International Standard

ISO 5201

First edition
2024-04

Financial services — Code-scanning payment security

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 and assumptions.

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 applicable to both implementation modes are the security baseline for all code-scanning payment service providers. Additional security guidelines are categorized by implementation modes, and presented as 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, *IT 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.

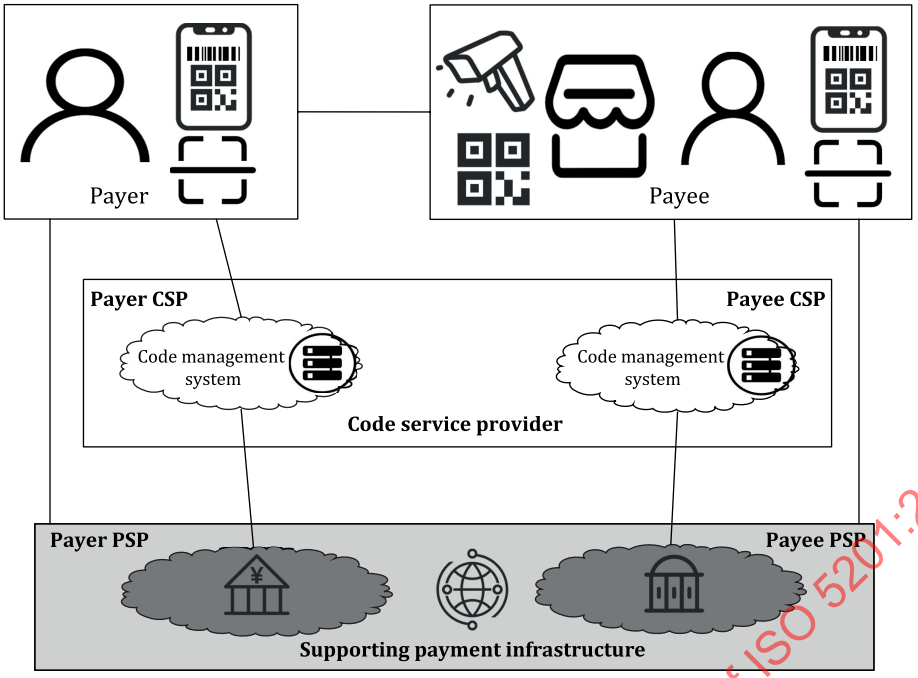


Figure 1 — Basic framework of code-scanning payment

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.

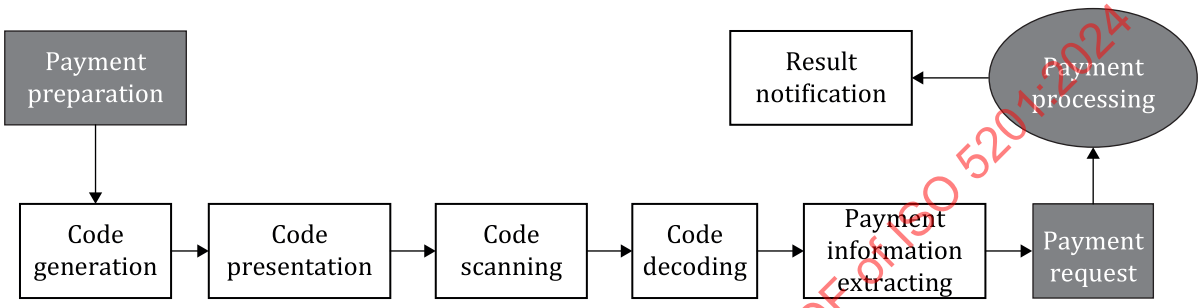
NOTE 2 The CSP needs to collect necessary information from the PSU account management system inside the supporting payment infrastructure. The composition of the code management system is very flexible. It can be an integrated part of the acquiring service provider's platform and/or the account service provider's platform or an independent service provided by a technical vendor.

Figure 1 provides an outline of the basic framework. The participants involved can vary based on implementation.

5.2 Mandatory steps and implementation modes of code-scanning payment

5.2.1 Mandatory steps

Figure 2 is an abstraction of the mandatory steps of code-scanning payment.



NOTE The white boxes are the target of evaluation (TOE) of this document. The grey boxes are out of scope.

Figure 2 — Mandatory steps of code-scanning payment

All the steps are mandatory, but the implementation of a code-scanning payment system is very flexible. The mandatory steps in Figure 2 can be carried out by different entities involved in a payment transaction. Variations of code-scanning payment systems can be roughly classified into two categories: payer-presented mode and payee-presented mode.

5.2.2 Payer-presented mode

In this mode, the payment code image is generally presented by the payer, as a symbol that is dynamically generated and displayed on the payer's mobile device. The payer-presented code is usually generated by the payer CSP and sent to the payer's mobile device at the time of payment; however, in some cases it can be prefetched and stored locally, or locally generated from a shared secret between the payer's mobile device and the payer CSP.

In some cases, a code image that is pre-generated by the payer CSP is sent to the payer in a static form, such as printed on a card medium, and displayed to the payee at the time of payment.

At the time of payment, the code is presented to the payee, who then scans the presented code using the payee's POI.

A payer-presented payment code should contain the information or the secure link to appropriate information to directly or indirectly identify a payer and can at the same time serve as an authorization credential.

More details can be found in Clause A.2.

5.2.3 Payee-presented mode

In this mode, the payment code image is generally presented by the payee as a symbol that is:

— printed on a printable surface (e.g. paper card, adhesive sticker or a receipt); or

— displayed on the merchant's POI.

At the time of payment, the code is presented to the payer, who then scans it using their mobile device. The code can be static or dynamic.

A static payee-presented code contains information that is intended for repetitive use. At a minimum, it should contain the information or the secure link to appropriate information to directly or indirectly identify the payee.

A dynamic payee-presented code should contain the information or the secure link to appropriate information to directly or indirectly identify a payee as well as to a specific payment transaction, such as the amount to be paid. Information included in a dynamic code varies by transaction (e.g. the payment amount, transaction ID).

More details can be found in Clause A.3.

6 Security target objectives and assumptions

This document specifies the following as the high-level security target objectives for the code-scanning payment schemes:

a) Only the intended payer can initiate and/or authorize the transaction.

b) Only the intended payee can receive funds.

c) The payment amount is equal to the transferred value as intended by both payer and payee.

