Technical Specification

ISO/TS 9546

First edition
2024-12

Guidelines for security framework of information systems of third-party payment services

Lignes directrices relatives au cadre de sécurité des systèmes d'information des prestataires de services de paiement

Reference number
ISO/TS 9546:2024(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

Third-party payment (TPP) is an evolving model for payment services provided by third-party payment service providers (TPPSPs) to end users using payment accounts held in another entity, usually a bank. Globally, mobile payment, online payment, e-wallet and open banking (payment services) can all be supported by TPP. TPP plays an important role by complementing the offer of the traditional financial market players and contributes to the efficiency of payment transactions and financial systems.

This document follows the methodology of the ISO/IEC 15408 series and continues the work of ISO 23195, in which the security objectives of TPP are defined. It is supposed to define security functional requirements (SFRs). However, due to the fast development of the TPP, this document is positioned to provide some security guidelines for the TPP services and aims to provide some essential security functional recommendations (SFCs) to achieve the security objectives defined in ISO 23195.

This document is intended to assist stakeholders, such as TPPSPs and developers of the TPP information system, to mitigate the threats arising from the TPPSP intermediary role in the processing of payment transactions. It specifies the security framework, design principles, responsibilities, and functional recommendations to support the security mechanism defined and applied by TPPSPs. In the actual construction of the technical architecture, the users of this document can select, add or delete relevant components according to the framework of this document, to constitute the customized architecture according to the actual business and development expectations of TPPSPs. After that, the implementer of this document can select, add or delete the applicable functions from the corresponding security functions assigned by this document for each component, to design a TPP system conforming to the security objectives specified in ISO 23195.

Clause 5 introduces two types of TPP logical structural models from ISO 23195, which constitute the basic models of this document. The components within the target of evaluation (TOE) (defined by ISO/IEC 15408-1 as a set of software, firmware and/or hardware possibly accompanied by guidance, which is the subject of an evaluation) depicted in the models, such as TPPSP credentials carrier (C2), TPP payment terminal (C3), TPPSP gatekeeper (C5), TPP-BIS (C6) and TPP-AIS (C15), are specified in this document.

Clause 6 introduces the SFCs based on the security objectives for the TPP services. 6.1 provides several common SFCs for TPP services, which are the core elements of the security framework. 6.2 to 6.6 provide component-specific SFCs, which are based on the business characteristics of TOE components (C2, C3, C5, C6, C15).

Clause 7 introduces a three-layer security framework of TPP services which systematically presents the logic of the security services and mechanisms used in TPP services and supports the SFCs in Clause 6. This framework is based on the implementation of a set of security services and mechanisms on three different functional layers required to provide TPP services, namely:

— process layer;

— application layer;

— infrastructure layer.

Clause 8 introduces guidelines for users that can help them adopt the TPP security framework set out in this document. 8.1 provides three steps to implement the TPP security framework:

— identify the SPD elements;

— determine the security objectives;

— adopt appropriate SFCs to achieve the security objectives.

8.2 describes several real-world practices of the typical components of TPPSPs.

Annex A provides some typical implementation examples, which are widely used in real life all over the world.

Guidelines for security framework of information systems of third-party payment services

1 Scope

This document provides guidelines for a security framework to address the implementation of security mechanisms in technical infrastructures designed for the provision of third-party payment (TPP) services in order to achieve the security objectives defined in ISO 23195. The security framework is intended to protect critical systems and objects within the TPP system environment, either under the direct control of the third-party payment service provider (TPPSP) or by another entity (e.g. a bank).

This document is applicable to the provision of any TPP service, including:

— the TPP logical structural model;

— the definition of the security framework;

— the design principles, responsibilities and functional recommendations to support the security mechanism;

— guidelines for applying the security framework defined in this document.

2 Normative references

There are no normative references in this document.

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
TPP
third-party payment
payment transaction (3.2) involving at least one *intermediary* (3.3) *third-party payment service provider (TPPSP)* (3.4)

[SOURCE: ISO 23195:2021, 3.1.3]

3.2
payment transaction
act of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee

[SOURCE: ISO 12812-1:2017, 3.40, modified — Additional preferred term "payment" removed.]

3.3
intermediary
commercial party that provides services to customers, suppliers or authorities within the supply chain

Note 1 to entry: The customer is the payment service user, who can be a payer or a payee, such as a merchant.

[SOURCE: ISO 23195:2021, 3.1.4]

3.4
TPPSP
third-party payment service provider
payment service provider offering *third-party payment (TPP)* (3.1) services where they are not the *account servicing payment service provider (ASPSP)* (3.5) itself

Note 1 to entry: Comparison with the term "third-party payment service provider" defined in ISO/TR 21941:2017, 3.1.11:

a) the abbreviated form of "third-party payment service provider" has been clarified as "TPPSP" instead of "TPP" because "TPP" is a business mode which has been defined in this document;

b) the abbreviated form ASPSP is utilized instead of "account servicing payment service provider";

c) the term "payment initiation service" has been changed to "TPP" since the "TPP" contains "the payment initiation services";

d) "account information service on accounts" has been removed because it is not linked to TPP closely.

[SOURCE: ISO 23195:2021, 3.1.5]

3.5
ASPSP
account servicing payment service provider
payment service provider providing and maintaining a payment account for a payment service user

Note 1 to entry: In ISO/TR 21941, an ASPSP is defined as "providing and maintaining a payment account for a payer" only. In the context of this document, an ASPSP can be a bank or other institution which opens and maintains a payment account for the payment service user.

[SOURCE: ISO 23195:2021, 3.1.6]

3.6
information system
set of applications, services, information technology assets or other information-handling components

[SOURCE: ISO/IEC 27000:2018, 3.35]

3.7
TPP-BIS
third-party payment business information system
information system (3.6) that enables business functions of *third-party payment service providers (TPPSPs)* (3.4) and deals with *payment transactions* (3.2) based on TPPSP *credentials* (3.17)

[SOURCE: ISO 23195:2021, 3.2.2]

3.8
TPPSP gatekeeper
third-party payment service provider gatekeeper
function implemented by a *third-party payment service provider (TPPSP)* (3.4) that performs access control services to the *third-party payment business information system (TPP-BIS)* (3.7)

Note 1 to entry: The TPPSP gatekeeper can protect the TPP platform by preventing and mitigating the attack against the TPP-BIS and set up the trusted channel while the message is transferred via the transaction channel.

