



OESTERREICHISCHE NATIONALBANK
Eurosystem



Leitfaden

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

über die

zur Gewährleistung der Systemsicherheit getroffenen Maßnahmen

E-Geld-Systeme

V2

Inhalt

1.	Einleitung	3
2.	Begriffsbestimmungen	4
3.	Auskünfte	8
Anhang 1	Mindestinhalt der Systembeschreibung	17
Anhang 2	Informationen an Teilnehmer und Endkunden	19

1. Einleitung

Der vorliegende Leitfaden beinhaltet die Mindestanforderungen für die gemäß § 44a Abs. 7 NBG von den Betreibern von E-Geld-Systemen zu erteilenden Auskünfte über die zur Gewährleistung der Systemsicherheit des Zahlungssystems getroffenen Maßnahmen. Die hinsichtlich der organisatorischen und technischen Systemsicherheit formulierten Fragestellungen beinhalten die „Terms of Reference“ (EZB, 2006) zum [Report on Electronic Money System Security Objectives According to the Common Criteria Methodology](#)¹ (EZB, 2003)“.

Die Auskünfte gelten als vollständig erteilt, wenn zu den in Kapitel 3 aufgelisteten Fragen in anschaulicher Weise einzeln schriftlich Stellung genommen wird.

Die Stellungnahmen sind zumindest mit folgenden Dokumenten zu unterlegen:

- Geschäftsbedingungen,
- Systembeschreibung (siehe Anhang 1),
- Informationen an Teilnehmer und an Endkunden (siehe Anhang 2).

Die in den Stellungnahmen gegebenen Auskünfte können in Form von eindeutigen Bezugnahmen auf die übermittelten 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 der behaupteten Sicherheitsniveaus von systemsicherheitsrelevanten Komponenten und Verfahren vorzulegen.

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

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.

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 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 In Entsprechung der RL 2000/46/EC.

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. Auskünfte

Zu folgenden Fragen ist einzeln und begründet Stellung zu nehmen:

Rechtliche Systemsicherheit

1. Auf welche Rechtsgrundlagen stützt sich das E-Geld-System?
2. Auf welche Weise werden den Teilnehmern und Endkunden die hinsichtlich der Systemsicherheit für sie jeweils relevanten Rechtsgrundlagen des E-Geld-Systems bekannt gemacht?
3. Sind die wesentlichen Rechte und Pflichten der Teilnehmer im Umgang mit dem E-Geld-System in den Geschäftsbedingungen des Systems enthalten und ausreichend abgebildet? Welche Hinweise werden gegeben?
4. Auf welche Weise wird die Durchsetzbarkeit der für die Systemsicherheit relevanten Teile der Geschäftsbedingungen gegenüber Teilnehmern und Endkunden, insbesondere auch gegenüber solchen, die nicht österreichischem Recht unterliegen, überprüft?
5. Welche Kriterien existieren für die Teilnahme am E-Geld-System (bzw. für die Nutzung durch Endkunden) sowie für deren Beendigung auf Verlangen eines Teilnehmers bzw. eines Endkunden, und auf welche Weise werden sie bekannt gemacht?
6. Welche Regelungen bestehen für die gerichtliche Zuständigkeit?
7. Auf welche Weise wird sichergestellt, dass die für die Systemsicherheit relevanten Teile der Geschäftsbedingungen laufend aktualisiert werden?

Finanzielle Systemsicherheit

1. Welche finanziellen Risiken können sich im Missbrauchsfall aus dem Systembetrieb, aus der Systemteilnahme oder aus der Systemnutzung ergeben?
2. Welche Vorkehrungen werden getroffen, um allen Beteiligten³ die Kenntnisnahme von den sie im Missbrauchsfall betreffenden finanziellen Risiken zu ermöglichen?
3. Auf welche Weise werden die Endkunden über die Rücktauschbarkeit von E-Geld in Zentralbankgeld sowie über die diesbezüglich allenfalls bestehenden Bedingungen aufgeklärt?
4. Welche Vorkehrungen werden getroffen, um den Teilnehmern die Absicherung der finanziellen Risiken zu ermöglichen?
5. Sind Begrenzungen des maximalen finanziellen Risikos, das dem E-Geld-System durch einzelne Teilnehmer entstehen kann, vorgesehen? Welche Begrenzungen sind vorgesehen?
6. Wann und in welcher Form erfolgt das finale Settlement?