NOTE If, for example, a tip needs to be added in the payment amount, it still needs to be agreed by both payer and payee. In this case, the payment amount is made up of the invoice amount and the tip amount.

d) Sensitive information and data, such as payment account and payment amount, are only accessible by authorized entities.

e) Code-scanning payment services do not elevate the level of traditional risks in an electronic payment system, such as cyberattacks, money laundering or fraud.

Further guidance on risk management is provided in ISO/IEC 27005.

The following security assumptions are made for the risk analysis in Clause 7 and security measures in Clause 8:

— A properly developed and secured payment application shall be provided to each PSU before the code-scanning payment service is activated.

— The code content shall be designed to disallow the initiation of payment transaction by insufficiently secured applications.

7 Risk assessment of code-scanning payment

7.1 General

The risks listed in 7.2, 7.3 and 7.4 are sorted according to the steps in Figure 2.

7.2 Common risks to both modes as defined in Clause 5

7.2.1 Com_Risk_1: unauthorized user

The payment application is used by an unauthorised user to make payments through code-scanning.

NOTE This could be the result of, for example, loss or theft of the mobile device or loss or theft of user credentials.

7.2.2 Com_Risk_2: illegitimate code content

The presented code contains content which can be harmful to the PSU, the scanning device or the payment scheme.

EXAMPLE 1 The data retrieved from the code directs the PSU to malicious resources, causing fraudulent payment transactions, enabling identity theft, presenting offending information, etc.

EXAMPLE 2 The data retrieved from the code fails the demanded integrity verification due to various reasons such as lack of digital signature.

EXAMPLE 3 The scanning device is interfered, corrupted or infected when decoding or processing the code content.

7.2.3 Com_Risk_3: tampered code image

The printed or displayed image of the presented code is replaced or modified.

7.2.4 Com_Risk_4: insecure message transmission

The payment transaction messages are eavesdropped, modified or replayed when they are transmitted over the communication channel between the payer and the payer's CSP or PSP and/or between the payee and the payee's CSP or PSP.

7.2.5 Com_Risk_5: payer sensitive information leakage

The payer's sensitive information, except the code values and/or related parameters as in PrP_Risk_1 (see 7.3.1) and PrP_Risk_2 (see 7.3.2), is stolen by attackers and leveraged for malicious purposes, such as fraud.

EXAMPLE The payer's authentication credential(s), user ID.

NOTE Such information could be stored in the payer's device; obtained from the payer-presented code and stored in the payee's POI and/or the payee's backend; stored at the CSP; or transmitted on the network.

7.2.6 Com_Risk_6: payee sensitive information leakage

The payee's sensitive information, except the code image, is stolen by attackers and leveraged for malicious purposes, such as fraud.

EXAMPLE The shared secrets between the payee and the payee CSP or PSP, the payee's IBAN.

NOTE Such information could be obtained from the payee-presented code and stored in the payer's device; stored in the payee's POI and/or the payee's backend; stored at the CSP; or transmitted on the network.

7.2.7 Com_Risk_7: routing conflict

The format of code content of multiple code-scanning payment schemes allows interpretation of content in a way that a different routing destination is identified than intended.

EXAMPLE See the case study in Clause B.3.

7.3 Risk assessment of payer-presented mode

7.3.1 PrP_Risk_1: stolen code value

The payer-presented code value is stolen and used without authorization when it is generated on the payer's CSP server, when it is transmitted over the communication channel between the payer and the payer's CSP server or when it is stored in the payer's mobile device.

NOTE This risk is applicable when the payment application fetches the code value from the server in real time or when it pre-fetches several code values to the device side in case there is a bad network connection when making a payment. See the case study in Clause B.2.

7.3.2 PrP_Risk_2: stolen code-generation parameters

The parameters used to generate the payer-presented code are stolen and used without authorization when they are generated at the payer's CSP or PSP, when they are transmitted over the communication channel between the payer and the payer's CSP or PSP or when they are stored in the payer's mobile device.

NOTE This risk is specific to those implementations which allow the payment application to generate the payer-presented code locally using some parameters shared with the payer's CSP. See the case study in Clause B.2.

7.3.3 PrP_Risk_3: breached encoding and decoding processes

The code generation and related payment information extracting processes are attacked and a legitimate code value is exploited and used without authorization.

7.3.4 PrP_Risk_4: captured code image

The code image is captured and used without authorization by an attacker or malicious merchant when being displayed.

7.3.5 PrP_Risk_5: tempered transaction parameters

The transaction parameters on the payee side are modified by an attacker or by the payee, intentionally or unintentionally.

7.4 Risk assessment of payee-presented mode

7.4.1 PeP_Risk_1: code abuse

The payee-presented code is misused for payment acceptance in scenarios which are not allowed as per the payee PSP's requirements.

EXAMPLE The code issued for in-store payment is misused for online payment or the code issued for a payee is misused for accepting payment by another illegitimate payee.

7.4.2 PeP_Risk_2: sensitive information in clear

The payee-presented code contains the payee's sensitive information in clear text. This information is obtained by attackers and leveraged for malicious purposes, such as fraud.

7.4.3 PeP_Risk_3: unintentional repeated payments

The payer(s) scans the same payee-presented code (static or dynamic) and makes repeated payments by mistake due to temporary network failure or other reasons.

7.4.4 PeP_Risk_4: attack on decoding process

The attacker impersonates the payer(s), obtains payee-sensitive information from the payee's CSP or PSP and leverages it for malicious purposes, such as fraud.

NOTE 1 This risk is applicable when some or all of the data required for payment initiation need to be retrieved from the payee's CSP or PSP based on a token, index or proxy contained in the payee-presented code. Refer to A.3.2.2.2 for an example code format.

NOTE 2 Token refers to a surrogate value for PSU identification and/or transaction data. If the token is included in the payee-presented data, it is referred to as a payee token; if the token is included in the payer-presented data, it is referred to as a payer token.

NOTE 3 Index refers to a pointer which can be used to retrieve a record from a database.

NOTE 4 Proxy, sometimes referred to as an “alias”, is the data required in order to retrieve a payment account identifier. For example, a mobile phone number or email address is used as a proxy to replace an international bank account number (IBAN).

7.4.5 PeP_Risk_5: forged payment notification

The payer or attacker forges a payment completion notification to fraudulently obtain the product or service.

