24.6.2016

# Fragen und Antworten

**zu den**

# Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSI)

Veröffentlicht mit BaFin-Rundschreiben Nr. 4/2015 vom 5. Mai 2015

## 1. Allgemeines

### *1a) Ab wann gelten die Mindestanforderungen?*

Die Mindestanforderungen gelten seit Veröffentlichung des Rundschreibens, d. h. seit dem 5. Mai 2015. Den Instituten wurde eine 6-monatige Übergangsfrist eingeräumt, d. h. die Institute müssen seit dem 5. November 2015 mit Prüfungen der Bankenaufsicht rechnen.

### *1b) Wie verbindlich sind die Anforderungen?*

Im vorliegenden Rundschreiben wird im Wesentlichen der Terminus „sollte" verwendet. Dieser ist als grundsätzlich umzusetzende Anforderung zu interpretieren.

### *1c) Müssen alle Anforderungen im genauen Wortlaut erfüllt werden?*

Gibt das Rundschreiben ein Ergebnis vor, so kann dieses durch verschiedene Mittel erreicht werden. Grundsätzlich bestehen daher mehrere Möglichkeiten, wie eine Anforderung erfüllt werden kann.

### *1d) Gelten die Anforderungen nur für deutsche Kreditinstitute?*

Nein, die Europäische Bankenaufsicht (EBA) setzt die „Guidelines on the security of internet payments"[1] europaweit um. Zuständig für die jeweilige nationale Umsetzung sind die jeweils zuständigen nationalen Bankaufsichtsbehörden. Als Frist für die Implementierung der Guidelines in das jeweilige nationale Recht hat die EBA den 1. August 2015 gesetzt. Aufgrund des BaFin-Rundschreibens müssen deutsche Zahlungsdienstleister erst ab dem 5. November 2015 mit Prüfungen der Bankenaufsicht rechnen.

### *1e) Gelten die Anforderungen auch für „Dritte Zahlungsdienstleister"?*

Die MaSI sind auf sogenannte „Dritte Zahlungsdienstleister" nicht anwendbar, da diese heute noch nicht vom Zahlungsdienstaufsichtsgesetz gemäß der EU-Zahlungsdiensterichtlinie von 2007[2] (PSD1) erfasst werden.

Aufsichtsrechtliche Anforderungen an dritte Zahlungsdienstleister werden aber nach Umsetzung der Zweiten EU-Zahlungsdiensterichtlinie[3] (PSD2) gelten (voraussichtlich ab 13. Januar 2018). Dritte Zahlungsdienste werden laut PSD2 sein

- Zahlungsauslösedienste, über die Nutzer Internet-Zahlungen via Online-Banking auslösen lassen können,
- Kontoinformationsdienste, mit deren Hilfe Nutzer Informationen über Konten abrufen können, die sie bei verschiedenen Banken und Zahlungsinstituten führen, sowie
- Herausgeber von Zahlungsinstrumenten, die beispielsweise Karten herausgeben, ohne kontoführender Zahlungsdienstleister zu sein.

Gehen kontoführende Zahlungsdienstleister zum Zwecke der Funktionsauslagerung Verträge mit „Dritten Zahlungsdienstleistern" ein und betrifft die Auslagerung die Sicherheit von Internetzahlungsdiensten, so haben die Institute die aufsichts-

---

[1] siehe http://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments

[2] RICHTLINIE 2007/64/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 13. November 2007 über Zahlungsdienste im Binnenmarkt

[3] siehe u. a. http://europa.eu/rapid/press-release_IP-15-4916_de.htm?locale=en

rechtlichen Anforderungen nach Nr. II 4.7 der MaSI, sowie die allgemeinen aufsichtsrechtlichen Anforderungen an die Geschäftsorganisation zu beachten (insbesondere AT 7.2 und AT 9 MaRisk).

### *1f) Wie sollen die Kreditinstitute mit Widersprüchen zwischen den Mindestanforderungen und der PSD2 umgehen?*

Dritte Zahlungsdienstleister werden von den Mindestanforderungen an die Sicherheit von Internetzahlungen nicht erfasst (s. o.). Deshalb würde z. B. die Umsetzung einer sicheren Ende-zu-Ende-Verschlüsselung zwischen Kunde und Zahlungsdienstleister, wie in Anforderung Nr. II.11.2 gefordert, Drittdienste nicht berücksichtigen müssen. Inwieweit auch dritte Zahlungsdienstleister einbezogen werden und in welcher Art und Weise Zahlungsdienstleister Anpassungen an den technischen Verfahren vornehmen müssen, wird im Wesentlichen von den Ergebnissen der Regulierungsstandards abhängen, die die EBA nach Artikel 98 PSD2 zu erarbeiten hat.

Vor dem 12. Januar 2016 schon aktive dritte Zahlungsdienstleister können ihre Dienste gemäß der PSD2 bis zum Ende der technischen Umsetzungsfrist wie bisher ausüben und dürfen bis dahin nicht auf die noch zu spezifizierende Schnittstelle für Drittdienste gezwungen werden (Artikel 102 (5) PSD2[4]). Die Anpassung oder Änderung von Sicherheitsverfahren für die Authentifizierung von Kunden durch kontoführende Zahlungsdienstleister unter Berücksichtigung der Sicherheitslage und der notwendigen technologischen Weiterentwicklung gemäß dem Stand der Technik ist in jedem Fall auch in der Zeit bis zum Ende der technischen Umsetzungsfrist möglich.

