## INTERNATIONAL STANDARD

ISO 23195

First edition 2021-06

# Security objectives of information systems of third-party payment services

## iTeh Standards (https://standards.iteh.ai) Document Preview

ISO 23195:2021

https://standards.iteh.ai/catalog/standards/iso/d5dfc4ed-e810-4514-b25e-33c3878b2eb2/iso-23195-2021



## iTeh Standards (https://standards.iteh.ai) Document Preview

ISO 23195:2021

https://standards.iteh.ai/catalog/standards/iso/d5dfc4ed-e810-4514-b25e-33c3878b2eb2/iso-23195-2021



#### **COPYRIGHT PROTECTED DOCUMENT**

© ISO 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Introduction  Scope  Normative references  Terms, definitions, and abbreviated terms 3.1 TPP business 3.2 TPP information system 3.3 TPP security.  TPP logical structural model in an open ecosystem 4.1 Logical structural model 4.1.1 General 4.1.2 Direct connection between TPP-BIS and ASPSP 4.1.3 Communication between TPP-BIS and ASPSP via TPP-AIS 4.2 Protected assets 4.2.1 General 4.2.2 User data 4.2.3 TPPSP's TSF data	Fore	word			i
Terms, definitions, and abbreviated terms  3.1 TPP business 3.2 TPP information system 3.3 TPP security  4 TPP logical structural model in an open ecosystem 4.1 Logical structural model 4.1.1 General 4.1.2 Direct connection between TPP-BIS and ASPSP 4.1.3 Communication between TPP-BIS and ASPSP via TPP-AIS 4.2.1 General 4.2.2 User data 4.2.1 General 4.2.3 TPPSP's TSF data  5 Security problem definition 5.1 General 5.2 Threats 5.2.1 Threats to business configuration data 5.2.2 Threats to business configuration data 5.2.3 Threats to TPPSP's TSF data 5.2.4 Threats to TPP transmitting data 5.2.5 Threats to TPP transmitting data 5.2.6 Threats to TPP transmitting data 5.2.7 Threats to particulation data provided by ASPSP 5.2.8 Threats to TPP transmitting data 5.2.9 Torganizational security policies 5.3.1 Operation authorization 5.3.2 Security event audit 5.3.3 Connection security control 5.3.4 Business management control 5.3.5 Systems management control 5.3.4 Business management control 5.4 Assumptions 6 Security objectives 6.1 General 6.2 Security objectives 6.1 General 6.2 Security objectives 6.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and cumulative business data 6.2.2 Prevention of counterfeiting repudiation and unauthorized changes of input data and confidential data 6.2.4 Prevention of ounterfeiting and unauthorized changes of input data and confidential data 6.2.5 Prevention of objectives of TPP TDF TSF Confidential data 6.2.6 Generation of security logs 6.3 Security objectives for TPP TDF operation genvionment 6.3 Security objectives for TPP TDF operation genvionment 6.4 Prevention of objectives of TPP's TSF confidential data 6.5 Prevention of objectives of TPP's TSF confidential data 6.6 Generation of security logs 6.7 Prevention of objectives of TPP's TSF confidential data 6.8 Security objectives for TPP TDF operation genvionment					
7 Terms, definitions, and abbreviated terms 3.1 TPP business 3.2 TPP information system 3.3 TPP security  7 TPP logical structural model in an open ecosystem 4.1 Logical structural model 4.1.1 General 4.1.2 Direct connection between TPP-BIS and ASPSP 4.1.3 Communication between TPP-BIS and ASPSP via TPP-AIS 4.2 Protected assets 4.2.1 General 4.2.2 User data 4.2.3 TPPSP's TSF data 5.2 Threats 5.2 Threats 5.2.1 Threats to business configuration data 5.2.2 Threats to business cumulative data 5.2.3 Threats to business cumulative data 5.2.4 Threats to TPP transmitting data 5.2.5 Threats to authentication data provided by ASPSP 5.2.6 Threats to TPP's TSF data 5.3 Organizational security policies 5.3.1 Operation authorization 5.3.2 Security event audit 5.3.3 Connection security control 5.3.4 Business management control 5.3.5 Systems management control 5.3.4 Susiness management control 5.3.4 Business management control 5.3.4 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2 Security objectives 6.1 General 6.2 Security objectives 6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data 6.2.3 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data 6.2.4 Prevention of counterfeiting and unauthorized changes of protected data and confidential data 6.2.4 Prevention of oscernity logs 6.5 Security objectives for TPP TOE operating environment 6.6 Generation of security logs 6.7 Security objectives for TPP TOE operating environment 6.8 Security objectives for TPP TOE operating environment	_				
Terms, definitions, and abbreviated terms 3.1 TPP business 3.2 TPP information system 3.3 TPP security  4 TPP logical structural model in an open ecosystem 4.1 Logical structural model 4.1.1 General 4.1.2 Direct connection between TPP-BIS and ASPSP 4.1.3 Communication between TPP-BIS and ASPSP via TPP-AIS 4.2 Protected assets 4.2.1 General 4.2.2 User data 4.2.3 TPPSP's TSF data  5 Security problem definition 5.1 General 5.2 Threats 5.2.1 Threats to business configuration data 5.2.2 Threats to transaction input data 5.2.3 Threats to transaction input data 5.2.4 Threats to TPP transmitting data 5.2.5 Threats to TPP transmitting data 5.2.5 Threats to TPPSP's TSF data  5.3 Organizational security policies 5.3.1 Operation authorization 5.3.2 Security event audit 5.3.3 Connection security control 5.3.4 Business management control 5.3.5 Systems management control 5.3.5 Systems management control 6.2 Security objectives 6.1 General 6.2 Security objectives 6.1 General 6.2 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data 6.2.4 Prevention of counterfeiting, repudiation and unauthorized changes of input data and confidential data 6.2.4 Prevention of counterfeiting and unauthorized changes of protected data and confidential data 6.2.4 Prevention of counterfeiting and unauthorized changes of provided by an ASPSP 6.2.5 Prevention of security logs 6.3 Security objectives for TPP TOE operating environment  Annex A (informative) Typical transaction scenarios on TPP logical structural model		•			