EXAMPLE The payee confirms payment completion visually by looking at the payment notification information displayed on the payer’s mobile device; the payer cheats the payee by presenting a screenshot from a previous transaction.

8 Security measures to mitigate the risks in Clause 7

8.1 General

The security measures given in Clause 8, including requirements and recommendations, are sorted based on the steps in Figure 2. They do not reflect a priority order.

For less straightforward provisions, implementation guidance is provided.

These security measures are also roughly sorted against the risks identified in Clause 7. However, the relationship between risks and countermeasures are not strictly 1:1. Most of the risks are tangled with each other, correspondingly the security measures are also coordinated with each other to construct multi-layer protection to secure the code-scanning payment system.

Clause 8.2 provides common security measures which shall be applied together with the additional security measures in 8.3 or 8.4 which are specific to payer-presented mode or payee-presented mode, respectively.

8.2 Security measures to mitigate the risks in 7.2

8.2.1 Com_Measure_1: risk communication

The PSPs shall communicate the security risks associated with code-scanning payment to their PSUs and recommend good behaviours, including at least the following:

— Promote code-scanning payment security knowledge to improve safety awareness.

— Provide clear information on potential security risks and countermeasures that are likely to occur during the payment process, as in Figure 2.

— Enhance education on protection and management of sensitive data, such as transaction passwords and biometrics data.

— If static payer- or payee-presented payment codes are supported, disclose the corresponding risks and recommend countermeasures to the PSUs.

8.2.2 Com_Measure_2: payment application security

8.2.2.1 General

The payment application and the relevant data on the PSU’s device shall be protected from being compromised.

8.2.2.2 Implementation guidance

Relevant data means the data managed by the payment application.

Security hardening technologies, such as secure element (SE), trusted execution environment (TEE) and software code obfuscation, can be leveraged where appropriate.

Application-layer encryption and authentication shall be used to protect data flows, in addition to transport layer security.

8.2.3 Com_Measure_3: payer authentication

8.2.3.1 General

The payer shall be authenticated to the payer's PSP before they can use the code-scanning payment service.

8.2.3.2 Implementation guidance

The PSP can delegate the authentication to the payer's device, the payment application or the payment scheme.

8.2.4 Com_Measure_4: security protocols

8.2.4.1 General

Security protocols shall be used on the external open communication channels and should be updated to the latest stable versions.

8.2.4.2 Implementation guidance

Implement appropriate security controls such as transport layer security (TLS) and Internet Protocol Security (IPsec). TLS 1.2 or later version should be applied where appropriate.

Security protocols with mutual authentication should be used on the external open communication channels between the payee and the payee CSP or the payer and the payer CSP.

8.2.5 Com_Measure_5: anti cyber attacks

8.2.5.1 General

CSP and PSP shall implement security controls and practices to mitigate cyberattacks.

8.2.5.2 Implementation guidance

Obtaining an ISO/IEC 27001, ISO/IEC 27032 or similar certification can demonstrate such security capabilities.

8.2.6 Com_Measure_6: risk control

8.2.6.1 General

Transaction risk control functions shall be added to reduce the potential damages caused by the security risks associated with code-scanning payment.

8.2.6.2 Implementation guidance

The risk control system can identify abnormal payment transactions and take effective measures, such as refusing the transaction, sending an additional authentication challenge to PSU and sending a warning to PSU.

The risk control system can set payment amount limits, such as a daily limit, monthly limit and per-transaction limit according to the risk control policies. For an amount greater than the limits, the payment request can be declined or an additional PSU authorization can be launched.

8.2.7 Com_Measure_7: server-side sensitive information protection

8.2.7.1 General

The payer or payee's CSP server(s) shall protect the payer or payee's sensitive information at rest, in transit and in use.

8.2.7.2 Implementation guidance

Encryption should be applied where appropriate. The requirements on cryptography in Annex C shall be applied when encryption is implemented.

8.2.8 Com_Measure_8: avoid mis-routing

8.2.8.1 General

Mis-routing of the payment codes shall be avoided.

8.2.8.2 Implementation guidance

The identification of the CSP(s) should be coordinated (e.g. maintaining a registry for it) so that conflict can be avoided (e.g. when generating a payment code).

8.2.9 Com_Measure_9: protect printed code images

8.2.9.1 General

Printed code images shall be protected from being replaced, modified, covered or stained.

8.2.9.2 Implementation guidance

Besides the logical measures specified in 8.3.1 and 8.4.2, both PSUs shall take physical measures to protect the printed payment code images

Anti-counterfeiting measures should be applied to physically printed code images, e.g. covering the code images with physical medium, or accompanied with a security label which contains a unique security code.

In some cases, the code image is generated beforehand, distributed to the PSU on demand after appropriate identification and needs to be bound to the PSU's account before use. In such cases, the PSU should be reminded to bind the code image with their account immediately after the material is received and to keep the material attended when using.

For electronically displayed code images, the displaying screen should be attended or physically covered.

8.2.10 Com_Measure_10: reject illegitimate payment code

8.2.10.1 General

The payment application(s) or the payee's POI shall recognize illegitimate code format, reject them and prompt a warning message.

The payment application(s) or the payee's POI, the PSU's CSP or PSP, shall verify the integrity and authenticity of the payment code presented by the PSU, and reject illegitimate ones.

8.2.10.2 Implementation guidance

Encourage the PSU to scan a payment code with a properly developed, secured and personalized payment application or POI.

If a native camera application, instead of such a payment application, is used to scan the code, the payment application should be activated to process the following transaction steps.

8.2.11 Com_Measure_11: unique transaction ID

8.2.11.1 General

Each payment transaction shall be assigned a unique ID.

8.2.11.2 Implementation guidance

The transaction ID can be generated with or without semantic meaning.

Incorporating a timestamp, a counter or a random number as part of the transaction ID can make it unique.

8.2.12 Com_Measure_12: payment result notification

8.2.12.1 General

The PSUs shall be notified of the transaction result promptly, including the status, the amount and the payee, and be provided with a dispute resolution mechanism if they need to make a complaint.

8.2.12.2 Implementation guidance

Several notification methods can be offered to the payer, such as in-application messages or system notifications.

On the payee side, the point is to let the payee know the payment status so that they can decide when to deliver the service, e.g. by displaying payment status on the cashier screen or a voice announcement of payment status by the payee's payment application.