### *1g) Was ist unter dem Begriff „sensible Zahlungsdaten" zu verstehen?*

Der Begriff „sensible Zahlungsdaten" ist u. a. beim Zugriffschutz in Nr. II.7.2 und bei der Verschlüsselung in Nr. II.11.2 von entscheidender Bedeutung für die Reichweite der aufsichtsrechtlichen Anforderungen. Jedoch enthalten die MaSI selber keine Definition dieses Begriffes. Daher ist der Begriff nach Sinn und Zweck der EBA-Leitlinien auszulegen. Aus den Materialien der den MaSI zugrunde liegenden EBA-Leitlinien ist zu entnehmen, dass nur solche Daten gemeint sind, die für Betrugszwecke bei Internetzahlungen missbraucht werden können.

---

[4] Die Vorschrift lautet: „ Die Mitgliedstaaten untersagen juristischen Personen, die vor dem 12. Januar 2016 in ihrem Hoheitsgebiet Tätigkeiten von Zahlungsauslösedienstleistern und Kontoinformationsdienstleistern im Sinne dieser Richtlinie ausgeübt haben, nicht, dieselben Tätigkeiten in ihrem Hoheitsgebiet während der Übergangsfrist nach den Absätzen 2 und 4 im Einklang mit dem derzeit geltenden Rechtsrahmen weiterhin auszuüben.

Dazu gehören (i) Daten, die dazu dienen, eine Internetzahlung auszulösen, (ii) Daten, die für die Kundenauthentifizierung verwendet werden, (iii) Daten, die der Bestellung und Übermittlung von Zahlungsinstrumenten für die Durchführung von Internetzahlungen oder Kundenauthentifizierung dienen, sowie (iv) Daten, welche – wenn diese verändert werden – die Fähigkeit des jeweils legitimierten Kunden z.B. Internetzahlungen zu verifizieren oder den Online-Account zu kontrollieren, wie z.B. durch die Veränderung von weißen Listen oder Zahlungslimits, beeinflussen.

Ob es sich um sensible Daten handelt, ist immer im Einzelfall zu entscheiden und steht im Zusammenhang mit der jeweiligen Verwendung der jeweils betroffenen Daten. Auch wenn ein Datum einzeln als nicht sensibles Zahlungsdatum bewertet wird, kann die Kombination dieser Daten zu einer anderen Bewertung führen. Folgende Beispiele sollen dies verdeutlichen. Diese sind nicht abschließend.

a) Kombination von Daten mit Bezug zu der Auslösung von Internetzahlungen können z.B. die folgenden Daten darstellen:

    - Kontonummer bzw. Kundenkennung des Kunden, die in Kombination mit Passwort, PIN zur Anmeldung im Online-Banking genutzt werden
    - Karteninformationen (Kombination aus Kartennummer [PAN], Gültigkeitsdatum, Prüfnummern)

b) Daten, die für die Kundenauthentifizierung verwendet werden

    - Kundenkennnummer (z.B. Kundenummer, LogIn-Name) in Kombination mit
    - Passwörter, PINs, geheime Fragen, Zurücksetzungspasswörter
    - Telefonnummer
    - Zertifikate

c) Daten, die als Zieladresse für die Bestellung von Zahlungsinstrumenten zur Bezahlung und Kundenauthentifizierung verwendet werden und somit vor missbräuchlicher Änderung besonders zu schützen sind.

    - Postalische Adresse
    - Telefonnummer, E-Mail-Adresse

d) Daten, die z.B. Internetzahlungen verifizieren oder den Online-Account kontrollieren und – wenn sie verändert werden –die Möglichkeiten des jeweils legitimierten Kunden beeinflussen.

    - Weiße Listen, durch den Kunden definierte Zahlungslimits, etc.
    - Daten, wie in (a) bis (c) genannt, abhängig von der Anwendbarkeit und verwendeten Methode

Diese Bewertung bezieht sich nur auf den Begriff sensible Zahlungsdaten im Zusammenhang mit dem vorliegenden Rundschreiben. Der Begriff kann aber mit Blick auf andere Anforderungen z.B. im Zusammenhang mit dem Datenschutzrecht weiter verstanden werden.

Unabhängig von der Einordnung als sensible Zahlungsdaten sind für alle Daten die Schutzbedarfe bezogen auf ihre Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität festzustellen und daraus angemessene Maßnahmen abzuleiten und umzusetzen.

### *1h) Gibt es Anforderungen, die die Institute heute bereits aufgrund ähnlicher aufsichtsrechtlicher Anforderungen erfüllen müssen?*

Viele der Mindestanforderungen müssen die Institute heute bereits durch andere rechtliche und regulatorische Anforderungen abdecken (u. a. KWG, MaRisk, §§ 675c ff. BGB i.V.m. Art. 248 EGBGB, §§ 13 Abs. 7 TMG i.V.m. §§ 675m Abs. 1 Satz 1 Nr. 1 BGB). Hinzu kommen Archivierungspflichten gemäß GoBD[5] oder Sicherheits-Standards, die dem heutigen Rechenzentrums-Betrieb zugrunde liegen (u. a. ISO 27001, BSI-Grundschutz). Auch finden sich im Datenschutzrecht Anforderungen. Zum Beispiel müssen bei der Erhebung, Verarbeitung und Nutzung von sensiblen Zahlungsdaten – stellen diese zugleich auch personenbezogene Daten dar – technische und organisatorische Maßnahmen (§ 9 BDSG) getroffen werden. Insofern sind viele der genannten Anforderungen nicht neu, sondern gelten zumindest in ähnlicher Form bereits heute. Allerdings ist zu beachten, dass die bisher geltenden Vorgaben meist allgemeiner Natur sind, die Anforderungen an sichere Internetzahlungen dagegen aber im Kontext des jeweiligen konkreten Internetzahlungsdienstes erfüllt sein müssen.

