INTERNATIONAL STANDARD

ISO 23195

First edition
2021-06

Security objectives of information systems of third-party payment services

Reference number
ISO 23195:2021(E)

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 ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms, definitions, and abbreviated terms ... **1**
3.1 TPP business ... 1
3.2 TPP information system ... 4
3.3 TPP security ... 5
4 TPP logical structural model in an open ecosystem ... **7**
4.1 Logical structural model ... 7
4.1.1 General ... 7
4.1.2 Direct connection between TPP-BIS and ASPSP ... 8
4.1.3 Communication between TPP-BIS and ASPSP via TPP-AIS ... 9
4.2 Protected assets ... 10
4.2.1 General ... 10
4.2.2 User data ... 11
4.2.3 TPPSP's TSF data ... 14
5 Security problem definition ... **14**
5.1 General ... 14
5.2 Threats ... 15
5.2.1 Threats to business configuration data ... 15
5.2.2 Threats to business cumulative data ... 15
5.2.3 Threats to transaction input data ... 15
5.2.4 Threats to TPP transmitting data ... 16
5.2.5 Threats to authentication data provided by ASPSP ... 16
5.2.6 Threats to TPPSP's TSF data ... 17
5.3 Organizational security policies ... 17
5.3.1 Operation authorization ... 17
5.3.2 Security event audit ... 18
5.3.3 Connection security control ... 19
5.3.4 Business management control ... 19
5.3.5 Systems management control ... 19
5.4 Assumptions ... 19
6 Security objectives ... **20**
6.1 General ... 20
6.2 Security objectives for TPP TOE ... 20
6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data ... 20
6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data ... 21
6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data ... 21
6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP ... 21
6.2.5 Prevention of disclosure of TPP's TSF confidential data ... 21
6.2.6 Generation of security logs ... 21
6.3 Security objectives for TPP TOE operating environment ... 21
Annex A (informative) **Typical transaction scenarios on TPP logical structural model** ... **22**
Bibliography ... **40**

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

For an explanation 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

The global third-party payment (TPP) service is booming and has a profound impact on payment methods. The third-party payment service providers (TPPSPs) act as an intermediary entity between the payment service user (PSU) and the account servicing payment service provider (ASPSP), usually a financial institution. TPPSPs provide payment and other financial services (referred to in this document as TPP services). From the security point of view, the intermediary nature of TPPSPs raises the specific threat of customer impersonation in payment processing. Payment service providers increasingly seek to mitigate the risks of payment fraud in order to protect PSUs and enhance their own business.

Following the CC methodology (see the ISO/IEC 15408 series), this document: i) establishes two logical structural models centred around the TPP services, ii) identifies assets to be protected within this open ecosystem and iii) specifies the security objectives of TPPSP information systems to counter threats faced by the TPP. It aims to assist stakeholders, such as TPPSPs and developers of their information systems, to mitigate specific threats arising from the intermediary role of TPPSPs in the processing of financial transactions, with a focus on payments.

The logical structural models, assets, threats and security objectives in this document are based on real-world practices and are described in a way that is independent of the specific payment instrument used for the TPP payment.

In particular, security objectives focus on the mitigation of identified threats against the integrity, non-repudiation and confidentiality of TPP payment data. Consequently, the TPPSP needs to define the security mechanisms to ensure the protection of sensitive payment data when offering a new TPP service. Conformity with the security objectives set out in this document can help stakeholders gain trust when establishing a business relationship with TPPSPs.

With regards to the scope of this document, it makes full sense to refer to “complementary” or “additional” security objectives compared with other payment circuits where a direct communication link is established between an ASPSP and a PSU. It is worth noting that the integration of the TPPSP has an impact on the security of those entities connected with the TPPSP. However, this document only focuses on the security aspects for TPPSPs.

Financial regulatory authorities have either taken or considered a range of legal initiatives related to TPPs in their respective jurisdictions. Therefore, it is the responsibility of the user of this document to analyse and decide whether the payment processing procedures in this document comply with regional financial regulations related to TPP services.

Security objectives of information systems of third-party payment services

1 Scope

This document defines a common terminology to be used in the context of third-party payment (TPP). Next, it establishes two logical structural models in which the assets to be protected are clarified. Finally, it specifies security objectives based on the analysis of the logical structural models and the interaction of the assets affected by threats, organizational security policies and assumptions. These security objectives are set out in order to counter the threats resulting from the intermediary nature of TPPSPs offering payment services compared with simpler payment models where the payer and the payee directly interact with their respective account servicing payment service provider (ASPSP).

This document assumes that TPP-centric payments rely on the use of TPPSP credentials and the corresponding certified processes for issuance, distribution and renewal purposes. However, security objectives for such processes are out of the scope of this document.

NOTE This document is based on the methodology specified in the ISO/IEC 15408 series. Therefore, the security matters that do not belong to the TOE are dealt with as assumptions, such as the security required by an information system that provides TPP services and the security of communication channels between the entities participating in a TPP business.

2 Normative references

There are no normative references in this document.

3 Terms, definitions, and abbreviated terms

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

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

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

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

3.1 TPP business

3.1.1
payment transaction
act of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the *payer* (3.1.9) and the *payee* (3.1.8)

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

3.1.2
payment account
account held in the name of a *payment service user* (3.1.7) which is used for the execution of a *payment transaction* (3.1.1)

Note 1 to entry: The original definition in ISO 21741 is “account held in the name of one or more payment service users which is used for the execution of payment transactions”. However, only cases in which one account is held by one payment service user are considered in this document.

[SOURCE: ISO/TR 21941:2017, 3.1.7, modified — Note 1 to entry has been added.]