[SOURCE: ISO 23195:2021, 3.2.4]

3.9
TPP-AIS
third-party payment agent information system
information system (3.6) that receives requests for a *payment transaction* (3.2) from a multilateral *third-party payment service provider (TPPSP)* (3.4) and forwards them to a multilateral *account servicing payment service provider (ASPSP)* (3.5), then receives responses from the ASPSP and forwards them to the relevant TPPSP

Note 1 to entry: When the TPP-AIS is constructed as the common financial infrastructure, the TPP-AIS may directly connect with a *clearing and settlement system (CASS)* (3.10) and deliver the clearing information based on their payment transaction log.

Note 2 to entry: Regarding *third-party payment (TPP)* (3.1) as a whole, TPP-AIS can be deemed an internal component. However, TPP-AISs do not belong to any TPPSP or ASPSP generally. The operation of the TPP-AIS is independent of the information systems owned by TPPSP and/or ASPSP.

[SOURCE: ISO 23195:2021, 3.2.5]

3.10
clearing and settlement system
CASS
system responsible for inter-bank funds clearing and funds transfer

Note 1 to entry: CASS may provide instant funds clearing; it may also provide batch clearing, in which the funds clearing can be completed in a conventional period.

[SOURCE: ISO 23195:2021, 3.2.6]

3.11
TPP-API
third-party payment application program interface
logical interface within the *account servicing payment service provider (ASPSP)* (3.5) *information system* (3.6) designed for access by *third-party payment service providers (TPPSPs)* (3.4) to the end users' payment accounts required for *third-party payment (TPP)* (3.1) services

3.12
security framework
set of processes, applications and infrastructures for security of *third-party payment (TPP)* (3.1) *information systems* (3.6) and services

Note 1 to entry: Infrastructures include hardware, software, firmware and operational environments.

3.13
identity
set of attributes related to an entity

Note 1 to entry: In this document, an entity can be a payment service user or a system.

[SOURCE: ISO/IEC 24760-1:2019, 3.1.2, modified — Notes to entry replaced.]

3.14
identification
process of recognizing the attributes that identify an entity

Note 1 to entry: In this document, an entity can be a payment service user or a system.

[SOURCE: ISO 23195:2021, 3.1.16, modified — Note 1 to entry revised.]

3.15
authentication
process of corroborating an entity or attributes with a specified or understood level of assurance

[SOURCE: ISO 22300:2021, 3.2.8, modified — Notes to entry removed.]

3.16
authorization
right or permission that is granted to an entity to access a resource

[SOURCE: ISO/TR 22100-4:2018, 3.4, modified — Term "system" removed from "system entity" and "system resource".]

3.17
credential
data provided to the payment service user for *identification* (3.14) and/or *authentication* (3.15) purposes

[SOURCE: ISO 23195:2021, 3.1.12, modified — Notes to entry removed.]

3.18
payment password
secret sequence of characters or a word that a user submits to a system for purposes of authentication, validation, or verification of the payment transaction

[SOURCE: ISO/IEC 24775-2:2021, 3.1.44, modified — Clarification "of the payment transaction" added.]

4 Abbreviated terms

MFA multi-factor authentication

PIN personal identification number

SFA single-factor authentication

SFC security functional recommendation

SPD security problem definition

TEE trusted execution environment

TOE target of evaluation

TSF target of evaluation security functionality

2FA two-factor authentication

5 TPP logical structural models

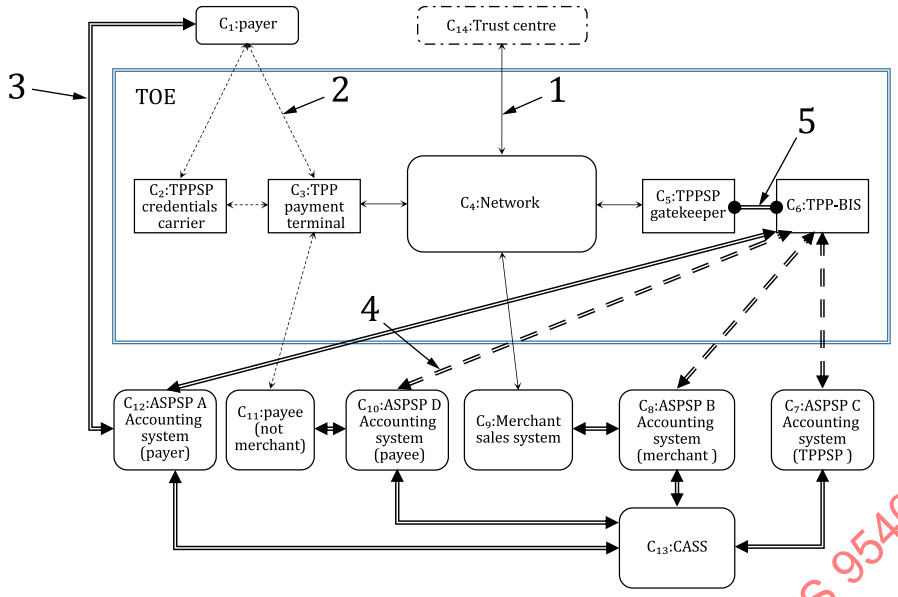
5.1 General introduction

There are two types of logical structural models for TPP according to ISO 23195. Figure 1 shows the direct connection between TPP-BIS and ASPSP. Figure 2 shows the indirect connection between TPP-BIS and ASPSP via TPP-AIS. See ISO 23195:2021, 4.1 for more details.

