



OESTERREICHISCHE NATIONALBANK
HAUPTABTEILUNG ANALYSE UND REVISION

Oesterreichische Nationalbank
- Zahlungssystemaufsicht -

Leitfaden

zur Erteilung von Auskünften gemäß § 44a Abs. 7 NBG

über die

zur Gewährleistung der Systemsicherheit getroffenen Maßnahmen

Multilaterale Kleinbetragszahlungssysteme

1	EINLEITUNG	3
2	AUSKÜNFTE	4
	Teil I: Systemkonzept.....	4
	Teil II: Spezifische Fragestellungen	7
	ANHANG: INFORMATIONEN AN TEILNEHMER UND ENDKUNDEN	11

1 Einleitung

Der vorliegende Leitfaden beinhaltet die Mindestanforderungen für die gemäß § 44a Abs. 7 NBG von den Betreibern multilateraler Kleinbetragszahlungssysteme zu erteilenden Auskünfte über die zur Gewährleistung der rechtlichen, finanziellen, organisatorischen und technischen Systemsicherheit des Zahlungssystems getroffenen Maßnahmen.

Die Auskünfte gelten als vollständig erteilt, wenn

- ein Systemkonzept gemäß Kapitel 2 (Teil I.) vorgelegt wird,
- zu den in Kapitel 2 (Teil II.) aufgelisteten spezifischen Fragestellungen einzeln und begründet schriftlich Stellung genommen wird. Für das System nicht zutreffende Fragestellungen sind explizit als „nicht zutreffend“ zu bezeichnen. Die Stellungnahme ist zumindest mit folgenden Dokumenten zu unterlegen:
 - Geschäftsbedingungen
 - Informationen an Teilnehmer und an Endkunden (siehe Anhang).

Auf von externen Unternehmen im Auftrag des Zahlungssystembetreibers erbrachte und für den sicheren Systembetrieb relevante Dienstleistungen ist explizit hinzuweisen. Die in diesem Zusammenhang an externe Unternehmen gerichteten Vorgaben bzw. sonstige zwischen dem Zahlungssystembetreiber und externen Unternehmen bestehende Vereinbarungen sind vollständig zu übermitteln.

Systemspezifische Abkürzungen und Sachbegriffe sind bei der ersten Verwendung in allgemeinverständlicher Form zu erläutern.

Alle Dokumente sind nach Möglichkeit in elektronischer Form zu übermitteln.

2 Auskünfte

Teil I Systemkonzept

Die Darstellung des Systemkonzeptes soll nach folgender Systematik erfolgen:

1. Allgemeine Übersicht

1.1. Systemdarstellung

- 1.1.1. graphische Übersicht über alle am System beteiligten Stellen (Betreiber und externe Dienstleister, Teilnehmer, Points of Sale, Endkunden)
- 1.1.2. Beschreibung der Rollen und Verantwortlichkeiten aller am System beteiligten Stellen

1.2. Systemfunktionen

- 1.2.1. Transaktionen
 - Transaktionsablauf (anhand eines zeitunterlegten Ablaufdiagramms)
 - Transaktionsdaten (übertragene und gespeicherte Daten)
- 1.2.2. Settlement (anhand eines zeitunterlegten Ablaufdiagramms)
- 1.2.3. Limitprüfungsverfahren
- 1.2.4. Systeminterne Funktionen (insbesondere Sperre, Protokollierung, Auswertung)

1.3. Netzwerktechnische Systemtopologie

- zentrale Komponenten (insbesondere Server mit relevanten Applikationen und Datenbanken)
- dezentrale Komponenten (insbesondere Terminals, andere Endgeräte)
- Kommunikationsverbindungen (insbesondere Netzwerke, Firewalls, VPN-Komponenten)

