



OESTERREICHISCHE NATIONALBANK
HAUPTABTEILUNG ANALYSE UND REVISION

Oesterreichische Nationalbank
- Zahlungssystemaufsicht -

Aufsichtsgrundsätze

für

elektronische Zahlungssysteme

Multilaterale Kleinbetragszahlungssysteme

INHALT

1	Einleitung	3
2	Begriffsbestimmungen	3
3	Anforderungen	6
4	Nachweise	9

1 Einleitung

Die vorliegenden Aufsichtsgrundsätze für multilaterale Kleinbetragszahlungssysteme beinhalten die von der OeNB für die Gewährleistung der Systemsicherheit als erforderlich erachteten Anforderungen und dienen als Evaluierungsmaßstab für die von den Betreibern von multilateralen Kleinbetragszahlungssystemen gemäß § 44a Abs. 7 NBG zu erteilenden Auskünfte.

2 Begriffsbestimmungen / Anwendungsbereich

2.1. Multilaterales Kleinbetragszahlungssystem:

Der Begriff „Zahlungssystem“ ist gemäß § 44a Abs. 4 NBG wie folgt definiert: „Zahlungssystem im Sinne dieses Bundesgesetzes ist jedes System gemäß § 2 des Finalitätsgesetzes, BGBl. I Nr. 123/1999, sowie jede gewerbliche Einrichtung mit mindestens drei Teilnehmern, die dem elektronischen Transfer von Geldwerten dient“.

§ 44a Abs. 4 NBG sieht somit zwei Fälle vor, in denen ein System als „Zahlungssystem“ zu qualifizieren ist:

Erstens, wenn ein System gemäß § 2 Finalitätsgesetz vorliegt.

Zweitens, wenn

- a) eine gewerbliche Einrichtung
- b) mit mindestens drei Teilnehmern¹
- c) dem elektronischen Transfer von Geldwerten dient.

Erforderlich ist jedenfalls, dass eine Mindestzahl von drei Teilnehmern an einer Zahlungsvereinbarung beteiligt ist. Zentrales Kriterium für die Qualifikation als Zahlungssystem ist somit die Abgrenzung zwischen bilateralen und multilateralen Zahlungsvereinbarungen.

Bilaterale Zahlungsvereinbarungen über den Datenaustausch zwischen zwei Banken und die damit verbundene Kontoführung (Giroverkehr) oder die zwischen einer Bank und ihren Kunden (keine Teilnehmer i.S. des § 44a Abs. 6 NBG) abgeschlossenen Vereinbarungen über ein spezielles Kommunikationssystem, welches diesen die Disposition auf ihren Konten (inklusive der über dieses Kommunikationssystem direkt an die Bank gerichteten Erteilung von im Giroverkehr durchzuführenden Überweisungsaufträgen) ermöglicht (Kontozugangssysteme), bilden kein Zahlungssystem und fallen daher nicht in den Anwendungsbereich der Zahlungssystemaufsicht.

¹ Zum Teilnehmerbegriff siehe 2.2.

Wird hingegen mit mindestens drei Teilnehmern eine Zahlungsvereinbarung geschlossen, die den elektronischen Transfer von nicht vorausbezahlten monetären Geldwerten², die hauptsächlich nicht von hohem Einzelwert sind, nach Autorisierung über spezielle Bezahlmedien oder Zugangscodes nach gleichen Regeln (i.d.R. auf der Grundlage einer Ermächtigung bzw. Beauftragung eines Zahlungssystembetreibers zur Belastung von Kundenkonten und Kreditierung von Händlerkonten, wobei die betroffenen Konten bei verschiedenen Banken geführt werden) zum Gegenstand hat, so liegt ein multilaterales Kleinbetragszahlungssystem vor, das der Zahlungssystemaufsicht unterliegt.

2.2. Teilnehmer:

Der Begriff „Teilnehmer“ ist gemäß § 44a Abs. 6 NBG wie folgt definiert: *„Teilnehmer an einem Zahlungssystem im Sinne dieses Bundesgesetzes ist, wer gewerblich tätig ist und mit dem Zweck der direkten oder indirekten Erzielung von Einnahmen am Transfer von Geldwerten innerhalb eines Zahlungssystems oder aus einem oder in ein Zahlungssystem mitwirkt.“*

Damit eine Person als Teilnehmer iS des § 44a Abs. 6 NBG qualifiziert werden kann, müssen drei Voraussetzungen erfüllt sein: Sie muss

- a) gewerblich tätig sein (Abgrenzung zu Privatpersonen),
- b) am Transfer von Geldwerten innerhalb eines Zahlungssystems oder aus einem oder in ein Zahlungssystem mitwirken (wobei für die Art bzw. Form der Mitwirkung keine besonderen Kriterien verlangt werden),
- c) mit der Mitwirkung am Geldtransfer einen bestimmten Zweck verfolgen, nämlich die unmittelbare oder mittelbare Erzielung von Einnahmen.

