ISO 23195:2021 (E)

Security objectives of information systems of third-party payment services

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 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
4.2.2.1 General
4.2.2.2 TPP business configuration data
4.2.2.3 TPP business cumulative data
4.2.2.4 TPP transaction input data
4.2.2.5 TPP transmitting data
4.2.2.6 Authentication data provided by ASPSP
4.2.3 TPPSP's TSF data
4.2.3.1 General
4.2.3.2 TPPSP's TSF protected data
4.2.3.3 TPPSP's TSF confidential data

5 Security problem definition

5.1 General
5.2 Threats
5.2.1 Threats to business configuration data
5.2.1.1 Unauthorized disclosure
5.2.1.2 Unauthorized changes
5.2.2 Threats to business cumulative data
5.2.2.1 Unauthorized disclosure
5.2.2.2 Unauthorized changes
5.2.3 Threats to transaction input data
5.2.3.1 Counterfeiting
5.2.3.2 Repudiation
5.2.3.3 Unauthorized changes
5.2.4 Threats to TPP transmitting data
5.2.4.1 Counterfeiting
5.2.4.2 Repudiation
5.2.4.3 Unauthorized changes
5.2.5 Threats to authentication data provided by ASPSP
5.2.5.1 Unauthorized disclosure
5.2.5.2 Unauthorized utilization
5.2.6 Threats to TPPSP's TSF data
5.2.6.1 Threats to TPPSP's TSF protected data
5.2.6.1.1 Counterfeiting

5.2.6.1.2 Unauthorized changes
5.2.6.2 Threats to TPPSP's TSF confidential data
5.2.6.2.1 Counterfeiting
5.2.6.2.2 Unauthorized disclosure
5.2.6.2.3 Unauthorized changes
5.3 Organizational security policies
5.3.1 Operation authorization
5.3.1.1 Systemic operations on TPP payment credential carriers
5.3.1.2 Operations on TPP payment terminals
5.3.1.3 Operations on the TPPSP gatekeeper and TPP-BIS
5.3.1.4 Operations on the TPP-AIS
5.3.2 Security event audit
5.3.2.1 Security event audit of payment credential carriers
5.3.2.2 Security event audit of payment terminals
5.3.2.3 Security event audit of TPPSP gatekeeper and TPP-BIS
5.3.2.4 Security event audit of TPP-AIS
5.3.3 Connection security control
5.3.3.1 Connection security control between TPP credential carrier and TPP payment terminal
5.3.3.2 Connection security control between TPP payment terminal and TPPSP gatekeeper
5.3.4 Business management control
5.3.4.1 Business management control of payment terminal
5.3.4.2 Business management control of TPPSP gatekeeper and TPP-BIS
5.3.4.3 Business management control of TPP-AIS
5.3.5 Systems management control
5.3.5.1 System management control of payment terminal
5.3.5.2 System management control of TPPSP gatekeeper and TPP-BIS
5.3.5.3 System management control of TPP-AIS
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

A.1 General
A.2 Scenario 1: paying for goods using a personal computer via TPP
A.3 Scenario 2: paying for dinner using a mobile phone via TPP
A.4 Scenario 3: to go Dutch via TPP on mobile device
A.4.1 General
A.4.2 Phase 1: the payee initiates the payment collection
A.4.3 Phase 2: the TPP-BIS performs the payment collection
A.4.4 Phase 3: the TPP-BIS notices the payee
A.5 Substantial elements affecting transaction information flow
A.5.1 General
A.5.2 Suitable payer
A.5.3 Suitable payee
A.5.4 Types of payment accounts
A.5.5 Types of payment currencies
A.5.6 Types of payment credentials
A.5.7 Types of payment credential carriers
A.5.8 Types of places of payment
A.5.9 Types of payment modes
A.5.10 Types of trading results

A.5.11 Types of account features
A.5.12 Types of fund assurance methods
A.5.13 Types of funds interest calculation methods
A.5.14 Types of multi-accounts linkage modes
A.5.15 Types of service charge
A.5.16 Payment contract period
A.5.17 Payment service channels
A.5.18 Payment service area

Page count: 0