authentication takes place locally, the mobile device authentication may take place remotely over this secure channel.

Beyond authentication methods, a strong financial institution Security Policy should also include other factors, such as recognition of the Mobile Device, fraud monitoring, and use of multi-channel notifications to customers.

12.3 Security requirements

12.3.1 An authentication process shall be implemented.

12.3.2 A secure process for the enrolment of the customer and the delivery of identification and authentication credentials shall be implemented.

12.3.3 A secure process to download in the mobile device authentication credentials shall be implemented.

12.3.4 A secure environment for identification and authentication credentials shall be available in the mobile.

12.3.5 An access control mechanism for identification and authentication credentials, including a UVM shall be implemented.

12.3.6 A secure transmission mechanism for authentication-related messages shall be available.

13 Electronic money

13.1 General

This clause details requirements for electronic money (e-Money) stored locally in a secure element in the mobile device or remotely accessed by the consumer in an account stored in a server.

The security requirements for e-money represent a trade-off between the need to emulate a transfer of physical cash, protect the users and ensure the security of the e-Money system.

This clause includes requirements intended to provide electronic money with some anonymity features and those intended to reduce fraud and generating trust in the electronic money system.

13.2 Anonymity requirements

13.2.1 e-money solutions conforming to this document shall not reveal any personal identification information (PII) other than a pseudonym. This feature is sometimes referred to as “weak anonymity”. In other words, it will be impossible for a criminal (no attack pattern) or for the legitimate payee to retrieve the identity of the payer from any attribute of the received e-money. However, this document recognizes that legal prospects may require full traceability by authorized persons.

NOTE If the payer and the payee know each other, the payee already knows the identity of the payer. However, it could try to prove to a third person that this particular payment was generated by the payer. In that case, this requirement prevents the e-money transaction from generating data linking the identity of the payer to that particular transaction.

13.2.2 e-money units shall guarantee the unlinkability of the e-money payment operations unless they correspond to an individual creation and subsequent downloading in the mobile device.

13.3 Security requirements

13.3.1 The e-money system shall be designed so that the e-money issuer, even cooperating with malicious users, cannot falsely accuse (with a fake proof) an honest user of having double-spent an e-money unit.

13.3.2 The mobile application managing e-money shall provide the user with a means to check that an e-Money payment transaction has been correctly executed.

13.3.3 The e-money shall enable the detection of double-spending and the identification of double-spender.

13.3.4 The e-money shall not be forgeable. It shall not be possible to create e-money units without the authorization of the e-money issuer and the secure environment storing the e-money.

13.3.5 The e-money transaction shall provide information enabling the payee to identify the e-money issuer.

13.3.6 It shall be possible to verify the e-money authenticity off-line, meaning, that it was effectively created by the claimed e-money issuer.

Additional information on e-money security can be found in the bibliography.

14 Data protection requirements

14.1 General considerations and legal framework for compliance

MFSPs should ensure effective customer control of personal data. Collection of personal data (including internet usage information and IP addresses) should be made through free, informed and positive consent (opt-in), and only when strictly necessary, in an open and transparent way. Confidential personal data should be protected against unauthorized use, and in any event, its use should be minimized. Those affected by any personal data breach shall be promptly notified of the details of the breach and of the available means of redress. This document recognizes that a balanced solution may be required when the operational and even legal requirements may potentially be in conflict with data protection concerns. Therefore, communication protocols shall balance access control with protecting client's privacy. The liability arising from any breach of privacy should extend beyond actions taken directly by the MFSP and include other handlers of the information including authorized agents. MFSPs should put in place an effective mechanism guaranteeing the security of customer information and accepting liability for breaches even when attributable to their authorized agents.

For instance, records are needed for dispute resolution, auditing and other privacy management purposes. In that case, it matters that records be only generated when explicit consent is obtained from the user of the signing secure element. The digital signature functionality of the signing secure element may serve that purpose. These records shall be protected against unauthorized access, alteration, and deletion. A good means to conciliate these requirements could be that such records are locally stored in the secure element, but that raises memory capacity storage issues, or be stored in a secure way in a remote database, with the mobile device enabling access under the only control of the user.

MFSPs should seek cooperation with statutory bodies charged with consumer protection in this domain to oversee the development and effective application of data protection practice.

The recommendations set forth in the next clause are intended to be compatible with other standardization efforts and, in particular, with ISO/IEC 29100.

This document provides examples for the choice of the signing secure element functionalities for privacy safeguarding.

14.2 Requirements and recommendations for data protection

14.2.1 Requirements

14.2.1.1 Mechanisms of authentication shall be provided, so that only duly authorized requesters (e.g. government officers) gain access to the personal data of the consumer.

14.2.1.2 The authorized requester shall obtain the needed information without disclosing it, either intentionally or unintentionally.

14.2.1.3 The authorized requester shall destroy or dispose the information when no longer needed.

14.2.2 Recommendations for data protection

14.2.2.1 The customer and the duly authorized requester identities should not be divulged.

14.2.2.2 The MFSP should take steps to ensure that a third party cannot easily determine that different transactions have been generated by the same mobile device. Two queries from the same mobile device should not be computationally bounded.