³ Betreiber, Teilnehmer und Endkunden.

7. Welche Aktiva werden für das Settlement eingesetzt?
8. Welche Vorkehrungen werden getroffen, damit das E-Geld-System keinen Anreiz für kriminellen Missbrauch, wie z.B. Geldwäsche, bietet?

Organisatorische und technische Systemsicherheit

Führung- und Verwaltungsstruktur.

1. Wie ist die Führungs- und Verwaltungsstruktur des E-Geld-Systems organisiert?
2. Wie ist die interne Systemkontrolle organisiert?
3. Basiert die Sicherheitspolitik des E-Geld-Systems auf fortlaufenden Risikoanalysen? Bitte um Erläuterung der Methodik.
4. Werden die sensitiven Systembereiche/-beteiligten entsprechend ihrer Bedeutung für die Funktionsfähigkeit des Systems identifiziert und klassifiziert? Bitte um Erläuterung des Verfahrens.
5. Werden die Träger wichtiger Systemfunktionen (insbesondere System Supervisor, Operator) regelmäßigen Assessments unterzogen, die nachweisen, dass sie in Ausübung ihrer Funktion die Sicherheitspolitik des E-Geld-Systems einhalten?

Integrität.

6. Auf welche Weise wird die Integrität der insbesondere den EV betreffenden Assets in sämtlichen Subsystemen des E-Geld-Systems gewahrt?
 - i. Auf welche Weise wird sichergestellt, dass nur autorisierte Transaktionen den EV-Betrag verändern können?
 - ii. Auf welche Weise wird sichergestellt, dass der in einem Subsystem gutgeschriebene EV dem in einem anderen Subsystem belasteten EV entspricht?
 - iii. Erfolgt die Schöpfung oder Tilgung von EV in Form einer Transaktion zwischen Subsystemen? Wird dabei der geschöpfte/getilgte EV genau in den Transaktionsdaten abgebildet?

Vertraulichkeit.

7. Auf welche Weise wird die Vertraulichkeit der Assets gewährleistet?
 - i. Welche Sicherheitsmaßnahmen (kryptografische Algorithmen, PIN-Codes, etc.) werden eingesetzt?
 - ii. Auf welche Weise wird die Vertraulichkeit der System Supervisor Information gewährleistet?
 - iii. Auf welche Weise wird gewährleistet, dass System Supervisor Information nur autorisierten Personen zugänglich ist?

Identifikation.

8. Welche Identifikationsverfahren kommen betreffend
 - System Supervisor,
 - EV Issuer,

- Subsystemen,
- Transaktionen,
- Secrets,
- IT- und Telekommunikationsdienstleistern,
- Händlern und Endkunden

zum Einsatz?

9. Auf welche Weise erfolgt die Zustellung der Komponenten an Teilnehmer bzw. der Subsysteme an Endkunden? Welche Anhaltspunkte werden den Teilnehmern und Endkunden zur Prüfung der Authentizität und Integrität der von ihnen verwendeten Komponenten und Subsysteme zur Verfügung gestellt?

Authentizität.

10. Authentifizieren sich die EV-austauschenden Subsysteme vor jeder Transaktion wechselseitig? Auf welche Weise erfolgt diese Authentifizierung?
11. Authentifiziert das EV-gutschreibende Subsystem den gutzuschreibenden EV vor der Transaktion? Auf welche Weise erfolgt diese Authentifizierung?
12. Übermittelt das zu belastende Subsystem vor der Transaktion einen Nachweis hinsichtlich seiner Teilnahme an der Transaktion an das EV-gutschreibende Subsystem, und vice versa?
13. Authentifiziert das RD an den System Supervisor sendende Subsystem diesen vor jedem Datentransfer? Auf welche Weise erfolgt diese Authentifizierung?
14. Authentifiziert der System Supervisor erhaltene RD? Auf welche Weise erfolgt diese Authentifizierung?
15. Welche Vorkehrungen trifft das E-Geld-System zur Übermittlung authentifizierter AD an den EV Issuer? Ist ein Empfangsnachweis möglich? Worin besteht dieser Nachweis?
16. Authentifiziert der EV Issuer die erhaltenen AD? Auf welche Weise erfolgt diese Authentifizierung?

