



OESTERREICHISCHE NATIONALBANK
Eurosystem



Aufsichtsgrundsätze

für

elektronische Zahlungssysteme

E-Geld-Systeme

V2

INHALT

1	Einleitung	3
2	Begriffsbestimmungen	3
3	Anforderungen	7
4	Nachweise	16

1 Einleitung

Die vorliegenden Aufsichtsgrundsätze beinhalten die von der OeNB für die Gewährleistung der Systemsicherheit als erforderlich erachteten Anforderungen und dienen als Evaluierungsmaßstab für die von den Betreibern von E-Geld-Systemen gemäß §44a Abs. 7 NBG zu erteilenden Auskünfte. Die hinsichtlich der organisatorischen und technischen Systemsicherheit gestellten Anforderungen beinhalten jene des [„Report on Electronic Money System Security Objectives According to the Common Criteria Methodology“](#) (EZB, Mai 2003, in der Folge kurz EMSSO¹)“.

2 Begriffsbestimmungen

2.1 E-Geld-System

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 Teilnehmern
- c) dem elektronischen Transfer von Geldwerten dient.

Wird somit mit mindestens drei Teilnehmern eine Zahlungsvereinbarung geschlossen, die den elektronischen Transfer von vorausbezahlten monetären Geldwerten („E-Geld“ gem. § 2 Z 58 BWG bzw. „Electronic Value/EV“ gem. EMSSO) unter Verwendung von „Elektronischen Geldbörsen“ („Subsysteme“ gem. EMSSO) nach gleichen Regeln (wobei die betroffenen Konten auch bei nur einer Bank geführt werden können) zum Gegenstand hat, so liegt ein Zahlungssystem - E-Geld-System - vor, das der Zahlungssystemaufsicht unterliegt.

Der Begriff „E-Geld-System“ inkludiert im Rahmen der gegenständlichen Aufsichtsgrundsätze jenen des „**Target of Evaluation/TOE**“ gem. EMSSO, welches die „Subsysteme“, den „Electronic Value/EV“, die „Reporting Data/RD“, die „Accounting Data/AD“ sowie alle „Transaktionen“ und die Prozesse zur Überwachung des E-Geld-Systems durch den „System Supervisor“ umfasst.

¹ <http://www.ecb.int/pub/pdf/other/emoneysecurity200305en.pdf>

Die folgenden Komponenten und Daten des E-Geld-Systems werden gem. EMSSO als „**Assets**“ bezeichnet:

- a) Hardware-und Softwarekomponenten,
- b) die den EV repräsentierenden Daten,
- c) Transaktionsdaten,
- d) Reporting Data/RD sowie daraus extrahierte Analysen,
- e) Accounting Data/AD,
- f) Systemparameter und
- g) Systemgeheimnisse („Secrets“ gem. EMSSO, wie z. B. Passwörter oder kryptografische Schlüssel).

2.2 Betreiber

Der Begriff „Betreiber eines Zahlungssystems“ ist gemäß § 44a Abs. 5 NBG wie folgt definiert: *„Betreiber eines Zahlungssystems im Sinne dieses Bundesgesetzes ist, wer gewerblich tätig ist und mit dem Zweck der direkten oder indirekten Erzielung von Einnahmen die zentrale Verantwortung für das Systemkonzept, die Aufbau- und Ablauforganisation, die Ordnungsmäßigkeit des laufenden Betriebes und die technische Sicherheit eines Zahlungssystems trägt“.*

Der Begriff „Betreiber“ inkludiert im Rahmen der gegenständlichen Aufsichtsgrundsätze jenen des „**Administrators**“ gem. EMSSO. Dieser ist für die Definition und das Management der Gesamtsicherheit des Systems verantwortlich. Er ist üblicherweise der Eigner des Systems. Er erfüllt die Systemfunktionen entweder selbst oder überträgt sie an andere Akteure wie beispielsweise den „System Supervisor“, den „EV Issuer“ oder sonstige Serviceprovider.