14.2.2.3 It shall be unpractical to decipher transmitted encrypted information unduly captured by a third party.

14.3 Privacy assessment

ISO 22307 defines a methodology to help organizations in private and public sectors identify privacy issues and mitigate risks associated with processing the financial data of customers and consumers, business partners and citizens.

Rapid advances in the performance of computer systems and networking, along with a reduction of their cost, allow financial institutions to record, store and retrieve vast amounts of data faster and more efficiently than ever before. Advanced data processing, storage, collection, and retrieval technology is now available to all sectors of business and government.

The privacy impact assessment (PIA) should be carried out by the MFSP at the onset of the development of a proposed MFS. The PIA provides a way to ensure the system complies with applicable laws and regulations governing customer and consumer privacy as well as identify optimal privacy options and solutions. When used effectively, the PIA can identify risks associated with privacy and help organizations plan to mitigate those risks.

Annex A
(informative)

Risk analysis guidelines

A.1 Principles for a security program for an MFS

Implementing an MFS requires the adoption of a suitable business model and interoperable technologies between a number of different stakeholders (see ISO 12812-1). Fraud and misuse of MFS will jeopardize the sustainability of the business model and may undermine the confidence of the customer.

The security of an MFS is the direct result of the complex and multiple interactions of all the entities involved in the related operations. Each MFS program will have its own set of operating procedures and/or requirements (e.g. "membership rules") that govern how the parties will interact, how transactions will be handled, and what recourse each party has if a transaction fails or is the subject of a security breach, including what authentication mechanisms are available or shall be used.

A security risk is the potential that a given threat will exploit the MFS vulnerabilities. Individual MFSPs are responsible for the identification, assessment and mitigation of security risks. The objective of a security program is to minimize the adverse impact on the MFS of the identified security risks. Furthermore, in order to optimize risk-reduction improvement efforts, it is essential to understand the structure of risks related to fraud, misuse and data security breaches for the MFS.

To minimize risks it is necessary to combine different countermeasures intended to

a) reduce the attack surface of MFS infrastructures,

b) minimize the consequences of an attacker intercepting MFS data during a transaction,

c) protect MFS application and data at rest, and

d) compensate service failures by using redundant components.

MFSPs should develop, adopt, and evaluate a risk evaluation and a security program. The program should include the following items:

— an assessment of the security risks associated with the MFS, their relevance, and the early identification of security mechanisms to mitigate them;

— the identification of MFS data valuable for fraudsters:

  — personal identifiable information (PII) with commercial value;

  — authentication credentials;

  — information facilitating access to the bank accounts;

  — information allowing access to the electronic money accounts.

— the identification of MFS data that may be used to track customers;

— the financial losses resulting from a successful attack and a calculation of the probability of such attack to succeed. Then an assessment as to whether the risk is acceptable or not along with an evaluation of the investment in security required to minimize the risk. Methodologies can be found in bibliography;

— the analysis of the impact in terms of customer inconvenience if the MFS is successfully attacked. For example, if customers will be forced to deactivate the application or if they will be unable to access their accounts until the security incident is fixed;

— the individual contribution of each MFSP to the global cost for implementing the MFR program risk mitigation policy.

The implementation of a successful security program requires that

— the MFSPs involved in the program know and fulfil their obligations in terms of security policy requested to their respective providers (e.g. security evaluation and certification for products involved in the MFS);

— the MFSP implementers have sufficient training and the MFSP customers have been properly educated in good practices in terms of risk prevention, and

— the MFSP and their subcontractors have the technical and operational means to monitor and if necessary to enforce the fulfilment of these security obligations (e.g. assignment of a "system supervisor").

A.2 Structure of the risks for mobile financial services

Each MFSP program is expected to implement the processes required for the proper management of the following risks:

— settlement risk, or risk that a participant in the MFSP program becomes insolvent;

— business risk, or risk that one of the participants in the MFSP program can no longer continue to operate the MFS (e.g. recurrent financial losses);

— operational risk or risk that MFS is disrupted for any reason: component or network failure of successful attack (e.g. denial of service attack);

— financial losses for different reasons including

  a) unexpected level of fraud,

  b) costs to investigate and fix technical incidents,

  c) reputational loss due to poor MFS availability,

  d) costs due to legal suits by customers or fines due to the improper implementation of regulatory provisions, and

  e) evolution of exchange rates;

— legal risks, or risks resulting from unstable regulatory frameworks that may constrain or modify the roles and responsibilities of the MFS program (e.g. by imposing a liability shift). Legal risks also arise because of the difficulty to comply with new regulatory requirements such as anti-money laundering provisions or data privacy.

MFSPs are susceptible to operational, legal and operational risks, due to the intrinsic complexity of MFS. Tighter interdependencies among systems, however, change the nature of risks for the MFSPs and they also create new challenges for achieving effective overall risk management. One example is when the MFSPs share common infrastructures, whose disruption provokes loss of transactions for all the MFSPs and increases the probability of the other types of risk to arise (business, settlement). In that case, operational risks may be minimized by using redundant infrastructures, which requires investment the corresponding cost vs benefit analysis.

Additional information on methodologies for risk assessment and control can be found in the bibliography.

A.3 Security, data protection and MFS misuse risks

— Data security risks, including the unauthorized modification, destruction or disclosure of data used in support of a MFS. These risks are minimized by the use of mobile financial application security countermeasures, tamper-resistant secure environments and certified cryptographic modules.

