



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**

Teil 2

Betrieb von Infrastruktureinrichtungen  
für Zahlungssysteme

# 1 Einleitung

Der vorliegende Leitfaden beinhaltet die Mindestanforderungen für die von Betreibern von Infrastruktureinrichtungen für Zahlungssysteme (Infrastrukturbetreiber) gemäß § 44a Abs. 8 NBG zu erteilenden Auskünfte.

Die Auskünfte gelten als vollständig erteilt, wenn

- ein Betriebskonzept gemäß Kapitel 2 (Teil I.) vorgelegt wird,
- zu den in Kapitel 2 (Teil II.) aufgelisteten spezifischen Fragestellungen einzeln und begründet schriftlich Stellung genommen wird. Der Stellungnahme sind die aktuellen Geschäftsbedingungen beizulegen. Die auf die Infrastruktureinrichtung nicht zutreffenden Fragestellungen sind explizit als „*nicht zutreffend*“ zu bezeichnen.

Auf von externen Unternehmen im Auftrag des Infrastrukturbetreibers erbrachte und für den sicheren Betrieb der Infrastruktur relevante Dienstleistungen ist in den betreffenden Teilbereichen der Stellungnahme explizit hinzuweisen. Die in diesem Zusammenhang an externe Unternehmen gerichteten Vorgaben bzw. sonstigen Vereinbarungen (beispielsweise Service Level Agreements, Spezifikationen, etc.) sind vollständig zu übermitteln.

Alle Dokumente sind nach Möglichkeit in elektronischer Form zu übermitteln.

## 2 Auskünfte

### Teil I Betriebskonzept

Die Darstellung des Betriebskonzeptes soll nach folgender Gliederung erfolgen:

#### 1. Allgemeine Übersicht

##### 1.1. Gesamtübersicht

- 1.1.1. Angabe der Zahlungssysteme, für die Infrastruktureinrichtungen betrieben werden (bzw. für die Dienstleistungen erbracht werden)
- 1.1.2. graphische Gesamtübersicht über die Infrastruktureinrichtung und ihre Funktionen für die Zahlungssysteme (inklusive aller beteiligten Unternehmen und sonstigen Einrichtungen),

##### 1.2. Netzwerktechnische Darstellung der Infrastruktureinrichtung (Topologie)<sup>1</sup>

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

##### 1.3. Infrastruktureinrichtungen und Dienstleistungen (einzeln für jedes servierte Zahlungssystem)

- 1.3.1. bereitgestellte Infrastruktur (insbesondere Hard- und Software, Kommunikationsverbindungen, Firewalls, Terminals, Zahlungsmedien, Server, Datenbanken, Call Center Dienste)
- 1.3.2. Transaktionsablauf (sofern überwiegend in der Zuständigkeit des Infrastrukturbetreibers)
- 1.3.3. transaktionsbezogene Funktionen (insbesondere Identifikation, Autorisierung, Limitprüfung, Sammeln und Weiterleiten von Transaktionen, Generierung von Überweisungsdatenträgern)
- 1.3.4. weitere Funktionen (insbesondere Sperre, Protokollierung, Auswertung)
- 1.3.5. Schnittstellen (insbesondere zum Zahlungssystem, zu anderen Teilnehmern, zu Kunden)

##### 1.4. Mehrere Zahlungssysteme übergreifende Funktionen

- 1.4.1. Add-On Dienste<sup>2</sup>
- 1.4.2. Protokollierung, Auswertung, Monitoring der für Add-On Dienste verwendeten Infrastruktureinrichtungen
- 1.4.3. Schnittstellen der Add-On Dienste (insbesondere zu Zahlungssystemen, anderen Teilnehmern, Kunden)

---

<sup>1</sup> Aus der Darstellung soll die Zuordnung der Komponenten des Infrastrukturproviders zu den einzelnen Zahlungssystemen ersichtlich sein.

<sup>2</sup> Dienste, die Zahlungssysteme integrieren, benutzen oder erweitern (z.B. Integration mehrerer Zahlungssysteme in einem Online Shop).