Der „**System Supervisor**“ gem. EMSSO ist für die Sicherheit des Transaktionsablaufes, inklusive jenes zur Schöpfung/Tilgung des EV, sowie für das Monitoring der EV-Zirkulation verantwortlich. Die vom System Supervisor unter Verwendung von RD erstellten Analysen und Auswertungen werden als „**System Supervisor-Information**“ bezeichnet. Der „**EV Issuer**“ gem. EMSSO ist der Emittent des EV. Er ist der hinsichtlich des EV gegenüber den Endkunden rechtlich Verpflichtete. Die Funktionen des System Supervisors und des EV Issuers werden im Rahmen der gegenständlichen Aufsichtsgrundsätze dem Begriff des Betreibers zugeordnet.

2.3 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 i.S. 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 (E-Geld-Systems) oder aus einem oder in ein Zahlungssystem (E-Geld-System) 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 (E-Geld-System) in der Weise mitwirken, dass sie mit dem Zweck der Erzielung von Einnahmen aus dem Vertrieb ihrer Waren die vom Betreiber des Zahlungssystems (E-Geld-Systems) aufgestellten Regeln akzeptieren und bei diesem ein Konto führen (bzw. führen lassen), auf das die aus ihrer gewerblichen Tätigkeit eingehenden Zahlungen gutzuschreiben sind.

Der Begriff „Teilnehmer“ inkludiert im Rahmen der gegenständlichen Aufsichtsgrundsätze jenen des „**Operators**“ gem. EMSSO. Operator ist, wer an der Implementierung bzw. am operativen Betrieb und der Sicherheit des Systems mitwirkt.

2.4 Endkunde

Der Endkunde ist nicht Teilnehmer, weil er das E-Geld-System nicht zum Zweck der Einnahmenerzielung nutzt, sondern vielmehr unter Verwendung des E-Geld-Systems an den Händler Zahlungen leistet. Der Begriff „Endkunde“ inkludiert jenen des „**EV Holders**“ gem. EMSSO. EV Holder ist, wer EV besitzt und einen entsprechenden Rechtsanspruch gegenüber dem EV Issuer hat.

2.5 E-Geld

E-Geld ist „Elektronisches Geld“ i.S. des § 2 Z.58 BWG². Der Begriff „E-Geld“ inkludiert im Rahmen der gegenständlichen Aufsichtsgrundsätze jenen des „**Electronic Value/EV**“ gem. EMSSO. EV ist ein in Form einer Forderung gegen den EV Issuer ausgedrückter monetärer Wert, der

- gegen Geldmittel emittiert wird, die seinem Wert entsprechen,
- auf einem Subsystem gespeichert ist,
- von anderen Unternehmen (als dem EV Issuer) als Zahlungsmittel akzeptiert wird.

2.6 Elektronische Geldbörse

„Elektronische Geldbörse“ ist jeder Speicher für E-Geld, unabhängig davon, ob dieser z.B. auf einer Chipkarte (oder sonstigen elektronischen Speichern), als Software auf einer Festplatte oder in einem Netzwerk abgelegt ist.

Der Begriff „Elektronische Geldbörse“ inkludiert im Rahmen der gegenständlichen Aufsichtsgrundsätze jenen des „**Subsystems**“ gem. EMSSO. Subsystem ist jede Einheit, die EV senden oder empfangen kann sowie die korrespondierenden [RD](#) erzeugt und

² In Entsprechung der RL 2000/46/EC.

verfügbar hält. Subsysteme sind Chipkarten, POS-Terminals, Terminals für EV-Schöpfung/Tilgung, sowie das den [Float](#) verwaltende Zentralsystem.

2.7 Transaktion

Eine Transaktion gem. EMSSO bezeichnet die Schöpfung/Tilgung und Zirkulation von EV. Sie besteht insbesondere aus Initialisierung, Gutschrift und Belastung des EV in den verschiedenen Subsystemen.

2.8 Reporting Data (RD)

RD gem. EMSSO sind die eine EV-Transaktion dokumentierenden Datensätze. RD werden von den Subsystemen an den System Supervisor übermittelt, um diesem das Monitoring der EV Zirkulation zu ermöglichen.

2.9 Accounting Data (AD)

AD gem. EMSSO sind die eine EV-Schöpfung/EV-Tilgung dokumentierenden Datensätze. AD werden von den Subsystemen an den EV Issuer zwecks Clearing und finalem Settlement übermittelt.