— Mobile devices introduces new privacy risks. The mobile device includes technical features such as GPS and location-based services, camera technology, etc. that can potentially expose sensitive consumer PII to be used without the consumer's explicit consent ("i.e. opt-in) and could lead to potential harm and unintended consequences. Mobile financial applications installed on the mobile device often draw on location, contact lists and other personal data, raising the need for additional safeguards for how data is appropriately collected and used. MFSPs shall use data only for the purposes of processing and settling transactions, and not any other purpose without the explicit consent of a customer.

  MFSP should be aware that there are risks both to themselves and to customers associated with the over-collection of personal data, particularly if such data are stolen or lost;

— Illicit use risk, related to the misuse of mobile financial service for financial crime, for instance of money laundering or financing terrorism. In order to mitigate them, three major countermeasures are legally enforced:

  — the Know-Your-Customer (KYC) rules, that MFSPs must apply;

  — the obligation for the MFSPs to identify sufficiently the payer and the payee involved in a transfer of funds;

  — the MFSP report to the financial supervision authority of suspicious transactions.

Refer to Annex B for additional information.

From the MFSP's prospective, threats arise specially from the vulnerabilities of those parts of the MFS infrastructure that are not under its direct control, including the mobile device, wireless and internet networks.

The following list consists of a series of recommended "security management good practices" for MFSPs.

a) Employ appropriate risk management practices already implemented and extend these practices, as available, to any wireless communications protocol employed by the MFS (e.g. wireless channels, cloud, NFC) by

   — using robust standard cryptography, and

   — elaborating a complete security evaluation and certification program, covering mobile financial applications, mobile devices, platforms, and other related components that participate in transaction processing.

b) Establish a customer protection program.

c) Provide application management to control mobile financial applications (pre-) installation and lifecycle management in the mobile device.

d) Advise and/or to provide to the end-user mobile device security software (e.g. mobile device anti-virus regularly updated).

f) Adapt security methods to ensure fraud prevention and detection at mobile financial application level and in the back-office infrastructures.

g) Provide with appropriate customer authentication means.

h) Comply with the applicable rules related to Anti-Money Laundering and prevention of Financial Crime (i.e. know-your-customer).

i) Educate and inform users for the proper use and risks of MFS, including what to do in case the mobile device is lost or stolen or a suspicious transaction has been detected. However, it shall be recognized that consumers' possible actions are limited to measures such as choosing a strong mobile code, keeping the mobile code secret and reporting loss of a device.

j) Develop products and application compliant with ISO 12812 as contractually agreed with the MFSP.

k) Use exclusively components duly evaluated according to the certification program.

q) Ensure that security controls (e.g. one or more secure elements) are correctly powered up for "worst-case" consumption scenarios (e.g. fast execution of a cryptographic mechanism).

This document assumes that any MFSP may be the provider of security controls. Although the document largely assumes that a secure element should be used to protect the commercial assets related to an MFS, mobile devices that do not contain an SE may be able to perform some mobile payments. Therefore, the document should not be read as an absolute requirement that an SE be employed in protecting more sophisticated mobile banking services, given the present landscape of mobile.

A.4 Guidelines for establishing a liability policy

Unauthorized charges, legal protection, industry protection and mobile payment liabilities are described in Reference [14], pp 20-22. Extracts are given hereafter.

Unauthorized charges

Unauthorized charges in online and mobile payments include

— charges debited from an online consumer's account following misuse of financial or other personal information (such as a password enabling access to an online account, or credit/debit card number processed online), and

— charges that are otherwise debited from an online account without consumer consent. They may result from fraud, but this is not always the case. For example, they may arise through a payment being processed by a child in the absence of parental knowledge and/or consent.

Unauthorized charges occur when a third party uses the customer's financial information to purchase online without the consent and/or the knowledge of the customer. Stakeholders indicate that this type of fraud remains a major issue for online and m-payments. In many instances, such fraud is committed when a fraudster acquires and uses the personal data that a consumer has disclosed previously online; this is referred to as inline identity theft.

Despite efforts to enhance security, most online payment systems remain vulnerable to the problem of unauthorized charges. The types of vulnerability vary according to the payment means. Credit and debit cards, for example, were not originally designed for Internet use; those who steal credit card details can use the information to purchase an item without the need to physically possess the card.

Legal protection

Substantial efforts have been made by regulators to address concerns through the implementation of chargeback mechanisms.

Industry protection

Industry has also taken steps to provide consumers with protection through chargeback mechanisms.

Mobile payment liabilities

As regards mobile payments, some have called for enhanced protection of consumers against unauthorized charges. While incidents of theft and unauthorized charges are frequent, in a number of countries, consumers in most cases bear liability for potential financial loss. Under most countries' frameworks, if a consumer makes a mobile payment using a credit card or debit card (through a remote

mobile payment), the consumer is entitled to the protections attached to the card. However, if a payment service is provided directly by a mobile operator and the charges appear on the consumer's mobile phone bill, there may be no legal protections. Moreover, if a mobile operator asks a consumer to make a prepaid deposit to cover future charges, protections may also be absent.

OECD Recommendation on limitation of liability in e-commerce

The 1999 OECD e-commerce guidelines make the following recommendation:

"Section V Payment: Consumers should be provided with easy-to-use, secure payment mechanisms and information on the level of security such mechanisms afford.