Der Teilnehmerbegriff des § 44a Abs. 6 NBG erfasst somit auch Unternehmer („Händler“), die an einem Zahlungssystem in der Weise mitwirken, dass sie mit dem Zweck der Erzielung von Einnahmen aus dem Vertrieb ihrer Waren die vom Betreiber des Zahlungssystems aufgestellte Regeln akzeptieren und bei diesem ein Konto führen (bzw. führen lassen), auf das die aus ihrer gewerblichen Tätigkeit eingehenden Zahlungen gutzuschreiben sind.

Der Endkunde (nicht notwendigerweise Konsument) ist demgegenüber nicht Teilnehmer, weil er das Zahlungssystem nicht zum Zweck der Einnahmenerzielung nutzt, sondern vielmehr unter Verwendung des Zahlungssystems an den Händler Zahlungen leistet.

Wie die Betreiber unterliegen auch die Teilnehmer an einem Zahlungssystem der Aufsicht nach § 44a NBG. Zur Auskunftserteilung nach § 44a Abs. 8 NBG werden jene Teilnehmer aufgefordert, die an systemrelevanten Zahlungssystemen in der Definition

² Zahlungssysteme mit Vorauszahlung (Prepaid-Systeme) fallen in die Kategorie „E-Geld-Systeme“.

der Core Principles for Systemically Important Payment Systems (SIPS)³ teilnehmen bzw. systemrelevante Funktionen⁴ ausüben⁵.

2.3. Bezahlmedium⁶:

Hardwareprodukt⁷, das den Endkunden gegenüber dem Zahlungssystem als Nutzungsberechtigten ausweist.

2.4. Zugangscode:

Eingebende Kennung, die den Endkunden (teilweise in Ergänzung zu einem Bezahlmedium) gegenüber dem Zahlungssystem als Nutzungsberechtigten ausweist⁸.

2.5. POS:

Point of Sale. Standort eines Händlers, an dem unter Verwendung des Zahlungssystems bezahlt werden kann⁹.

2.6. ATM:

Automated Teller Machine. Geldausgabeautomat, der gegen Bezahlung unter Verwendung des Zahlungssystems die Behebung von Bargeld ermöglicht¹⁰.

³ Kriterien für SIPS (zumindest eines der folgenden Merkmale): 1. Das ZS ist das einzige oder das in Bezug auf den Gesamtwert der Zahlungen wichtigste ZS eines Landes, 2. es verarbeitet hauptsächlich Zahlungen von hohem Einzelwert, 3. es wird für die Abwicklung von Finanzmarkttransaktionen oder für den Ausgleich anderer ZS benutzt (BIS 2001).

⁴ Dazu zählen üblicherweise nicht die der allgemeinen Datenübertragung dienenden Kommunikationsschienen (Postnetz, Internet, etc.), die gegebenenfalls auch von Zahlungssystembetreibern für die Erbringung der Zahlungsverkehrsdienstleistungen eingesetzt werden.

⁵ Vgl. Aufsichtsgrundsätze „Systemrelevante Teilnahme“.

⁶ Synonyme Bezeichnung: „Token“.

⁷ Heute üblicherweise über Bezahlkarten mit Hochprägung und Magnetstreifen oder Computerchips, zunehmend auch über Mitnutzung der SIM-Chipkarte von Mobiltelefonen.

⁸ Heute üblicherweise über Benutzername mit Passwort, PIN oder TAN.

⁹ Heute üblicherweise an einem Terminal mit Hilfe eines Bezahlmediums und eines Zugangscodes (z.B. PIN) oder mit Hilfe eines Bezahlmediums und der Unterschrift des Endkunden.

¹⁰ Heute üblicherweise mit Hilfe eines Bezahlmediums und eines Zugangscodes.