2.10 Float

Float gem. EMSSO ist der in Umlauf befindliche Teil des EV. Float ist somit jener Teil des EV, der von den Endkunden für Zahlungen oder für EV Tilgungen verwendet werden kann.

3 Anforderungen

Rechtliche Systemsicherheit

- (1) **Kenntnis der Rechtsgrundlage.** 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) **Geschäftsbedingungen.** Die Geschäftsbedingungen 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) **Teilnahmekriterien.** Die Teilnahme bzw. die Nutzung des E-Geld-Systems soll auf objektiven Kriterien beruhen. Diese sollen explizit bekannt gemacht werden.
- (4) **Beendigung der Teilnahme.** 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) **Gerichtliche Zuständigkeit.** Die gerichtliche Zuständigkeit soll möglichst eindeutig geklärt sein.
- (6) **Aktualität.** Die für die Systemsicherheit relevanten Teile der Geschäftsbedingungen sollen stets aktuell gehalten werden.

Finanzielle Systemsicherheit

- (1) **Kenntnis der finanziellen Risiken.** Alle Beteiligten³ sollen die sich aus dem Systembetrieb, aus der Systemteilnahme oder aus der Systemnutzung im Missbrauchsfall ergebenden finanziellen Risiken kennen.
- (2) **Information über finanzielle Risiken.** Den Teilnehmern und Endkunden soll vom Betreiber die Kenntnisnahme der sie im Missbrauchsfall betreffenden finanziellen Risiken in leicht verständlicher Weise ermöglicht werden.
- (3) **Rücktauschbarkeit.** Die Endkunden sollen nachweislich über die Rücktauschbarkeit von E-Geld in Zentralbankgeld sowie über die diesbezüglich allenfalls bestehenden Bedingungen aufgeklärt werden.

³ Betreiber, Teilnehmer und Endkunden.

- (4) **Settlement.** Das finale Settlement soll möglichst rasch erfolgen. Die für das Settlement eingesetzten Aktiva sollen kein bzw. nur ein geringes Kredit- oder Liquiditätsrisiko bergen.
- (5) **Design gegen kriminellen Missbrauch.** 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 und technische Systemsicherheit

- (1) **Führung- und Verwaltungsstruktur sowie Systemkontrolle.** Das E-Geld-System soll über eine transparente, nachvollziehbare und effiziente Führungs- und Verwaltungsstruktur sowie über eine transparente und wirksame interne Systemkontrolle verfügen.
- (2) **Integrität.** Die Integrität der insbesondere den EV betreffenden Assets soll in sämtlichen Subsystemen des E-Geld-Systems gewahrt werden.
 - Der in Subsystemen gehaltene EV soll nur durch autorisierte Transaktionen verändert werden können.
 - Bei jeder Transaktion soll der in einem Subsystem gutgeschriebene EV dem in einem anderen Subsystem belasteten EV entsprechen.
 - Die Schöpfung oder Tilgung von EV soll in Form einer Transaktion zwischen Subsystemen erfolgen. Der Wert einer EV-Schöpfung/Tilgung soll jenem der Transaktionsdaten entsprechen.
- (3) **Vertraulichkeit.** Vertrauliche Assets sollen ausreichend geschützt werden.
 - Das E-Geld-System soll die Vertraulichkeit aller Secrets gewährleisten.
 - Das E-Geld-System soll die Vertraulichkeit der System Supervisor-Information gewährleisten.
 - RD sowie System Supervisor-Information sollen nur autorisierten Personen zugänglich sein.
- (4) **Identifikation.** In folgenden Bereichen des E-Geldsystems sollen eindeutige Identifikationsverfahren (bzw. Zustellverfahren für Systemkomponenten) zum Einsatz kommen:
 - System Supervisor,
 - EV Issuer,

- Subsysteme,
- Transaktionen,
- Secrets,
- ggf. bei sonstigen Systembeteiligten (wie IT- und Telekommunikationsdienstleistern, Händlern und Endkunden).

(5) **Authentizität.** Der Austausch von EV-Transaktions- und Monitoringdaten soll in authentifizierter Weise erfolgen.