Limitations of liability for unauthorized or fraudulent use of payment systems, and chargeback mechanisms offer powerful tools to enhance consumer confidence and their development and use should be encouraged in the context of electronic commerce".

These original guidelines were further confirmed in 2014 by the OECD policy guidance on Mobile and Online Payments and by the revised E-commerce guidelines issued in March 2016.

Annex B
(informative)

Mobile financial system implementation of Know-Your-Customer requirements

The potential of innovative MFS to facilitate financial crime is a concern for the regulators.

Legal frameworks have been established worldwide for the prevention of the use of the financial system for the purpose of facilitating financial crime (Law on the Prevention of Money Laundering and Terrorism Financing). They are also usually known as AML/CFT rules. In the context of this document, these rules apply to MFSPs which have to

— properly enroll new customers,

— identify the payer and the payee,

— report suspicious transactions to the authorities, and

— establish internal controls to prevent money laundering.

This Annex provides insight into the monitoring of mobile financial transactions in order to prevent, detect and block fraudulent mobile payments before they are executed.

A central requirement for MFSPs the process named “Know Your Customer” (KYC). This is reflected, though not exclusively, in the request to identify their customers (the so-called identification obligation) which results in laws introducing some rules in relation to non-face to face situations. In the financial services sector, these are the situations where the customer is not physically present when entering into a business relation or performing a transaction. For this standard, that corresponds to both mobile remote payments and mobile banking services.

In practice, application of AML/CFT rules results in:

a) the implementation by the MFSP of an Identification Management system able to proceed to a strong authentication of the originator (and the beneficiary in case of a payment transaction);

b) the implementation of specific processes for monitoring transactions and identify abnormal customer behaviours when using the MFS;

c) the eventual rejection of the authorization for a mobile financial transaction considered suspicious.

With this respect, the contactless capability of the mobile device and its ability to communicate with another contactless device such as a contactless card may provide a solution. A contactless card storing identity and authentication credentials might be used to strongly identify a customer. This card will then provide the KYC service to a mobile financial application using identity credentials issued by government authorities. This solution is under evaluation by several jurisdictions that have issued a National ID card with a contactless interface.

Annex C
(informative)

Cryptographic mechanisms for mobile financial services

C.1 General recommendations

ISO sub-committees JTC 1/SC 27 and TC 68/SC 2 collaborate in order to identify and select cryptographic mechanisms:

— primitives (e.g. algorithms, symmetric and asymmetric ciphers, key lengths);

— schemes (e.g. modes of encryption, authentication);

— protocols (e.g. authentication, electronic signature);

which are in principle suitable for use for MFS.

For MFS, the following cryptographic mechanisms should apply:

— as a general recommendation, ISO/TR 14742, maintained by ISO TC 68/SC 2 should be followed;

— ISO 9564-2 specifies which encryption algorithms may be used for encrypting PINs. They may apply as well to encrypt UVM (e.g. a mobile code);

— only cryptographic schemes which are provable in a strict mathematical sense should be used.

C.2 Implementing cryptographic solutions for mobile financial services

— Designers of cryptographic solutions for MFS have to make choices on the cryptographic algorithms and key lengths to be used taking into account security-cost trade-offs.

— The strength of a key is related to the "security in bits" of the key. A key strength "k" means that the complexity of the best known attack to recover the key is 2^k. The "k" factor for different key lengths is noted in Table C.1.

— National Security Bodies regularly publish recommendations for implementing (e.g. key lengths) cryptographic algorithms. In the bibliography, some useful references are available for implementers of cryptographic solutions for MFS. These references are not exhaustive, but provide a good overview of best practices.

— These recommendations, which may be legally binding, often set deadlines for migration towards more secure solutions (e.g. extended key lengths), facilitating the planning for the renewal of systems. However these recommendations are not always consistent and therefore, implementers should directly consult the applicable versions.

— As for any technical document, some of the provisions of published standards may at present be no longer appropriate (e.g. reported weaknesses/attacks after the standard publication). It is therefore recommended to regularly consult the ISO JTC 1/SC 27 Standing Document 12 (SD12) "Assessment of cryptographic algorithms and key lengths". It provides a help to make choices based on up-to-date information on the level of security of proved cryptographic algorithms using different key lengths.

— When appropriate, this Annex provides with examples (e.g. recommended key lengths for some crypto-algorithms).

C.3 Cryptographic algorithms and keys for mobile financial services

Standard Symmetric Ciphers

Symmetric ciphers constitute the basic mechanism for confidentiality of mobile financial transactions. Symmetric cipher is divided into block ciphers and stream ciphers. Block ciphers are much more used by the financial applications. Recommendations for use of Block Ciphers according to ISO/IEC 18033-3 are found in ISO/TR 14742. However, the fact that stream ciphers tend to be smaller and faster they can be relevant for applications with little computational resources like some mobile devices. If used, they should comply with ISO/IEC 18033-4.

Usually, the recommended key size is a lower bound which is specified by assuming that the best known attack against the symmetric cipher is the key exhaustive search. Once an attack better than the key exhaustive search is known, the key nominal length is no longer relevant as a measure of its security and instead the effective key size is used.