## 2. Sicherheitsziele

## 3. Maßnahmen zur Erreichung der Sicherheitsziele

### 3.1. Organisatorische Maßnahmen

- 3.1.1. Sicherheitsorganisation und Revision, Verantwortlichkeiten (insbesondere Rollenverteilung, Berechtigungsvergabe, Genehmigung durch die Geschäftsleitung)
- 3.1.2. organisatorische und infrastrukturelle Maßnahmen für die Sicherheit der internen Einsatzumgebung (insbesondere physikalischer Schutz, Zutrittskontrolle, Vertrauenswürdigkeit, Eignung des Personals)

### 3.2. IT-Sicherheitsmaßnahmen

- 3.2.1. Identifikation, Authentisierung und Rechteverwaltung (insbesondere von Operatoren, Administratoren und Benutzern)
- 3.2.2. Sicherheit der bereitgestellten Kommunikationsverbindungen
- 3.2.3. Kryptokonzept der Infrastruktur (insbesondere Key-Management, Algorithmen, kryptographische Komponenten)
- 3.2.4. Systemintegrität (insbesondere Integritätssicherung von Komponenten und Daten)
- 3.2.5. Einrichtungen zur Erkennung und Abwehr von Angriffen

### 3.3. Sicherheit in der Entwicklung, Produktion und Inbetriebnahme (von Hard- und Software)

- 3.3.1. Konfigurationskontrolle
- 3.3.2. Sicherheit in der Entwicklung
- 3.3.3. Sicherheit in der Produktion
- 3.3.4. definierte Test-, Abnahme- und FreigabeprozEDUREN
- 3.3.5. Installations- und Inbetriebnahmevorschriften
- 3.3.6. Vorschriften zur Außerbetriebnahme der Komponenten

## 4. Business Continuity Planung (BCP)

### 4.1. Strategie und Service Level

- 4.1.1. Ziele
- 4.1.2. Service Level im Normalbetrieb
  - Betriebs- und Cut-Off-Zeiten, Verfügbarkeit
- 4.1.3. Service Level in Fehler- und Katastrophensituationen
  - mögliche Änderungen von Betriebszeiten, Verfügbarkeit, Notlaufmaßnahmen

### 4.2. Verantwortlichkeiten für die BCP

- Rollenverteilung
- Genehmigung durch die Geschäftsleitung

### 4.3. Risikoanalyse

- Identifikation kritischer Geschäftsprozesse

### 4.4. Notfallplanung und Notlauforganisation

Notfallshandbuch (Inhalt, Speicherort, Szenarien, kritische Prozesse)  
Unterweisung des Personals  
Eskalationsprozeduren

#### **4.5. Ausweichplanung**

Redundanz von Standorten und Komponenten (Hard- und Software)  
Redundanz und Übertragungskapazität der Kommunikationsverbindungen

#### **4.6. Wiederanlaufplan**

Manuelle Umschaltprozeduren- und -zeiten (falls vorgesehen)  
Wiederinbetriebnahme von Komponenten

#### **4.7. Ersatzbeschaffungsplan**

Wartungsverträge  
Reservekomponenten

#### **4.8. Datensicherungskonzept**

Applikationen, Betriebssystem, Disaster Recovery Backup  
Zahlungssystemdaten, Änderungsprotokolle  
Aufbewahrungszeiten

#### **4.9. Ausfalltests und Übungen**

#### **4.10. Aktualisierung der BCP**

## **Teil II      Spezifische Fragestellungen**

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

### **Rechtliche und finanzielle Sicherheit der Systemteilnahme**

1. Auf welchen Rechtsgrundlagen basiert die Teilnahme des Infrastrukturbetreibers am Zahlungssystem?
2. Welche Regelungen bestehen für die gerichtliche Zuständigkeit?
3. Nach welchen Kriterien ist der Zugang zu den Infrastruktureinrichtungen für Zahlungssystembetreiber möglich?
4. Welche Regelungen bestehen hinsichtlich der Haftung des Infrastrukturbetreibers? Welche konkreten Vorkehrungen werden getroffen, um die finanziellen Risiken aus einer allfälligen Haftung abzusichern?
5. Welche Regelungen bestehen hinsichtlich der Haftung der relevanten Vertragspartner gegenüber dem Infrastrukturbetreiber?
6. Welche Regelungen bestehen hinsichtlich der Kündigung der Teilnahme des Infrastrukturbetreibers am Zahlungssystem (sowohl durch den Infrastrukturbetreiber als durch den Zahlungssystembetreiber)?
7. In welcher Form wird sichergestellt, dass dem Infrastrukturbetreiber die für ihn relevanten datenschutzrechtlichen Bestimmungen in der jeweils aktuellen Fassung bekannt sind? Welche Vorkehrungen bestehen, um die jederzeitige Einhaltung der datenschutzrechtlichen Bestimmungen zu gewährleisten?