- Vor jeder Transaktion sollen sich die EV austauschenden Subsysteme wechselseitig authentifizieren.
- Vor jeder Transaktion soll das gutschreibende Subsystem den gutschreibenden EV authentifizieren.
- Vor jeder Transaktion soll das zu belastende Subsystem dem gutschreibenden Subsystem seine Teilnahme an der Transaktion nachweisen, und vice-versa.
- Das RD an den System Supervisor sendende Subsystem soll diesen vorweg authentifizieren.
- Der System Supervisor soll erhaltene RD authentifizieren.
- Das E-Geld-System soll geeignete Vorkehrungen treffen, die eine authentifizierte Übermittlung der AD an den EV Issuer und einen Nachweis des Empfangs der AD ermöglichen.
- Der EV Issuer soll die erhaltenen AD authentifizieren.

(6) **Zugangskontrolle.** Der unautorisierte Zugang zu Assets soll auch im Falle von Systemstörungen vermieden werden.

- Das E-Geld-System soll Sicherheitsfunktionen vorsehen, die den unbefugten Zugang zu Secrets auch im Falle einer Systemstörung verhindern.
- Das E-Geld-System soll Sicherheitsfunktionen vorsehen, die den unbefugten Zugang zu System Supervisor-Information verhindern.
- Jeder Beteiligte soll über seiner Funktion entsprechende, eindeutige Zugangsrechte verfügen.

(7) **Vereinbarung zwischen den Parteien und Transaktionsbestätigung.** Eine Transaktion soll nur auf der Grundlage einer zwischen den Beteiligten vorab getroffenen Vereinbarung erfolgen.

- Die Initialisierung einer Transaktion soll nur möglich sein, nachdem die an der Transaktion beteiligten Parteien eine Vereinbarung zur Durchführung dieser Transaktion unter Verwendung des E-Geld-Systems getroffen haben. Diese Vereinbarung soll den auszutauschenden EV sowie eine Regel zur abschließenden Bestätigung der Transaktion beinhalten.
- Jede Vereinbarung soll nur eine Transaktion ermöglichen.
- Jede Transaktion soll von beiden Parteien abschließend nach jener Regel bestätigt werden, die in der Vereinbarung festgelegt wurde.

- (8) **Eindeutigkeit der Transaktionsdurchführung.** Das E-Geld-System soll Sicherheitsfunktionen vorsehen, die eine Transaktion in eindeutiger Weise entweder vollständig durchführen oder vor dem Transaktionsabschluss annullieren.
- (9) **Definierter Transaktionsablauf.** Jede Transaktion soll als Abfolge von definierten Verfahrensschritten erfolgen. Jeder Verfahrensschritt soll pro Transaktion nur einmalig anfallen.
- Bei jeder Transaktion zwischen zwei Subsystemen sollen die Verfahrensschritte folgende Grundfolge einhalten:
 - Initialisierung,
 - EV-Belastung vor EV-Gutschrift,
 - Transaktionsabschluss.
 - Bei jeder Transaktion zur Schöpfung/Tilgung von EV sollen die Verfahrensschritte folgende Grundfolge einhalten:
 - EV- Schöpfung /Tilgung vor Transaktionsabschluss,
 - Übermittlung der AD an den EV-Issuer nach EV-Schöpfung /Tilgung,
 - Übermittlung der AD an den EV-Issuer nur nach Transaktionsabschluss zwischen den Subsystemen.
- (10) **Autorisierte EV-Tilgung.** Das E-Geld-System soll vorsehen, dass EV-Tilgungstransaktionen nur zwischen zwei für diesen Zweck eigens autorisierten Subsystemen vorgenommen werden können.
- (11) **Limite.** Die EV-Menge soll Beschränkungen unterliegen. Für jedes Subsystem sollen folgende Parameter festgelegt werden:
- Maximum des aufladbaren EV,
 - Maximum des bei einer Transaktion transferierbaren EV,
 - Maximum der bei einer Transaktion schöpfbaren EV-Menge (betrifft nur den EV Issuer).
- (12) **Nachvollziehbarkeit.** Der System Supervisor soll in der Lage sein, alle relevanten Ereignisse nachvollziehen und prüfen zu können. Die Subsysteme sollen zu diesem Zweck die vom System Supervisor geforderten Aufzeichnungen genau führen und über den verlangten Zeitraum verfügbar halten.
- Als relevante Ereignisse gelten:
 - die Generierung, die Stilllegung, der Austausch oder der Widerruf von Secrets,
 - die Initialisierung und Modifikation von Parametern der Subsysteme,