3 Anforderungen

Rechtliche Systemsicherheit

- (1) Der Betreiber soll die für das Zahlungssystem relevanten Rechtsnormen (gesetzliche und vertragliche Rechtsgrundlagen) kennen. Im jeweils relevanten Umfang sollen diese auch den Teilnehmern und Endkunden bekannt gemacht werden.
- (2) Die vertraglichen Rechtsgrundlagen des Systems sollen die für die Systemsicherheit relevanten Rechte und Pflichten der Teilnehmer und Endkunden im Umgang mit dem Zahlungssystem enthalten und gegenüber diesen rechtlich durchsetzbar sein.
- (3) Die Teilnahme am Zahlungssystem bzw. die Nutzung des Zahlungssystems soll auf objektiven Kriterien beruhen. Diese sollen explizit bekannt gemacht werden.
- (4) Es sollen klare Regeln und Vorgehensweisen für die geordnete Beendigung der Teilnahme bzw. der Nutzung auf Verlangen eines Teilnehmers bzw. eines Endkunden festgelegt sein.
- (5) Die gerichtliche Zuständigkeit soll möglichst eindeutig geklärt sein.
- (6) Die für die Systemsicherheit relevanten Teile der vertraglichen Rechtsgrundlagen sollen stets aktuell gehalten werden.

Finanzielle Systemsicherheit

- (1) Alle Beteiligten¹¹ sollen die sich aus dem Systembetrieb, aus der Systemteilnahme oder aus der Systemnutzung im Missbrauchsfall ergebenden finanziellen Risiken kennen. Den Teilnehmern und Endkunden soll dabei vom Betreiber die Kenntnisnahme der sie im Missbrauchsfall betreffenden finanziellen Risiken in leicht verständlicher Weise ermöglicht werden.
- (2) Vom Betreiber sollen Vorkehrungen getroffen werden, die den Teilnehmern die Absicherung der von ihnen zu tragenden finanziellen Risiken ermöglichen.
- (3) Es sollen Begrenzungen des maximalen finanziellen Risikos, das für das Zahlungssystem durch einzelne Teilnehmer verursacht werden kann, vorgesehen werden.
- (4) Die Geschäftsbedingungen des Zahlungssystems sollen klare Verantwortlichkeiten für die Risikoabsicherung und -begrenzung bei allen Beteiligten vorsehen.
- (5) Das finale Settlement soll möglichst rasch erfolgen. Die für das Settlement eingesetzten Aktiva sollen vorzugsweise in Form von Guthaben auf Konten der

¹¹ Betreiber, Teilnehmer und Endkunden.

OeNB vorliegen. Wenn dies nicht der Fall ist, soll sichergestellt werden, dass sie kein bzw. nur ein geringes Kredit- oder Liquiditätsrisiko bergen.

- (6) Design und Implementierung des Zahlungssystems sollen so gestaltet sein, dass kein Anreiz für einen kriminellen Missbrauch des Systems, wie etwa Geldwäsche, besteht. Es sollen geeignete Limits für die Höhe der Einzeltransaktionen sowie geeignete Protokollierungs- und Auswertungssysteme vorgesehen sein.

Organisatorische Systemsicherheit

- (1) Das Zahlungssystem soll über eine transparente, nachvollziehbare und effiziente Führungs- und Verwaltungsstruktur verfügen.
- (2) Das Zahlungssystem soll über eine transparente und wirksame interne Systemkontrolle durch den Betreiber verfügen.
- (3) Es sollen Eskalationsmechanismen für den Fehler- und Katastrophenfall vorgesehen sein, die insbesondere der rechtzeitigen Beendigung des Tagesabschlusses dienen.
- (4) Es sollen sichere Zustellverfahren für die Komponenten an die Teilnehmer bzw. für die Bezahlmedien oder Zugangscodes an die Endkunden gewählt werden.
- (5) Design und Implementierung des Zahlungssystems sollen so gestaltet sein, dass kein Anreiz für einen kriminellen Missbrauch des Systems, wie etwa Fälschung von Bezahlmedien oder Ausspähung von Daten, besteht.
- (6) Wird das Zahlungssystem international eingesetzt, so sollen die Sicherheitsniveaus in den betroffenen Ländern denen des nationalen Zahlungssystems in Bezug auf die organisatorische und technische Sicherheit adäquat sein. Dazu sollen entsprechende Abnahme-/Freigabe- und Überprüfverfahren existieren.
- (7) Es sollen internationale Standards zum Einsatz kommen, die die Durchführung grenzüberschreitender Transaktionen bzw. die grenzüberschreitende Systemkompatibilität unterstützen.

Technische Systemsicherheit

Gewährleistung der Vertraulichkeit und Integrität

- (1) Zur Gewährleistung der Vertraulichkeit und Integrität des Zahlungssystems sollen vom Betreiber etablierte, dem jeweiligen Stand der Technik entsprechende Sicherheitsmaßnahmen gesetzt werden.
- (2) Ist das Bezahlmedium gemeinsam mit anderen Applikationen auf einer Multiapplikationskarte implementiert, so soll eine strenge logische und

sicherheitstechnische Trennung von den anderen Applikationen vorgenommen werden.

