TECHNICAL REPORT

ISO/TR 21941

First edition
2017-07

Financial services — Third-party payment service providers

Services financiers — Prestataires de services de paiement tiers

Reference number
ISO/TR 21941:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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 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 on 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 the following URL: www.iso.org/iso/foreword.html.

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

Introduction

This document was initiated 2 years ago with the aim of conducting research into the interface between third-party payment (TPP) and account servicing payment service providers.

As TPP is a fast-developing area, it was critical to provide guidance quickly.

This document gives an overview of the situation in different regions as it was at the end of 2015 and the beginning of 2016. There have been new developments in several of the regions since then.

For the purposes of this document, payment initiation service providers (PISP) and account information service providers (AISP) are commonly named as TPPs. Furthermore, while there could be other relevant documents to choose from in other markets with regard to terms, definitions and abbreviated terms, the choice has fallen on PSD2[2], as a key reference, as this document can be seen as a good place to start. It should also be noted that the verbal forms are used and interpreted as follows:

— “should” indicates a recommendation;

— “can” indicates a possibility or a capability;

— “must” indicates an external constraint.

NOTE External constraints are not requirements of the document. They are given for the information of the user. Examples of external constraints are laws of nature and legal requirements.

Financial services — Third-party payment service providers

1 Scope

This document reports the findings of research into the interface between third-party payment service providers (TPPs) and account servicing payment service providers (ASPSPs).

2 Normative references

There are no normative references in this document.

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

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

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

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

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

3.1.1
account information service
online service to provide consolidated information on one or more *payment accounts* (3.1.7) held by the *payment service user* (3.1.2) with either another payment service provider or with more than one payment service provider

[SOURCE: Directive (EU) 2015/2366, definition 16]

3.1.2
payment service user
natural or legal person making use of a payment service in the capacity of payer, payee, or both

[SOURCE: Directive (EU) 2015/2366, definition 10]

3.1.3
account servicing payment service provider
payment service provider providing and maintaining a *payment account* (3.1.7) for a payer

[SOURCE: Directive (EU) 2015/2366, definition 17]

3.1.4
authentication
procedure which allows the payment service provider to verify the identity of a *payment service user* (3.1.2) or the validity of the use of a specific *payment instrument* (3.1.9), including the use of the user's *personalized security credentials* (3.1.6)

[SOURCE: Directive (EU) 2015/2366, definition 29]

3.1.5
strong customer authentication
authentication (3.1.4) based on the use of two or more elements categorized as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data

[SOURCE: Directive (EU) 2015/2366, definition 30]

3.1.6
personalized security credentials
personalized features provided by the payment service provider to a *payment service user* (3.1.2) for the purposes of *authentication* (3.1.4)

[SOURCE: Directive (EU) 2015/2366, definition 31]

3.1.7
payment account
account held in the name of one or more *payment service users* (3.1.2) which is used for the execution of payment transactions

[SOURCE: Directive (EU) 2015/2366, definition 12]

3.1.8
payment initiation service
service to initiate a payment order at the request of the *payment service user* (3.1.2) with respect to a *payment account* (3.1.7) held at another payment service provider

[SOURCE: Directive (EU) 2015/2366, definition 15]

3.1.9
payment instrument
personalized device(s) and/or set of procedures agreed between the *payment service user* (3.1.2) and the payment service provider and used in order to initiate a payment order

[SOURCE: Directive (EU) 2015/2366, definition 14]

3.1.10
sensitive payment data
data, including *personalized security credentials* (3.1.6) which can be used to carry out fraud

Note 1 to entry: For the activities of payment initiation service providers and account information service providers, the name of the account owner and the account number do not constitute sensitive payment data.

[SOURCE: Directive (EU) 2015/2366, definition 32, modified — Part of the definition has been formatted as Note 1 to entry.]

3.1.11
third-party payment service provider
payment service provider offering *payment initiation services* (3.1.8) or *account information services* (3.1.1) on accounts where they are not the account-servicing payment service provider themselves

3.1.12
interface
device or program for connecting two items of hardware or software so that they can be operated jointly or communicate with each other

3.1.13
gatekeeper
function that ensures that admittance is limited to *third-party payment service providers* (3.1.11) who comply with regulatory and technical requirements

Note 1 to entry: This function can be provided by individual banks or a common actor within finance industry.

Note 2 to entry: The third-party payment service provider itself can provide the gatekeeper function if certified.

3.2 Abbreviated terms

ACH	automated clearing house
AISP	account information service provider
API	application program interface
ASPSP	account servicing payment service provider
ATM	automated teller machine
EFT	electronic funds transfer (or e-funds transfer)
OAuth	open authentication
PISP	payment initiation service provider
PSD2	Payment Services Directive II
PSP	payment service provider
PSU	payment service user
SAML	security assertion markup language
TPP	third-party payment service provider

4 Overview of the current TPP landscape

4.1 General

There are two main types of third-party payment service provider:

a) payment initiation service providers (PISPs);

b) account information service providers (AISPs).

Much taxonomy describing third-party services also consider payment instrument issuing providers, who are financial institutions other than those servicing the account of the customer, and who issue a payment card or a payment instrument.

The idea behind third-party providers is for customers (payment service users) to perceive them as added value to the service of their account servicing payment service provider. Added value could be new online payment services and more variety in payments instruments, better or simpler user experience, etc.