Zugangskontrolle.

17. Sieht das E-Geld-System Sicherheitsfunktionen vor, die den unbefugten Zugang zu Secrets auch im Falle einer Systemstörung verhindern? Worin bestehen diese Sicherheitsfunktionen?
18. Sieht das E-Geld-System Sicherheitsfunktionen vor, die den unbefugten Zugang zu System Supervisor Information auch im Falle einer Systemstörung verhindern? Worin bestehen diese Sicherheitsfunktionen?
19. Verfügt jeder Beteiligte über eindeutige Zugangsrechte, die der Bedeutung seiner Funktion entsprechen? Wie sind diese geregelt?

Vereinbarung zwischen den Parteien und Transaktionsbestätigung.

20. Ist die Initialisierung einer Transaktion im Rahmen des E-Geld-Systems nur möglich, nachdem die an der Transaktion beteiligten Parteien eine Vereinbarung zur Durchführung dieser Transaktion getroffen haben? Beinhaltet diese

Vereinbarung den auszutauschenden EV sowie eine Regel zur abschließenden Bestätigung der Transaktion?

21. Erfordert jede Transaktion eine gesonderte Vereinbarung?

22. Wird jede Transaktion von beiden Parteien abschließend nach jener Regel bestätigt, die in der Vereinbarung festgelegt wurde?

Eindeutigkeit der Transaktionsdurchführung.

23. Sieht das E-Geld-System eine Funktion vor, die sicherstellt, dass eine Transaktion in eindeutiger Weise entweder einem Abschluss oder einer Annullierung zugeführt wird? Worin besteht diese Funktion?

24. Sieht das E-Geld-System eine Funktion vor, die eine nicht abgeschlossene Transaktion aufgezeigt würde? Worin besteht diese Funktion?

Definierter Transaktionsablauf.

25. Erfolgt jede Transaktion auf der Grundlage von vorweg definierten Verfahrensschritten? Fällt jeder Verfahrensschritt pro Transaktion nur einmal an?

26. Wird beim Ablauf jeder Transaktion zwischen zwei Subsystemen die folgende Abfolge eingehalten:

1. Initialisierung,
2. EV-Belastung vor EV-Gutschrift,
3. Transaktionsabschluss?

27. Wird beim Ablauf jeder Transaktion zur Schöpfung/Tilgung von EV die folgende Abfolge eingehalten:

1. EV- Schöpfung /Tilgung vor Transaktionsabschluss,
2. Übermittlung der AD an den EV-Issuer nach EV- Schöpfung /Tilgung,
3. Übermittlung der AD an den EV-Issuer nur nach Transaktionsabschluss zwischen den Subsystemen?

Autorisierte EV-Tilgung.

28. Sieht das E-Geld-System vor, dass EV-Tilgungstransaktionen nur zwischen zwei für diesen Zweck eigens autorisierten Subsystemen vorgenommen werden können? Worin bestehen diese Vorkehrungen?

Limite.

29. Sieht das E-Geld-System die Festlegung der folgenden Parameter für jedes Subsystem vor:

- Maximum des aufladbaren EV,
- Maximum des bei einer Transaktion transferierbaren EV,
- Maximum der bei einer Transaktion schöpfbaren EV-Menge (betrifft nur den EV Issuer)?

Nachvollziehbarkeit.