Standard Block Ciphers

Symmetric-key block ciphers encrypt an entire block of plaintext bits at a time with the same key.

— 3-DES is widely used for card payment online transactions. However, AES is therefore expected to be the dominant encryption algorithm next generation.

— AES is a modern block cipher which supports three key lengths of 128, 192 and 256 bits, providing excellent long-term security against brute-force attacks. There is no known attack on the full AES-128 which has any practical implementation on AES security. However, in 2011, a theoretical attack on AES was published (refer to bibliography).

Notice that ISO/TR 14742 for block cipher encryption recommends at least 96 bits of security. This value is not clearly justified and other choices appear preferable. For instance, France ANSSI recommends as a minimum 100 bits of security before year 2020, and 128 bits after 2020.

Standard Random Number Generation (RNG)

Good cryptography requires good Random Number Generation (RNG).

a) Almost all cryptographic protocols require the generation and use of secret values that shall be unknown to attackers.

b) Random Number Generators are required as an initial component to generate public/private key pairs for asymmetric (public key) algorithms.

c) Keys for symmetric cryptosystems are also generated randomly. RNGs are also used to create challenges, nonces (salts).

d) The generation of digital signature algorithms requires a high quality random number (e.g. for EC-DSA signatures, see below).

Because security protocols rely on the unpredictability of the keys they use, great care shall be taken in the development, testing, and selection of RNGs.

ISO/IEC 18031 provides guidance on mechanisms for high quality random number generation. The term “high quality” refers to both reliable and generating numbers with a high level of entropy. Statistical tests for randomness testing has been published by NIST/SP 800-22.

ISO/IEC 18032 completes ISO/IEC 18031, and specifies how to generate prime numbers once a good random is available.

Public-Key-Cryptography: RSA-based cryptosystem

RSA is the most widely used public-key cryptosystem that is going to increasingly coexist with ECC-based implementations.

Even if currently 1024-bit numbers cannot be factored, it is strongly advised to use RSA with a 2048-bit modulus when long-term security is a requirement.

NOTE EMVCo publishes every year an assessment for the validity period for the length of RSA keys for EMV cards and terminals.

Public-Key-Cryptography: Elliptic Curve implementation (ECC)

Elliptic curves can be used for digital signatures, key exchange protocols and for data encryption. ECC provides the same level of security as RSA or discrete logarithm systems with much shorter operands and therefore shorter cipher texts and signatures. ECC security level corresponding to AES-128 would require RSA-3072 and EC-DSA-256. Furthermore, NSA has recently published Suite B algorithms recommending only elliptic curves-based algorithms, and excluding RSA. The advantage for mobile payments usage is to shorten transaction time. Table C.1 provides the comparison in terms of required key length for a given level of security (first column from 80-bit level up to 256-bit) of symmetric key algorithms, RSA and ECC cryptosystems.

NOTE Table C.1 is just for comparison purposes and no particular level of security is recommended. Notice that ISO/TR 14742 for block cipher encryption recommends at least 96 bits of security.

Bits of security	Symmetric key algo's.	Discrete Logs (e.g. DSA,DH,MQV)	RSA	ECC (e.g. ECDSA)
80	2TDEA	L = 1024 N = 160	k = 1024	f = 160-223
112	3TDEA	L = 2048 N = 224	k = 2048	f = 224-255
128	AES-128	L = 3072 N = 256	k = 3072	f = 256-383
192	AES-192	L = 7680 N = 384	k = 7680	f = 384-511
256	AES-256	L = 15360 N = 512	k = 15360	f = 512

Table C.1 — Comparison between different levels of security

Until now, ECC implementations have not been widely used by the payments industry. However, on-going work has been launched by international payment schemes in order to specify ECC cryptosystems.

Standard Digital Signature

Digital Signature shall provide a signed mobile financial message with the security properties of message integrity, message authentication and non-repudiation.

Standard RSA Digital Signature

ISO/IEC 9796-2 covers RSA-based signatures which give message recovery. The last revision of this standard includes a new mechanism to avoid a published attack on a payment card.

The modulus of RSA digital signature schemes should be at least 1024-bit long. For long-term security, a modulus of length k = 3072 bits should be used.

Standard Digital Signature Algorithm (DSA)

It is a federal US government standard for digital signatures proposed by the NIST. It is a variant of the Elgamal signature algorithm. Its main advantage over the Elgamal signature scheme are that the signature is only 320-bit long and that it resists to some attacks proposed for the Elgamal signature.

The 1024-bit DSA variant is currently secure. The 2048-bit and 3072-bit variants provide with good long-term security.

Standard Elliptic Curve Digital Signature Algorithm (ECDSA)

The elliptic curve digital signature standard is ECDSA. There are national implementations standardized in ISO/IEC 14888-3. When comparing RSA and ECDSA performances, a difference is to be established between digital signature generation and digital signature verification.

ECDSA signature is always faster than the RSA whatever the component and the security level targeted. Moreover, the efficiency of the ECC in signature mode increases with the security level. For ECDSA, bit lengths in the range of 160-256 bit can be chosen which provide security equivalent to 1024-3072 bit RSA.

On the other side, the execution time of verification with ECC is longer than the execution time of verification with RSA. Verification with ECC requires the same cryptographic means and the same kind of execution time than for the signature with ECC which could not be the case for RSA. For RSA in case of small public exponent (this is the case here), the verification is very fast (since it is simpler in terms of cryptographic computations).