3.1 TPP business 3.2 TPP information system 3.3 TPP security  4 TPP logical structural model in an open ecosystem 4.1 Logical structural model 4.1.1 General 4.1.2 Direct connection between TPP-BIS and ASPSP 4.1.3 Communication between TPP-BIS and ASPSP via TPP-AIS 4.2 Protected assets 4.2.1 General 4.2.2 User data 4.2.3 TPPSP's TSF data  5 Security problem definition 5.1 General 5.2 Threats 5.2.1 Threats to business configuration data 5.2.2 Threats to business cumulative data 5.2.3 Threats to TPP transmitting data 5.2.4 Threats to TPP transmitting data 5.2.5 Threats to TPP sys TSF data 5.3 Organizational security policies 5.3.1 Operation authorization 5.3.2 Security event audit 5.3.3 Connection security control 5.3.4 Business management control 5.3.5 Systems management control 5.3.5 Systems management control 5.3.6 Security objectives 6.1 General 6.2 Security objectives 6.1 General 6.2 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.3 Prevention of counterfeiting, repudiation and unauthorized changes of input data and confidential data 6.2.4 Prevention of counterfeiting and unauthorized changes of input data and confidential data 6.2.4 Prevention of counterfeiting and unauthorized changes of protected data and confidential data 6.2.4 Prevention of counterfeiting and unauthorized changes of protected data and confidential data 6.2.4 Prevention of counterfeiting and unauthorized changes of protected data and confidential data 6.2.5 Prevention of counterfeiting and unauthorized changes of protected data and confidential data 6.2.6 Generalion 6 security logs 6.3 Security objectives for TPP TOE operating environment  Annex A (informative) Typical transaction scenarios on TPP logical structural model	2				
3.2 TPP information system. 3.3 TPP security.  4 TPP logical structural model in an open ecosystem. 4.1 Logical structural model. 4.1.1 General. 4.1.2 Direct connection between TPP-BIS and ASPSP. 4.1.3 Communication between TPP-BIS and ASPSP via TPP-AIS. 4.2 Protected assets. 4.2.1 General. 4.2.2 User data. 4.2.3 TPPSP's TSF data. 5.2 Threats. 5.2 Threats. 5.2.1 Threats to business configuration data. 5.2.2 Threats to business cumulative data. 5.2.3 Threats to transaction input data. 5.2.4 Threats to transaction input data. 5.2.5 Threats to authentication data provided by ASPSP. 5.2.6 Threats to TPPSP's TSF data. 5.3 Organizational security policies. 5.3 Organizational security policies. 5.3.1 Operation authorization. 5.3.2 Security event audit. 5.3.3 Connection security control. 5.3.4 Business management control. 5.3.5 Systems management control. 5.3.5 Systems management control. 5.3.5 Systems management control. 5.4 Assumptions. 6 Security objectives. 6.1 General. 6.2 Security objectives for TPP TOE. 6.2.1 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data. 6.2.2 Prevention of counterfeiting and unauthorized changes of protected data and confidential data. 6.2.4 Prevention of ocunterfeiting and unauthorized changes of protected data and confidential data. 6.2.4 Prevention of ocunterfeiting and unauthorized changes of protected data and confidential data. 6.2.5 Prevention of ocunterfeiting and unauthorized changes of protected data and confidential data. 6.2.6 Generation of security logs 6.3 Security objectives for TPP TOE operating environment.  Annex A (informative) Typical transaction scenarios on TPP logical structural model.	3				
4.1 Logical structural model in an open ecosystem. 4.1 Logical structural model. 4.1.1 General. 4.1.2 Direct connection between TPP-BIS and ASPSP. 4.1.3 Communication between TPP-BIS and ASPSP via TPP-AIS. 4.2 Protected assets. 4.2.1 General. 4.2.2 User data. 4.2.3 TPPSP's TSF data. 5.2 Threats 5.2 Threats 5.2 Threats 5.2.1 Threats to business configuration data. 5.2 Threats to business comfiguration data. 5.2.2 Threats to business cumulative data. 5.2.3 Threats to TPP bransmitting data. 5.2.4 Threats to TPP bransmitting data. 5.2.5 Threats to authentication data provided by ASPSP. 5.2.6 Threats to TPPSP's TSF data. 5.3 Organizational security policies. 5.3.1 Operation authorization. 5.3.2 Security event audit. 5.3.3 Connection security control. 5.3.4 Business management control. 5.3.5 Systems management control. 5.3.5 Systems management control. 5.3.6 Security objectives. 6.1 General. 6.2 Security objectives for TPP TOE. 6.2.1 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data. 6.2.2 Prevention of counterfeiting and unauthorized changes of input data and transmitting data. 6.2.4 Prevention of counterfeiting and unauthorized changes of protected data and confidential data. 6.2.4 Prevention of or of security in formal provided by an ASPSP. 6.2.5 Prevention of security logs. 6.3 Security objectives for TPP TOE operating environment.  Annex A (informative) Typical transaction scenarios on TPP logical structural model.		_			
4.1 Logical structural model in an open ecosystem. 4.1 Logical structural model. 4.1.1 General. 4.1.2 Direct connection between TPP-BIS and ASPSP. 4.1.3 Communication between TPP-BIS and ASPSP via TPP-AIS. 4.2 Protected assets 4.2.1 General. 4.2.2 User data. 4.2.3 TPPSP's TSF data. 5.2 Security problem definition. 5.1 General. 5.2 Threats. 5.2.1 Threats to business configuration data. 5.2.2 Threats to transaction input data. 5.2.3 Threats to transaction input data. 5.2.4 Threats to TPP transmitting data. 5.2.5 Threats to TPPSP's TSF data. 5.2.6 Threats to TPPSP's TSF data. 5.2.1 Operation authorization. 5.3.1 Operation authorization. 5.3.2 Security event audit. 5.3.3 Connection security control. 5.3.4 Business management control. 5.3.5 Systems management control. 5.3.5 Systems management control. 5.3.6 Security objectives. 6.1 General. 6.2 Security objectives for TPP TOE. 6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data. 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data. 6.2.3 Prevention of ounterfeiting and unauthorized changes of protected data and confidential data. 6.2.4 Prevention of ounterfeiting and unauthorized changes of protected data and confidential data. 6.2.5 Prevention of ounterfeiting and unauthorized changes of protected data and confidential data. 6.2.4 Prevention of ounterfeiting and unauthorized changes of protected data and confidential data. 6.2.5 Prevention of ounterfeiting and unauthorized changes of protected data and confidential data. 6.2.6 Generation of security logs 6.3 Security objectives for TPP TOE operating environment.  Annex A (informative) Typical transaction scenarios on TPP logical structural model.		_			