8.3 Additional security measures to mitigate the risks in 7.2 and 7.3

8.3.1 PrP_Measure_1: code content

8.3.1.1 General

The payer-presented code should contain certain information which can only be generated or resolved by the payer's CSP.

8.3.1.2 Implementation guidance

This recommendation applies to both static and dynamic payer-presented code.

Encryption should be applied where appropriate. The requirements on cryptography in Annex C shall be applied when encryption is implemented.

8.3.2 PrP_Measure_2: code generation and resolution requests

The payer's CSP should detect and refuse abnormal code generation or resolution requests.

8.3.3 PrP_Measure_3: encoding and decoding processes

8.3.3.1 General

The code generation and payment information extracting processes of the payer's CSP should be designed to protect against brute force attacks.

8.3.3.2 Implementation guidance

The length of the information retrieval ID in the payment code (refer to A.2.2.2) should be determined considering the time-to-live (TTL) of the payment code.

The CSP should be equipped with security measures to identify and combat brute force attacks, e.g. limiting the frequency of code-parsing requests.

8.3.4 PrP_Measure_4: pre-generated code

8.3.4.1 General

If multiple payment codes need to be generated beforehand, they should be encrypted at rest and in transit, and updated periodically.

8.3.4.2 Implementation guidance

The requirements on cryptography in Annex C shall be applied when encryption is implemented.

8.3.5 PrP_Measure_5: prefetched code storage

8.3.5.1 General

If the payment application needs to prefetch multiple payment codes beforehand, these codes should be stored on the mobile device in a secure way and should be bound to the unique ID of the mobile device and the operating system.

8.3.5.2 Implementation guidance

The requirements on cryptography in Annex C shall be applied when encryption is implemented.

Refer to Com_Measure_2 in 8.2.2 regarding requirements on payment application security.

8.3.6 PrP_Measure_6: prefetched code TTL

8.3.6.1 General

If the payment application needs to prefetch multiple payment codes beforehand, these codes should be stored with a limited TTL.

8.3.6.2 Implementation guidance

The TTL can be set according to the business requirements and the risk control capabilities of the CSP or PSP, e.g. 24 h. At the end of the TTL, the pre-fetched codes should be securely deleted.

8.3.7 PrP_Measure_7: secure code presentation

8.3.7.1 General

The payment application should detect and protect from side channel attacks, such as screenshot or memory scraping, when displaying the payment code.

8.3.7.2 Implementation guidance

The payment application can protect the payment code using strong authenticated encryption. The requirements on cryptography in Annex C shall be applied when encryption is implemented.

The payment application can also prohibit the screenshot function when displaying the payment code or provide corresponding security measures, such as reminding the user promptly or notifying the provider side to invalidate the displayed payment code when detecting a screenshot attack.

8.3.8 PrP_Measure_8: payee side sensitive information protection

8.3.8.1 General

The payee's POI and backend should take security measures to protect sensitive information obtained from the payment codes presented by the payer.

8.3.8.2 Implementation guidance

The payer-presented code usually contains a token which is used to authorize a payment transaction. This information is sensitive and should be encrypted in storage and transit to protect it from being disclosed and reused by an attacker.

In some cases, the payer-presented code also contains personal information about the payer. Such information should also be encrypted in storage and transit to protect it from being disclosed to an attacker.

The requirements on cryptography in Annex C shall be applied when encryption is implemented.

8.3.9 PrP_Measure_9: payee side tamper-proofing

The payee should be able to prevent external attackers or internal employees from maliciously modifying transaction parameters.

8.3.10 PrP_Measure_10: anti-replay

8.3.10.1 General

Payment processing should prevent attacks of replaying payer-presented codes.

8.3.10.2 Implementation guidance

If the payer-presented code is designed for a single use, it should be valid for only a defined duration (e.g. no longer than 60 s) after presentation.

If the payer-presented code is designed for multiple use, the payer should be asked to grant each payment transaction.

8.4 Additional security measures to mitigate the risks in 7.2 and 7.4

8.4.1 PeP_Measure_1: code data set

8.4.1.1 General

The data set contained in the payee-presented code should be minimized to avoid leaking sensitive information.

8.4.1.2 Implementation guidance

Some reference information to retrieve the payee's details from the provider side is recommended where appropriate, rather than including payee details in the payment code itself.

8.4.2 PeP_Measure_2: encryption in the code

8.4.2.1 General

If the payment code contains the payee's sensitive information, the sensitive information should be encrypted when the code value is generated.

8.4.2.2 Implementation guidance

The requirements on cryptography in Annex C shall be applied when encryption is implemented.

8.4.3 PeP_Measure_3: code presentation

Payee information should be printed or displayed clearly beside the code image so that the payer can verify.

8.4.4 PeP_Measure_4: CSP data set

For payee-presented code which contains some reference information to retrieve the payee's details from the provider side, the payee's CSP should only provide the minimum data set to the payer for payment initiation.

8.4.5 PeP_Measure_5: dynamic code

For payee-presented dynamic code that is intended for single use, the code value should be limited to a single payment transaction usage to avoid repeated payments, with a specific amount within a predefined time frame from the moment the code value is generated.

8.4.6 PeP_Measure_6: payer side sensitive information protection

8.4.6.1 General

The payment application should take security measures to protect sensitive information obtained from the payment codes presented by the payee.

8.4.6.2 Implementation guidance

Refer to Com_Measure_2 in 8.2.2 regarding requirements on payment application security.

The requirements on cryptography in Annex C shall be applied when encryption is implemented.

8.4.7 PeP_Measure_7: payer verification

After scanning and resolving the payment code, the payment application should remind the payer of the key transaction parameters, such as payee information and transaction amount, and ask for the payer's confirmation either before sending the payment request to the PSP or after the PSP has made additional analysis on submitted data and is waiting for payment release.

8.4.8 PeP_Measure_8: avoid repeated payments

8.4.8.1 General

The payment application should avoid inducing the payer to make repeated payments when there is an error, such as network failure.

8.4.8.2 Implementation guidance

When the network connection is unstable and the payment request and/or response is delayed, the payment application can freeze the payment button and display a progress bar to the user to avoid repeated attempts.

8.4.9 PeP_Measure_9: payee code management

The payee's PSP should take measures to ensure that the payee-presented code is used for payment acceptance in scenarios which are consistent with the payee PSP's requirements.