30. Sieht das E-Geld-System vor, dass der System Supervisor in der Lage ist, alle relevanten Ereignisse, d.s.:
- die Generierung, die Stilllegung, der Austausch oder Widerruf von Secrets,
 - die Initialisierung und Modifikation von Parametern der Subsysteme,
 - die Initialisierung und Modifikation von Parametern betreffend die EV-Schöpfung/Tilgung,
- nachzuvollziehen bzw. prüfen zu können? Worin bestehen diese Vorkehrungen?
31. Ist das E-Geld-System in der Lage, RD für Monitoringzwecke zeitgerecht an den System Supervisor zu kommunizieren? Welche Vorkehrungen sind hierfür vorgesehen?
32. Ist jedes Subsystem in der Lage, die vom System Supervisor geforderten RD genau zu führen und über den verlangten Zeitraum verfügbar zu halten. Welche Vorkehrungen sind hierfür vorgesehen?
33. Spiegeln die RD die Transaktionen exakt wider?
34. Führt jedes Subsystem Aufzeichnungen über die von ihm an den System Supervisor übermittelten RD? In welcher Form werden diese Aufzeichnungen geführt?
35. Führt jedes AD erzeugende Subsystem Aufzeichnungen über die von ihm an den EV Issuer übermittelten AD? In welcher Form werden diese Aufzeichnungen geführt?
36. Spiegeln die AD die Transaktionen zur EV-Schöpfung/Tilgung exakt wider?

Erkennen von Attacken.

37. Ist das E-Geld-System in der Lage, Ereignisse wie Transaktionsfälschungen oder die tatsächliche oder versuchte Modifikation von Datenbeständen zu erkennen und derartige Attacken an den System Supervisor zu melden? Sind insbesondere Verfahren zur Erkennung folgender Ereignisse vorgesehen:
- 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 bzw. Fälschungen betreffend die Schöpfung/Tilgung von EV,
 - tatsächlicher/versuchter unbefugter Zutritt zur Monitoringdomäne bzw. Modifikation von Datenbeständen der Monitoringdaten.

Sind diese Verfahren geeignet, bis zum Ursprung der Attacke nachvollziehbare RD an den System Supervisor zu übermitteln? Um welche Verfahren handelt es sich?

Reaktion auf Attacken.

38. Welche Verfahren sind zur Begrenzung möglicher Folgewirkungen von Attacken bzw. zur Aufrechterhaltung des Betriebes nach Attacken vorgesehen?
39. Ist das E-Geld-System in der Lage, jede einer Attacke ausgesetzte Transaktion annullieren zu können? Welche Vorkehrungen sind hierfür vorgesehen?
40. Welche Verfahren sind zur Sperre von als manipuliert erkannten Subsystemen vorgesehen?
41. Ist das E-Geld-System in der Lage, die Anordnungen des System Supervisors zur Begegnung von Attacken innerhalb einer angemessenen Zeit umsetzen zu können? Welche Vorkehrungen sind hierfür vorgesehen?
42. Ist das E-Geld-System in der Lage, auf Attacken auf die Monitoringdomäne (tatsächlicher/versuchter unbefugter Zugriff auf bzw. Modifikation von Monitoringdaten) reagieren zu können? Worin bestehen diese Vorkehrungen?

Kryptografie und Protokolle.

43. Weist das E-Geld-System ein dem Stand der Technik entsprechend hohes Sicherheitsniveau auf? Worauf stützt sich diese Beurteilung?
44. Können die im Rahmen des E-Geld-Systems zum Einsatz kommenden kryptografischen Algorithmen und Verschlüsselungsverfahren⁴ einer öffentlichen Überprüfung unterzogen werden? Wann und in welcher Form erfolgte eine derartige Überprüfung?
45. Beruht die Kommunikationsarchitektur des E-Geld-Systems auf standardisierten Protokollen und Sicherheitsverfahren? Um welche Verfahren handelt es sich?
46. Auf welche Weise werden die RD, AD bzw. die Änderungen von Systemparametern protokolliert? Wie lange werden diese Protokolle aufbewahrt?

Secrets Management.

47. Werden zur Erzeugung und Verteilung von Secrets standardisierte Verfahren angewandt? Um welche Verfahren handelt es sich?
48. Werden die Secrets in einer nicht vorhersagbaren Weise erzeugt? Wodurch wird dies gewährleistet?
49. Weist jedes Secret eine verwendungsabhängige Lebensdauer auf? Welche Regelungen kommen diesbezüglich zur Anwendung?
50. Kann jedes Secret jederzeit ausgewechselt werden? Wodurch wird dies ermöglicht?
51. Werden Secrets nur in Geräten (HSMs)⁵ transportiert und aufbewahrt, die physischen Sabotageakten standhalten können? Welche Geräte kommen dabei zum Einsatz? Wodurch wird sichergestellt, dass Secrets außerhalb solcher Geräte

⁴ Mit Ausnahme jener Verfahren, die für militärische Zwecke entwickelt wurden.