The major difference between the two models is that Figure 2 has one more component, “TPP-AIS”, than Figure 1, which brings about some additional security recommendations and measures to be considered, such as the security considerations for authorization, authentication, data protection and interaction through TPP-APIs of the TPP services.

5.2 TPP logical structural model without the TPP-AIS

In the direct connection mode, TPP-BIS connects to multiple ASPSPs who have business with it, and vice versa. With the gradual increase of the number of both sides, this connection mode aggravates the connection complexity and cost of both sides.



Key

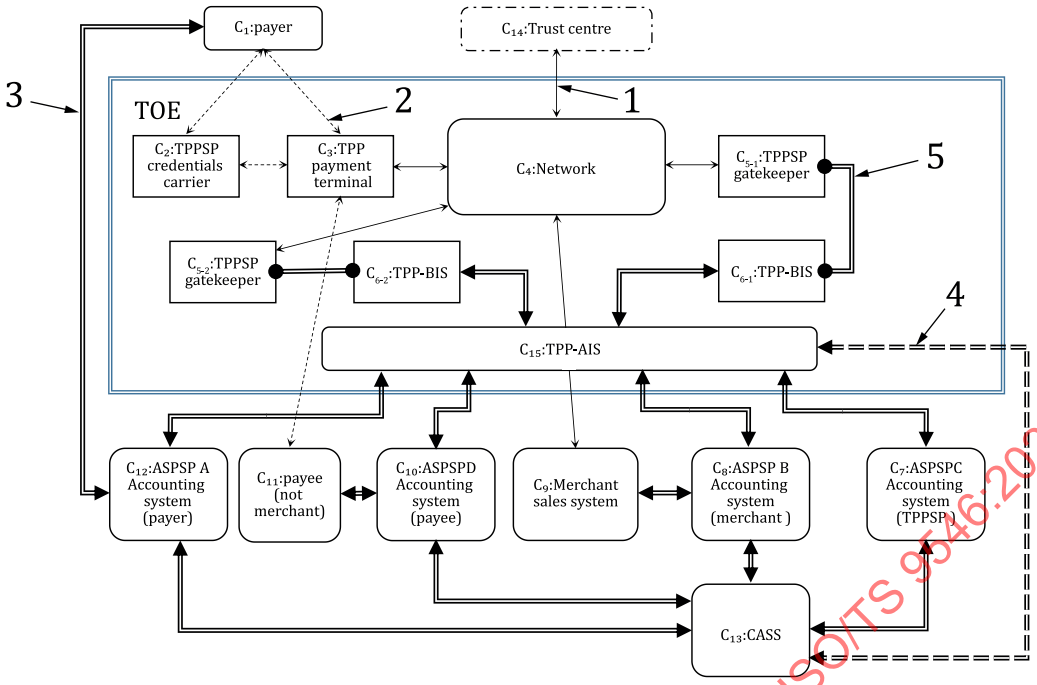
1 communication channel through a network
2 communication channel involves man-machine interface
3 trusted channel
4 optional trusted channel
5 internal trusted channel

NOTE The graphical interpretation of the links connecting the different components is described in ISO 23195:2021, Table 1.

Figure 1 — TPP logical structural model without the TPP-AIS

5.3 TPP logical structural model with the TPP-AIS

In the indirect connection mode, TPP-BIS connects to TPP-AIS, then transactions with multiple ASPSPs can be made through and vice versa. TPP-AIS undertakes the responsibility for transferring transaction information from both sides. Based on the transaction logs in which clearing and settlement information is recorded, information is generated by the TPP-AIS and sent to the clearing and settlement system (CASS) to perform the settlement between each ASPSP.



Key

1 communication channel through a network
2 communication channel involves man-machine interface
3 trusted channel
4 optional trusted channel
5 internal trusted channel

NOTE The graphical interpretation of the links connecting the different components is described in ISO 23195:2021, Table 1.

Figure 2 — TPP logical structural model with the TPP-AIS

6 TPP security functional recommendations

6.1 General security functional recommendations

6.1.1 General

This clause describes the general security recommendations for TPP services. To fulfil the recommendations, some or all of the components within the TOE should cooperate with each other, use appropriate security services and implement security mechanisms which are introduced in this clause.

6.1.2 Identification and authentication

Identification is the process of recognizing the attributes or identity that identify an entity. In TPP business, an entity is generally a payment service user or a system. Identity is the representation of an entity in the form of one or more information elements (known as “attributes”) which allow the entity to be sufficiently distinguished within a context. Identification of a payment service user, known as electronic know-your-customer (eKYC) in the financial sector, includes identity proofing, enrolment and continuous maintenance of the user’s identity attributes required to provide payment services according to ISO 5158.

Authentication is the process of corroborating an entity or attributes with a specified or understood level of assurance. In TPP services, authentication technology supports access control for payment processes by checking to see if the user’s credentials match with the credentials in an authorized user database or a

data authentication server. By doing so, authentication ensures secure operation, secure login and secure transaction.

There are several authentication types: single-factor authentication (SFA), two-factor authentication (2FA) and multi-factor authentication (MFA). The practice of requiring a user ID and password is typical SFA. The practice of asking for additional authentication factors, such as a biometric signature or a one-time code sent to the user's mobile device before the transaction is attempted, is 2FA. When three or more identity verification factors are used for authentication, for example a user ID and password, a biometric signature and a personal question only the user knows, this is MFA.

For TPP services, authentication is the central security property. There are generally two types of authentication: for users and between systems.

Security functional recommendations on identification and authentication are as follows:

a) The user's identity should be authenticated when he or she logs in to the payment application or initiates a payment transaction.

b) The validity of payment terminal identity should be authenticated when it calls the TPPSP gatekeeper.

c) The validity of TPP-BIS should be authenticated when it interacts with TPP-AIS and vice versa.

d) Effective data authentication methods should be taken to protect the data from unauthorized changes, counterfeiting and repudiation by all the components within the TPP TOE.

e) A suitable authentication technique should be chosen to substantiate the claimed identity of a user, software, messages and other entities.

f) The strength of authentication should match with the risk level of the information being accessed. Where strong authentication and identity verification are required, alternative methods other than passwords should be used, such as digital certificates, smart cards, tokens and/or biometric means.

g) Cryptographic technology should be used to ensure the confidentiality, integrity and availability of identifier, identity credential and identity information.