4.1 Logical structural model 4.1.1 General 4.1.2 Direct connection between TPP-BIS and ASPSP 4.1.3 Communication between TPP-BIS and ASPSP via TPP-AIS 4.2 Protected assets 4.2.1 General 4.2.2 User data 4.2.2 User data 4.2.3 TPPSP's TSF data  5.2 Threats 5.2 Threats 5.2.1 Threats to business configuration data 5.2.2 Threats to business cumulative data 5.2.3 Threats to transaction input data 5.2.4 Threats to transaction input data 5.2.5 Threats to authentication data provided by ASPSP 5.2.6 Threats to TPPSP's TSF data 5.2.1 Threats to withentication data provided by ASPSP 5.2.6 Threats to TPPSP's TSF data 5.3 Organizational security policies 5.3 Connection security control 5.3.4 Business management control 5.3.5 Systems management control 5.3.5 Systems management control 5.3.6 Security objectives 6.1 General 6.2 Security objectives 6.2 General 6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data 6.2.3 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP 6.2.5 Prevention of security logs 6.3 Security objectives for TPP TOE operating environment  Annex A (informative) Typical transaction scenarios on TPP logical structural model				•	
4.1.1 General 4.1.2 Direct connection between TPP-BIS and ASPSP 4.1.3 Communication between TPP-BIS and ASPSP via TPP-AIS 4.2 Protected assets 4.2.1 General 4.2.2 User data 4.2.3 TPPSP's TSF data 5.2 General 5.2 Threats 5.2 Threats 5.2.1 Threats to business configuration data 5.2.2 Threats to Threats to business cumulative data 5.2.3 Threats to transaction input data 5.2.4 Threats to authentication data provided by ASPSP 5.2.6 Threats to SPSP data 6.3 Organizational security policies 6.3.1 Operation authorization 5.3.2 Security event audit 6.3.3 Connection security control 6.3.4 Business management control 6.3.4 Susumptions 6 Security objectives 6.1 General 6.2 Security objectives 6.1 General 6.2 Security objectives for TPP TOE 6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data 6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data 6.2.4 Prevention of disclosure of TPP's TSF confidential data 6.2.5 Prevention of disclosure of TPP's TSF confidential data 6.2.6 Generation of security logs 6.3 Security objectives for TPP TOE operating environment  Annex A (informative) Typical transaction scenarios on TPP logical structural model	4		TPP logical structural model in an open ecosystem		
4.1.2 Direct connection between TPP-BIS and ASPSP 4.1.3 Communication between TPP-BIS and ASPSP via TPP-AIS 4.2 Protected assets 4.2.1 General 4.2.2 User data 4.2.2 User data 4.2.3 TPPSP's TSF data  5 Security problem definition 5.1 General 5.2 Threats 5.2.1 Threats to business configuration data 5.2.2 Threats to transaction input data 5.2.3 Threats to transaction input data 5.2.4 Threats to TPP transmitting data 5.2.5 Threats to authentication data provided by ASPSP 5.2.6 Threats to TPPSP's TSF data  5.3 Organizational security policies 5.3.1 Operation authorization 5.3.2 Security event audit 5.3.3 Connection security control 5.3.4 Business management control 5.3.5 Systems management control 5.3.4 Assumptions  6 Security objectives 6.1 General 6.2 Security objectives 6.1 General 6.2 Security objectives for TPP TOE 6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.2 Prevention of counterfeiting repudiation and unauthorized changes of input data and transmitting data 6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data 6.2.4 Prevention of disclosure or usage of the authentication data provided by an ASPSP 6.2.5 Prevention of disclosure or TPP's TSF confidential data 6.2.6 Generation of security logs 6.3 Security objectives for TPP TOE operating environment  Annex A (informative) Typical transaction scenarios on TPP logical structural model		4.1	_		
4.2 Protected assets 4.2.1 General 4.2.2 User data 4.2.3 TPPSP's TSF data  5. Security problem definition 5.1 General 5.2 Threats 5.2.1 Threats to business configuration data 5.2.2 Threats to transaction input data 5.2.3 Threats to TPP TOE 5.2.6 Threats to TPP TOE 5.3 Organizational security policies 5.3 Connection security control 5.3 Security event audit 5.3.3 Connection security control 5.3.4 Business management control 5.3.5 Systems management control 5.3.6 Security objectives 6.1 General 6.2 Security objectives 6.2 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and confidential data 6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP 6.2.5 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP 6.2.5 Prevention of security logs 6.3 Security objectives for TPP TOE operating environment. 6.3 Security objectives for TPP TOE operating environment. 6.4 Prevention of security logs 6.3 Security objectives for TPP TOE operating environment. 6.4 Annex A (informative) Typical transaction scenarios on TPP logical structural model			4.1.1		
4.2.1 General 4.2.2 User data 4.2.3 TPPSP's TSF data  5.2 General 5.2 Threats 5.2.1 Threats to business configuration data 5.2.2 Threats to business cumulative data 5.2.3 Threats to transaction input data 5.2.4 Threats to TPP transmitting data 5.2.5 Threats to authentication data provided by ASPSP 5.2.6 Threats to TPPSP's TSF data 5.3 Organizational security policies 5.3.1 Operation authorization 5.3.2 Security event audit 5.3.3 Connection security control 5.3.4 Business management control 5.3.5 Systems management control 5.4 Assumptions 6 Security objectives 6.1 General 6.2 Security objectives for TPP TOE 6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data 6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data 6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP 6.2.5 Prevention of disclosure of TPP's TSF confidential data 6.2.6 Generation of security logs 6.3 Security objectives for TPP TOE operating environment.  Annex A (informative) Typical transaction scenarios on TPP logical structural model			4.1.2		
4.2.1 General 4.2.2 User data 4.2.3 TPPSP's TSF data  5.2 Threats 5.2 Threats 5.2.1 Threats to business configuration data 5.2.2 Threats to business cumulative data 5.2.3 Threats to transaction input data 5.2.4 Threats to authentication data provided by ASPSP 5.2.5 Threats to TPPSP's TSF data 5.2.3 Threats to TPPSP's TSF data 5.2.4 Threats to TPPSP's TSF data 5.2.5 Threats to TPPSP's TSF data 5.3 Organizational security policies 5.3.1 Operation authorization 5.3.2 Security event audit 5.3.3 Connection security control 5.3.4 Business management control 5.3.5 Systems management control 5.3.6 Security objectives 6.1 General 6.2 Security objectives 6.1 General 6.2 Security objectives for TPP TOE 6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data 6.2.3 Prevention of counterfeiting, repudiation and unauthorized changes of input data and confidential data 6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP 6.2.5 Prevention of security logs 6.3 Security objectives for TPP TOE operating environment.  Annex A (informative) Typical transaction scenarios on TPP logical structural model			_		