⁵ Hardware Security Modul; ein Gerät zur sicheren Erzeugung und Speicherung von Secrets, das Manipulationsversuchen entweder widersteht oder die Daten der Secrets löscht.

- keinesfalls in Klartext vorkommen? Wodurch wird sichergestellt, dass - im Falle einer Verwendung von privaten und geheimen kryptografischen Schlüsseln⁶ außerhalb solcher Geräte - die Sicherheit des E-Geldsystems nicht gefährdet wird?
52. Wodurch wird sichergestellt, dass die Verfahren zur Erzeugung von Secrets nur einem befugten Personenkreis bekannt sind?
53. Wodurch wird sichergestellt, dass die Verfahren zur Erzeugung von Secrets nur einem befugten Personenkreis zugänglich sind?

Gesicherte Kommunikationswege.

54. Welche Kommunikationswege bestehen zwischen den Teilnehmern und den Subsystemen des E-Geld-Systems?
55. Wodurch wird sichergestellt, dass über diese Kommunikationswege übertragene Assets nicht abgehört oder modifiziert werden können?
56. Wodurch erfolgt die gegenseitige, eindeutige Authentifizierung der Kommunikationspartner?

Gesicherter Standort.

57. Welche Schutzmechanismen sind für den physikalischen Standort sicherheitsrelevanter Komponenten/Daten vorgesehen?

Kompetenz und Verantwortung.

58. Wodurch wird gewährleistet, dass alle am System beteiligten Personen die sie betreffenden Obliegenheiten kennen und befolgen?
59. Wodurch wird gewährleistet, dass diese Personen über die für die Erfüllung ihrer Aufgaben erforderlichen Ressourcen, Schulungen und Informationen verfügen?
60. Wodurch wird gewährleistet, dass die für Secret-Management, Installation, Administration und Betrieb von Subsystemen verantwortlichen Personen, bzw. indirekt am Betrieb mitwirkende Personen, wie beispielsweise Service Provider, über die jeweils erforderliche Kompetenz und Expertise verfügen?
61. Wodurch wird gewährleistet, dass das Personal jener Unternehmen, die für die Produktion und Verteilung von beim E-Geld-System eingesetzter Hard- oder Software zuständig sind, nach entsprechenden Kriterien rekrutiert wird, einer angemessenen Gebäudezugangskontrolle unterliegt und geeignete Awarenessprogramme absolviert?

Tests.

62. Werden die zum Einsatz kommende Hard-/Software sowie die organisatorischen Abläufe vor der Inbetriebnahme Qualifikations-/Funktionstests unterzogen? In welcher Form erfolgen diese Tests?

⁶ Private (asymmetrische) kryptografische Schlüssel und symmetrische Master- oder Root-Keys einer hierarchischen Schlüsselstruktur gelten als sicherheitsrelevant.

63. Wird die für öffentliche Standorte vorgesehene Hardware zudem vor dem produktiven Einsatz physikalischen Penetrationstests unterzogen? In welcher Form erfolgen diese Tests?
64. Wird die zum Einsatz kommende Hardware auch während des produktiven Einsatzes Funktionstests unterzogen? In welcher Form erfolgen diese Tests? Wird durch diese Tests die Verfügbarkeit des Systems beeinträchtigt?
65. Wird jedes Subsystem einer Überprüfung der folgenden Funktionen (sofern diese von ihm unterstützt werden) unterzogen:
- 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?

Assessments.

66. Werden die Erbringer der Systemfunktionen (i) Administrator, (ii) System Supervisor, (iii) Operator regelmäßigen Assessments unterzogen, die feststellen, ob sie die Sicherheitspolitik des E-Geld-Systems einhalten? In welcher Form erfolgen diese Assessments?

Security updates.

67. Wird die Hard- und Softwaresicherheit der sensitiven Systemkomponenten in periodischen Abständen nach dem Stand der Technik aktualisiert? In welcher Form erfolgt diese Aktualisierung?