Annex A
(informative)

Implementation modes of code-scanning payment

A.1 General

This annex provides more details to support the overview of code-scanning payment in Clause 5.

A.2 Payer-presented mode

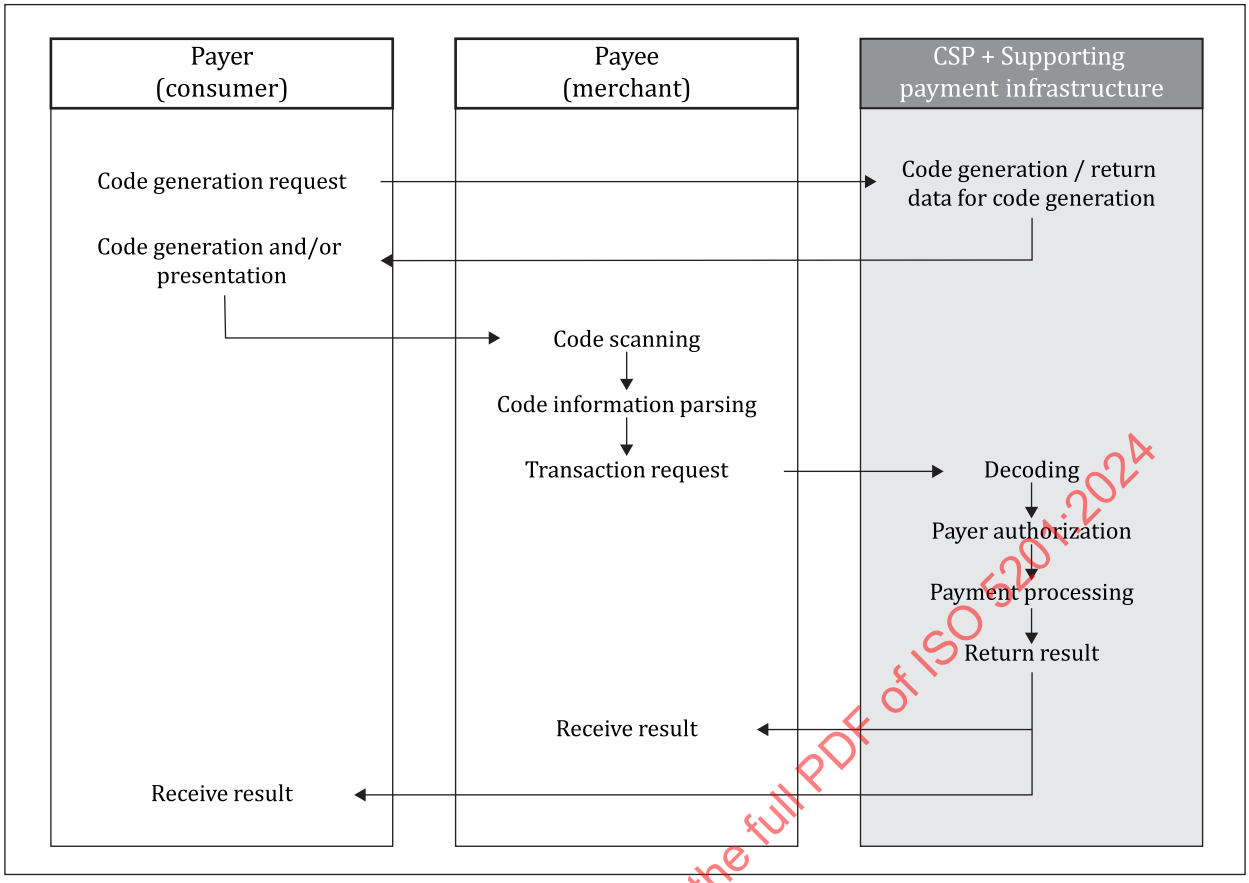
A.2.1 General

In this mode, the code image is displayed on the payer's mobile device at the time of the payment and presented to the payee equipment, which then scans (optically reads) the code.

A.2.2 Dynamic code

A.2.2.1 Steps

Figure A.1 illustrates a typical dynamic payer-presented mode implementation of the mandatory steps in Figure 2.



NOTE The grey boxes on the right side indicate that some of the components and processing details are out of scope. See Figure 1 and Figure 2 for details.

Figure A.1 — Payer-presented mode payment process — B2C transactions

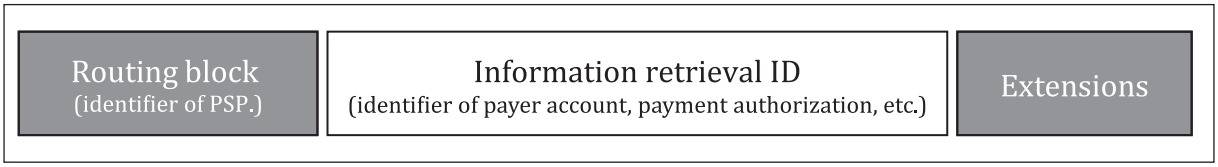
A.2.2.2 Code formats

A.2.2.2.1 General

A payer-presented payment code should contain the information or the secure link to necessary information to identify a payer and at the same time as an authorization credential of paying the required amount of money.

A.2.2.2.2 Example 1

One example composition of payer-presented payment code is presented in Figure A.2. This form of code can consist of pure digits and symbolized using one-dimensional codes, such as Code 128 defined in ISO/IEC 15417, or two-dimensional codes, such as QR code defined in ISO/IEC 18004. Since this form of code can be symbolized using one-dimensional codes, payees (merchants, in the case of B2C transactions) can make use of conventional one-dimensional code scanning equipment, which they have implemented in the past for product barcode scanning or other purposes.