One of the main points of attention is related to security, especially strong customer authentication and secured communication, which is key to achieving the objective of enhancing consumer protection and promoting innovation. Ensuring the security of payments and the protection of sensitive payment data are a critical part of the infrastructure of robust payment systems knowing all actors should act on

the same level playing field, i.e. the new players should ensure the actual highest levels of security are implemented. Security recommendations are designed for TPPs and ASPSPs and include matters, such as

— segregation of duties in information technology,

— hardening servers with secure configurations,

— applying “least privilege” principles to access control,

— limiting login attempts,

— end-to-end encryption, and

— non-sharing user credentials.

One of the key points is that strong authentication for customers when registering cards, making credit transfers and/or making card payments should be implemented.

Third-party access to accounts, the use of APIs to connect merchant and the bank directly and the ability to consolidate account information in a unique portal are likely to affect payment services around the world. With external APIs, customers will have more options to interact with their TPPs or ASPSPs, next to usual online and mobile banking applications.

PISPs and AISPs can be any type of PSP authorized to offer payment initiation services or account information services and thus could be, for example, a credit institution or a payment institution. TPPs in the context of payment initiation services and account information services are not just the ASPSP in terms of the accounts to which they are obtaining access. In other markets, TPPs may not themselves offer payment accounts, but gather information or perform payment initiation functions where they require access to the payment account. The interface between the TPP and the ASPSP is considered security sensitive; this applies both to AISPs and PISPs. This is due to the following.

a) Entity authentication: the PISP and AISP should provide authentication ensuring that the TPP trying to access an account is an agreed TPP and is approved by the ASPSP in advance based on a contractual relationship or listed on a public authority white list.

b) Strong customer authentication: the PSU should be authenticated in a way that ensures the account servicing payment service providers that the correct PSU is present and has given its consent to the transaction and given access to its account to a third party. The split of information and authentication functions between TPP and ASPSP might be organized in several ways. Nevertheless, user credentials should always be protected and should never be stored. Security standards and protocols such as OAuth or SAML can be used, without the need to store credentials.

c) Authorization: the ASPSP should authorize the PSU’s transaction or operation request before execution.

d) Confidentiality: the TPPs get lots of information about the PSUs and this should be handled according to privacy laws and good practice for banking.

e) Integrity: deletion, manipulation or insertion of information should not occur. In particular, a payment transaction submitted by a PSU should be protected all the way from initiation to ASPSP.

f) Availability: the TPPs should not influence negatively upon availability and uptime of the ASPSP.

The relation between TPP and ASPSP may be bilateral using a contractual agreement between the parties, it may be part of a multilateral scheme or an alternative. A multilateral scheme should give the ASPSP full control and knowledge about which TPPs have access to which types of services.

Management of the multilateral scheme may be performed by the financial supervisory authority of a jurisdiction, by the ASPSPs themselves or by another body. To be approved as a participant in the scheme may require a formal evaluation of the third party, licensing based on a self-assessment or simply a registration. A number of models are possible for this. If the scheme is managed by a financial

supervisory authority, it is likely that they will give a set of rules with supplementary technical regulatory guidelines.

A working paper from SWIFT[6] points out that there is currently no global unified approach regarding regulatory initiatives concerning TPPs. The first challenge is getting to a common understanding of terminology and characteristics of the various TPPs as a foundation for future standardization and definition of regulatory environment.

4.2 Europe

4.2.1 Europe and the revised Payment Services Directive

The revised EU Payment Services Directive (PSD2) entered into force in January 2016 and is intended to be transposed into member states' national law and applied by 13 January 2018. It will enable third-party payment service providers to access customer payment accounts. Account-servicing payment service providers will be required to make available access and all relevant information to third-party payment service providers. Specifically, this covers the following three services:

a) payment initiation services;

b) account information services;

c) "confirmation on the availability of funds" checking services.

With regard to the electronic interface, the European Banking Authority (EBA) is required to draft and present to the European Commission regulatory technical standards (RTSs) for strong customer authentication and secure communication within 12 months after the entry into force of PSD2. Following their adoption by the Commission, the market will have a period of 18 months to implement them. In this regard, the EBA sent out a discussion paper[3] in December 2015, inviting stakeholders to submit their views on a number of identified issues key to the development of the technical standards. Among the stakeholders consulted were the European Payments Council (EPC) and the European Banking Federation (EBF). Their replies to the discussion paper may be of interest for further reading. An official consultation will follow this summer.

There are several options when it comes to implementation. Uniform and interoperable communication between third-party payment service providers and banks in Europe would be preferable. However, this, in turn, presupposes a common interface standard or schema.

4.2.2 Advantages of a common standard

Recital 93 of PSD2 says: "In order to ensure secure communication between the relevant actors in the context of those services, EBA should also specify the requirements of common and open standards of communication to be implemented by all account servicing payment service providers that allow for the provision of online payment services. This means that those open standards should ensure the interoperability of different technological communication solutions." Ideally, interoperability of interacting market participants is achieved through standardization. Open standards are standards that can be developed jointly by all interested market participants.

As there is no international account interface standard at present and EBA will merely define generic requirements, uniform EU-wide implementation cannot be ensured. There are no plans either for EBA to mandate a standard-setter such as European Committee for Standardization (CEN) or International Organization for Standardization (ISO) to draft specifications for an interface.

Implementation of the technical requirements will ultimately be left to the market. This harbours the danger that both banks and third-party payment service providers would have to support several different standards, which immediately raises the question of interoperability. While external parties could provide appropriate transmission services, they would certainly not do so free of charge. In a worst-case scenario, there could, however, be a large number of different interfaces if banks and third-