

ISO 5201:2024-04 (E)

Financial services - Code-scanning payment security

Contents

Page

- Foreword..... v
- Introduction..... vi
- 1 Scope..... 1
- 2 Normative references..... 1
- 3 Terms and definitions..... 1
- 4 Abbreviated terms..... 4
- 5 Overview of code-scanning payment..... 4
 - 5.1 Basic framework of code-scanning payment..... 4
 - 5.2 Mandatory steps and implementation modes of code-scanning payment..... 6
 - 5.2.1 Mandatory steps..... 6
 - 5.2.2 Payer-presented mode..... 6
 - 5.2.3 Payee-presented mode..... 6
- 6 Security target objectives and assumptions..... 7
- 7 Risk assessment of code-scanning payment..... 7
 - 7.1 General..... 7
 - 7.2 Common risks to both modes as defined in [Clause 5](#)..... 7
 - 7.2.1 Com_Risk_1: unauthorized user..... 7
 - 7.2.2 Com_Risk_2: illegitimate code content..... 8
 - 7.2.3 Com_Risk_3: tampered code image..... 8
 - 7.2.4 Com_Risk_4: insecure message transmission..... 8
 - 7.2.5 Com_Risk_5: payer sensitive information leakage..... 8
 - 7.2.6 Com_Risk_6: payee sensitive information leakage..... 8
 - 7.2.7 Com_Risk_7: routing conflict..... 8
 - 7.3 Risk assessment of payer-presented mode..... 8
 - 7.3.1 PrP_Risk_1: stolen code value..... 8
 - 7.3.2 PrP_Risk_2: stolen code-generation parameters..... 9
 - 7.3.3 PrP_Risk_3: breached encoding and decoding processes..... 9
 - 7.3.4 PrP_Risk_4: captured code image..... 9
 - 7.3.5 PrP_Risk_5: tempered transaction parameters..... 9
 - 7.4 Risk assessment of payee-presented mode..... 9
 - 7.4.1 PeP_Risk_1: code abuse..... 9
 - 7.4.2 PeP_Risk_2: sensitive information in clear..... 9
 - 7.4.3 PeP_Risk_3: unintentional repeated payments..... 9
 - 7.4.4 PeP_Risk_4: attack on decoding process..... 9
 - 7.4.5 PeP_Risk_5: forged payment notification..... 10
- 8 Security measures to mitigate the risks in [Clause 7](#)..... 10
 - 8.1 General..... 10
 - 8.2 Security measures to mitigate the risks in [7.2](#)..... 10
 - 8.2.1 Com_Measure_1: risk communication..... 10
 - 8.2.2 Com_Measure_2: payment application security..... 10
 - 8.2.3 Com_Measure_3: payer authentication..... 11
 - 8.2.4 Com_Measure_4: security protocols..... 11
 - 8.2.5 Com_Measure_5: anti cyber attacks..... 11
 - 8.2.6 Com_Measure_6: risk control..... 11
 - 8.2.7 Com_Measure_7: server-side sensitive information protection..... 12
 - 8.2.8 Com_Measure_8: avoid mis-routing..... 12
 - 8.2.9 Com_Measure_9: protect printed code images..... 12
 - 8.2.10 Com_Measure_10: reject illegitimate payment code..... 12

8.2.11	Com_Measure_11: unique transaction ID	13
8.2.12	Com_Measure_12: payment result notification	13
8.3	Additional security measures to mitigate the risks in 7.2 and 7.3	13
8.3.1	PrP_Measure_1: code content	13
8.3.2	PrP_Measure_2: code generation and resolution requests	13
8.3.3	PrP_Measure_3: encoding and decoding processes	13
8.3.4	PrP_Measure_4: pre-generated code	14
8.3.5	PrP_Measure_5: prefetched code storage	14
8.3.6	PrP_Measure_6: prefetched code TTL	14
8.3.7	PrP_Measure_7: secure code presentation	14
8.3.8	PrP_Measure_8: payee side sensitive information protection	15
8.3.9	PrP_Measure_9: payee side tamper-proofing	15
8.3.10	PrP_Measure_10: anti-replay	15
8.4	Additional security measures to mitigate the risks in 7.2 and 7.4	15
8.4.1	PeP_Measure_1: code data set	15
8.4.2	PeP_Measure_2: encryption in the code	16
8.4.3	PeP_Measure_3: code presentation	16
8.4.4	PeP_Measure_4: CSP data set	16
8.4.5	PeP_Measure_5: dynamic code	16
8.4.6	PeP_Measure_6: payer side sensitive information protection	16
8.4.7	PeP_Measure_7: payer verification	16
8.4.8	PeP_Measure_8: avoid repeated payments	16
8.4.9	PeP_Measure_9: payee code management	17
Annex A (informative) Implementation modes of code-scanning payment		18
Annex B (informative) Case study to support the risk assessment		27
Annex C (normative) Requirements on cryptography		29
Bibliography		30