4.2.2 User data 4.2.3 TPPSP's TSF data  5.2 General 5.2 Threats 5.2.1 Threats to business configuration data 5.2.2 Threats to business configuration data 5.2.2 Threats to transaction input data 5.2.3 Threats to TPP transmitting data 5.2.4 Threats to TPP transmitting data 5.2.5 Threats to authentication data provided by ASPSP 5.2.6 Threats to TPPSP's TSF data 5.3 Organizational security policies 5.3.1 Operation authorization 5.3.2 Security event audit 5.3.3 Connection security control 5.3.4 Business management control 5.3.5 Systems management control 5.3.5 Systems management control 5.4 Assumptions  6 Security objectives 6.1 General 6.2 Security objectives for TPP TOE 6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data 6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data 6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP 6.2.5 Prevention of disclosure of TPP's TSF confidential data 6.2.6 Generation of security logs 6.3 Security objectives for TPP TOE operating environment  Annex A (informative) Typical transaction scenarios on TPP logical structural model		4.2			
4.2.3 TPPSP's TSF data  5.2 General 5.2 Threats 5.2.1 Threats to business configuration data 5.2.2 Threats to business cumulative data 5.2.3 Threats to transaction input data 5.2.4 Threats to authentication data provided by ASPSP 5.2.6 Threats to authentication data provided by ASPSP 5.2.6 Threats to TPPSP's TSF data 5.3 Organizational security policies. 5.3.1 Operation authorization 5.3.2 Security event audit 5.3.3 Connection security control 5.3.4 Business management control 5.3.5 Systems management control 5.3.5 Systems management control 5.4 Assumptions  6 Security objectives 6.1 General 6.2 Security objectives for TPP TOE 6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data 6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data 6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP 6.2.5 Prevention of disclosure of TPP's TSF confidential data 6.2.6 Generation of security logs 6.3 Security objectives for TPP TOE operating environment  Annex A (informative) Typical transaction scenarios on TPP logical structural model					
Security problem definition  5.1 General  5.2 Threats  5.2.1 Threats to business configuration data  5.2.2 Threats to business cumulative data  5.2.3 Threats to transaction input data  5.2.4 Threats to TPP transmitting data  5.2.5 Threats to authentication data provided by ASPSP  5.2.6 Threats to TPPSP's TSF data  5.3 Organizational security policies  5.3.1 Operation authorization  5.3.2 Security event audit  5.3.3 Connection security control  5.3.4 Business management control  5.3.5 Systems management control  5.4 Assumptions  6 Security objectives  6.1 General  6.2 Security objectives for TPP TOE  6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data  6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data  6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data  6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP  6.2.5 Prevention of disclosure of TPP's TSF confidential data  6.2.6 Generation of security logs  6.3 Security objectives for TPP TOE operating environment  Annex A (informative) Typical transaction scenarios on TPP logical structural model					
5.1 General 5.2 Threats 5.2.1 Threats to business configuration data 5.2.2 Threats to business cumulative data 5.2.3 Threats to transaction input data 5.2.4 Threats to TPP transmitting data 5.2.5 Threats to TPPS's TSF data 5.3 Organizational security policies 5.3 Organizational security policies 5.3.1 Operation authorization 5.3.2 Security event audit 5.3.3 Connection security control 5.3.4 Business management control 5.3.5 Systems management control 5.3.6 Security objectives 6.1 General 6.2 Security objectives for TPP TOE 6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data 6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data 6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP 6.2.5 Prevention of disclosure of TPP's TSF confidential data 6.2.6 Generation of security logs 6.3 Security objectives for TPP TOE operating environment  Annex A (informative) Typical transaction scenarios on TPP logical structural model			4.2.3	TPPSP's TSF data	
5.1 General 5.2 Threats 5.2.1 Threats to business configuration data 5.2.2 Threats to business cumulative data 5.2.3 Threats to transaction input data 5.2.4 Threats to TPP transmitting data 5.2.5 Threats to TPPS's TSF data 5.3 Organizational security policies 5.3 Organizational security policies 5.3.1 Operation authorization 5.3.2 Security event audit 5.3.3 Connection security control 5.3.4 Business management control 5.3.5 Systems management control 5.3.6 Security objectives 6.1 General 6.2 Security objectives for TPP TOE 6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data 6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data 6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP 6.2.5 Prevention of disclosure of TPP's TSF confidential data 6.2.6 Generation of security logs 6.3 Security objectives for TPP TOE operating environment  Annex A (informative) Typical transaction scenarios on TPP logical structural model	<b>5</b> s://sta	Security problem definition			1
5.2 Threats 5.2.1 Threats to business configuration data 5.2.2 Threats to business cumulative data 5.2.3 Threats to transaction input data 5.2.4 Threats to TPP transmitting data 5.2.5 Threats to authentication data provided by ASPSP 5.2.6 Threats to TPPSP's TSF data 5.3 Organizational security policies 5.3.1 Operation authorization 5.3.2 Security event audit 5.3.3 Connection security control 5.3.4 Business management control 5.3.5 Systems management control 5.3.6 Security objectives 6.1 General 6.2 Security objectives 6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data 6.2.3 Prevention of counterfeiting and unauthorized changes of input data and transmitting data 6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP 6.2.5 Prevention of disclosure of TPP's TSF confidential data 6.2.6 Generation of security logs 6.3 Security objectives for TPP TOE operating environment.  Annex A (informative) Typical transaction scenarios on TPP logical structural model					