2. Sicherheitskonzept

2.1. Allgemeine Sicherheitsziele des Systems

2.2. Maßnahmen zur Erreichung der Sicherheitsziele seitens des Betreibers

- 2.2.1. Organisatorische Maßnahmen
 - Sicherheitsorganisation und Revision, Verantwortlichkeiten (insbesondere Rollenverteilung, Berechtigungsvergabe)
 - organisatorische und infrastrukturelle Maßnahmen für die Sicherheit der internen Einsatzumgebung (insbesondere physikalischer Schutz, Zutrittskontrolle, Vertrauenswürdigkeit und Kompetenz des Personals)
- 2.2.2. Sicherheitsanforderungen an die Einsatzumgebung im Feld (insbesondere Aufstellungsrichtlinien für Terminals, Hinweise für die sichere Benutzung)
- 2.2.3. IT-Sicherheitsmaßnahmen
 - Identifikation und Authentisierung (insbesondere der Endkunden, Teilnehmer, Operatoren, Administratoren)

- Autorisierung (insbesondere der Transaktionen)
 - Rechteverwaltung (für Benutzer)
 - Kryptokonzept (insbesondere Key-Management, Algorithmen, kryptographische Komponenten)
 - Systemintegrität (insbesondere Integritätssicherung von Komponenten und Daten z.B. durch Signieren, Prüfsummen, Tamper-Resistance)
 - Protokollierung (insbesondere von Transaktionsdaten und Änderungen an Zahlungssystemparametern und Komponenten)
- 2.2.4. Sicherheit in der Entwicklung, Produktion und Inbetriebnahme
- Konfigurationskontrolle
 - Sicherheit beim Entwickler (von Hard- und Software)
 - Sicherheit in der Produktion (v.a. der Hardware)
 - definierte Test-, Abnahme- und FreigabeprozEDUREN (für Hard- und Software)
 - Sicherheit bei Initialisierung und Personalisierung von Bezahlmedien, Zugangscodes und Sicherheitsmodulen
 - Installations- und Inbetriebnahmevorschriften (für Hard- und Software)
 - Vorschriften zur Außerbetriebnahme der Komponenten
- 2.2.5. Maßnahmen zur Gewährleistung eines einheitlichen Sicherheitsniveaus bei internationalem Einsatz

2.3. Maßnahmen zur Erreichung der Sicherheitsziele seitens der Teilnehmer

- geforderte Sicherheitsorganisation, Verantwortlichkeiten
- organisatorische und infrastrukturelle Sicherheitsmaßnahmen
- Monitoring der Teilnehmer durch den Betreiber
- Maßnahmen bei Regelverstößen

2.4. Auflagen an die Endkunden für den sicheren Umgang mit dem System

3. Business Continuity Planung (BCP)

3.1. Service Level

- 3.1.1. Angabe des Service Levels im Normalbetrieb
- Betriebs- und Cut-Off-Zeiten
 - Verfügbarkeit
 - Settlement und Zeitpunkt der Finalität von Zahlungen
 - durchschnittliche Dauer der einzelnen Transaktionsarten
- 3.1.2. Angabe des Service Levels in Fehler- und Katastrophensituationen
- mögliche Änderungen von Betriebszeiten
 - Verfügbarkeit
 - Notlaufmaßnahmen

3.2. Verantwortlichkeiten für die BCP

3.3. Datensicherungskonzept

- Zahlungssystemdaten
- Applikationen

- Betriebssystem, Disaster Recovery Backup
- Aufbewahrungszeiten

3.4. Notfallplanung und Notlauforganisation

- Notfallhandbuch (Inhalt, Speicherort)
- Unterweisung des Personals

3.5. Ausweichplanung

- Redundanz von Standorten und Komponenten (Hard- und Software).
- Redundanz und Übertragungskapazität der Kommunikationsverbindungen
- allfällige manuelle Umschaltprozeduren

3.6. Wiederanlaufplan

3.7. Ausfalltests und Übungen

3.8. Ersatzbeschaffungsplan

- Wartungsverträge
- Reservekomponenten

3.9. Aktualisierung der BCP

Teil II: Spezifische Fragestellungen

Zu folgenden Fragen ist einzeln und ausreichend begründet Stellung zu nehmen, wobei gegebenenfalls auch direkt auf entsprechende Ausführungen in übermittelten Unterlagen verwiesen werden kann.