Key

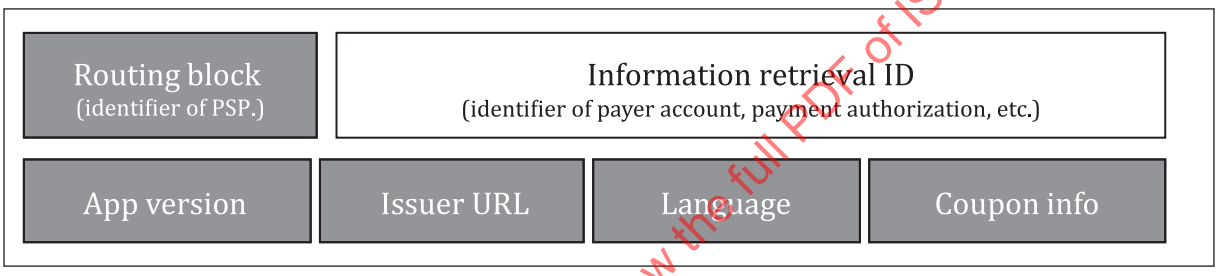
necessary information

optional information

Figure A.2 — Payer-presented mode code format — Example 1

A.2.2.2.3 Example 2

Another composition of payer-presented payment code is presented in Figure A.3. Two-dimensional codes, such as QR code defined in ISO/IEC 18004, which is able to contain more information, is more suitable for this form of code.



Key

necessary information

optional information

Figure A.3 — Payer-presented mode code format — Example 2

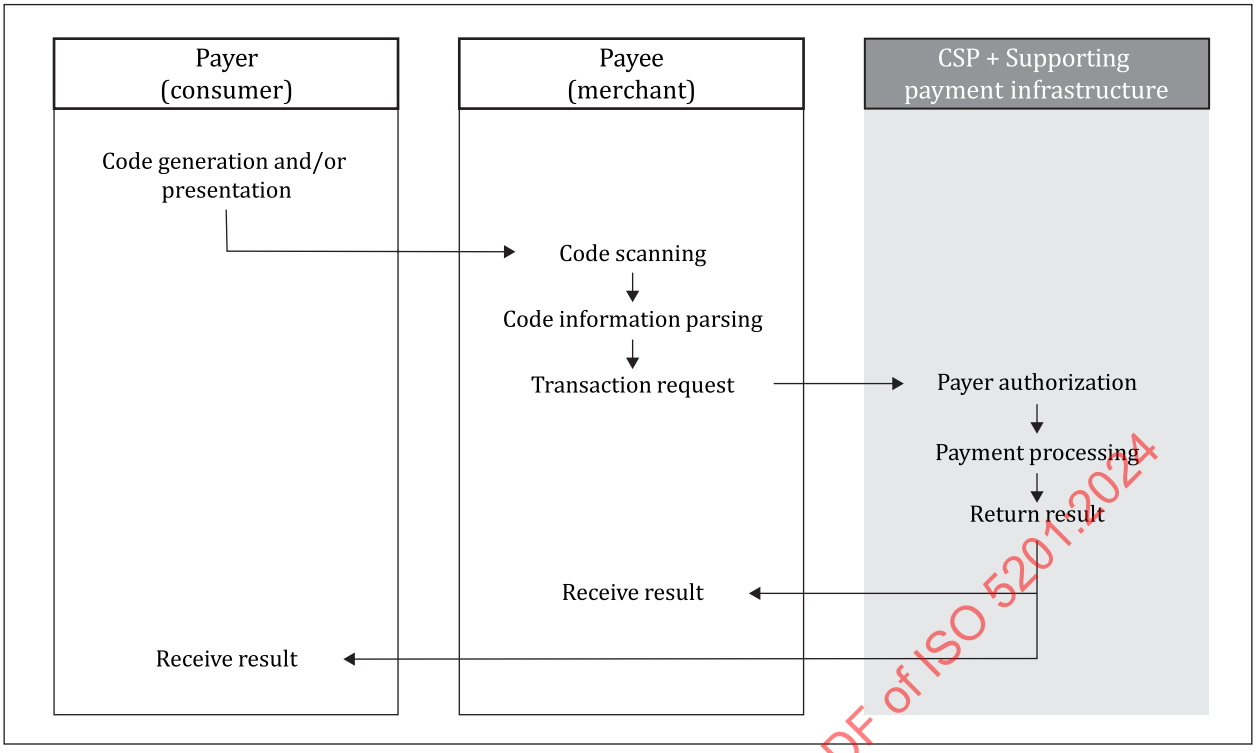
A.2.3 Static code

A.2.3.1 General

In some cases, a static payer-presented code is employed in a physical or virtual form. In such case, the code contains, for example, payer information, traditionally in the form of a magnetic stripe or a bar code. Recently, some merchant promotion programmes have developed a dedicated mobile application that is displayed at the storefront in place of plastic cards. In such cases, barcodes are often used as the interface to communicate the information stored on the card to the merchant. In order to accept payments from both card and applications using the same system, as well as to simplify online system processing mechanisms, untokenized static payer-presented codes are implemented in some services.

A.2.3.2 Steps

Figure A.4 illustrates an example implementation of the mandatory steps in Figure 2 for a static payer-presented mode.

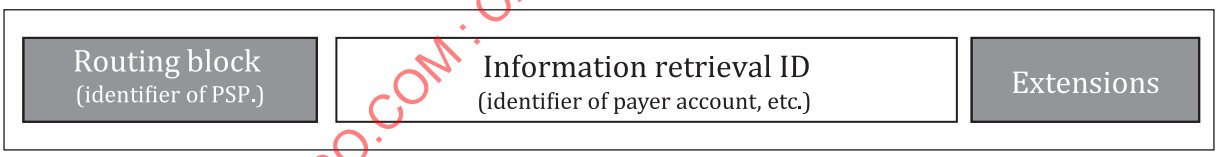


NOTE The grey boxes on the right side indicate that some of the components and processing details are out of scope. See Figure 1 and Figure 2 for details.

Figure A.4 — Static payer-presented mode steps (in the case of B2C transactions)

A.2.3.3 Code format

An example composition of a static payer-presented code is presented in Figure A.5.