5.2.1 Threats to business configuration data 5.2.2 Threats to business cumulative data 5.2.3 Threats to transaction input data 5.2.4 Threats to TPP transmitting data 5.2.5 Threats to authentication data provided by ASPSP 5.2.6 Threats to TPPSP's TSF data 5.3 Organizational security policies 5.3.1 Operation authorization 5.3.2 Security event audit 5.3.3 Connection security control 5.3.4 Business management control 5.3.5 Systems management control 5.3.5 Systems management control 5.3.6 Security objectives 6.1 General 6.2 Security objectives 6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data 6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data 6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP 6.2.5 Prevention of disclosure of TPP's TSF confidential data 6.2.6 Generation of security logs 6.3 Security objectives for TPP TOE operating environment.  Annex A (informative) Typical transaction scenarios on TPP logical structural model					
5.2.2 Threats to business cumulative data 5.2.3 Threats to transaction input data 5.2.4 Threats to TPP transmitting data 5.2.5 Threats to authentication data provided by ASPSP 5.2.6 Threats to TPPSP's TSF data 5.3 Organizational security policies 5.3.1 Operation authorization 5.3.2 Security event audit 5.3.3 Connection security control 5.3.4 Business management control 5.3.5 Systems management control 5.3.6 Security objectives 6.1 General 6.2 Security objectives for TPP TOE 6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data 6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data 6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP 6.2.5 Prevention of disclosure of TPP's TSF confidential data 6.2.6 Generation of security logs 6.3 Security objectives for TPP TOE operating environment  Annex A (informative) Typical transaction scenarios on TPP logical structural model		0			
5.2.3 Threats to transaction input data 5.2.4 Threats to TPP transmitting data 5.2.5 Threats to authentication data provided by ASPSP 5.2.6 Threats to TPPSP'S TSF data 5.3 Organizational security policies 5.3.1 Operation authorization 5.3.2 Security event audit 5.3.3 Connection security control 5.3.4 Business management control 5.3.5 Systems management control 5.3.5 Systems management control 5.4 Assumptions 6 Security objectives 6.1 General 6.2 Security objectives for TPP TOE 6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data 6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data 6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP 6.2.5 Prevention of disclosure of TPP's TSF confidential data 6.2.6 Generation of security logs 6.3 Security objectives for TPP TOE operating environment  Annex A (informative) Typical transaction scenarios on TPP logical structural model					
5.2.4 Threats to TPP transmitting data 5.2.5 Threats to authentication data provided by ASPSP 5.2.6 Threats to TPPSP's TSF data  5.3 Organizational security policies 5.3.1 Operation authorization 5.3.2 Security event audit 5.3.3 Connection security control 5.3.4 Business management control 5.3.5 Systems management control 5.3.5 Systems management control 5.3.6 Security objectives 6.1 General 6.2 Security objectives 6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data 6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data 6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP 6.2.5 Prevention of disclosure of TPP's TSF confidential data 6.2.6 Generation of security logs 6.3 Security objectives for TPP TOE operating environment  Annex A (informative) Typical transaction scenarios on TPP logical structural model			_		
5.2.5 Threats to authentication data provided by ASPSP 5.2.6 Threats to TPPSP's TSF data  5.3 Organizational security policies 5.3.1 Operation authorization 5.3.2 Security event audit 5.3.3 Connection security control 5.3.4 Business management control 5.3.5 Systems management control 5.4 Assumptions  6. Security objectives 6.1 General 6.2 Security objectives for TPP TOE 6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data 6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data 6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP 6.2.5 Prevention of disclosure of TPP's TSF confidential data 6.2.6 Generation of security logs 6.3 Security objectives for TPP TOE operating environment  Annex A (informative) Typical transaction scenarios on TPP logical structural model					
5.2.6 Threats to TPPSP's TSF data 5.3 Organizational security policies 195.2021  //standards it 5.3.1 Operation authorization 5.3.2 Security event audit 5.3.3 Connection security control 5.3.4 Business management control 5.3.5 Systems management control 5.4 Assumptions  6 Security objectives 6.1 General 6.2 Security objectives for TPP TOE 6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data 6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data 6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP 6.2.5 Prevention of disclosure of TPP's TSF confidential data 6.2.6 Generation of security logs 6.3 Security objectives for TPP TOE operating environment.  Annex A (informative) Typical transaction scenarios on TPP logical structural model					
5.3 Organizational security policies 1.05.2021  //standards.ii 5.3.1 or Operation authorization 1.04.10.45.14.15.15.2023.23.23.25.25.2023.2023.2023.2023.2					
Standards   1 5.3.1 car   Operation authorization   1 5.3.2   Security event audit		5.3			
5.3.2 Security event audit 5.3.3 Connection security control 5.3.4 Business management control 5.3.5 Systems management control 5.4 Assumptions  6 Security objectives 6.1 General 6.2 Security objectives for TPP TOE 6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data. 6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data. 6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP 6.2.5 Prevention of disclosure of TPP's TSF confidential data. 6.2.6 Generation of security logs 6.3 Security objectives for TPP TOE operating environment.  Annex A (informative) Typical transaction scenarios on TPP logical structural model		standards it 5.3.1 cat Operation authorization 4.4.4.8.1.4.4.5.4.4.5.2.23.23.8.7.8.6.2.6.2.4.6.2.2.2		Operation authorization 4 d. a810. 4514. h25a. 23a. 2878h2ah2/iaa. 23195. 20	12.1