Standard Hash Functions

Hash functions shall at least have 160-bit output length in order to withstand collision attacks. Hash functions providing with a 256-bit output are strongly recommended for long-term security.

The on-going NIST SHA-3 competition shall result in new standardized hash functions likely by the time this standard will be published.

Standard Message Authentication Codes (MAC)

MAC provide with two security services, mobile financial message integrity and message authentication. The sender and the receiver (verifier) of the message share a secret key (of K bits). The first step of the MAC procedure consists therefore in the generation of session key.

They are based on block ciphers and hash functions.

Block Cipher MACs, using a Block Cipher in CBC (Cipher Chaining Mode) were standardized in the US and were widely used to provide integrity to financial transactions. NIST Special Publication 800-38D specified a MAC algorithm based on symmetric key block cipher, named CMAC.

CBC-MACs containing CMAC using a 128-bit (16-bytes) block cipher algorithm (ALG) such as AES in CBC mode is available in ISO/IEC 9797-1.

Hash function-based MACs are used with SHA-1; migration is expected towards modern Hash functions such as SHA-2 and SHA-3.

A MAC standard covering MACs based on universal hash functions (UMAC) is available in ISO/IEC 9797-3.

Standard Key establishment protocols

All the above security services assume that cryptographic keys have been generated and distributed between the parties involved in a mobile financial transaction. From the security point of view, the secure distribution of keys is one of the most sensitive issue. Usually, one party generates and distributes a secret key to the other part, using a Key Transport protocol.

In a second step, a Key Agreement protocol is executed to generate a session key derived from the original one. Standard mechanisms for key distribution may use either

— symmetric cryptosystems (ISO/IEC 11770-2), or

— asymmetric cryptosystems (ISO/IEC 11770-3).

Standard Cryptographic mechanisms for very short-time transactions

Last generation mobile devices have significant computing resources. Still, many mobile financial applications do not perform well due to the shortage of resources for computation, data storage, network bandwidth, and battery capacity. MFS involve the execution of applications, requiring complex crypto protocols to be executed.

The most straightforward architectural fix to the problems is to choose cryptography based on a standard, publicly scrutinized algorithm with an adequate key length. For instance, ISO/IEC 18033 provides with strong encryption algorithms based in both symmetric and asymmetric techniques with a large range of security levels. These and other well-proven and robust ISO cryptographic mechanisms for Authentication, Hash, MAC, Digital Signature and Key Management are available in ISO/TR 14742.

In addition, ISO/IEC 29192 (all parts) describes cryptographic mechanisms, designed for a good compromise in the triad security-execution times-complexity that makes them a possible complementary choice for mobile payments/banking for some applications.

For instance, ISO/IEC 29192-4 provides with a mechanism for fast secure element authentication and subsequent key exchange adapted to very fast contactless transactions. Depending on the length of the exchanged key, the lightweight protocol may be used to execute an encryption (e.g. as per ISO/IEC 18033-3).

Annex D
(informative)

Vulnerabilities and attacks on mobile financial services

D.1 Common to mobile financial services

Customers inevitably download files of many formats providing a door to vulnerabilities, especially if the customer does not proceed to install anti-virus/malware software. Mobile devices contain components (e.g. central processors and operating system, communication interfaces with the external world, mobile device booting subsystem, secure components) which are potential targets for attackers.

a) Malware as the source of many security threats

Often, mobile malware is designed to capture and misuse customer's financial and personal data.

— Malware installed in the mobile device may capture the UVM (e.g. the mobile code) entered by the legitimate customer to grant access to a payment application. Then the payment application may transmit genuine data to another mobile device which is being used in a proximate contactless transaction.

— Installation of malware in the mobile device also may allow for a series of attacks on transactional data that are detailed bellow.

— Malware may also be used in a Denial-of-Service attack preventing the legitimate customer to initiate a payment.

b) Eavesdropping

Eavesdropping is a specific passive attack that requires a passive attacker with an antenna to tamper the communication channels established over-the-air by the mobile device and record the transaction details, without disturbing either the message or the channel. For mobile proximate payments, the NFC interface implements a bidirectional communication over the air and transactions can be eavesdropped by a spying probe. The main point is how close the attacker needs to be to record an exploitable signal. The published results are controversial. The reason is probably that the environmental conditions have a major impact on the reading distance. On the other hand laboratory results do not necessary reproduce in-field conditions.

Establishing a secure channel between the mobile device and the terminal or to a remote MFS gateway is an obvious countermeasure to protect against eavesdropping and any kind of data modification attack.

This secure channel, using a key exchange protocol, can be performed with or without executing a previous mutual authentication:

— with no authentication;

— with secure element/mobile financial application authentication;

— with mutual authentication.

c) Skimming

Skimming refers to an active attack to start a transaction with a mobile device unaware of the legitimate owner. It requires the remote activation of the mobile device NFC interface or another data communication channel of the mobile device without the consent of the owner. Skimming is perceived as a considerable threat by payers and from a business prospective represents a key security concern for mobile payment contactless products.

A possible countermeasure is to include an anti-skimming feature in the mobile device. The second concern relates to the protection of any confidential data that can be guaranteed by the creation of a secure channel with a negotiated cryptographic session key having the sufficient entropy.