### *1i) Welchen Einfluss haben die Mindestanforderungen auf aufsichtsrechtliche Anforderungen für Internet-Zahlungen, die die Institute heute bereits erfüllen müssen?*

Die bisherigen MaRisk-Anforderungen, die über die Mindestanforderungen hinausgehen, gelten unverändert weiter. Auch alle sonstigen rechtlichen und regulatorischen Anforderungen, die heute schon für Internetzahlungen gelten (z. B. zum Datenschutz), gelten unverändert weiter.

---

[5] Die „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff" (GoBD) regeln die Aufbewahrung von handelsrechtlich und steuerrechtlich relevanten Daten und Dokumenten in elektronischer Form. Die GoBD wurden durch Schreiben des Bundesfinanzministeriums am 14. November 2014 (Aktenzeichen V A 4 - S 0316/13/10003 | DOK 2014/0353090) publiziert. Diese GoBD sind seit 1. Januar 2015 gültig.

### *1j) Welchen Stellenwert hat der Assessment Guide der EZB im Rahmen der Prüfung?*

Die EZB hat auf ihrer Internetseite einen Leitfaden zur Beurteilung der Sicherheit von Internetzahlungen (Assessment Guide) veröffentlicht, den das SecuRePay Forum erarbeitet hat. Dieser Leitfaden richtet sich nicht an die Institute, sondern an die Aufseher. Er stellt jedoch keine Auslegung der Mindestanforderungen an die Sicherheit von Internetzahlungen durch die Aufsicht dar und ersetzt auch nicht eigene Überlegungen der Aufseher. Maßgeblicher Regelungstext bleibt das Rundschreiben. Im Zweifel wird die BaFin also stets auf dieser Grundlage entscheiden.

### *1k) Werden sich durch die geänderte Zahlungsdiensterichtlinie (PSD2) Änderungen an den MaSI ergeben?*

Im Internet-Zahlungsverkehr kommen durch die bis Ende 2017 in nationales Recht umzusetzenden PSD2 zahlreiche Neuerungen auf Zahlungsdienstleister, Online-Händler, Kunden und weitere Marktteilnehmer zu. In der PSD2 ist vorgesehen, dass die EBA auf Grundlage der PSD2 überarbeitete technische Regulierungsstandards erlassen wird, insbesondere zu Detailfragen der Kundenauthentifizierung, der sicheren Kommunikation sowie zum Meldewesen.

Die MaSI haben daher Übergangscharakter. Die Aufsicht erwartet jedoch von den Zahlungsdienstleistern, dass sie sich durch die konsequente Umsetzung der MaSI rechtzeitig fit für die Welt der PSD2 machen. Änderungen, die sich bei der Erarbeitung der technischen Regulierungsstandards der EBA ergeben können, sind dabei als Projektrisiken zu berücksichtigen.

## 2. Betroffene Zahlungsdienste

### *2a) Welche kreditwirtschaftlichen Anwendungen sind von den Anforderungen umfasst?*

Gemäß Rundschreiben unterliegen die folgenden Internet-Zahlungsdienste den Mindestanforderungen:

- *"[Karten] die Ausführung von Kartenzahlungen im Internet einschließlich virtueller Kartenzahlungen, sowie die Registrierung von Kartenzahlungsdaten zur Nutzung in "elektronischen Geldbörsen" (im englischen Original „Wallets"):* Hierunter sind insbesondere Kreditkartenzahlungen im Internet zu verstehen. Sofern in Deutschland Zahlungen mit Debitkarten, Wallets, virtuellen Karten oder wieder aufladbaren, kontobezogenen Prepaidkarten im Internet angeboten werden, unterliegen auch diese den Mindestanforderungen.

- *„[Überweisungen] die Durchführung von Überweisungen im Internet"*: Hiermit werden die webbasierten Online-Banking-Anwendungen der Institute adressiert. Die Anforderungen gelten jedoch nur für diejenigen Online-Banking-Geschäftsvorfälle, bei denen Zahlungen ausgeführt werden, d. h. neben Standard-Überweisungen bspw. auch terminierte Überweisungen, Sammelüberweisungen und Daueraufträge. Auch wenn bspw. Online-Brokerage (s. a. „Gelten die Anforderungen auch für Online-Broker?") nicht vom Anwendungsbereich dieses Rundschreibens erfasst ist, so sollte auch für diesen Dienst ein entsprechend hohes Niveau an IT-Sicherheit gewährleistet werden.

- *„[elektronische Einzugsermächtigung] die Erteilung und Änderung elektronischer Einzugsermächtigungen":* Die in Deutschland von Online-Händlern verwendeten *„Internetlastschriften"* sind nicht von den MaSI betroffen (näheres dazu unten), die Erteilung von Lastschriftmandaten per Online-Banking („E-Mandat") ist dagegen erfasst (s. a. 2b "Unterliegen auch Internet-Lastschriften den Anforderungen?").