### **Organisatorische Sicherheit der Systemteilnahme**

1. Wie ist die Führungs- und Verwaltungsstruktur organisiert (Organigramm)?
2. Wie ist die interne Kontrolle (Qualitätsmanagementsystem, Sicherheitspolicy, Risikomanagement und Revision) organisiert?
3. Wie sind Rollen und Verantwortlichkeiten des Infrastrukturbetreibers gegenüber dem Zahlungssystembetreiber definiert?
4. Welche Vorgaben bestehen seitens des Zahlungssystembetreibers? (Die diese spezifizierenden Dokumente sind vollständig beizulegen).
5. Wurden vom Zahlungssystembetreiber verlangte Zertifizierungsverfahren durchgeführt? (Diesbezügliche Unterlagen sind ggf. beizulegen).
6. Bestehen über die Vorgaben des Zahlungssystembetreibers hinausgehende eigene Richtlinien? Wenn ja, welchen Standards wurde dabei gefolgt? Wurden diese Richtlinien im Auftrag des Zahlungssystembetreibers oder in Abstimmung mit dem Zahlungssystembetreiber entwickelt? (Diesbezügliche Unterlagen sind ggf. beizulegen).

7. Wie erfolgen die Aktualisierung der Dokumentation beziehungsweise die Verwahrung der Vorgaben bzw. eigenen Richtlinien?
8. Durch welche organisatorischen Maßnahmen wird die jederzeitige Einhaltung der Vorgaben und Richtlinien sichergestellt?
9. Welche Infrastrukturkomponenten (z.B. Terminals, Bezahlmedien, Software, Zugangscodes) werden für Teilnehmer oder Endkunden bereitgestellt? Wie werden diese zugestellt?
10. Auf welche Weise wird sichergestellt, dass ausreichend, ausgebildetes und vertrauenswürdige Personal sowohl für den Normalbetrieb als auch in Ausnahmesituationen zur Verfügung steht?
11. Welche kritischen Prozesse/Komponenten wurden identifiziert?
12. Für welche Szenarien gibt es Notfallmaßnahmen?
13. Welche Eskalationsmechanismen sind für den Fehler- und Katastrophenfall vorgesehen?
14. Wie oft werden Übungen für Notfallmaßnahmen durchgeführt?
15. Welche Kommunikationsverfahren mit dem Zahlungssystembetreiber bestehen für den Fehler- oder Katastrophenfall? In welchen Abständen werden diese getestet?

## Technische Sicherheit der Systemteilnahme

1. Welche konkreten Richtlinien<sup>3</sup> bestehen im einzelnen für
  - die Gewährleistung der Verfügbarkeit und Betriebssicherheit der Infrastruktur,
  - das Erkennen und die Abwehr von Angriffen auf die Infrastruktur,
  - die Nachprüfbarkeit der Authentizität und Integrität der von den Teilnehmern und Endkunden verwendeten Infrastrukturkomponenten,
  - die Integrität und Vertraulichkeit der Transaktionsdaten und Parameter der jeweiligen Zahlungssysteme,
  - die Möglichkeit der eindeutigen Nachverfolgung von Systemänderungen,
  - die korrekte Authentisierung der Teilnehmer und Endkunden, die korrekte Autorisierung der Transaktionen sowie die wirksame Sperre (sofern diese Funktionen über die Infrastruktur ausgeübt werden).
2. Welche Maßnahmen werden für die Umsetzung der Richtlinien ergriffen? In welchen Abständen werden die eingesetzten Maßnahmen an den neuesten Stand der Technik angeglichen?

---

<sup>3</sup> Vorgaben des Zahlungssystembetreibers oder eigene Richtlinien.

3. Wie wird – sofern Infrastruktureinrichtungen und Dienste von mehreren Systemen (Zahlungssysteme oder Systeme für andere Zwecke) benutzt werden – eine gegenseitige negative Beeinflussung insbesondere in Bezug auf Verfügbarkeit und Sicherheit ausgeschlossen? Wurden Prioritäten für die Verteilung der verfügbaren Ressourcen auf die Zahlungssysteme festgelegt?
4. Falls Dienste angeboten werden, die andere Zahlungssysteme integrieren, benutzen oder erweitern (Add-on-Dienste): Wodurch wird sichergestellt, dass die Vorgaben der Zahlungssysteme eingehalten werden?
5. Wodurch wird sichergestellt, dass die für die Zahlungssysteme relevanten Sicherheitsfunktionen auch in Fällen von Betriebsstörungen oder Fehlbedienungen aufrecht bleiben?