Some crypto-protocols do not implement anti-skimming features, which results in the uncontrolled disclosure of information by the mobile device at the beginning of any transaction, legitimate or not. Other than fraud risks, there is a concern for privacy, due to the problem raised for the transmission in the clear of the certificate stored in the secure element at the beginning of the execution of the protocol. Therefore, the traceability of the user is in theory possible. In a privacy-respective, design protocols should include a first stage so that this certificate be transmitted encrypted.

d) Relay Attack

In a Relay Attack, a fake NFC mobile device is used to pay to a legitimate contactless POI (e.g. a PCD according to ISO/IEC 14443) by using application-level data generated by a legitimate mobile payment application (e.g. resident in a contactless card or in a secure element) that has been skimmed by using a fake reader (e.g. a second NFC, see Note). Actually, the contactless transaction takes place between two legitimate contactless applications, unaware of the attack.

With remote relay attacks, malware installed in the rich-OS of the victim mobile device could conduct unauthorized payments by channelling for instance legitimate NFC communications to a remote attacker, allowing to make purchases without the physical possession of the victim mobile device.

Relay attacks are not so easy to circumvent because, the attacker does not need to get access to the data in-clear.

Transaction blocking is possible with an active attack by merely emitting spurious radio signals centred in the carrier frequency of 13,56 MHz that saturate the receiver stage of the communicating devices.

e) Denial of service/data modification

The mobile device becomes irresponsive because the communication channel is blurred or modified. This attack is possible because the signals exchanged are very weak. While this attack does not bring any economical benefit for the attacker nor results in a financial loss for the victim, it may damage the reputation of the MFSP.

f) Man-in-the-Middle

Man-in-the-Middle attacks are not considered to represent a significant risk in the NFC context, in the current state-of-the-art, provided that the two communicating parties are legitimate. The reason is that a man-in-the-middle involves eavesdropping the signal sent by A to B, then avoiding (for instance, blurring the B receiver) B to receive the eavesdropped data and finally resending B a message generated by the attacker as it was from A, when A is still sending the original message to B. This scenario is considered practically unfeasible by using RF signals. With remote Man-in-the-Middle attacks, the fraudster will use different techniques, such as phishing and pharming, to redirect the customer to a rogue website.

NOTE These attacks are also possible during a transaction between a contactless card and a contactless reader. However, the computational capabilities of the mobile device and their ability to emulate both a contactless reader and a contactless card increases the risk of misuse of a NFC mobile devices for active attack purposes.

D.2 Vulnerabilities and attacks specific to remote MFS

The mobile device connects to a remote gateway using a wireless network.

Figure D.1 indicates the main elements of a standard secured architecture for the operation of remote MFS. The objective is to establish a secure communication channel between the application resident in the mobile device and the server of the Institution.

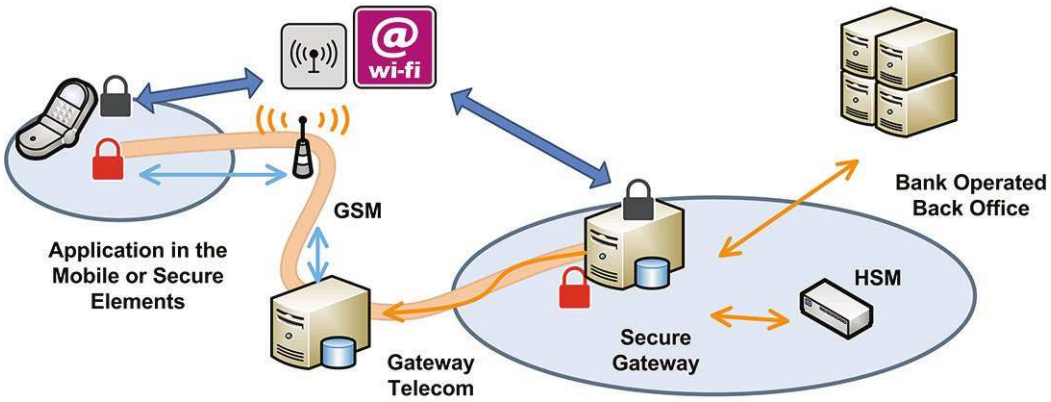

Figure D.1 — Typical architecture for the provision of remote MFSs

To proceed to the remote payment, the payer's mobile device is directly connected to a wireless infrastructure whose security provisions have not been designed to support payments. At this point, the payer is acting exclusively as an authenticated customer by the operator of the network.

The payer, for instance, may select a remote mobile payment application stored in the secure environment of the mobile device. If the payer is successfully authenticated, then s/he is permitted to select a mobile application to initiate a connection request with the remote mobile payment service gateway, which in turn shall proceed to its customer authentication process for the selected payment application

Compared with proximity contactless payments, remote mobile payments raise different risk issues. Whereas the main concerns for NFC payments are represented by skimming and eavesdropping, the main threats to mobile remote payments are the need to implement a strong user authentication, the confidentiality and integrity of the exchanged messages and the need to generate a strong proof of consent.

The security channel leading from the mobile financial application to the MFSP is longer and is out of control of the MFSP. Secondly, physical authentication of the payer is no possible and strong online authentication process is required to verify a claimed identity and authorize the service. This means that authentication information is to be transmitted through unsecure networks.