Rechtliche Systemsicherheit

1. Auf welche Rechtsgrundlagen (gesetzliche und vertragliche) stützt sich das Zahlungssystem?
2. Welche Regelungen bestehen für die gerichtliche Zuständigkeit?
3. Welche Kriterien existieren für die Teilnahme am Zahlungssystem (bzw. für dessen Nutzung durch Endkunden) sowie für deren Beendigung auf Verlangen des Betreibers, eines Teilnehmers bzw. eines Endkunden? Auf welche Weise werden sie bekannt gemacht?
4. Auf welche Weise werden die Teilnehmer und Endkunden über die für sie jeweils relevanten Rechtsgrundlagen des Zahlungssystems in Kenntnis gesetzt?
5. An welcher Stelle sind die wesentlichen Rechte und Pflichten der Teilnehmer und Endkunden im Umgang mit dem Zahlungssystem – unter Berücksichtigung der jeweils relevanten gesetzlichen Rechtsgrundlagen – in den vertraglichen Rechtsgrundlagen des Systems abgebildet?
6. Welche Regelungen bestehen hinsichtlich der Haftung aller Beteiligten¹?
7. Auf welche Weise wird die Einhaltung der Bestimmungen des Datenschutzgesetzes sichergestellt?
8. Kommen andere Jurisdiktionen, insbesondere im Zusammenhang mit Teilnehmern und Endkunden, die nicht österreichischem Recht unterliegen, zur Anwendung? Auf welche Weise wird in diesen Fällen die Durchsetzbarkeit der für die Systemsicherheit relevanten Teile der vertraglichen Rechtsgrundlagen gegenüber Teilnehmern und Endkunden überprüft?
9. Auf welche Weise wird sichergestellt, dass die für die Systemsicherheit relevanten vertraglichen Rechtsgrundlagen laufend aktualisiert werden?

Finanzielle Systemsicherheit

1. Welche finanziellen Risiken können sich im Missbrauchsfall aus dem Systembetrieb, aus der Systemteilnahme oder aus der Systemnutzung ergeben? Welche Vorkehrungen werden getroffen, um dabei allen Beteiligten die Kenntnisnahme der sie im Missbrauchsfall betreffenden finanziellen Risiken zu ermöglichen?

¹ Betreiber, Teilnehmer und Endkunden.

2. Welche konkreten Vorkehrungen (z.B. Sperrmöglichkeit, Setzen von Limits, Haftungsbeschränkungen u.ä.) werden seitens des Betreibers getroffen, um den Teilnehmern die Absicherung der finanziellen Risiken zu ermöglichen?
3. Auf welche Weise werden die Verantwortlichkeiten für die Risikoabsicherung und -begrenzung geregelt? Welche Vorkehrungen werden im Rahmen des Risikomanagements getroffen, um allfällige Risiken abzusichern bzw. zu begrenzen? (Teilnahmebedingungen, Bonitätsprüfungen, Betrugsprävention)
4. Welche Regelungen bestehen für den Fall einer Insolvenz bzw. Zahlungsunfähigkeit eines Beteiligten? Sind Begrenzungen des maximalen finanziellen Risikos, das durch einzelne Teilnehmer für das Zahlungssystem entstehen kann, vorgesehen?
5. Wann und in welcher Regelmäßigkeit erfolgt das finale Settlement? Welche Aktiva werden für das Settlement eingesetzt?
6. Welche Vorkehrungen werden getroffen, damit das Zahlungssystem keinen Anreiz für kriminellen Missbrauch, wie z.B. Geldwäsche, bietet? Welche Limits sind für die Höhe der Einzeltransaktionen vorgesehen?