Verfügbarkeit.

68. Welche Maßnahmen werden gesetzt, um den vertraglich festgelegten Service Level einzuhalten?
69. Wodurch wird im Fall des Austauschs eines/mehrerer/aller Secrets des E-Geld-Systems eine möglichst geringe Serviceunterbrechung gewährleistet?
70. Wodurch wird eine kontinuierliche Schöpfung/Tilgungsmöglichkeit von EV ermöglicht, insbesondere während Geräte zur Speicherung/Weiterleitung von AD ausgetauscht werden?
71. Existiert ein Business Continuity Plan, durch den die Auswirkungen einer Funktionsstörung des E-Geld-Systems (oder Teilen davon) auf dessen Verfügbarkeit begrenzt werden kann? Welche Maßnahmen sieht der BCP vor? Auf welche Weise wird insbesondere die Verfügbarkeit der Autorisierungssysteme während der Betriebszeiten des E-Geld-Systems gewährleistet?
72. Wodurch wird ein permanentes Monitoring des E-Geld-Systems erreicht, insbesondere während Geräte zur Speicherung/Bearbeitung von RD ausgetauscht werden?
73. Durch welche Maßnahmen wird eine langfristige Speichermöglichkeit von Assets und Daten erreicht?

Lebenszyklus.

74. Entsprechen die während der gesamten Geltungsdauer des EV bzw. der gesamten Funktionsdauer der Subsysteme eingesetzten Sicherheitsverfahren dem Stand der Technik, insbesondere betreffend:

- den 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?

Um welche Verfahren handelt es sich?

75. Sieht das E-Geld-System für jedes EV-speichernde Gerät ein Außerbetriebnahme-Verfahren in technischer und in organisatorischer Hinsicht vor, das insbesondere Folgendes beinhaltet:

- Vorlage und Tilgung des EV,
- Übermittlung von RD an den System Supervisor,
- Übermittlung von AD an den EV Issuer?

Applikationstrennung.

76. Werden Komponenten des E-Geld-Systems von anderen Applikationen mitbenutzt? Wodurch wird gegebenenfalls eine logische Trennung der dem E-Geld-System zuzuschreibenden Daten und Prozesse sichergestellt?

77. Benutzt das E-Geld-System seinerseits Komponenten anderer Applikationen mit? Wodurch wird gegebenenfalls sichergestellt, dass dies entsprechend den technischen Sicherheitsstandards dieser Applikationen erfolgt?

78. Wodurch wird sichergestellt, dass nur dem E-Geld-System zuzurechnende Prozesse in der Lage sind, Datenbestände des E-Geld-Systems zu modifizieren?

Internationaler Einsatz.

79. Wird im Falle des internationalen Einsatzes des E-Geld-Systems hinsichtlich der organisatorischen und technischen Systemsicherheit in den betreffenden Ländern auf ein gegenüber dem nationalen System adäquates Sicherheitsniveau geachtet? Existieren für diesen Zweck entsprechende Abnahme-/Freigabe- und Überprüfungsverfahren?

Anhang 1: Mindestinhalt des Systembeschreibung

Bitte um Beschreibung des E-Geldsystems nach folgender Systematik⁷:

1. Allgemeine Beschreibung des E-Geld-Systems

- 1.1. Systemfunktionen
 - 1.1.1. Anwendung und Systemfunktionen
 - 1.1.2. Transaktionsabläufe
 - 1.1.3. Rollen und Verantwortungen aller Beteiligten
- 1.2. Einsatzumgebung
 - 1.2.1. Sicherheitsaspekte der Einsatzumgebung der zentralen Komponenten
 - 1.2.2. Sicherheitsaspekte der Einsatzumgebung im Feld
 - 1.2.3. Abnahme-, Inbetriebnahme- und Einsatzbedingungen
- 1.3. Settlementverfahren
- 1.4. Umgang mit finanziellen Risiken und Festlegung der Verantwortlichkeiten
- 1.5. Gewährleistung eines einheitlichen Sicherheitsniveaus bei internationalem Einsatz

