International Standard

ISO 5201

First edition

Financial services — Code-scanning payment security

PROOF/ÉPREUVE

Reference number
ISO 5201:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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 document 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of 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 www.iso.org/iso/foreword.html.

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Code-scanning payment is a type of mobile payment service in which the payer uses a mobile device to present a payment code image to a payee for scanning or scans a payment code image presented by the payee.

This document focuses on the security aspects of code-scanning payment. This document is structured according to a risk-based analysis approach as specified in ISO 31000 and ISO/IEC 27005.

Clause 5 sets up the scope and context of the security analysis by giving an overview of code-scanning payment. The basic framework is defined and the major roles are described. Some basic steps are mandatory for these types of payment services, but there are many variations in practice because flexibility is one of the major benefits of code-scanning payment. Various implementations can be roughly classified into two categories: payer-presented mode and payee-presented mode. The risk assessment (see Clause 7) and security requirements and guidelines (see Clause 8) are based on these two implementation modes.

Clause 6 clarifies the security target objectives.

Clause 7 is the risk assessment of code-scanning payment. Security risks are identified and categorized according to the implementation modes.

Clause 8 presents the security principles, requirements and guidelines on how to impose countermeasures to control (mitigate or reduce) the risks identified in Clause 7. Minimum security requirements are the security baseline for all code-scanning payment service providers. Security guidelines are categorized by implementation modes, which are the best practices recommended for the code-scanning payment service providers.

Annex A provides more details of the two implementation modes described in Clause 5, including the payment transaction processes and payment code examples.

Annex B provides more details to support the risk assessment in Clause 7.

Annex C provides common requirements on the approved algorithms and mechanisms for any cryptographic security measures used for code-scanning payment as defined in Clause 8.

Financial services — Code-scanning payment security

1 Scope

This document provides an overview, risk assessment, minimum security requirements and extended security guidelines for code-scanning payment in which the payer uses a mobile device to operate the payment transaction.

This document is applicable to cases where the payment code is used to initiate a mobile payment and presented by either the payer or the payee.

The following is excluded from the scope of this document:

— details of payer and payee onboarding;

— details of the supporting payment infrastructure, as described in 5.1.

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

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

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

ISO 20038, *Banking and related financial services — Key wrap using AES*

ISO/IEC 9796 (all parts), *Information technology — Security techniques — Digital signature schemes giving message recovery*

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

ISO/IEC 10118-1:2016/Amd 1:2021, *Information technology — Security techniques — Hash-functions — Part 1: General*

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

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

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

ISO/IEC 18033 (all parts), *Information security — Security techniques — Encryption algorithms*

ISO/IEC 19772, *Information security — Authenticated encryption*

NIST/FIPS PUB 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*

3 Terms and definitions

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

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

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

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

3.1
code image
symbolization of string constructed according to a defined format

EXAMPLE Code 128 as defined in ISO/IEC 15417 and QR code as defined in ISO/IEC 18004.

3.2
code-scanning
recognize and reveal the content of a *code image* (3.1)

Note 1 to entry: Not including interpretation of the code content.

3.3
code-scanning payment
payment transaction (3.10) initiated by *code-scanning* (3.2)

3.4
code service provider
CSP
logical role that manages the *payment code* (3.12) for the *payer* (3.9) or the *payee* (3.8), including generating, distributing and (optionally) resolving

Note 1 to entry: The responsibility of this logical role can be split between several physical entities.

3.5
eavesdropping
unauthorized interception and interpretation of information-bearing emanations

[SOURCE: ISO/IEC 18013-3:2017, 3.5]

3.6
mobile device
device that utilizes communication networks while in motion

[SOURCE: ISO/IEC 24771:2014, 3.1.17]

3.7
mobile payment
payment (3.10) involving a *mobile device* (3.6) and using a *payment instrument* (3.13) and associated infrastructures

[SOURCE: ISO 12812-1:2017, 3.29]

3.8
payee
person or legal entity who is the intended recipient of funds which have been the subject of a *payment transaction* (3.10)

[SOURCE: ISO 12812-1:2017, 3.38]

3.9
payer
person or legal entity who authorizes a *payment transaction* (3.10)

Note 1 to entry: The payer can be a *payment service provider* (3.15).

[SOURCE: ISO 12812-1:2017, 3.39, modified —Note to entry added.]

3.10
payment
payment transaction
act of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the *payer* (3.9) and the *payee* (3.8)

[SOURCE: ISO 12812-1:2017, 3.40]

3.11
payment application
application resident in the *payer's* (3.9) *mobile device* (3.6) which offers payment functionality

3.12
payment code
data string constructed according to a defined format or retrieved from a *code image* (3.1) used for the purpose of making *payments* (3.10)

Note 1 to entry: The symbolized form of a payment code is called a "payment code image".

EXAMPLE The payment code to represent an account or an order.

3.13
payment instrument
personalized device and/or set of procedures agreed between the *payer* (3.9) and the institution and used by the payer in order to conduct a *payment transaction* (3.10)

EXAMPLE Credit transfer, card payment and electronic money.

[SOURCE: ISO 12812-1:2017, 3.43]

3.14
payment scheme
set of rules, practices, standards and/or implementation guidelines agreed between scheme participants for the functioning of payment services and which is separated from any infrastructure or payment system that supports its operation

[SOURCE: ISO 12812-1:2017, 3.44]

3.15
payment service provider
PSP
entity that provides payment services to a *payment service user* (3.16)

EXAMPLE Account servicing payment service provider (ASPSP), payment initiation service provider (PISP), acquirer.