6.1.3 Authorization

6.1.3.1 Agreement aspect

From a TPP business aspect, users should authorize TPP-BIS to send payment instructions to ASPSP on their behalf, such as checking the account balance and initiating and inquiring the payment transactions. On the other hand, TPP-BIS and ASPSP can also make certain authorization decisions based on the details of the payment transactions, such as the types of the user, the location of the payment, the frequency of the payment and the amount of the payment, to mitigate potential risks.

Security functional recommendations on agreement authorization are as follows:

a) The TPPSP should obtain the payer's authorization before using the payer's data and conducting any operations on the payer's payment account managed by ASPSP.

b) The TPPSP should authorize users with different authorization processes in order to deter fraud.

6.1.3.2 Technical aspect

From a technical aspect, authorization is the process of granting an entity the access rights to a resource. It generally comes after the entity has been successfully authenticated.

Security functional recommendations on technical authorization are as follows:

a) The payment application and TPP-BIS should grant appropriate access rights to users based on their proven identities.

b) All components of TPP TOE should grant appropriate access rights to their TPP-APIs based on the proven identities of other components.

c) When a payment instruction is sent from the TPPSP to the ASPSP of the payer (e.g. the payer's bank), it should contain a proof of consent generated by the payer.

d) In the logical structural model in Figure 2, the TPP-AIS should authorize the TPP-BIS to access its system according to the attributes and transaction types of the TPP-BIS.

6.1.4 Audit logging

Audit logging is the process of documenting activities within the software systems used across the information systems. An audit log contains the sequential records of data that are relevant and/or crucial to maintaining the security of the system or business, such as the key operations of an event, the time at which it occurred and the responsible user or service.

In TPP services, by reviewing the audit logs the organization can track the system activities or payment transactions, investigate breaches, resolve disputes of transaction errors, ensure conformity to organizational security policies and achieve the security objectives defined in ISO 23195.

Security functional recommendations on audit logging are as follows:

a) All components of TPP TOE should generate logs for business events and security events.

b) The audit logs should not contain payment-sensitive information.

6.1.5 Asset protection

In TPP, according to ISO 23195, protected assets are defined as user data and TPPSP'S TSF data. The user data include TPP business configuration data, business cumulative data, transaction input data, transmitting data and authentication data provided by ASPSP. The TPPSP's TSF data include protected data and confidential data.

Asset protection recommendations include many aspects, such as the security of data in transmit, data at rest, data sharing, key management, cyberattacks resistance and risk control. In order to achieve the security objectives defined in ISO 23195, the following security recommendations should be met:

a) Security of network connectivity should be guaranteed between any two components within the TPP TOE.

b) Confidentiality, integrity, non-repudiation and authenticity of data transmitted, shared and stored in the information system should be guaranteed by all components within the TPP TOE.

c) For payment-sensitive information, some higher level of security measures should be adopted.

d) Rules for key management should be established and implemented based on business and system characteristics.

e) Effective measures should be taken to resist cyberattacks.

f) TPPSP should have the ability to prevent and control transaction risks according to ISO 31000.

6.2 Security functional recommendations for TPPSP credentials carrier (C2)

6.2.1 Encryption

a) The appropriate encryption method should be adopted to encrypt the credential and the reference PIN according to ISO/TR 14742, to prevent payment credential from being stolen or forged.

b) The key management service should be provided according to ISO 11568, to safeguard the security of key life cycle.

6.2.2 User authentication

a) The user should be identified and authenticated by the credential carrier before credential-based financial operations are performed according to ISO 5158.

b) PIN verification mechanisms can prevent replay attacks.

6.2.3 Access control

a) A credential carrier should be issued to implement the appropriate access control policies of TPPSPs before the user wants to initiate a TPP transaction.

b) TPPSP credential carriers should prohibit unauthorized access to the credential from the applications and systems based on the identification, authentication and authorization information.

6.3 Security functional recommendations for payment terminal (C3)

6.3.1 Encryption

a) TPP payment terminals should protect the transaction and key processing operations by adopting cryptographic algorithms according to ISO/TR 14742 and ISO 11568.

b) The cryptographic algorithms and key length should have adequate strength to ensure the security of transactions according to ISO/TR 14742.

c) The key management service should be provided according to ISO 11568, to safeguard the security of key life cycle.

d) The keys used for user or terminal authentication, TEE management, communication security and data storage encryption should be different from each other.

6.3.2 User authentication

a) Appropriate authentication factors should be used for payment application software login.

b) TPP payment terminal should provide security measures to ensure the security of user authentication information input by the user according to ISO 13491-1.

c) The payer should be authenticated before he or she uses the TPP service through the application.

6.3.3 Logical security

a) The TPP payment terminal should feature basic security counter measures according to ISO 13491-1 and ISO/TS 12812-2.

b) The rationale of process design about the security functions should be fully considered in order to avoid logical vulnerability and to ensure that the security functions cannot be bypassed.

6.3.4 Transaction security

a) A security transmission channel should be established between the TPP payment terminal and TPPSP gate keeper.

b) The payment application should protect the transaction information to prevent it from being changed without authorization.

c) Non-repudiation of the transactions should be ensured by the TPP payment terminal.

d) Replay attacks of the transactions should be prevented by the TPP services.

e) The security of the working environment should be guaranteed when the TPP payment terminal initiates payment transactions.

6.3.5 Payment-sensitive information protection

a) The TPP payment terminal should not store users' payment-sensitive information by any means, in order to prevent the disclosure of payment-sensitive information.

b) Payment-sensitive information should not be displayed in plain text by the TPP payment terminal.

c) When a process of payment application software is terminated or unloaded, residual payment-sensitive information that is not required should be deleted in order to ensure the security of sensitive information.

d) Security measures should be taken to ensure confidentiality when payment-sensitive information is transmitted between client application software and other local application software.

