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

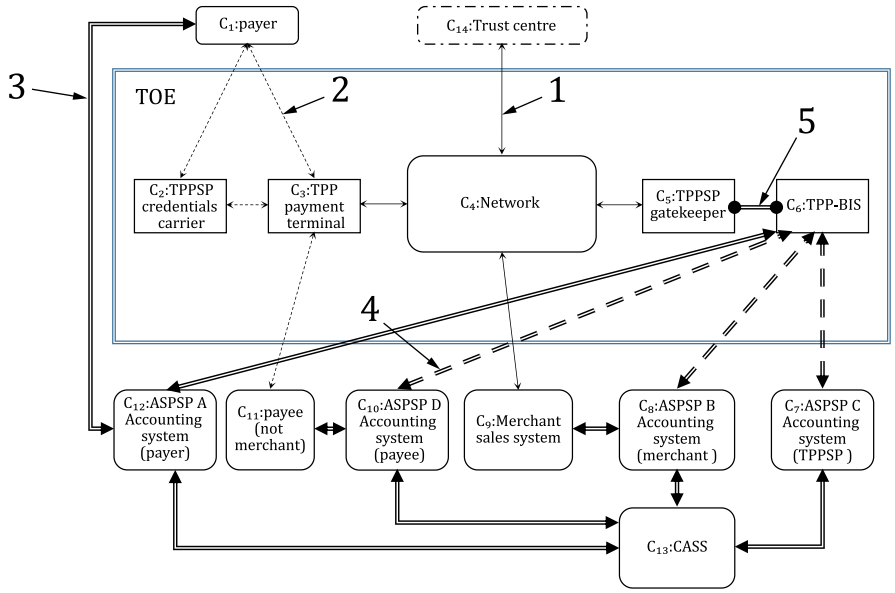
5.1 General introduction

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.