- die Initialisierung und Modifikation von Parametern betreffend die EV-Schöpfung/Tilgung.
- Das E-Geld-System soll die Möglichkeit vorsehen, RD an den System Supervisor zeitgerecht zu kommunizieren.
- Jedes Subsystem, das RD für den System Supervisor erzeugt, soll RD über die von ihm abgewickelten Transaktionen sowie über die von ihm an den System Supervisor übermittelten RD aufzeichnen.
- RD sollen die Transaktionen exakt wiedergeben.
- Jedes Subsystem, das AD erzeugt, soll Aufzeichnungen über die von ihm an den EV Issuer übermittelten AD führen.
- AD sollen die Transaktionen zur EV-Schöpfung/Tilgung exakt wiedergeben.

(13) **Erkennen von Attacken.** Das E-Geld-System soll in der Lage sein Ereignisse wie Transaktionsfälschungen oder die tatsächliche/versuchte Modifikation von Datenbeständen zu erkennen und derartige Attacken an den System Supervisor zu melden. Insbesondere soll das E-Geld-System Verfahren zur Erkennung folgender Ereignisse vorsehen:

- tatsächlicher/versuchter unbefugter Zutritt zu Secrets, sowie deren Modifikation oder unbefugte Verwendung,
- tatsächliche/versuchte Modifikation von Transaktionsdaten,
- tatsächliche/versuchte Transaktionsfälschungen (inklusive versuchte Wiedereinspielung von authentischen Transaktionen),
- tatsächliche/versuchte Modifikation von Datenbeständen betreffend die Schöpfungs-/Tilgung von EV,
- tatsächlicher/versuchter unbefugter Zutritt zur Monitoringdomäne bzw. Modifikation von Monitoringdaten.

Zudem soll das E-Geld-System Verfahren zur Übermittlung von bis zum Ursprung dieser Attacken nachvollziehbaren RD an den System Supervisor vorsehen.

(14) **Reaktion auf Attacken.** Das E-Geld-System soll in der Lage sein, Attacken standzuhalten bzw. deren Auswirkungen zu begrenzen.

- Das E-Geld-System soll Verfahren zur Begrenzung der möglichen Folgewirkungen von Attacken bzw. zur Aufrechterhaltung des Betriebes nach erfolgten Attacken vorsehen.
- Das E-Geld-System soll Verfahren zur Sperre von als manipuliert erkannten Subsystemen vorsehen.
- Das E-Geld-System soll in der Lage sein, jede Anordnung des System Supervisors zur Begegnung von Attacken umsetzen zu können.

- Das E-Geld-System soll in der Lage sein, jede einer Attacke ausgesetzte Transaktion annullieren zu können.
- Das E-Geld-System soll Verfahren zur Begrenzung der möglichen Folgewirkungen von Attacken auf die Monitoringdomäne vorsehen.

(15) **Kryptografie und Protokolle.** Die zum Einsatz kommenden Kryptografie-, Protokollierungs- und Sicherheitsverfahren sollen dem Stand der Technik entsprechen und ein hohes Sicherheitsniveau aufweisen.

- Die vom E-Geld-System verwendeten kryptografischen Algorithmen und Schlüsselmanagementverfahren sollen standardisiert und öffentlich bekannt sein. Ihr Sicherheitsniveau soll öffentlich analysiert worden sein; es sollen keine kryptografischen Algorithmen eingesetzt werden, die Geheimhaltungsverpflichtungen unterliegen und daher keiner öffentlichen Überprüfung unterzogen werden können.
- Die Kommunikationsarchitektur des E-Geld-Systems soll auf standardisierten Protokollen und Sicherheitsverfahren beruhen.