6.4 Security functional recommendations for TPPSP gatekeepers (C5)

6.4.1 Access control

a) The TPP gatekeeper should control access to the interface based on the identification, authentication and authorization information to prevent unauthorized access.

b) A traffic-flow control mechanism should be put in place to protect the TPP gatekeeper from traffic overload.

c) A security inspection should be performed on the interface of the TPP gatekeeper.

6.4.2 Transaction security

a) Effective measures should be taken to ensure communication security between the network (C4) and the TPPSP gatekeeper (C5), as well as TPP-BIS (C6) and TPPSP gatekeeper (C5).

b) Effective measures should be taken to protect the integrity and non-repudiation of the transaction information.

c) The TPPSP gatekeeper should not store payment-sensitive information, which should only be used for completing transaction authorization.

6.4.3 Audit logging

a) The TPPSP gatekeeper should implement the audit logging function.

b) Effective measures should be taken to prevent system logs and transaction logs from being illegally tampered with.

c) The logs should not contain payment-sensitive information.

6.5 Security functional recommendations for TPP-BIS (C6)

6.5.1 User authentication

a) TPP-BIS should adopt user authentication in order to prevent fraud.

b) When biometric recognition technology is adopted, the security of biometric recognition information should be ensured.

6.5.2 Transaction security

a) Security measures should be taken to protect transactions from counterfeiting and repudiation.

b) Security measures should be taken to prevent transaction replay attacks.

6.5.3 Payment-sensitive information protection

a) Payment-sensitive information should only be accessed by authorized users and application components.

b) Payment-sensitive information should be stored and used according to the risk-control policies of the TPPSPs.

c) Payment-sensitive information should not be displayed in plain text by the TPP-BIS.

6.5.4 Risk control

a) TPPSP should have the ability to prevent and control transaction risks in accordance with ISO 31000.

b) A transaction risk-control system should be constructed to identify and dispose of abnormal and high-risk payment transactions in a timely manner.

c) TPPSP should adopt strong user authentication or set a reasonable payment amount limit for high-risk transactions.

6.6 Security functional recommendations for TPP-AIS (C15)

6.6.1 Encryption

a) The security of a cryptographic key life cycle should conform to ISO 11568.

b) The cryptographic algorithms and key length should have adequate strength to ensure the security of transactions according to ISO/TR 14742.

c) The security of the certificate life cycle should be ensured according to ISO 21188.

6.6.2 Identity verification

a) The identities of TPP-BIS and ASPSP should be verified by the TPP-AIS.

6.6.3 Transaction security

a) Effective measures should be taken to ensure communication security between TPP-BIS and TPP-AIS, TPP-AIS and ASPSP.

b) Sensitive information in the messages or documents should be encrypted.

c) Effective measures should be taken to prevent unauthorized changes to the transaction data.

7 TPP security framework

7.1 Security framework overview

This clause describes a three-layer security framework to systematically present the logic of the security services and mechanisms used in TPP services and support the security recommendations in Clause 6. This framework is based on the implementation of security services and mechanisms on the three different functional layers needed to provide TPP services, namely:

— the process layer;

— the application layer;

— the infrastructure layer.

Figure 3 illustrates the three layers of the security framework and provides examples of security standards that implementers can find useful for the design of the security framework for TPP services.

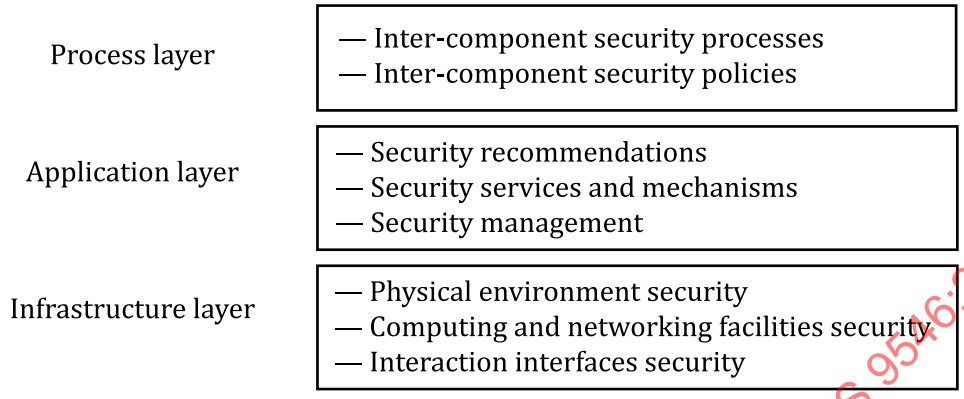


Figure 3 — TPP security framework

— The process layer includes inter-component security processes and associated policies implemented by the TPPSP in order to minimize the risks during the TPP services.

— The application layer refers to TPP service-related security recommendations, the security services, mechanisms and management underpinning them (e.g. authorization, authentication, logging, data protection, key management) and corresponding security guidelines.

— The infrastructure layer refers to the security measures of the physical environment, computing and networking facilities, interaction interfaces generating, storing, processing or transporting TPP data, which are not TPP-specific.

7.2 Process layer

7.2.1 Overview

At the process layer, every component in the TOE exchanges TPP data with each other and the organizations behind these components define their policies. Meanwhile, inter-component security measures are introduced in 7.2 in order to provide guidelines for implementors to fulfil the recommendations given in 6.1.

7.2.2 Identification and authentication

In order to complete identification and authentication, different functional entities in TPP reach an agreement on using one or more identification and authentication methods. Common methods include passwords, digital certificates and biometric recognition. A single method or a combination of these may be used.

When using a password, the user should set the password at the time of registration and ensure that the strength of the password follows the recommendations. The password should be protected when it is stored in the back-end system using encryption mechanisms, such as hash function. Since the password is verified in the back-end system (C6), the password transmission in the network should be protected using a security protocol, such as the most recent version of TLS. A good security practice is the agreement or establishment of a password encryption key. Refer to ISO 11568 for guidance.