Organisatorische Systemsicherheit

1. Wie ist die Führungs- und Verwaltungsstruktur des Systems organisiert? Wie ist die interne Systemkontrolle organisiert (Qualitäts- und Sicherheitsmanagement, Organisation des Risikomanagements, Revision)?
2. Auf welche Weise wird die korrekte Umsetzung der ggf. an externe Unternehmen gerichteten bzw. von diesen unter Vertrag genommenen Vorgaben sichergestellt?
3. Welche Eskalationsmechanismen sind für den Fehler- und Katastrophenfall (insbesondere den Tagesabschluss betreffend) vorgesehen?
4. Auf welche Weise erfolgt die Zustellung von Komponenten an Teilnehmer bzw. von Bezahlmedien und Zugangscodes an Endkunden?
5. Welche Vorkehrungen werden getroffen, damit das Zahlungssystem keinen Anreiz für kriminellen Missbrauch bietet (wie insbesondere Fälschung von Bezahlmedien, Ausspähung von Daten)?
6. Wird im Falle des internationalen Einsatzes des Zahlungssystems hinsichtlich der organisatorischen und technischen Systemsicherheit in den betreffenden Ländern auf ein in Bezug auf das nationale Zahlungssystem adäquates Sicherheitsniveau geachtet? Existieren für diesen Zweck entsprechende Abnahme-/Freigabe- und Überprüfverfahren?
7. Welche Maßnahmen werden bezüglich der grenzüberschreitenden Systemkompatibilität gesetzt? Welche internationalen Standards kommen zur Anwendung?

Technische Systemsicherheit

Gewährleistung der Vertraulichkeit und Integrität

1. Welche Maßnahmen werden zur Gewährleistung der Vertraulichkeit und Integrität gesetzt? Wie und in welchen Intervallen werden diese dem jeweiligen Stand der Technik angeglichen?
2. Verwendet das System eigene Bezahlmedien? Wenn ja: Sind auf diesen Bezahlmedien neben den systemspezifischen Bezahlfunktionen auch andere Applikationen implementiert? Wenn ja: Welche? Durch welche Mechanismen erfolgt die logische und sicherheitstechnische Trennung der Zahlungssystemfunktionen von den anderen Applikationen?
3. Verwendet das Zahlungssystem Bezahlmedien oder Komponenten anderer Zahlungssysteme? Wenn ja: Welche Vorkehrungen werden getroffen, um sicherzustellen, dass diese Verwendung entsprechend der technischen Systemsicherheitsstandards der betroffenen Systeme erfolgt? Wie wird die sicherheitstechnische Trennung von Applikationen auf diesen Medien oder Komponenten verifiziert?
4. Welche Möglichkeiten haben Teilnehmer und Endkunden, die Authentizität und Integrität der von ihnen verwendeten Komponenten festzustellen?
5. Auf welche Weise erfolgt die Authentisierung der Endkunden?
6. Welche Verfahren sind im Kompromittierungsfall zur Sperre des Systemzugangs (insbesondere Sperre von Sicherheitsmodulen oder Bezahlmedien bzw. Sperre von Zugangscodes) vorgesehen?
7. Wie werden Transaktionsdaten vor unbefugten Zugriffen und Veränderungen geschützt (insbesondere bei deren Generierung, Übertragung, Speicherung und Archivierung)?
8. Welche Vorkehrungen werden getroffen, damit ein unbefugtes Wiedereinspielen von Transaktionsdaten vom System erkannt und verhindert wird?
9. Wie lange und an welchen Speicherorten/Medien werden Transaktionsdaten im Zahlungssystem gespeichert?
10. Auf welche Weise wird ein unbefugter Zugriff auf Zahlungssystemparameter (insbesondere auf Zugangscodes, Limits, relevante Kunden- und Teilnehmerdaten, kryptographische Schlüssel, Terminaldaten) erkannt bzw. werden Veränderungen verhindert?
11. Welche Vorkehrungen werden zur Erkennung bzw. Verhinderung von unbefugten Modifikationen an den Komponenten (Hard- und Software) des Zahlungssystems getroffen?
12. Auf welche Weise werden Änderungen an Zahlungssystemparametern und Komponenten protokolliert und wie lange und an welchen Speicherorten/Medien werden diese Protokolle aufbewahrt?