- *„[E-Geld] die Übertragung von elektronischem Geld zwischen zwei E-Geld-Konten über das Internet":* Hiermit ist insbesondere das Bezahlen mit der GeldKarte/girogo im Internet umfasst.

### *2b) Unterliegen auch von Online-Händlern genutzte „Internet-Lastschriften" den Anforderungen?*

Lastschriften unterliegen nur dann den Mindestanforderungen, wenn bei deren Mandatserteilung per Internet der kontoführende Zahlungsdienstleister des Zahlers (Zahlstelle) beispielsweise durch Nutzung des Online-Banking für den Autorisierungsprozess unmittelbar beteiligt ist (sogenanntes „E-Mandat", vgl. dazu auch das EPC-Regelwerk zu SEPA-Basislastschriften zum Einsatz von „E-Mandaten"). In Deutschland wird aber bislang das Lastschriftmandat des Zahlers im E-Commerce ausschließlich im Verhältnis zwischen Online-Händler und Kunde ausgetauscht, ohne das bei diesem Vorgang die Zahlstelle involviert ist. In diesem Fall liegt mangels Beteiligung der Zahlstelle kein „E-Mandat" vor. Im Bereich der deutschen Kreditwirtschaft werden E-Mandat-Lösungen bislang noch nicht angeboten.

Zu beachten ist ferner, dass die Einreichung von Lastschriftdateien beim kontoführenden Zahlungsdienstleister nicht den Mindestanforderungen unterliegt. Die Freigaben regeln das Institut bzw. die SRZ- oder EBICS-Bedingungen.

### *2c) Gelten die Anforderungen auch für Online-Broker?*

Online-Brokerage ist vom Anwendungsbereich des Rundschreibens ausgeschlossen. Insofern unterliegt der Kauf oder Verkauf von Wertpapieren, die über einen Online-Broker durchgeführt werden, nicht den Mindestanforderungen. Auch wenn

Online-Brokerage nicht vom Anwendungsbereich dieses Rundschreibens erfasst ist, so sollte auch für diesen Dienst ein entsprechend hohes Niveau an IT-Sicherheit gewährleistet werden. Davon getrennt zu betrachten sind Überträge finanzieller Mittel im Rahmen eines Kaufs oder Verkaufs von Wertpapieren oder der Gutschrift von Zins- oder Dividendenzahlungen zwischen einem Konto des Online-Brokers und einem bei einem anderen Institut geführten Referenzkonto. Im Regelfall kann hier gemäß Anforderung II.7.1 der im ersten Spiegelstrich genannte Ausnahmetatbestand in Anspruch genommen werden, da Zahlungsab- und -eingänge auf ein bei einem Online-Broker geführtes Konto standardmäßig nur auf vom Kunden im Vorfeld festgelegte Konten („Whitelist") möglich sind.

### *2d) Ist auch Telefon-Banking von den Anforderungen umfasst?*

Das Telefon-Banking stellt keinen Internet-Zahlungsdienst im Sinne des Rundschreibens dar. Explizit ausgeschlossen sind z. B. Zahlungen, die über telefonische Bestellung oder Voicemail angewiesen werden.

Allerdings sind die Institute bereits auf Grundlage der MaRisk verpflichtet, Risikoanalysen für die angebotenen Dienste zu erstellen, auch wenn diese nicht direkt in den Anwendungsbereich der MaSI fallen.

### *2e) Inwieweit sind Zahlungen über Finanzverwaltungsprogramme betroffen?*

Die MaSI beziehen sich auf die Kommunikation zwischen einem Web-Server und einem Kunden-Browser (browsergestütztes Online-Banking). Folglich sind Zahlungen mittels vom Kunden eingesetzter Online-Banking-Softwareprodukte, die über den FinTS- oder EBICS-Standard mit dem Kreditinstitut kommunizieren, nicht von den MaSI erfasst. Allerdings sind die Institute bereits auf Grundlage der MaRisk verpflichtet, Risikoanalysen für die angebotenen Dienste zu erstellen, auch wenn diese nicht direkt in den Anwendungsbereich der MaSI fallen.

### *2f) Sind auch Zahlungsverkehrs-Standards für Firmenkunden („Electronic Banking") von den Anforderungen erfasst?*

Die Bestimmungen des Rundschreibens finden auf Zahlungsdienstleister i.S.d. § 1 Abs. 1 ZAG Anwendung, die Zahlungsdienste im Massenzahlungsverkehr über das Internet sowohl für Verbraucher als auch für Unternehmen anbieten. Die in Rede stehenden Bestimmungen setzen als offizielle Übersetzung die Guidelines on the security of internet payments der EBA als Rundschreiben um. Die EBA-Leitlinien basieren auf den Vorschriften der Richtlinie 2007/64/EG2 (PSD1). Gem. Artikel 2 Abs. 1 der PSD1 gilt die PSD für Zahlungsdienste, die innerhalb der Gemeinschaft geleistet werden. Zahlungsdienste richten sich an Zahlungsdienstnutzer. Zahlungsdienstnutzer wird in Artikel 4 Nr. 10 PSD1 wie folgt definiert:

,,Zahlungsdienstnutzer [ist] eine natürliche oder juristische Person, die einen Zahlungsdienst als Zahler oder Zahlungsempfänger oder in beiden Eigenschaften in Anspruch nimmt."

Demzufolge fallen sowohl Verbraucher als auch Unternehmern in den Anwendungsbereich der PSD1 und damit auch in den des Rundschreibens.