In the case of a digital certificate, the user implements identification and authentication by signing with his or her own digital certificate private key. The private key should be properly protected at the end side using secure hardware (e.g. SE or TEE) or cryptographic mechanisms.

When biometric authentication is used, there are two methods for this. The first is local authentication. After the payment device recognizes the biometrics, the user's biometric information is encoded into a unique token as the user's authentication information and sent out to the back end for verification. The second is remote authentication, where the user's biometric information is transferred securely to the back end to be compared and verified. For security recommendations and controls for financial biometric authentication, see ISO 19092.

7.2.3 Authorization

In TPP, authorization processes mainly focus on the fact that the payer authorizes the TPP-BIS to operate on his or her payment account managed by ASPSP. The operations include payment initiation (e.g. credit or debit payment) and account information inquiries. The authorization can be implemented by users signing agreements with TPPSP and ASPSP before the initiation of the payment.

In addition, TPPSP can select different authorization processes using various types of authentication measures based on the risk profiles and the nature of the transactions to deter fraud. For example, when the payment amount is very small, payers can authorize the TPP-BIS and ASPSP to complete the payment directly on their behalf. However, when the payment amount is larger, payers can be asked to input their payment passwords for additional authorization to TPP-BIS. Furthermore, for some high-risk transactions, TPP-BIS and ASPSP can ask for a dynamic verification code from payers.

7.2.4 Audit logging

All components within the TPP TOE should have the ability to generate logs for business events and security events. The payment application should record the login and payment requests of the users. The TPP-BIS should record the access requests, payment order details and transaction information of the payment application. The TPP-AIS should record access requests, payment information and the clearing results of TPP-BIS.

7.2.5 Asset protection

In TPP services, assets are mainly user data, business data and data generated during transaction processing. These data are used by all components within the TPP TOE and their protection should follow data security recommendations covering the data life cycle, including collection, transmission, storage, use, sharing and destruction. This protection should also be based on the differentiated confidential and integral protection recommendations of data classification and the privacy needs of users.

For data collection, a secure keyboard, safety camera and other equipment may be used to prevent the collection of user information.

The transmission network should adopt a firewall, intrusion detection system and other security equipment or solutions. The terminal should adopt technical measures such as access control and terminal authentication to prevent illegal or unauthorized terminals from accessing the internal network. Authentication of the identity of both communication parties should also be implemented to ensure that both data transmission parties are trusted. A digital signature, time stamp and other methods should be adopted to ensure the non-repudiation of data transmission. Security technologies, including cryptographic technology, should be used to ensure data integrity.

For data storage, sensitive data should be encrypted or desensitized and accumulated data should be backed up in real-time, asynchronous, incremental or full modes to provide local data back-up and recovery functions.

When using data, the main role, credit rating, business demands, timeliness and other factors should be comprehensively considered. Data access should be determined according to the principle of necessity and minimum rights and subject to identity authentication, association of data access rights with the identity or role of actual visitors and prevention of unauthorized access to data. Relevant operation logs should be kept during data access, which should include at least clear subjects, objects, operation time, specific operation types and operation results.

7.3 Application layer

7.3.1 Overview

At the application layer, components within the TOE can apply the security measures outlined in 6.2 to 6.6 to conform to security recommendations.

The threats and risks defined for a particular TPP service can be described depending on the terminals used, expected user behaviour, attack patterns and application environments. The risk assessment can then be conducted and the security countermeasures can be evaluated following the TPP service. This applies to the policies (e.g. roles and responsibilities) of each party in a TPP service.

7.3.2 Security measures for TPPSP credentials carrier (C2)

For a TPPSP credentials carrier, the following security measures should be implemented to prevent counterfeiting, unauthorized disclosure and changes of the credentials:

a) A secure carrier should be used to store and process the credentials and the reference PIN to realize anti-tamper and resist reverse analysis.

b) Strong cryptography and security protocols should be used to safeguard the credentials and the reference PIN to prevent leakage and modification.

c) The cryptographic algorithms and key length should be AES (128 bits and more), TDES/TDEA (at least three times the length of the secret key), RSA (2048 bits and more), ECC (224 bits and more) and DSA/D-H (2048/224 bits and more).

d) Effective measures, such as PIN verification, key-press confirmation or other authentication mechanisms, should be taken to authenticate the user when he or she accesses the credentials.

e) When firmware is updated, its integrity and authenticity should be verified.

f) When the credential carrier is attacked, it should immediately switch to an inoperable state.

g) Some credentials should be in addition protected using a security encapsulation approach that conforms to relevant standards, such as ISO 9564 and ISO 19092.

7.3.3 Security measures for TPP payment terminal (C3)

For a TPP payment terminal, the following security measures should be implemented to prevent counterfeiting, repudiation, unauthorized disclosure and changes of the input data and authentication data:

a) The keys used for user or terminal authentication, TEE management, communication security and data storage encryption protection should be different from each other.

b) When the user logs in to the payment application or the cashier opens the POS or logs in to the merchant system, authentication should be launched.

c) The authentication factors should be a combination of password, secure SMS verification code (to transport an OTP), gesture password or biometric features.

d) Effective measures such as a secure keyboard, obfuscation, cryptographic technologies or other authentication mechanisms should be taken to protect the authentication information entered by the user.

e) Effective measures should be taken to verify the permission of the user when he or she uses the TPP service, such as verification of the user's login state.

f) The payment application should encapsulate the client-side code into a safe area, including the real address and access credentials of the gatekeeper.

g) Cryptographic measures, such as TLS protocol and digital signature, should be adopted to achieve transmission security. Bidirectional authentication should be carried out to verify the legitimacy of C3 and C5.

h) Digital certificate technology should be adopted to resist repudiation.

i) The application or PC should work in a safe operating system environment.

j) Sensitive information stored in the memory should be automatically cleared when the transaction is completed or the response times out.

k) Payment-sensitive information should be displayed by shielding the key field of the information or using meaningless characters.