Key

necessary information

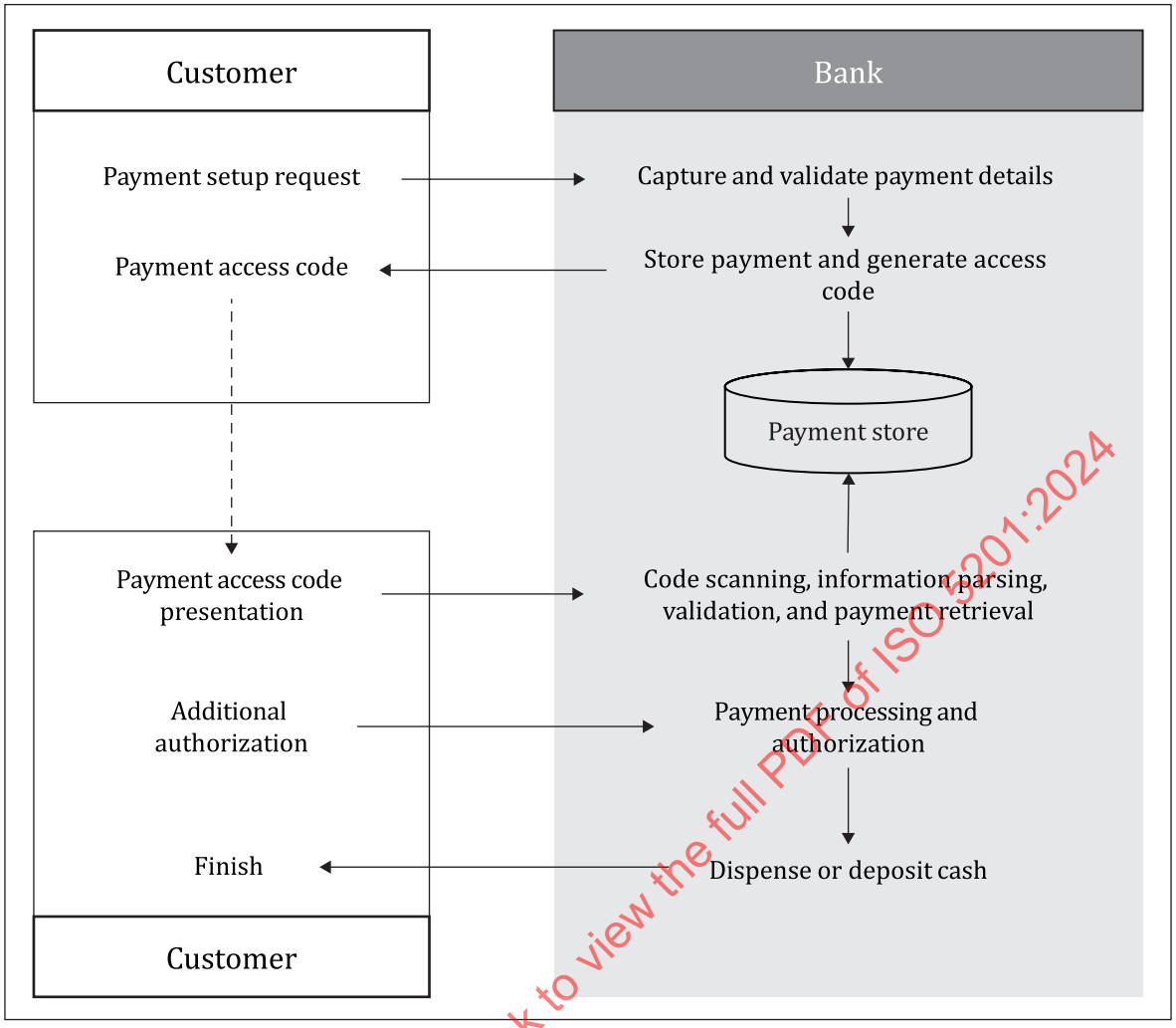
optional information

Figure A.5 — Payer-presented mode code format — Static

A.2.4 Deferred payment processing

Code-scanning payment solutions are also used in a deferred payment processing mode, where transactions are stored by the PSP and executed at a later time on presentation of the payment access code and, optionally, additional credentials.

This is a common pattern for pre-staging both deposit and withdrawal transactions at a bank, for example to perform cardless transactions at an automatic teller machine (ATM) or through a third-party agency, as in Figure A.6.



NOTE The grey boxes on the right side indicate that some of the components and processing details are out of scope. See Figure 1 and Figure 2 for details.

Figure A.6 — Payer-presented code used for cash deposit or withdrawal

A.3 Payee-presented mode

A.3.1 General

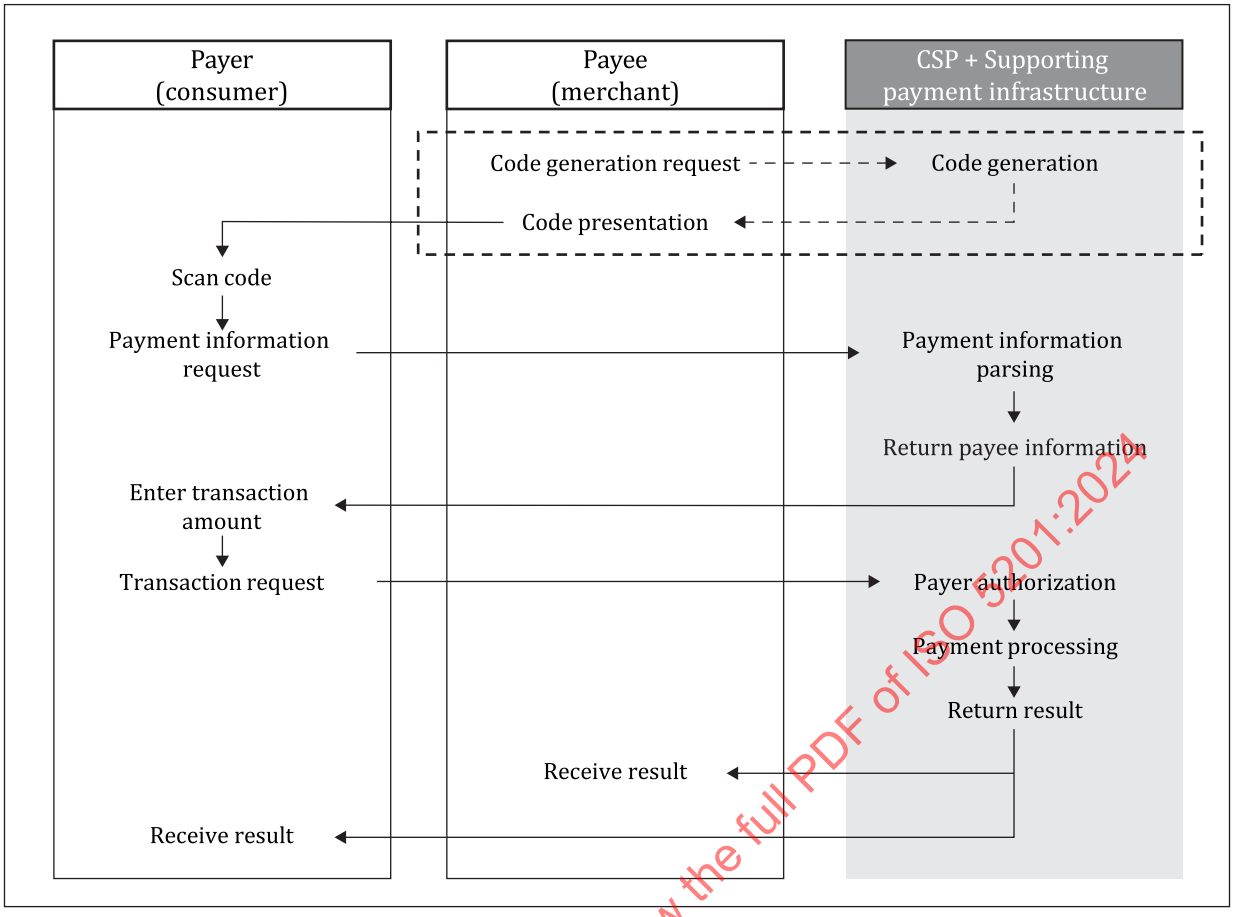
In this mode, the code image is presented by the payee, either statically or dynamically, at the time of payment and is scanned (optically read) by the application on the payer's mobile device.