5.3.3 Connection security control 5.3.4 Business management control 5.3.5 Systems management control 5.4 Assumptions  6 Security objectives 6.1 General 6.2 Security objectives for TPP TOE 6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data 6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data 6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP 6.2.5 Prevention of disclosure of TPP's TSF confidential data 6.2.6 Generation of security logs 6.3 Security objectives for TPP TOE operating environment  Annex A (informative) Typical transaction scenarios on TPP logical structural model					
5.3.4 Business management control 5.3.5 Systems management control 5.4 Assumptions  6 Security objectives 6.1 General 6.2 Security objectives for TPP TOE 6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data 6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data 6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP 6.2.5 Prevention of disclosure of TPP's TSF confidential data 6.2.6 Generation of security logs 6.3 Security objectives for TPP TOE operating environment  Annex A (informative) Typical transaction scenarios on TPP logical structural model				· · · · · · · · · · · · · · · · · · ·	
5.3.5 Systems management control 5.4 Assumptions  6 Security objectives 6.1 General 6.2 Security objectives for TPP TOE 6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data 6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data. 6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP 6.2.5 Prevention of disclosure of TPP's TSF confidential data. 6.2.6 Generation of security logs 6.3 Security objectives for TPP TOE operating environment.  Annex A (informative) Typical transaction scenarios on TPP logical structural model					
5.4 Assumptions 6 Security objectives 6.1 General 6.2 Security objectives for TPP TOE 6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data 6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data 6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP. 6.2.5 Prevention of disclosure of TPP's TSF confidential data 6.2.6 Generation of security logs 6.3 Security objectives for TPP TOE operating environment.  Annex A (informative) Typical transaction scenarios on TPP logical structural model					
6.1 General		5.4			
6.1 General 6.2 Security objectives for TPP TOE 6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data 6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data 6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP 6.2.5 Prevention of disclosure of TPP's TSF confidential data 6.2.6 Generation of security logs 6.3 Security objectives for TPP TOE operating environment  Annex A (informative) Typical transaction scenarios on TPP logical structural model	6	•			
6.2 Security objectives for TPP TOE. 6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data. 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data. 6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data. 6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP. 6.2.5 Prevention of disclosure of TPP's TSF confidential data. 6.2.6 Generation of security logs. 6.3 Security objectives for TPP TOE operating environment.  Annex A (informative) Typical transaction scenarios on TPP logical structural model.	0				
6.2.1 Prevention of unauthorized disclosure and change of business configuration data and cumulative business data 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data 6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data 6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP 6.2.5 Prevention of disclosure of TPP's TSF confidential data 6.2.6 Generation of security logs 6.3 Security objectives for TPP TOE operating environment  Annex A (informative) Typical transaction scenarios on TPP logical structural model					
configuration data and cumulative business data 6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data 6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data 6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP 6.2.5 Prevention of disclosure of TPP's TSF confidential data 6.2.6 Generation of security logs 6.3 Security objectives for TPP TOE operating environment  Annex A (informative) Typical transaction scenarios on TPP logical structural model		0.2			4
6.2.2 Prevention of counterfeiting, repudiation and unauthorized changes of input data and transmitting data 6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data 6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP 6.2.5 Prevention of disclosure of TPP's TSF confidential data 6.2.6 Generation of security logs 6.3 Security objectives for TPP TOE operating environment  Annex A (informative) Typical transaction scenarios on TPP logical structural model			0.4.1		
input data and transmitting data.  6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data			622	Prevention of counterfeiting regulation and unauthorized changes of	
6.2.3 Prevention of counterfeiting and unauthorized changes of protected data and confidential data			0.2.2		
and confidential data			623		
6.2.4 Prevention of unauthorized disclosure or usage of the authentication data provided by an ASPSP			0.2.3		
provided by an ASPSP			624	Prevention of unauthorized disclosure or usage of the authentication data	
6.2.5 Prevention of disclosure of TPP's TSF confidential data 6.2.6 Generation of security logs 6.3 Security objectives for TPP TOE operating environment  Annex A (informative) Typical transaction scenarios on TPP logical structural model			0.2.7		
6.2.6 Generation of security logs			625	Prevention of disclosure of TPP's TSF confidential data	
6.3 Security objectives for TPP TOE operating environment					
Annex A (informative) Typical transaction scenarios on TPP logical structural model		63		ty objectives for TPP TOF operating anyironment	
Bibliography	Ann	<b>ex A</b> (in	formative	e) Typical transaction scenarios on TPP logical structural model	2
	Rihli	ingranh	ıv		