7.3.4 Security measures for TPPSP gatekeeper (C5)

For a TPPSP gatekeeper, the following security measures should be implemented by stakeholders to prevent counterfeiting, repudiation and unauthorized changes of the transmitting data and business configuration data:

a) The gatekeeper should use a digital signature, white list, IP verification and location of C3 to verify the legitimacy of C3's calls.

b) Effective measures, including a leased line, HTTPS, TLS, message field encryption and bidirectional authentication, should be carried out to verify the legitimacy of C5 and C6.

c) Key domain encryption and message digest signature should be used.

d) The following payment-sensitive information should be verified but not stored by the gatekeeper after the authorization:

   — received transaction data;

   — all kinds of logs (e.g. transaction logs, history logs, debugging logs, error logs);

   — history files;

   — database information (e.g. database schemas, database contents).

e) Appropriate access control and encryption mechanisms should be implemented to protect the system logs and transaction logs from illegal tampering.

f) The cryptographic algorithms and key length should be AES (128 bits and more), TDES/TDEA (at least three times the length of the secret key), RSA (2048 bits and more), ECC (224 bits and more) and DSA/D-H (2048/224 bits and more).

7.3.5 Security measures for TPP-BIS (C6)

For TPP-BIS, the following security measures should be implemented by stakeholders to prevent counterfeiting, repudiation, unauthorized disclosure and changes to the cumulative business data, business configuration data and transmitting data:

a) The authentication factors should be a combination of password, secure SMS verification code (to transport an OTP), gesture password or biometric features.

   NOTE 1 The security of biometric information for financial applications is covered in ISO 19092.

b) For a high-risk transaction, two or more factors should be adopted by the TPP payment terminal to authenticate the identity of a user; if the transaction is a mobile financial service, it should be carried out according to ISO/TS 12812-2.

c) The payment transaction message should contain user-identity information and the user's signature to prevent the transaction from counterfeiting and repudiation.

d) The transaction message signature should contain a nonce, such as random data, or timestamp to prevent replay attacks.

e) When the authenticated users or application components apply to access the payment-sensitive information, the TPP-BIS should authorize them based on the authentication factors.

f) Payment-sensitive information should be displayed by shielding the key field of the information or using meaningless characters.

g) Risk-control measures involving monitoring, detection and incident response should be implemented, for example rejecting transactions made with a suspicious bank card number or merchant ID, setting limits for high-risk merchants, providing timely warnings of abnormal transactions, monitoring high-frequency logins and other abnormal behaviour, and responding in a timely manner to fraudulent or abnormal transactions.

h) For abnormal payment transactions, disposal options such as refusal, sending an additional authentication challenge and sending a warning to the user, should be implemented.

NOTE 2 TPP abnormal payment transactions refers to those deviating from normal payment patterns.

i) The strength of user authentication should be proportional to the risk of the transaction. TPPSP should adopt two factors of authentication or set a reasonable payment amount limit for high-risk transactions.

7.3.6 Security measures for TPP-AIS (C15)

For TPP-AIS, the following security measures should be implemented to prevent counterfeiting and unauthorized changes to the transmitting data and cumulative business data:

a) The cryptographic algorithms and key length should be AES (128 bits and more), TDES/TDEA (at least three-times length of the secret key), RSA (2048 bits and more), ECC (224 bits and more) and DSA/D-H (2048/224 bits and more).

b) TPP-AIS should verify the signature of a real-time interactive message sent by TPP-BIS or ASPSP for entity authentication.

c) Leased line, HTTPS, TLS and message field encryption should be used to protect the communication security between TPP-BIS and TPP-AIS, TPP-AIS and ASPSP.

d) TPP-AIS should verify the signature of real-time interactive messages sent by TPP-BIS or ASPSP to prevent unauthorized changes to the transaction data.

7.4 Infrastructure layer

At the infrastructure layer, the hardware, software, firmware, network management, operating systems and logging management of the TPP information systems should follow the general security recommendations set forth in existing ISO security standards. See the ISO 13491 series and ISO 11568 for information regarding cryptographic devices and key management processes.

8 Guidelines for implementation of the security framework

8.1 Overview of and steps for the guidelines

Figure 4 is taken from ISO/IEC 15408-1:2022, Figure 4, which presents the implementation guidelines for the security framework described in this document.

NOTE To better understand the analytical methodology used in this document and its different aspects, see ISO/IEC 15408-1.