Das Rundschreiben findet gem. Titel I Nr. 11 aber nicht auf Zahlungsvorgänge, die durch ein Unternehmen über dedizierte Netzwerke vorgenommen werden, Anwendung. Unter einem dedizierten Netzwerk ist z.B. das SWIFT-Netz zu verstehen.

Zahlungsverkehrsstandards für den Firmenkundenbereich, wie insbesondere E-BICS, sind nur dann von den Mindestanforderungen an die Sicherheit von Internet-Zahlungen erfasst, wenn sie über ein Web-Portal abgewickelt werden. Werden kundenseitig Electronic-Banking-Softwareprodukte verwendet, die über eine direkte Schnittstelle zum Server verfügen, sind diese Zahlungskanäle von der Regulierung ausgenommen. Allerdings sind die Institute bereits auf Grundlage der MaRisk verpflichtet, Risikoanalysen für die angebotenen Dienste zu erstellen, auch wenn diese nicht direkt in den Anwendungsbereich der MaSI fallen.

### *2g) Sind auch mobile Zahlungen betroffen?*

Mobile Zahlungen sind nur dann im Geltungsbereich des Rundschreibens, wenn sie browser-basiert erfolgen. Dagegen sind Zahlungen unter Nutzung einer vom Kunden eingesetzten „Banking-App", die über eine direkte Schnittstelle zum Server verfügen, nicht erfasst. Allerdings sind die Institute bereits auf Grundlage der MaRisk verpflichtet, Risikoanalysen für die angebotenen Dienste zu erstellen, auch wenn diese nicht direkt in den Anwendungsbereich der MaSI fallen.

### *2h) Gelten die Anforderungen auch für Kreditinstitute, die kein Retail-Geschäft betreiben?*

Die Bestimmungen des Rundschreibens finden auf Zahlungsdienstleister i.S.d. § 1 Abs. 1 ZAG Anwendung, die Zahlungsgeschäfte im Massenzahlungsverkehr über das Internet sowohl für Verbraucher als auch für Unternehmen anbieten. Die Mindestanforderungen richten sich an alle Zahlungsdienstleister. Dabei spielt es keine Rolle, ob es sich um Kreditinstitute mit oder ohne Publikumsverkehr (z. B. Förderbanken) handelt. Das Rundschreiben findet auch Anwendung auf Kreditinstitute ohne Publikumsverkehr, welche die relevanten Zahlungsdienste im Internet ausschließlich in sehr begrenzter Anzahl für Zahlungskonten von Mitarbeitern (Mitarbeiterkonten) anbieten. Auf die Anzahl der Zahlungskonten kommt es für die Anwendbarkeit des vorliegenden Rundschreibens nicht an.

## 3. Schwerwiegende Zahlungssicherheitsvorfälle

### *3a) Wie ist ein schwerwiegender Zahlungssicherheitsvorfall definiert?*

*Als „schwerwiegender Zahlungssicherheitsvorfall"* wird gemäß Titel I, Ziffer 12 des Rundschreibens ein Vorfall bezeichnet, der wesentliche Auswirkungen auf die Sicherheit, Integrität oder Kontinuität der Zahlungssysteme des Zahlungsdienstleisters und/oder die Sicherheit sensibler Zahlungsdaten oder -mittel hat oder haben könnte. Bei der Beurteilung der Wesentlichkeit sollte die Anzahl der potenziell betroffenen Kunden, der Risikobetrag und die Folgen für andere Zahlungsdienstleister oder sonstige Zahlungsinfrastrukturen berücksichtigt werden

### *3b) Wann ist ein Zahlungssicherheitsvorfall als schwerwiegend anzusehen und ab wann ist zu melden?*

Als schwerwiegend ist ein Zahlungssicherheitsvorfall dann zu betrachten, wenn die Verfügbarkeit, Integrität, Vertraulichkeit oder Authentizität von IT-Systemen, Anwendungen oder Daten mit einem hohen oder sehr hohen Schutzbedarf verletzt oder beeinträchtigt wird.

Beim Ausfall oder Teilausfall von bankfachlichen Prozessen ist die Meldung dann abzugeben, wenn erkennbar ist, dass der Ausfall oder Teilausfall eine Stunde überschreiten wird.

Als Beispiele für schwerwiegende Zahlungssicherheitsvorfälle nennt die BaFin im Anschreiben zum MaSI-Rundschreiben:

- Ausfälle oder Teilausfälle der nachgenannten bankfachlichen Prozesse über einen Zeitraum von mehr als einer Stunde:
    - Bargeldversorgung
    - Jeglicher Zahlungsverkehr einschließlich Kartenzahlung
    - Online-Banking einschließlich Mobile-Banking
- Vorfälle, die zu einer Verletzung der Vertraulichkeit analog § 42a BDSG geführt haben;
- Vorfälle, die zu signifikanten Reputationsschäden führen können und
- Vorfälle, die vom Institut als Notfall gewertet werden und bei denen definierte Notfallmaßnahmen zum Einsatz kommen.