3.16
payment service user
PSU
natural person or legal entity making use of a payment service in the capacity of *payer* (3.9) or *payee* (3.8), or both

3.17
point of interaction
POI
point at which *payer* (3.9) and *payee* (3.8) interact for the purpose of conducting a *payment transaction* (3.10)

EXAMPLE Point of sales (POS), vending machine, payment page on merchant website, quick response (QR) code on a poster, *mobile device* (3.6) of the merchant.

3.18
risk
qualitative or quantitative measure, or both, of possible harm to a specified asset in a given threat environment

Note 1 to entry: In the financial industry, assets include transaction financial value, payment systems integrity and information security and privacy.

3.19
risk assessment
systematic process of evaluating the potential *risks* (3.18) involved in a projected activity or undertaking

3.20
secure element
SE
tamper-resistant platform in the *mobile device* (3.6) capable of securely hosting and executing applications and associated confidential and cryptographic data (e.g. key management)

[SOURCE: ISO 12812-1:2017, 3.50, modified — Example deleted.]

3.21
trusted execution environment
TEE
aspect of the *mobile device* (3.6) comprising hardware and/or software which provides security services to the mobile device computing environment, protects data against general software attacks and isolates hardware and software security resources from the operating system

[SOURCE: ISO 12812-1:2017, 3.60]

4 Abbreviated terms

B2C business to customer

IBAN international bank account number

P2P person to person

POS point of sales

QR quick response

TTL time to live

URL uniform resource locator

5 Overview of code-scanning payment

5.1 Basic framework of code-scanning payment

Figure 1 is a basic framework of code-scanning payment that illustrates the relationship between the different functional roles in the system.

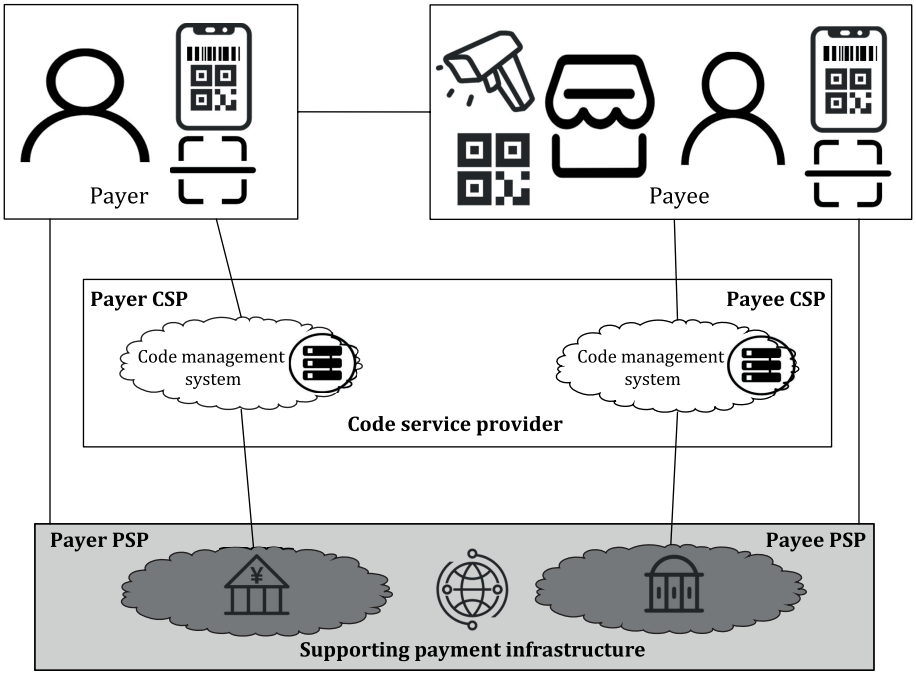

Figure 1 — Basic framework of code-scanning payment

The participants of a typical code-scanning payment transaction include the payer, the payee and the respective code service providers (CSPs) and payment service providers (PSPs). The payer CSP and the payer PSP can be the same entity; likewise, the payee CSP and the payee PSP can also be the same entity. In some cases, the payer CSP, the payer PSP, the payee CSP and the payee PSP can all be the same entity.

— Payer: The payer uses a mobile device to display and present their payment code image to the payee for scanning or to scan a payment code image presented by the payee. The payment application provided by the PSP or CSP and installed on the payer's mobile device offers these functions. In some cases, the payer can also use a static printout to present their payment code image. The payer can be either a person or a legal entity.

— Payee: The payee uses an appropriate equipment to scan the code image presented by the payer or any point of interaction (POI) equipment to display and present the payee code image to the payer for scanning. The payee can be either a person or a legal entity.

— PSP: The PSP accepts the payment instructions from the payer, or the payment requests from the payee, and processes the payments for them. This is a collective logical role which can contain several different physical entities. The major component in the PSP domain is the supporting payment infrastructure.

NOTE 1 As stated in Clause 1, the details of the supporting payment infrastructure are out of scope, so it will be treated as a secured black box and taken as a security assumption for the whole document. For a typical payment transaction, it usually consists of three physical entities: an acquiring service provider (acquirer) who serves the payee; an account service provider (ASPSP) who serves the payer; and a payment scheme which carries out clearing and settlement. An acquiring service provider usually maintains a payment service user (PSU) account management system, which contains necessary information for generating the payee's payment code. Similarly, an account service provider usually maintains a PSU account management system, which contains necessary information for generating the payer's payment code. For a person-to-person payment, there are two account service providers and no acquiring service provider. In some cases, the acquiring service provider and account service provider are the same physical entity, so there is no payment scheme involved.

— CSP: The basic function of the CSP is to generate and distribute the payment code for the payer or the payee. Optionally the CSP can resolve the payment code for the PSU.