



OESTERREICHISCHE NATIONALBANK  
HAUPTABTEILUNG ANALYSE UND REVISION

**Oesterreichische Nationalbank**  
- Zahlungssystemaufsicht -

**Leitfaden**

zur Erteilung von Auskünften gemäß § 44a Abs. 8 NBG

über die

zur sicheren Teilnahme getroffenen Vorkehrungen

**Systemrelevante Teilnahme**

## **INHALT**

1	Einleitung	3
2	Auskünfte	3
	Anhang 1: Mindestinhalt Teilnehmerpolicy	5

# 1 Einleitung

Der vorliegende Leitfaden beinhaltet die Mindestanforderungen für die von Teilnehmern an systemrelevanten Zahlungssystemen (gem. Core Principles for Systemically Important Payment Systems - SIPS)<sup>1</sup> bzw. von Teilnehmern, die systemrelevante Funktionen<sup>2</sup> ausüben, gemäß § 44a Abs. 8 NBG zu erteilenden Auskünfte über die zur sicheren Teilnahme getroffenen Vorkehrungen.

Die Auskünfte gelten als vollständig erteilt, wenn

- zu den in Kapitel 2 aufgelisteten Fragen einzeln schriftlich Stellung genommen wird und
- diese Stellungnahmen mit der in Kapitel 2 geforderten Dokumentation unterlegt werden.

# 2 Auskünfte

Zu folgenden Fragen ist einzeln und begründet Stellung zu nehmen:

## Rechtliche Sicherheit der Systemteilnahme

1. Auf welche Rechtsgrundlagen stützt sich das Zahlungssystem? Ist sichergestellt, dass die Geschäftsbedingungen jederzeit in aktualisierter Form bekannt sind?
2. Welche Regelungen bestehen für die gerichtliche Zuständigkeit?

## Finanzielle Sicherheit der Systemteilnahme

3. Auf welche Weise wird sichergestellt, dass mit der Teilnahme allenfalls verbundene Kredit- und Liquiditätsrisiken jederzeit bekannt sind und entsprechend bemessen werden?
4. In welcher Weise kann eine Heranziehung für Verbindlichkeiten eines anderen Teilnehmers bzw. für Verlustteilungsverfahren erfolgen?
5. Welche Vorkehrungen werden getroffen, damit die aus der Systemteilnahme gegebenenfalls resultierenden finanziellen Risiken abgesichert werden können?

---

<sup>1</sup> 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).

<sup>2</sup> 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.

6. Zu welchem Zeitpunkt und in welcher Form erfolgt das finale Settlement ?
7. Unter welchen Voraussetzungen kann ein Widerruf von Zahlungen erfolgen ?

## **Organisatorische und technische Sicherheit der Systemteilnahme**

8. Auf welche Weise wird sichergestellt, dass die vom Betreiber bekannt gegebenen Richtlinien für den Umgang mit dem System eingehalten werden ?
9. Auf welche Weise wird sichergestellt, dass ausreichend ausgebildetes und vertrauenswürdige Personal für eine sichere und effiziente Teilnahme am Zahlungssystem sowohl im Normalbetrieb als auch in Ausnahmesituationen zur Verfügung steht?
10. Auf welche Weise wird sichergestellt, dass alle berechtigten Mitarbeiter (Benutzer des Zahlungssystems) über das richtige Verhalten auch in Fehler- und Katastrophenfällen informiert und geschult sind ?
11. Auf welche Weise wird sichergestellt, dass alle Hardware- und Softwarekomponenten des Zahlungssystems, insbesondere auch kryptographische Komponenten, gemäß den technischen und organisatorischen Vorgaben des Betreibers installiert und betrieben werden ?
12. Wird die Einhaltung der vom Betreiber vorgeschriebenen Sicherheitsmaßnahmen einem laufenden Monitoring unterzogen ?

Die Stellungnahmen sind zumindest mit folgenden Dokumenten (nach Möglichkeit in elektronischer Form) zu unterlegen:

- den die Systemteilnahme konstituierenden Rechtsgrundlagen,
- einer schriftlichen Darstellung des Umgangs mit potentiell aus der Systemteilnahme entstehenden finanziellen, technischen und organisatorischen Risiken bzw. der diesbezüglich getroffenen Sicherheitsvorkehrungen ("Teilnehmerpolicy", Mindestinhalt s. Anhang A.1).

Die in den Stellungnahmen gegebenen Auskünfte können in Form von eindeutigen Bezugnahmen auf die Dokumente erfolgen.

Systemspezifische Abkürzungen und Sachbegriffe sind gesondert zu erläutern.

Zum Nachweis der organisatorischen und technischen Systemsicherheit sind auf Anforderung der OeNB Gutachten von zertifizierten Prüfinstituten hinsichtlich der Erfüllung behaupteter Sicherheitsniveaus für die systemsicherheitsrelevanten Komponenten und Verfahren vorzulegen.

## **Anhang 1: Mindestinhalt der Teilnehmerpolicy**

### **1. Finanzielle Risiken**

- 1.1 Darstellung der sich aus der Systemteilnahme potenziell ergebenden finanziellen Risiken
- 1.2 Darstellung der zur Absicherung dieser Risiken getroffenen Maßnahmen

### **2. Organisatorische/technische Risiken**

- 2.1 Darstellung der sich aus der Systemteilnahme potenziell ergebenden organisatorischen/technischen Risiken
- 2.2 Darstellung der vom Betreiber vorgegebenen Sicherheitsmaßnahmen
- 2.1 Darstellung der vom Teilnehmer getroffenen Sicherheitsmaßnahmen
  - 2.1.1 Benennung von Verantwortlichen
  - 2.1.2 Berechtigungssystem
  - 2.1.3 Zeitpunkte und Umfang der Protokollierung, Auswertung von Protokollen, Aufbewahrungsfristen
  - 2.1.4 Key-Management (Erzeugung, Speicherung, Übertragung und Ausserbetriebnahme kryptographischer Schlüssel)
  - 2.1.5 Umgang mit Sicherheitsmodulen (Einschubboards, Chipkarten, etc.)
- 2.2 Aufstellung von Systemkomponenten (falls relevant)
  - 2.2.1 Erfüllung baulicher und infrastruktureller Vorkehrungen
  - 2.2.2 Erfüllung der Anforderungen hinsichtlich der Kommunikationsverbindungen

Die Beschreibungen der funktionalen, topologischen und transaktionsablaufbezogenen Zusammenhänge sind mit grafischen Übersichten zu verdeutlichen.