***Hinweis:*** *Internetzahlungen dienen unmittelbar dem unbaren und mittelbar dem baren Liquiditätsfluss. Aufgrund dieses Zusammenhangs ist die Einbeziehung der Bargeldversorgung in die Anforderungen an Internetzahlungen konsequent. Die*

*strikte und risikounabhängige Festlegung auf Zeiträume von mehr als einer Stunde führt zu einer verhältnismäßigen Ausgestaltung der Meldepflichten. Denn in der Regel führen Ausfälle für Zeiträume unterhalb einer Stunde nicht zu einem schwerwiegenden Sicherheitsvorfall.*

### *3c) Welche Vorfälle sind nicht als schwerwiegende Zahlungssicherheitsvorfälle anzusehen?*

Zeiten der Nichtverfügbarkeit, die durch systembedingte, geplante Prozesse bedingt sind (z. B. angekündigte Releasewechsel oder das Befüllen von Geldautomaten), gehören nicht zu den meldepflichtigen schwerwiegenden Sicherheitsvorfällen. Liegt eine Nichtverfügbarkeit vor, die nicht durch systembedingte, geplante Prozesse bedingt ist (s.o.), ist auch dann von einem schwerwiegenden Zahlungssicherheitsvorfall auszugehen, wenn die Kunden bei Nichtverfügbarkeit eines Internetzahlungsdienstes die Möglichkeit haben, andere Vertriebskanäle des Zahlungsdienstleisters zu nutzen (z. B. Einreichung von Überweisungen per Zahlungsträger bei Nichtverfügbarkeit des Online-Banking).

### *3d) An wen sind schwerwiegende Zahlungssicherheitsvorfälle zu melden?*

Gemäß Nr. 3.2 der Mindestanforderungen sind schwerwiegende Zahlungssicherheitsvorfälle ggf. sofort an die zuständigen Aufsichts- und Datenschutzbehörden zu melden. Hierbei handelt es sich um die BaFin, die Bundesbank sowie die jeweils zuständige Datenschutzbehörde. Für die Meldung an die BaFin sind die Meldebögen zu verwenden, welche auf der BaFin-Homepage zu finden sind. Bei Meldungen an die Datenschutzbehörde ist § 42a Bundesdatenschutzgesetz zu beachten.

Hinweise zum Ausfüllen und zur Übersendung der Meldung an die BaFin sind der Anlage zum Meldeformular (Formular-Version: 1.0 Nov 2015) zu entnehmen.

Das Meldeverfahren wird künftig auf eine elektronische Einreichung umgestellt.

### *3e) Kann die Meldung auch durch einen Dritten erfolgen?*

Ausführungen hierzu sind der Anlage zum Meldeformular (Formular-Version: 1.0 Nov 2015) zu entnehmen.

## 4. Starke Kundenauthentifizierung

### *4a) Erfüllen die heutigen kreditwirtschaftlichen Authentisierungsverfahren im Online-Banking die Anforderungen an starke Kundenauthentifizierung?*

Inwieweit ein bestimmtes Verfahren die Anforderungen an starke Authentifizierung gemäß Nr. II.7.1 der MaSI erfüllt, ist am konkreten Einzelfall zu bestimmen. Die in der deutschen Bankenlandschaft eingesetzten Authentisierungsverfahren basieren grundsätzlich auf den beiden geforderten Elementen Wissen und Besitz. Exemplarisch sei hier auf die von der Deutschen Kreditwirtschaft eingesetzten Verfahren chipTAN und mobileTAN eingegangen:

Den Faktor *Wissen* bildet sowohl bei chipTAN als auch bei mobileTAN die Online-Banking-PIN ab. Diese entspricht den Forderungen (*„etwas, das nur der Nutzer weiß, z. B. ein statisches Passwort, ein Code, eine persönliche Identifikationsnummer*"). Der Faktor *Besitz* wird beim chipTAN-Verfahren durch die Chipkarte und beim mobileTAN-Verfahren durch das Mobilfunkgerät (bzw. genauer die SIM-Karte) dargestellt. Auch dies genügt den Mindestanforderungen (*„etwas, das nur der Nutzer besitzt, z. B. ein Token, eine Smartcard, ein Mobiltelefon"*). Beide Elemente sind unabhängig voneinander, da bspw. ein Verlust der Chipkarte oder des Mobiltelefons nicht die Online-Banking-PIN offenlegt. Das Besitzelement ist auch in beiden Fällen nicht wiederverwendbar und nicht reproduzierbar, da die einmal erzeugte TAN nicht für andere Aufträge verwendbar ist. Zudem ist die zur TAN-Erzeugung benötigte Karte weder kopierbar noch fälschbar. Abschließend wird gefordert, dass die Authentifizierungsdaten bei der Übertragung durch Verschlüsselungsverfahren geschützt werden müssen. Dies wird bspw. dann erreicht, wenn während eines Dialoges derzeit durchgängig eine TLS 1.2-Absicherung erfolgt.

Es sei darauf hingewiesen, dass sich diese Einschätzungen im Zeitablauf und mit dem technischen Fortschritt ändern können.

Neben dem Einsatz von geeigneten Authentisierungsverfahren durch das Kreditinstitut ist es für die Sicherheit des Online-Banking und von Kartenzahlverfahren auch wichtig, dass der Kunde selber seine Sorgfaltspflichten in Bezug auf die Handhabung der ihm vom Kreditinstitut zur Verfügung gestellten Authentifizierungsinstrumente beachtet (vgl. auch § 675l Satz 1 BGB und Artikel 248 § 4 Absatz 1 Nr. 5 a) und d) EGBGB).