#### **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 <a href="www.iso.org/directives">www.iso.org/directives</a>).

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 <a href="https://www.iso.org/patents">www.iso.org/patents</a>).

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 <a href="https://www.iso.org/iso/foreword.html">www.iso.org/iso/foreword.html</a>.

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 <a href="https://www.iso.org/members.html">www.iso.org/members.html</a>.

https://standards.iteh.ai/catalog/standards/iso/d5dfc4ed-e810-4514-b25e-33c3878b2eb2/iso-23195-202

#### 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.

## iTeh Standards (https://standards.iteh.ai) Document Preview

ISO 23195:2021

https://standards.jteh.aj/catalog/standards/jso/d5dfc4ed-e810-4514-b25e-33c3878b2eb2/jso-23195-2021

## 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://standards.iteh.ai)

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 <a href="https://www.iso.org/obp">https://www.iso.org/obp</a>
- IEC Electropedia: available at <a href="http://www.electropedia.org/">http://www.electropedia.org/</a>

#### 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.]

#### ISO 23195:2021(E)

#### 3.1.3

#### third-party payment

#### **TPP**

payment transaction (3.1.1) involving at least one intermediary TPPSP (3.1.5)

#### 3.1.4

#### intermediary

commercial party who provides services to customers, suppliers or authorities within the supply chain

Note 1 to entry: The customer is the *payment service user* (3.1.7), who may be a *payer* (3.1.9) or a *payee* (3.1.8), such as a merchant.

[SOURCE: ISO/TS 24533:2012, 2.31, modified — Note 1 to entry has been revised.]

#### 3.1.5

## third-party payment service provider TPPSP $\,$

payment service provider offering *TPP* (3.1.3) services where they are not the *ASPSP* (3.1.6) 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/TR 21941:2017, 3.1.11, modified — Note 1 to entry has been added.]

#### 3.1.6

#### account servicing payment service provider SO 23195:2021

ASPSP://standards.iteh.ai/catalog/standards/iso/d5dfc4ed-e810-4514-b25e-33c3878b2eb2/iso-23195-202

payment service provider providing and maintaining a payment account (3.1.2) for a payment service user (3.1.7)

Note 1 to entry: In ISO/TR 21941:2017, 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/TR 21941:2017, 3.1.3, modified — Note 1 to entry has been added.]

#### 3.1.7

#### payment service user

#### **PSU**

natural or legal person making use of a payment service in the capacity of *payer* (3.1.9), *payee* (3.1.8) or both

Note 1 to entry: Generally, a payment service user is an end user of a TPP information system.

Note 2 to entry: Generally, the payee is a merchant or a person who receives the money without offering goods or services directly. In this document they are called merchant and payee, respectively, if necessary.

Note 3 to entry: In situations where the payment service user is a natural person, this payment service user is deemed a *PII principal* (3.1.10).

[SOURCE: ISO/TR 21941:2017, 3.1.2, modified — Note 1 to entry, Note 2 to entry and Note 3 to entry have been added.]

#### 3.1.8

#### payee

person or legal entity who is the intended recipient of funds which have been the subject of a *payment* transaction (3.1.1)

[SOURCE: ISO 12812-1:2017, 3.38]

#### 3.1.9

#### payer

person or legal entity who authorizes a *payment transaction* (3.1.1)

[SOURCE: ISO 12812-1:2017, 3.39]

#### 3.1.10

#### personally identifiable information

#### ΡΠ

information that i) can be used to identify the *PII principal* (3.1.11) to whom such information relates or ii) is or is possibly directly or indirectly linked to a PII principal

Note 1 to entry: To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person.

[SOURCE: ISO/IEC 29100:2011, 2.9, modified]

#### 3.1.11

#### PII principal

natural person to whom the PII (3.1.10) relates

Note 1 to entry: Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym "data subject" can also be used instead of the term "PII principal".

[SOURCE: ISO/IEC 29100:2011, 2.11, modified — The full designation of "PII", i.e. "personally identifiable information", has been removed from the definition.]

#### 3.1.12

#### credential

data provided to the payment service user (3.1.7) for identification (3.1.16) and/or authentication (3.1.17) purposes

Note 1 to entry: The phrase "data provided to the payment service user" is used instead of "data provided to the customer" so that the definition is clearer in the context of this document.

Note 2 to entry: The expression of "identification and/or authentication" replaces "identification/authentication" in the definition to improve clarity.

[SOURCE: ISO 12812-1:2017, 3.10, modified — Note 1 to entry and Note 2 to entry have been added.]

#### 3.1.13

#### credential carrier

personal device held by payment service user (3.1.7) to store and transmit credential(s) (3.1.12)

Note 1 to entry: Under supporting of the state of the art of technologies, a credential can be stored in more than one credential carrier while a credential carrier can store more than one credential.

Note 2 to entry: A credential carrier may be a standalone device or a part of a payment instrument (3.1.19).

EXAMPLE A TPPSP issues a payer a USB key storing a digital certificate. In this case, the USB key is the TPPSP credential carrier.

#### 3.1.14

#### **ASPSP** credential

credential (3.1.12) which is provided by ASPSP (3.1.6) and used by the payment service user (3.1.7)

#### ISO 23195:2021(E)

#### 3.1.15

#### **TPPSP** credential

credential (3.1.12) which is provided by TPPSP (3.1.5) and used by the payment service user (3.1.7)

#### 3.1.16

#### identification

process of recognizing the attributes that identify an entity

Note 1 to entry: In TPP business, an entity generally is a payment service user (3.1.7).