13. Auf welche Weise wird ein unbefugter Zugriff auf Änderungsprotokolle der Zahlungssystemparameter und Komponenten erkannt und wie werden Veränderungen verhindert?
14. Welche Auswertungen von Transaktionsdaten und Änderungsprotokollen ermöglichen ein Erkennen von Angriffen und damit die Einleitung entsprechender Gegenmaßnahmen? Sieht das System Einzeltransaktionsverfolgung, Schattenkonten oder andere Mechanismen vor?
15. Durch welche Maßnahmen wird ein unbefugter Zugriff auf die Auswertungen erkannt bzw. wie werden Veränderungen verhindert?
16. Wodurch wird die unbeobachtete Eingabe von Zugangscodes an den Eingabegeräten (z.B. an POS-Terminals oder ATMs) unterstützt?
17. Nach welchen Sicherheitsstandards erfolgen Initialisierung und Personalisierung insbesondere bei Bezahlmedien, Zugangscodes und Sicherheitsmodulen? Wird die Umsetzung und Einhaltung solcher Standards laufend überprüft?

Gewährleistung der Verfügbarkeit und Betriebssicherheit

18. Auf welche Weise wird die Verfügbarkeit der zentralen Autorisierungssysteme während der Betriebszeiten des Systems gewährleistet?
19. Auf welche Weise wird sichergestellt, dass die Sicherheitsfunktionen des Systems auch in Fällen von Betriebsstörungen oder Fehlbedienungen aufrecht bleiben?

Anhang: Informationen an Teilnehmer und Endkunden

Welche der folgenden Informationen werden in welcher Form an Teilnehmer und Endkunden gegeben? Es wird gebeten, die entsprechenden Musterdokumente beizulegen.

Informationen an Teilnehmer über

1. Den vom Betreiber garantierten Service Level des Systems sowohl im Normalbetrieb als auch in Fehler- und Katastrophensituationen
2. Ansprechpartner auf Seiten des Betreibers
3. IT-Risiken, die aus der Teilnahme am System für den Teilnehmer entstehen können
4. Haftung bei Missbrauch oder Fehlbedienung
5. Den sicheren Umgang mit dem System und das Verhalten in Ausnahmefällen

a) Installation und Administration

- Installation des Systems, geeignete Räumlichkeiten, erforderliche bauliche und infrastrukturelle Vorkehrungen
- Anforderungen hinsichtlich der Kommunikationsverbindungen
- Administration
- Wartung
- Verhalten des Administrators/Operators des Teilnehmers im Falle von Betriebsstörungen oder (tatsächlichen oder vermuteten) Angriffen auf das System

b) erforderliche organisatorische Sicherheitsmaßnahmen

- Nominierung von Verantwortlichen/Ansprechpartnern
- Berechtigungsvergabe
- Zeitpunkte und Umfang der Protokollierung, Auswertung von Protokollen, Aufbewahrungsfristen
- Key-Management (Erzeugung, Speicherung, Übertragung und Außerbetriebnahme kryptographischer Schlüssel)
- Umgang mit Sicherheitsmodulen

c) Benutzerdokumentation

- Bedienung des Systems im Normalbetrieb
- Verhalten des Benutzers im Falle von Betriebsstörungen oder (tatsächlichen oder vermuteten) Angriffen auf das System

Informationen an Endkunden über

- die sichere Handhabung der Bezahlmedien und Zugangscodes
- Limits und deren Gültigkeitszeitraum
- Pflichten, Haftung und Beeinspruchungsmöglichkeiten des Endkunden