In addition, so far many in-field implementations are software based and make use of generic GSM or other standard short message services. Fraudsters have continued to develop and deploy more sophisticated, effective, and malicious methods to compromise authentication mechanisms and gain unauthorized access to customers' online accounts. In this context at least two different use cases are to be analysed:

a) the payer connects with his/her MFSP either directly or by the intermediate of a third-party payment;

b) the payer is connected with a MFSP during a mobile commerce transaction. In that case, the payee is an online retailer.

D.3 Vulnerabilities and attacks to mobile banking

Usually, a mobile banking operation involves an exchange of data between "entities" that have a separate and distinct existence that can be uniquely identified. Bank account holders, financial institutions, online system operators, relying parties and even a government agency are examples of such entities.

Different mobile banking services and the related transactions represent different risks to the financial institutions and the customer. These risks are to be addressed differently under the provisions of a global security policy. Authorization for a remote banking operation requires prior authentication

of the requesting user. Therefore user and bank authentication constitute key security processes for mobile banking.

The mobile banking transaction intends to connect a customer with a bank server, after some authentication procedure. If the procedure does not require the authentication of the bank server by the cardholder, the following vulnerabilities apply.

a) The user may not be connected to a genuine web server – hence it may be falsely redirected.

b) A genuine (but fraudulent) web server may falsely redirect the user browser.

c) False redirection is likely to mean that the user will be disclosing authenticating data.

Financial institutions implementing mass strong authentication and fraud management systems for online banking shall consider the impact on usability. A too-high rate of false rejections when authenticating is likely to cause a dramatic surge in customer service calls and irritated customers.

Bibliography

[1] Bank for International Settlements (2003), Risk Management Principles for Electronic Banking

[2] European Payments Service Directive (2007/64/EC)

[3] ENISA: Smartphones: Information Security risks, opportunities and recommendations for users. December 2010

[4] European Central Bank: Electronic Money System Security Objectives May 2003

[5] The World Bank- Committee in Payment and Settlement Systems. General principles for international remittance services. January 2007

[6] Global Platform-TEE Secure Element API Specification v1.0

[7] Global Platform-TEE System Architecture v1.0

[8] Payment Card Industry (PCI) Payment Application Data Security Standard Requirements and Security Assessment Procedures Version 2.0 October 2010

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

[10] NIST. Draft NIST SP 800-78-4 Cryptographic Algorithms and Key Sizes for Personal Identity Verification available at http://csrc.nist.gov/publications/drafts/800-78-4/sp800_78-4_draft.pdf

[11] ENISA. Algorithms, Key Sizes and Parameters Report- 2013 recommendations v1.0 October 2013 available at http://www.enisa.europa.eu/

[12] European Payments Council. EPC342-08 Guidelines on algorithms usage and key management v3.0 available at http://www.europeanpaymentscouncil.eu/

[13] ISO JTC1 SC27 Standing Document 12 – Assessment of cryptographic algorithms and key lengths available http://www.jtc1sc27.din.de/sbe/SD12

[14] OECD Digital Economy paper no 204. Report on consumer protection in online & mobile payments. 2012

[15] Consumer Policy guidance on mobile & online payments. OECD February 2014

[16] Recommendation of the OECD Council concerning guidelines for consumer protection in the context of electronic commerce.OECD 1999

[17] W3C Recommendation (2008): "XML Signature Syntax and Processing"

[18] ETSI EN 319 102*Electronic Signatures and Infrastructures (ESI) — Procedures for Signature Creation and Validation*

[19] FFIEC IT Examination Handbook

[20] Bogdanov Andrey, Khovratovich Dmitry, Rechberger Chirstian (2011) "Biclique Cryptanalysis of the Full AES"

[21] GlobalPlatform-Card Composition Model v1.1 (2012)

[22] OECD Consumer protection in e-commerce: OECD recommendation. Paris 2016

[23] ISO 15782, *Certificate management for financial services*

[24] ISO 16609, *Financial services — Requirements for message authentication using symmetric techniques*

[25] ISO 21188, *Public key infrastructure for financial services — Practices and policy framework*

[26] ISO/IEC 9796-2, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms*

[27] ISO/IEC 9796-3, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 3: Discrete logarithm based mechanisms*

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

[29] ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories*

[30] ISO/IEC 17065, *Conformity assessment — Requirements for bodies certifying products, processes and services*

[31] ISO/IEC 18031, *Information technology — Security techniques — Random bit generation*

[32] ISO/IEC 18092, *Information technology — Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1)*

[33] ISO/IEC 24759, *Information technology — Security techniques — Test requirements for cryptographic modules*

[34] ISO TS 12812-4, *Core banking — Mobile financial services — Part 4: Mobile payments-to-person*

[35] ISO TS 12812-5, *Core banking — Mobile financial services — Part 5: Mobile payments to business*

[36] ISO/IEC 9797 (all parts), *Information technology — Security techniques — Message Authentication Codes (MACs)*

[37] ISO/IEC 14888 (all parts), *Information technology — Security techniques — Digital signatures with appendix*

[38] ISO/IEC 18033 (all parts), *Information technology — Security techniques — Encryption algorithms*

[39] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

ICS 03.060

Price based on 56 pages