(16) **Secrets Management.** Die Vertraulichkeit und Integrität von Secrets soll durch deren korrekte Erzeugung, Verteilung, Aufbewahrung, begrenzte Lebensdauer und regelmäßige Erneuerung gewährleistet werden.

- Das E-Geld-System soll bei der Erzeugung und Verteilung von Secrets standardisierte Verfahren anwenden.
- Secrets sollen in einer nicht vorhersagbaren Weise erzeugt werden.
- Jedes Secret soll eine verwendungsabhängige Lebensdauer aufweisen.
- Jedes Secret soll jederzeit erneuert werden können.
- Secrets sollen nur in Geräten transportiert und aufbewahrt werden, die physischen Sabotageakten standhalten können (HSMs)⁴. Außerhalb solcher Geräte sollen sie keinesfalls in Klartext vorkommen. Sollten private und geheime kryptografische Schlüssel außerhalb solcher Geräte angewendet werden, so darf dadurch die Sicherheit des E-Geldsystems nicht gefährdet werden. Private (asymmetrische) kryptografische Schlüssel und symmetrische Master- oder Root-Keys einer hierarchischen Schlüsselstruktur gelten als sicherheitsrelevant.
- Alle Verfahren zur Erzeugung von Secrets sollen nur einem befugten Personenkreis bekannt sein.
- Secrets sollen nur einem befugten Personenkreis zugänglich sein.

(17) **Gesicherte Kommunikationswege.** Das E-Geld-System soll zwischen den Teilnehmern und Subsystemen gesicherte Kommunikationswege vorsehen, die sicherstellen, dass übertragene Assets nicht modifiziert und abgehört werden

⁴ Hardware Security Modul; ein Gerät zur sicheren Erzeugung und Speicherung von Secrets, das Manipulationsversuchen entweder widersteht oder die Daten der Secrets löscht.

können und die jeweils richtigen, authentischen Partner miteinander kommunizieren.

- (18) **Gesicherter Standort.** Sicherheitsrelevante Systemkomponenten sollen sich an einem physikalisch geschützten Standort befinden.
- (19) **Kompetenz und Verantwortung.** Alle am System beteiligten Personen sollen die sie betreffenden Obliegenheiten kennen und befolgen. Sie sollen über die zu deren Erfüllung erforderlichen Ressourcen, Ausbildung und Informationen verfügen. Dies gilt für Personal der Systembereiche Secret Management, Installation, Administration und Betrieb von Subsystemen, bzw. auch für indirekt am Betrieb mitwirkende Personen (z.B. Service Provider). Personal jener Unternehmen, die für die Produktion und Distribution von beim E-Geld-System zum Einsatz gelangender Hard- oder Software zuständig sind, soll nach entsprechenden Kriterien rekrutiert werden, einer angemessenen Gebäudezugangskontrolle unterliegen und geeignete Awarenessprogramme absolvieren.
- (20) **Tests.** Die Systemkomponenten sollen vor Inbetriebnahme und/oder während des produktiven Einsatzes getestet werden
- Hard-/Software sowie die organisatorischen Abläufe sollen vor der Inbetriebnahme Qualifikations-/Funktionstests unterzogen werden. Hardware soll zudem vor der Inbetriebnahme physikalischen Penetrationstests unterzogen werden. Jedes zum Einsatz kommende Gerät soll vor dem produktiven Einsatz isoliert sowie im Rahmen des Gesamtsystems getestet werden.
 - Hardware sollte auch während des produktiven Einsatzes Funktionstests unterzogen werden (ohne jedoch die Verfügbarkeit des Systems zu beeinträchtigen).
 - Jedes Subsystem sollte einer Überprüfung der folgenden Funktionen (sofern diese von ihm unterstützt werden) unterzogen werden:
 - der entgegengenommene EV kann zu einem Gesamtbetrag aggregiert werden, welcher der Summe der entgegengenommenen Einzelbeträge entspricht,
 - der Gesamtbetrag des gespeicherten EV kann in Einzelbeträge zerlegt werden, deren Summe dem Gesamtbetrag entspricht.
- (21) **Assessments.** Die Erbringer der Systemfunktionen (i) Administrator, (ii) System Supervisor, (iii) Operator sollen regelmäßigen Assessments unterzogen werden, die feststellen, ob sie die Sicherheitspolitik des E-Geld-Systems einhalten.