2. Beschreibung des Sicherheitskonzeptes

- 2.1 Sicherheitsziele
- 2.2. Sicherheitsmaßnahmen seitens des Betreibers
 - 2.2.1. Organisatorische Sicherheitsmaßnahmen
 - Sicherheitsorganisation des Betreibers, Verantwortlichkeiten
 - infrastrukturelle Sicherheitsmaßnahmen
 - 2.2.2. IT-technische Sicherheitsmaßnahmen
 - Identifikation und Authentisierung
 - Berechtigungssystem
 - Kryptokonzept
 - Systemintegrität
 - 2.2.3 Sicherheit in der Entwicklung, Produktion und Inbetriebnahme
 - Konfigurationskontrolle
 - Sicherheit beim Entwickler
 - Sicherheit in der Produktion
 - Test-, Abnahme- und FreigabeprozEDUREN
 - Sicherheit bei Initialisierung und Personalisierung
 - Installations- und Inbetriebnahmevorschriften für Systemkomponenten
 - Vorschriften zur Außerbetriebnahme von Systemkomponenten
- 2.3. Sicherheitsmaßnahmen seitens der Teilnehmer
 - geforderte Sicherheitsorganisation, Verantwortlichkeiten
 - infrastrukturelle Sicherheitsmaßnahmen
 - Monitoring der Teilnehmer durch den Betreiber hinsichtlich Einhaltung der Richtlinien (inklusive allfälliger Maßnahmen bei Regelverstößen)

⁷ Die Beschreibungen von funktionalen, topologischen und transaktionsablaufbezogenen Zusammenhängen sind nach Möglichkeit mit grafischen Übersichten zu unterlegen.

2.4. Sicherheitsvorschriften an die Endkunden

3. Beschreibung der Business Continuity Planung (BCP)

3.1 Service Level im Normalbetrieb

- Betriebs- und Cut-Off-Zeiten
- Zeitpunkt der Finalität
- angestrebte Verfügbarkeit
- durchschnittliche Transaktionsdauer

3.2 Datensicherungskonzept

3.3. Ausweichplanung

3.4 Maßnahmen im Fehler- oder Katastrophenfall

- Notfallplanung und Notlaufmaßnahmen
- Datenwiederherstellung
- Änderung der Betriebszeiten
- Wiederanlaufplanung

3.5 Verantwortlichkeiten für die BCP

3.6 Tests

3.7 Aktualisierung der BCP

Anhang 2: Informationen an Teilnehmer und Endkunden

Bitte um Angabe welche der nachfolgenden Informationen an Teilnehmer und Endkunden übermittelt werden sowie die Form von deren Übermittlung.

Informationen an Teilnehmer

1. Service Level des Systems
 - Betriebs- und Cut-Off-Zeiten
 - Zeitpunkt der Finalität
 - angestrebte Verfügbarkeit
 - durchschnittliche Transaktionsdauer
 - Notlaufmaßnahmen im Fehler- und Katastrophenfall (inklusive möglicher Änderungen von Betriebszeiten)
2. Kontaktdaten
3. Information über allfällige, mit der Teilnahme verbundene IT-Risiken
4. Anweisungen für den sicheren Umgang mit dem System und für das Verhalten in Ausnahmefällen
 - Anforderungen hinsichtlich der Aufstellung der Systemkomponenten
 - bauliche und infrastrukturelle Vorkehrungen
 - Kommunikationsverbindungen
 - Installation, Administration, Wartung
 - organisatorische Sicherheitsanforderungen
 - Nominierung von Verantwortlichen/Ansprechpartnern
 - Berechtigungsvergabe
 - Zeitpunkte und Umfang der Protokollierung, Auswertung von Protokollen, Aufbewahrungsfristen
 - Key-Management
 - Umgang mit Sicherheitsmodulen
 - Benutzerdokumentation
 - Bedienung des Systems im Normalbetrieb
 - Verhalten im Falle von Betriebsstörungen oder (tatsächlichen oder vermuteten) Angriffen auf das System
5. Haftung bei Missbrauch oder Fehlbedienung

Informationen an Endkunden

- Richtlinien zur sicheren Handhabung der Elektronische Geldbörse
- Limits, Gültigkeitsdauer und Rücktauschmöglichkeit des EV
- Rechte, Pflichten und Haftung des Endkunden