### *4b) Wie sind App-basierte Sicherungsverfahren in Bezug auf die starke Kundenauthentifizierung zu sehen?*

Viele Kreditinstitute bieten ihren Kunden für Smartphones und Tablets moderne App-basierte Sicherungsverfahren für das Online-Banking an. Auch hier liegt in der

Regel eine starke Kundenauthentifizierung vor. Denn hierbei wird die TAN über eine speziell gesicherte Internet-Verbindung empfangen. Diese Verfahren sind ähnlich zu bewerten wie das mobileTAN-Verfahren, d. h. der Faktor *Wissen* wird durch die Online-Banking-PIN abgebildet, den Faktor *Besitz* bildet das Smartphone bzw. Tablet. Beide Faktoren sind unabhängig voneinander. Allerdings gilt auch hier, dass nur auf Grundlage einer konkreten Implementierung überprüft werden kann, inwieweit ein bestimmtes Verfahren die Anforderungen an starke Authentifizierung erfüllt.

Besondere Sicherheitsrisiken bestehen dann, wenn das App-basierte Sicherheitsverfahren auf dem gleichen Gerät genutzt wird, wie das mobile Online-Banking.

Dem muss im Rahmen des Risikomanagements des Instituts besondere Rechnung getragen werden, damit dem Kunden keine Nachteile entstehen. Die Risiken sind insbesondere durch Anwendung von technischen und organisatorischen Maßnahmen zu minimieren. Dies kann z.B. durch die Anwendung der folgenden Maßnahmen geschehen:

- Sandboxing/Nutzung von vertrauenswürdiger Anwendungsumgebung;
- Ausgiebige Prüfung von Software auf Manipulationsmöglichkeiten;
- Verwendung von Device-Identity-Lösungen;
- Ausschluss der Nutzung von Geräten, die „jail-broken" sind;
- Aufklärung des Kunden über die etwaigen Risiken.

### *4c) Wie sind signaturbasierte Sicherungsverfahren in Verbindung mit einem Chipkartenleser in Bezug auf die starke Kundenauthentifizierung zu sehen?*

Auch signaturbasierte Sicherungsverfahren in Verbindung mit einem Chipkartenleser (Secoder) wie bspw. das HBCI-Verfahren werden von Kreditinstituten für das Online-Banking angeboten. Bei diesen Verfahren wird der Faktor *Wissen* durch die PIN für die Chipkartenanwendung abgebildet, den Faktor Besitz bildet die Chipkarte. Beide Faktoren sind unabhängig voneinander. Allerdings gilt auch hier, dass nur auf Grundlage einer konkreten Implementierung überprüft werden kann, inwieweit ein bestimmtes Verfahren die Anforderungen an starke Authentifizierung erfüllt.

### *4d) Welche Ausnahmen von der starken Kundenauthentifizierung sind in der Praxis anwendbar?*

In Ziffer II.7.1 des Rundschreibens sind in Bezug auf Überweisungen, E-Mandate und E-Geld-Zahlungen bestimmte Ausnahmen zur starken Kundenauthentifizierung formuliert, bei denen von geringen Risiken ausgegangen wird. Danach unterliegen im Online-Banking z.B. institutsinterne Umbuchungen zwischen Konten des

Kunden und Überweisungen an vertrauenswürdig eingestufte Begünstigte (gemäß „weißer Liste" des Zahlers oder der Zahlstelle) nicht der Vorgabe der starken Authentifizierung.

In Ziffer II.7.8. des Rundschreibens ist für Kartenzahlungen geregelt, dass für Kleinbetragszahlungen i. S. der PSD1 bis 30 Euro[6] oder für Transaktionen mit niedrigem Risiko alternative Authentifikationsansätze in Betracht gezogen werden können.

### *4e) Muss auch für den Login-Prozess (bspw. beim Online-Banking) ein Verfahren mit starker Kundenauthentifizierung verwendet werden?*

Anforderung Nr. II.7 definiert, dass eine starke Kundenauthentifizierung für die Auslösung von Internetzahlungen und für den Zugang zu sensiblen Zahlungsdaten zum Einsatz kommen sollte. Werden durch das Login noch keine Internetzahlungen ausgelöst und auch kein Zugriff auf sensible Zahlungsdaten (bspw. die Online-Banking-PIN) ermöglicht, ist ein Login-Prozess beim Online-Banking auch ohne starke Kundenauthentifizierung möglich. Allerdings kann nur auf Grundlage einer konkreten Implementierung des Login-Prozesses überprüft werden, ob ein starke Kundenauthentifizierung erforderlich ist oder nicht.

### *4f) Müssen Transaktionsdaten in die starke Kundenauthentifizierung eingehen?*

Bei modernen Sicherungsverfahren insbesondere im Online-Banking gehen sicherheitsrelevante Transaktionsdaten (bspw. Betrag, Empfängerkontonummer) in den TAN-Generierungsprozess ein. Damit ist eine Verwendung der TAN für eine andere als die intendierte Zahlung ausgeschlossen. Diese Vorgehensweise ist kein verpflichtender Bestandteil der Vorgabe der starken Authentifizierung, findet sich aber im Rundschreiben als Empfehlung (BV 8). Hierbei ist zu berücksichtigen, dass im Rahmen der geänderten EU-Zahlungsdiensterichtlinie (PSD2) diese „Transaktionsbindung" eine verbindliche Vorgabe für Internetzahlungen wird. Neue Sicherungsverfahren sollten daher auf einer Transaktionsbindung beruhen.