- (22) **Security updates.** Die Hard- und Softwaresicherheit der sensitiven Systemkomponenten sollen periodisch nach dem Stand der Technik aktualisiert werden.
- (23) **Verfügbarkeit.** Das E-Geld-System soll etablierte, dem Stand der Technik entsprechende Maßnahmen einsetzen, um eine hohe Verfügbarkeit aufweisen. Die Servicebereitschaft soll auch dann aufrechterhalten werden, wenn Einzelbereiche einer Wartung unterzogen werden.
- Das E-Geld-System soll eine möglichst geringe Serviceunterbrechung gewährleisten, wenn ein/mehrere/alle Secrets des E-Geld-Systems ausgetauscht werden müssen.
 - Das E-Geld-System soll Verfahren vorsehen, die eine kontinuierliche Schöpfung/Tilgung von EV ermöglichen, insbesondere auch während einige/alle Geräte, die AD speichern oder weiterleiten, ausgetauscht werden.
 - Die Servicebereitschaft des E-Geld-Systems soll durch die Existenz eines Business Continuity Planes, der die Auswirkungen einer Funktionsstörung des Systems (oder Teilen davon) auf dessen Verfügbarkeit begrenzen soll, gewährleistet werden.
 - Das E-Geld-System soll permanentes Monitoring vorsehen, insbesondere während einige/alle Geräte, die RD speichern/weiterleiten, einem Austausch unterzogen werden.
 - Die Datenbestände sollen in Geräten gespeichert werden, die geeignet sind, deren langfristigen Bestand zu gewährleisten.
- (24) **Lebenszyklus.** Während der gesamten Geltungsdauer des EV bzw. der gesamten Lebensdauer der Subsysteme sollen dem Stand der Technik entsprechende Sicherheitsverfahren eingesetzt werden. Dies betrifft insbesondere:
- die physischen und logischen Schutzmechanismen von Gebäuden, in denen vom E-Geld-System verwendete Geräte oder Software initialisiert werden,
 - die Initialisierung und Personalisierung von Subsystemen,
 - die Verpackung, Zustellung und Installation von Geräten und Software des E-Geld-Systems.
- Weiters soll das E-Geld-System für jedes EV-speichernde Gerät ein Außerbetriebnahme-Verfahren in technischer und in organisatorischer Hinsicht vorsehen, das insbesondere Folgendes beinhaltet:
- Vorlage und Tilgung von EV,
 - Übermittlung von RD an den System Supervisor,
 - Übermittlung von AD an den EV Issuer.

- (25) **Applikationstrennung.** Wenn ein E-Geld-System Komponenten mit anderen Applikationen (z. B. Zahlungssystemen) teilt, so soll das E-Geld-System innerhalb dieser Komponenten isoliert von den anderen Applikationen funktionieren.
- Werden Komponenten des E-Geld-Systems von anderen Applikationen mitbenutzt, so sollen die dem E-Geld-System zuzuschreibenden Daten und Prozesse logisch getrennt von den anderen sein. Nur dem E-Geld-System zuzurechnende Prozesse sollen Datenbestände des E-Geld-Systems modifizieren können.
 - Benutzt das E-Geld-System seinerseits Komponenten anderer Applikationen mit, so soll sichergestellt sein, dass dies entsprechend den technischen Sicherheitsstandards der betroffenen Systeme erfolgt.
- (26) **Internationaler Einsatz.** Wird das E-Geld-System international eingesetzt, so sollen die Sicherheitsniveaus in den betroffenen Ländern in Bezug auf die organisatorische und technische Sicherheit gegenüber jenem des nationalen E-Geld-Systems adäquat sein. Dazu sollen entsprechende Abnahme-/Freigabe- und Überprüfverfahren existieren.

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 – E-Geld-Systeme V2*“ binnen der im Aufforderungsschreiben genannten Frist nachzuweisen.

Die Nachweise sind bei wesentlichen Systemänderungen in aktualisierter Form vorzulegen.