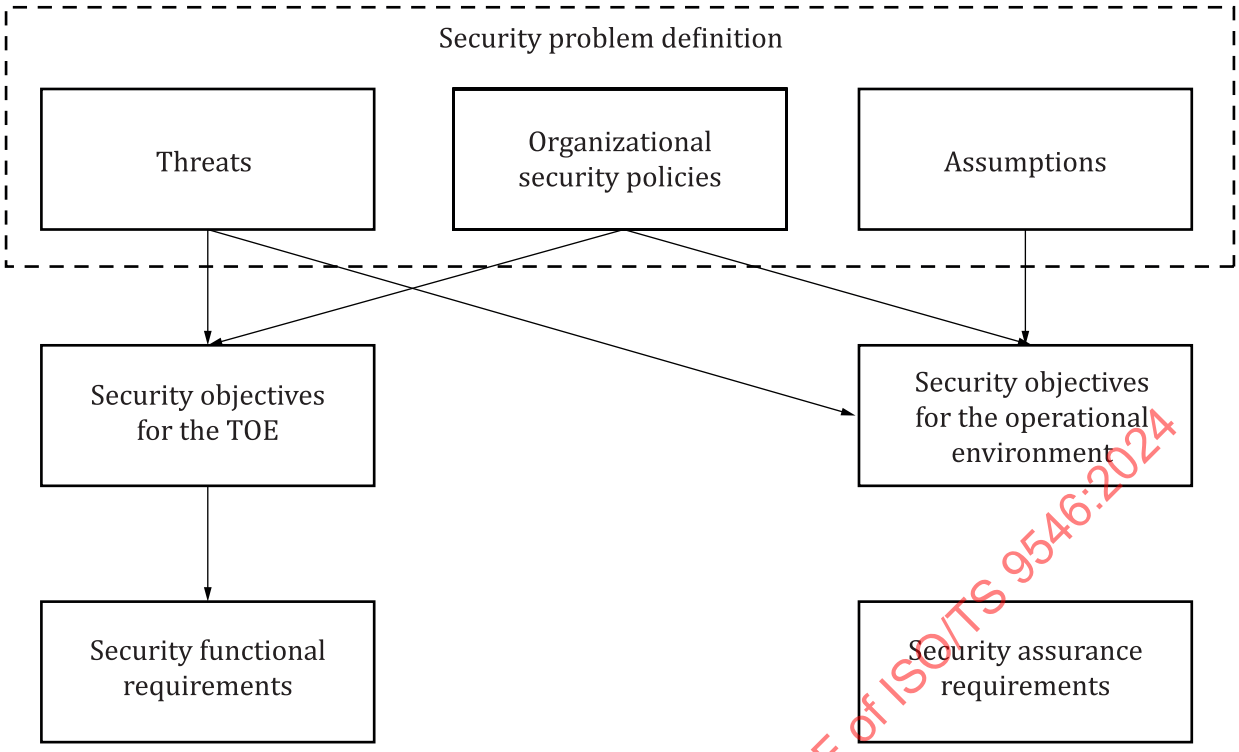


Figure 4 — Guidelines for security framework of TPP services

The first step is to identify the SPD elements faced by the asset. The possible threats, organisational security policies and assumptions are covered in ISO 23195:2021, 5.2, 5.3 and 5.4.

The next step is to determine the security objectives to address the SPD elements. The security objectives for the TOE and operational environment are described in ISO 23195:2021, Clause 6.

The final step is to adopt appropriate SFCs and corresponding security measures, as defined in Clauses 6 and 7, to achieve the security objectives specified in ISO 23195. The SFCs and security measures contribute to fulfilling the TOE's SPD and addressing the security objectives defined for the TOE. They are usually at a more detailed level of abstraction, according to ISO/IEC 15408-1.

To address the identified threats, this document provides SFCs and corresponding security measures based on the business characteristics of TOE-components (C2, C3, C5, C6, C15) under the security framework in general business models.

8.2 Real-world practices of the security framework

8.2.1 Overview

The guidelines in the previous clauses summarize and abstract the most typical and useful TPP security practices. In 8.2, several real-world practices are provided for stakeholders implementing the TPP security framework set out in this document.

8.2.2 Practices of payment application (C3)

8.2.2.1 User authentication

For user authentication of payment application, the following security measures are recommended to prevent counterfeiting, repudiation, unauthorized disclosure and changes of the input data and authentication data:

a) Users of TPPSP payment applications should log in with a password, SMS verification code or biometrics. It is not necessary to be authenticated each time the application is opened.

b) A login password requires adequate length and complexity and should be independent from the payment password.

c) Login on a new device should trigger MFA.

d) Users should input their password via a secure password keyboard (anti-steal).

e) Each time the user launches a payment transaction, a password should be used; the user can also configure the payment transaction to be password-free for a very small amount of money.

8.2.2.2 Logical security

For logical security of payment application, the following security measures are recommended to prevent counterfeiting and changes to the TSF data and authentication data:

a) TPPSP payment application should use obfuscation technology (e.g. virtualization technology, decompile protection, binary image information hiding) to resist static analysis, dynamic debugging and other operations.

b) Regular automated code audits and penetration tests should be used to avoid logical vulnerability.

8.2.2.3 Payment-sensitive information protection

For payment-sensitive information protection, the following security measures are recommended to prevent counterfeiting, unauthorized disclosure and changes of the input data and authentication data:

a) TPPSP payment application should not store any payment-sensitive information.

b) Sensitive information, such as factors for authentication, keys and key derivation parameters, should be protected in the TEE of the payment terminal.

8.2.3 Practices of TPPSP gatekeeper (C5) and TPP-BIS (C6)

8.2.3.1 Access control

For access control of TPPSP gatekeeper and TPP-BIS, the following security measures are recommended to prevent unauthorized disclosure and changes to the cumulative business data, business configuration data and transmitting data:

a) Communication between C5 and C6 or other entities should be via TLS protocol and RSA encryption should be used for sensitive payment information.

b) Calling the TPPSP gatekeeper's interface to complete transactions should need a hash message authentication code (HMAC) or message signature using PKI, a time stamp and a transaction serial number to prevent transaction forgery and replay. Refer to HMAC key management details in ISO 11568 and PKI management in ISO 21188.

8.2.3.2 Payment-sensitive information protection

C5 and C6 should not store any payment-sensitive information.

8.2.3.3 Risk control

For risk control of TPPSP gatekeeper and TPP-BIS, the following security measures are recommended to prevent counterfeiting, repudiation, unauthorized disclosure, and changes to the cumulative business data, business configuration data and transmitting data:

a) C5 and C6 should set a risk-control strategy and establish automatic risk identification and processing systems to monitor insecure traffic, detect fraud, interact with users and intercept high-risk transactions.

b) Payment limits should be set according to the different strengths of authentication, e.g. the use of digital certificates can help to increase payment limits.

c) Artificial intelligence and big data technology should be used to identify risky transactions.

8.2.4 Practices of TPP-AIS (C15)

For TPP-AIS, the following security measures are recommended to prevent counterfeiting, repudiation, unauthorized disclosure and changes to the cumulative business data, business configuration data and transmitting data:

a) Leased lines should be used between TPP-AIS and other entities (e.g. TPPSP, ASPSP).

b) Secure communication mechanisms, such as TLS protocol and one-way verification of initiator, should be used to maintain confidentiality and integrity.

c) A signature should be required for the transmission of exchange messages or files.

d) Sensitive information should be encrypted before being transmitted and stored.

e) The key for encrypting sensitive information should be encrypted by means of a digital envelope.