---

[6] bzw. national abweichender Beträge für innerstaatliche Zahlungsvorgänge gem. Art 34 (2) der PSD1 bzw. § 675i BGB

### *4g) Was bedeuten die Anforderungen für die Herausgabe von Kreditkarten?*

Von den durch die Mindestanforderungen erfassten Kartenzahlungen im Internet kommt die Kreditkarte besonders häufig zum Einsatz. Für die Umsetzung der Anforderungen spielen die Rahmenbedingungen der einzelnen Kartenzahlungsverfahren (z. B. VISA, MasterCard) eine wesentliche Rolle.

Mit PCI DSS (Payment Card Industry Data Security Standards) werden durch die internationalen Kartenorganisationen bereits heute Anforderungen an die Sicherheit an Kartenherausgeber und -akzeptanten und deren Dienstleister gestellt. Durch die Mindestanforderungen ergeben sich weitere Aspekte, die neben dem Risikomanagement und der Informationspflicht insbesondere das Authentisierungsverfahren, welches innerhalb von 3D Secure zum Einsatz kommt, betreffen. Zur Umsetzung der Anforderungen an 3D Secure bedienen sich Kartenausgeber in der Regel technischer Dienstleister (z. B. Kartenprozessoren).

Die Registrierung von Karten in einer Wallet erfordert starke Kundenauthentifizierung. Virtuelle Karten, die im Internet ausgestellt werden, erfordern ebenfalls eine starke Kundenauthentifizierung.

### *4h) Was ist bei Kartentransaktionen im Internet zu beachten?*

Bei Einsatz von Karten internationaler Kartenorganisationen im Internet kann eine starke Authentifizierung nur im Rahmen des 3D-Secure-Verfahrens (z. B. von MasterCard/VISA) eingesetzt werden. Welches Authentifikationsverfahren der Karteninhaber dabei verwendet, entscheidet der Kartenherausgeber. Als Authentifikationsverfahren werden nach erfolgter Registrierung des Karteninhabers innerhalb einer sicheren Umgebung beispielsweise ein statisches Passwort, dynamisches Passwort/TAN per SMS („mobile TAN", zum Teil mit Verifikation der Mobilfunknummer) oder eine Push-Nachricht auf dem registrierten Mobilgerät des Karteninhabers eingesetzt. Für die Unterstützung der starken Kundenauthentifizierung bei Karten nach II.7.3 ist im 3D-Secure-Verfahren die Absicherung über ein statisches bzw. dynamisches Passwort über den Internet-Kommunikationskanal alleine nicht ausreichend (fehlender zweiter Faktor).

Allerdings kann der Kartenherausgeber die starke Authentifizierung nur anwenden, wenn 3D-Secure vom jeweiligen Händler unterstützt wird. Daher bestimmen die Ziffern II.7.3 und 7.4, dass der Zahlungsdienstleister lediglich die technischen Vorkehrungen für den Einsatz starker Kundenauthentifizierung treffen muss.

Acquirer als Zahlungsdienstleister, die gegenüber dem Händler abrechnen, müssen gemäß Anforderung Nr. II.7.5 von ihren Händlern den Einsatz einer starken Authentifizierung verlangen. Entscheidet sich der Händler aber gegen eine starke Authentifizierung, so kann der kartenherausgebende Zahlungsdienstleister den

Händler nicht zum Einsatz der starken Authentifizierung zwingen, da der kartenausgebende und der gegenüber dem Händler abrechnende Zahlungsdienstleister in der Regel nicht identisch sind.

Die Haftung für einen entstanden Schaden liegt gemäß den Systemregeln der internationalen Kartenorganisationen bei der Partei, die nur ein schwächeres Authentifizierungsverfahren unterstützt. Solche Zahlungen ohne 3D-Secure durch den Händler können durch den kartenausgebenden Zahlungsdienstleister genehmigt werden, sofern seine Risikopolitik dies zulässt. Eine Risikoprävention des kartenausgebenden Institutes wird hierbei immer vorausgesetzt.

### *4i) Welche Ausnahmen von der starken Kundenauthentifizierung sind in der Praxis für Kartenzahlungen im Internet anwendbar?*

Es gelten nach Ziffer II.7.5. Ausnahmen für Kleinbetragszahlungen sowie für Transaktionen, die bei einer Risikoanalyse, die auf im Vorfeld identifizierten Kategorien basiert, mit niedrigem Risiko bewertet werden.

### *4j) Welche Rolle spielen die internationalen Kreditkartenorganisationen für die Sicherheit von Kartenzahlungen?*

Die Kreditkartenorganisationen wie VISA und MasterCard unterliegen der Zahlungsverkehrsüberwachung durch das Eurosystem unter der Federführung der Europäischen Zentralbank. Sie legen die Regeln und technischen Standards für die Herausgabe und Abwicklung von Kartenzahlungen mit ihren Marken in den entsprechenden Einsatzbereichen (z. B. Internet) weltweit und national fest. Dazu zählen beispielsweise das 3D-Secure-Verfahren oder die Schnittstellen zum Austausch von Zahlungsdaten. Ein Karten-herausgebendes Institut kann daher die Anforderungen der MaSI nur im Rahmen der von den Systemen gesetzten Bedingungen erfüllen. Beispielsweise ist für Kreditkartenzahlungen momentan keine Ende-zu-Ende-Verschlüsselung zwischen Karteneinsatz im Internet und Kartenherausgeber vorgesehen, sondern stattdessen nach Stand der Technik eine Verschlüsselung zwischen den jeweils kommunizierenden Parteien (Punkt-zu-Punkt).