A.3.2 B2C transaction

A.3.2.1 Steps

A.3.2.1.1 Static code

Figure A.7 illustrates a static payee-presented mode implementation of the mandatory steps in Figure 2.



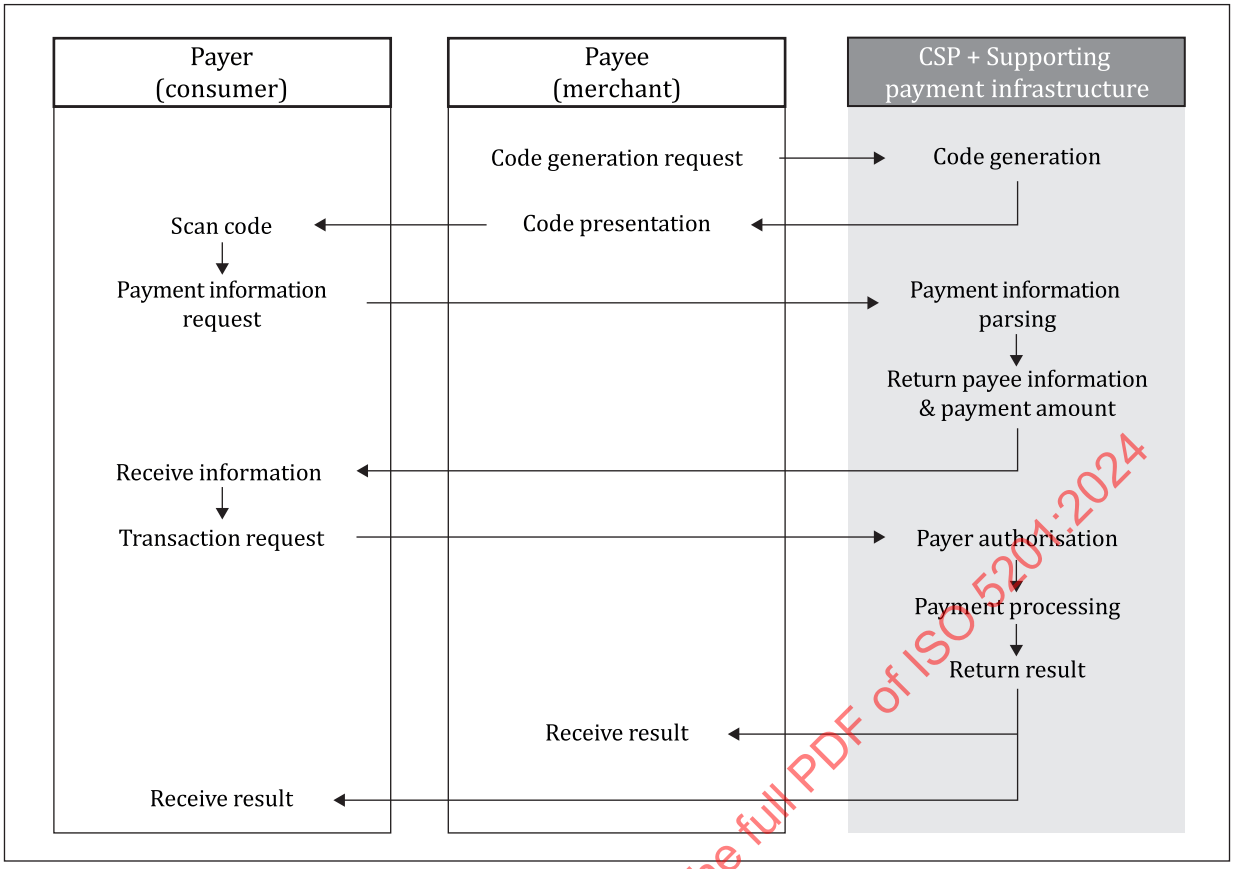
NOTE 1 The grey boxes on the right side indicate that some of the components and processing details are out of scope. See Figure 1 and Figure 2 for details.

NOTE 2 As mentioned in 5.2.3, a static payee-presented code contains information that is generally intended for repetitive use. The code is not generated for every transaction; thus, the code generation request and code presentation steps are put into a dashed line box.

Figure A.7 — Payee-presented mode payment process: B2C transactions, static code

A.3.2.1.2 Dynamic code

Figure A.8 illustrates a dynamic payee-presented mode implementation of the basic steps in Figure 2.



NOTE The grey boxes on the right side indicate that some of the components and processing details are out of scope. See Figure 1 and Figure 2 for details.

Figure A.8 — Payee-presented mode payment process — B2C transactions, dynamic code

A.3.2.2 Code formats

A.3.2.2.1 General

A payee-presented code should contain the necessary information to identify a payee.

A.3.2.2.2 Example 1

One example composition of a static payee-presented code is described in Figure A.9. Instead of directly coding the payment information into the code itself, usually the code only contains an information retrieval ID in the payload to retrieve the payment information remotely from the code parsing service provided by the payment institute.