[SOURCE: ISO 22300:2021, 3.1.117, modified — Note 1 to entry has been added]

#### 3.1.17

#### 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 1 and 2 to entry have been removed]

#### 3.1.18

#### strong customer authentication

authentication (3.1.17) based on the use of two or more elements categorized as knowledge (something only the user knows), possession (something only the user owns) 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: ISO/TR 21941:2017, 3.1.5, modified] Standards

#### 3.1.19

#### payment instrument

personalized device(s) and/or set of procedures agreed between the payment service user (3.1.7) and the payment service provider and used in order to initiate a payment order

Note 1 to entry: In the context of TPP, the payment service provider is a TPPSP.

[SOURCE: ISO/TR 21941:2017, 3.1.9, modified — Note 1 to entry has been added.]

#### 3.2 TPP information system

#### 3.2.1

#### information system

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

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

#### 3.2.2

#### **TPP business information system**

#### **TPP-BIS**

information system (3.2.1) that enables business functions of TPPSP (3.1.5) and deals with payment transactions (3.1.1) based on TPPSP credentials (3.1.15)

#### 3.2.3

#### **ASPSP** gatekeeper

function implemented by the ASPSP (3.1.6) that ensures that admittance is limited to TPPSP (3.1.5) who comply with the relevant regulatory and technical requirement

#### 3.2.4

#### **TPPSP** gatekeeper

function implemented by TPPSP (3.1.5) that performs access control services to the TPP-BIS (3.2.2)

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 (3.3.9) while the message is transferred via the transaction channel.

#### 3.2.5

## TPP agent information system TPP-AIS

*information system* (3.2.1), that receives requests of *payment transaction* (3.1.1) from multilateral *TPPSP* (3.1.5) and forwards them to multilateral *ASPSP* (3.1.6), 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 CASS (3.2.6) and deliver the clearing information based on their payment transaction log.

Note 2 to entry: Regarding TPP 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.

#### 326

### 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 may be completed in a conventional period.

#### 3.2.7

#### trust centre

entity implementing a trusted mechanism

Note 1 to entry: Trust centres can facilitate the establishment of both trusted channels and trusted paths. However, they are not a prerequisite for establishing both trusted channels and trusted paths.

#### 3.2.8

#### TPP payment terminal

terminal equipment which is utilized in order to interact with a TPPSP's credential carrier (3.1.13) to retrieve *TPPSP credentials* (3.1.15) and to perform payment transactions (3.1.1)

Note 1 to entry: The TPP payment terminal may be implemented in different devices operated by the *payment service user* (3.1.7), the merchant or both.

#### 3.3 TPP security

#### 3.3.1

#### sensitive payment data

data, including both TSF data (3.3.10) and user data (3.3.11), which can be used to carry out fraud

Note 1 to entry: For the activities of *TPPSP* (3.1.5), the name of the account owner and the account number do not constitute sensitive payment data.

Note 2 to entry: The ASPSP credential (3.1.14) and TPPSP credential (3.1.15) are two kinds of TSF data.

Note 3 to entry: Both the definition and Note 1 to entry have been rewritten based on ISO/TR 21941:2017, 3.1.10, so as to fit the context of ISO/IEC 15408-1:2009. In fact, protected entities are consistent.

[SOURCE: ISO/TR 21941:2017, 3.1.10, modified — Note 2 to entry and Note 3 to entry have been added.]

#### 3.3.2

#### security objective

statement of an intent to counter identified threats and/or satisfy identified organization security policies, assumptions or both

[SOURCE: ISO/IEC 15408-1:2009, 3.1.60, modified]

#### ISO 23195:2021(E)

#### 3.3.3

#### asset

entity that the owner of the *TOE* (3.3.4) presumably places value upon

[SOURCE: ISO/IEC 15408-1:2009, 3.1.2, modified]

#### 3.3.4

#### target of evaluation

#### TOE

set of software, firmware, hardware or a combination of all three, possibly accompanied by guidance

[SOURCE: ISO/IEC 15408-1:2009, 3.1.70, modified]

#### 3.3.5

#### security problem

statement which in a formal manner defines the nature and scope of the security that the TOE is intended to address

Note 1 to entry: This statement consists of a combination of:

- threats to be countered by the TOE;
- the OSPs enforced by the TOE;
- the assumptions that are upheld for the TOE and its operational environment.

[SOURCE: ISO/IEC 15408-1:2009, 3.1.61]

#### 336

### TOE security functionality https://standards.iteh.ai)

TSF

combined functionality of all hardware, software and firmware of a TOE (3.3.4) that must be relied upon for the correct enforcement of the SFRs (3.3.7)

[SOURCE: ISO/IEC 15408-1:2009, 3.1.74]

3.3.7ps://standards.iteh.ai/catalog/standards/iso/d5dfc4ed-e810-4514-b25e-33c3878b2eb2/iso-23195-2021

#### security functional requirement

#### **SFR**

requirement defining the rule by which the TOE (3.3.4) governs access to and use of its resources, and thus information and services controlled by the TOE

#### 3.3.8

#### trusted channel

means by which a TSF (3.3.6) and another trusted IT product can communicate with necessary confidence

[SOURCE: ISO/IEC 15408-1:2009, 3.1.78]

#### 3.3.9

#### covert channel

enforced, illicit signalling channel that allows a user to surreptitiously contravene the multi-level separation policy and unobservability requirements of the TOE (3.3.4)

[SOURCE: ISO/IEC 15408-1:2009, 3.5.1]

#### 3.3.10

#### trusted path

means by which a user and a TSF (3.3.6) can communicate with the necessary confidence

[SOURCE: ISO/IEC 15408-1:2009, 3.1.80]