- (3) Die Authentizität und Integrität der von Teilnehmern und Endkunden verwendeten Komponenten soll für diese nachprüfbar sein.
- (4) Das Zahlungssystem soll die korrekte Authentisierung der Endkunden sicherstellen.
- (5) Das Zahlungssystem soll im Kompromittierungsfall effektiv wirksame Verfahren zur Sperre des Systemzugangs (Sperre der Sicherheitsmodule des Teilnehmerzugangs, des Bezahlmediums oder des Zugangscodes) vorsehen.
- (6) Transaktionsdaten sollen im Zahlungssystem nach folgenden Regeln gespeichert werden:
 - Ein unbefugter Zugriff auf die Transaktionsdaten soll vom System erkannt und Veränderungen sollen verhindert werden.
 - Ein unbefugtes Wiedereinspielen von Transaktionsdaten soll vom System erkannt und verhindert werden.
 - Für die Transaktionsdaten sollen Aufbewahrungsfristen festgelegt werden, so dass Auswertungen nach AG (9) möglich sind.
- (7) Parameter des Zahlungssystems sollen nach folgenden Regeln gespeichert werden:
 - Ein unbefugter Zugriff auf Parameter soll vom System erkannt und Veränderungen sollen verhindert werden.
 - Veränderungen der Parameter sollen protokolliert werden.
 - Ein unbefugter Zugriff auf die Änderungsprotokolle soll vom System erkannt und Veränderungen sollen verhindert werden.
 - Für die Protokolle sollen Aufbewahrungsfristen festgelegt werden, so dass Auswertungen nach AG (9) möglich sind.
- (8) Komponenten (Hard und Software) des Zahlungssystems sollen wie folgt beschaffen sein:
 - Komponenten sollen gegen unbefugte Veränderungen geschützt sein.
 - Veränderungen an den Komponenten sollen protokolliert werden.
 - Ein unbefugter Zugriff auf die Änderungsprotokolle soll vom System erkannt und Veränderungen sollen verhindert werden.
 - Für die Protokolle sollen Aufbewahrungsfristen festgelegt werden, so dass Auswertungen nach AG (9) möglich sind.
- (9) Das Zahlungssystem soll Auswertungen von Transaktionsdaten und Änderungsprotokollen in einer Weise ermöglichen, dass eine Erkennung von Angriffen und damit die Einleitung entsprechender Gegenmaßnahmen möglich ist (z.B. Einzeltransaktionsverfolgung, Schattenkonten oder andere Mechanismen). Unbefugte Zugriffe auf solche Auswertungen sollen vom System erkannt und Veränderungen sollen verhindert werden.

- (10) Geräte zur Eingabe von Zugangscodes (z.B. an POS-Terminals oder ATMs) sollen derart gestaltet und aufgestellt sein, dass eine unbeobachtete Eingabe des Codes möglich ist.
- (11) Es soll sichergestellt sein, dass Initialisierung und Personalisierung insbesondere bei Bezahlmedien, Zugangscodes und Sicherheitsmodulen nach einheitlich hohen Sicherheitsstandards erfolgen. Die Umsetzung und Einhaltung solcher Standards soll laufend überprüft werden.
- (12) Wenn das Zahlungssystem Bezahlmedien und Komponenten anderer Zahlungssysteme benutzt, soll sichergestellt sein, dass dies in rechtlich zulässiger Weise sowie entsprechend der technischen Systemsicherheitsstandards der betroffenen Systeme erfolgt.

Gewährleistung der Verfügbarkeit und Betriebssicherheit

- (13) Zur Gewährleistung der Verfügbarkeit und Betriebssicherheit des Systems sollen etablierte, dem jeweiligen Stand der Technik entsprechende Maßnahmen gesetzt werden. Insbesondere soll die Verfügbarkeit der zentralen Autorisierungssysteme während der Betriebszeiten des Zahlungssystems gewährleistet sein.
- (14) Die Sicherheitsfunktionen des Systems sollen auch in Fällen von Betriebsstörungen oder Fehlbedienungen aufrecht bleiben.

4 Nachweise

Die Erfüllung der Anforderungen ist auf Verlangen der OeNB an Hand des „Leitfadens zur Erteilung von Auskünften gemäß § 44a Abs. 7 NBG über die zur Gewährleistung der Systemsicherheit getroffenen Maßnahmen – Multilaterale Kleinbetragszahlungssysteme“ binnen der im Aufforderungsschreiben genannten Frist nachzuweisen.

Die Nachweise sind bei wesentlichen Systemänderungen in aktualisierter Form vorzulegen.