Bundesanstalt für
Finanzdienstleistungsaufsicht

BaFin

Sicherheit im Zahlungsverkehr einschließlich Meldewesen

PSD2-Infoveranstaltung 05.12.2017

Barbara Buchalik / Tobias Schmidt
BaFin BA 51

Was macht BA 51?

- **BaFin-weites Kompetenzreferat für Fragen der IT-Sicherheit bei beaufsichtigten Unternehmen**
  - Umsetzung PSD2 (soweit Fragen der IT-Sicherheit betroffen)
  - MaSI (inkl. Meldewesen)
  - Relevante Teile der MaRisk (insb. AT 7.2, AT 7.3)
  - BAIT
  - Umsetzung IT-Sicherheitsgesetz
  - Unterstützung der Institutsaufseher bei Fragen mit IT-Bezug (z.B. rund um das Thema Cloud Computing)

BaFin

EBA, NCA und RTS
SCA, AIS und TPP
PIS, API und PSU – was mach‘ ich nu?

Was sind die Themen?

- Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA) and Secure Communication (SC)
- Guidelines on Major Incident Reporting
- Guidelines on the Security Measures for Operational and Security Risks
- Guidelines on Fraud Reporting
- Ausblick

Welche Einschränkungen gelten?

BaFin

Stand von heute, vorbehaltlich:

- Veröffentlichung der finalen „RTS on SCA SC“ im EU-Amtsblatt
- Finale Versionen der einzelnen Leitlinien

BaFin

Communication Interface

RTS SCA SC
Communication Interface

BaFin

Zugang zum Zahlungskonto

- Für Zahlungsauslösedienste und Kontoinformationsdienste
  mit den Zugangsdaten des Kunden, die diesem vom kontoführenden Institut bereitgestellt wurden.
- Initiierung eines Zahlungsvorgangs
  Bereitstellung aller für die Initiierung eines Zahlungsvorgangs benötigten Informationen.
- Zugriff auf Zahlungskontoinformationen
  alle Informationen, die auch der Kunde selber beim Zugriff über die Kundenschnittstelle für dieses Zahlungskonto sieht.
- Bestätigung der Verfügbarkeit eines Geldbetrags
  aber **keine** Zahlungsgarantie.

RTS SCA SC
Communication Interface

BaFin

Identifizierung beim Zugriff auf ein Zahlungskonto

- Nutzung qualifizierter Zertifikate auf Basis der eIDAS Verordnung
- Beantragung bei einem qualifizierten Vertrauensdiensteanbieter
  - Es gelten die Regeln dieser Anbieter
- Zugang zum Zahlungskonto erfolgt aber mit den Zugangsdaten des Kunden

RTS SCA SC

Communication Interface

BaFin

```
<input type="password" class="text-left" required="required" id="pin"
name="pin" autocomplete="off" maxlength="8" tabindex="2" data-h5-
errorid="invalid-pin" value="" placeholder="PIN" pattern="[A-Za-z0-9]{5,8}">
</input>
```

Ist jetzt das Screen Scraping verboten?

JEIN

RTS SCA SC

Communication Interface

BaFin

Das kontoführende Institut muss einen PSD2-konformen Zugang zu den Online-Konten seiner Kunden bereitstellen:

- **Möglichkeit A:** Dediziertes Interface (API)
- **Möglichkeit B:** „Klassische" Online-Banking-Website plus

<u>Zugang nur über PSD2-konformes „Communication Interface"</u>

RTS SCA SC

Communication Interface

BaFin

Aber was ist ein PSD2-konformes „Communication Interface“?

Nicht funktionale <u>allgemeine</u> Anforderungen:

- Insbesondere Identifizierungsmöglichkeit für PIS/AIS/PIISP
- Sichere Kommunikation u.a. durch die Anwendung von Kommunikationsstandards
- Zurverfügungstellung von Testmöglichkeiten (inkl. Support) und Dokumentation sechs Monate vor Inkrafttreten der RTS oder sechs Monate vor Markteinführung – falls diese nach Inkrafttreten der RTS stattfindet

RTS SCA SC

Communication Interface

BaFin

Nicht funktionale Anforderungen für das <u>dedizierte Interface:</u>

- Gleiche Verfügbarkeits-, Performanz- und Supportlevel wie die Kundenschnittstelle
- Definieren von KPIs und Service-Levels, die mindestens denen der „klassischen" Online-Banking-Website entsprechen; dies betrifft sowohl Verfügbarkeit als auch die zur Verfügung gestellten Daten
- Umfassendes Monitoring durch kontoführendes Institut
- Verpflichtung zur Veröffentlichung von Statistiken zur Verfügbarkeit und Performanz auf der Webseite (alle zwei Wochen)

RTS SCA SC

Communication Interface

BaFin

Nicht funktionale Anforderungen für das <u>dedizierte Interface:</u>

- ASPSPs dürfen **<u>keine Hürden</u>** für PIS und AIS schaffen, wie z.B.:
  - „**preventing** the **use** of the **credentials**"
  - „**imposing redirection** to the ASPSP's authentication or other functions, requiring additional authorisations and registrations in addition to those"
  - „**requiring additional checks of the consent** given by PSU to providers of PIS and AIS"

RTS SCA SC

Communication Interface

BaFin

Wann müssen Notfallmaßnahmen („contingency measures“) für das dedizierte Interface Anwendung finden?

- „does not perform in compliance“
- „there is unplanned unavailibility or a system breakdown“

  → „when five consecutive requests for access to information […] are not replied to within 30 seconds“

RTS SCA SC

Communication Interface

BaFin

Was sind die Notfallmaßnahmen („contingency measures“) für das dedizierte Interface?

- Kommunikationspläne (Maßnahmen zur Wiederherstellung und Beschreibung der sofort zur Verfügung stehenden Alternativen)
- ASPSP, PIS und AIS haben Probleme unverzüglich den NCAs zu melden
- Möglichkeit der Nutzung der Kundenschnittstelle (Fall-Back-Mechanismus) mit der Möglichkeit zur Identifizierung

RTS SCA SC

Communication Interface

BaFin

Was ist der Fall-Back-Mechanismus?

- PIS und AIS haben die Möglichkeit, die Kundenschnittstelle, wenn dediziertes Interface nicht – wie vorgeschrieben – funktioniert, zu nutzen. **Aber nur wenn**
  - Implementierung von Maßnahmen, die den unerlaubten Zugriff auf, die Speicherung und die Verarbeitung von Daten verhindern
  - Weiterhin Erfüllen der Anforderungen aus Artikel 66 (3) und Artikel 67 (2) PSD2
  - Erfassung der Daten, auf die durch die Schnittstelle zugegriffen wird, um diese auf Anforderung den NCAs unverzüglich zu liefern
  - Begründung der Nutzung des Fall-Back-Mechanismus unverzüglich nach Aufforderung durch die NCAs; so auch gegenüber dem ASPSP

BaFin

Wann gilt dieser Fall-Back-Mechanismus nicht? Gibt es Ausnahmen?

- ASPSPs können, wenn die NCA sich mit der EBA abgestimmt hat, auf die Bereitstellung des Fall-Back-Mechanismus verzichten, wenn die dedizierte Schnittstelle
  - den Anforderungen entspricht
  - den Anforderungen entsprechend getestet wurde
  - zudem im Markt für mindestens 3 Monate getestet wurde
  - bei auftretenden Probleme unverzüglich wiederhergestellt wurde

RTS SCA SC
Communication Interface

BaFin

Kann die Ausnahme widerrufen werden?

- Ja, wenn die Anforderungen für die Ausnahme für mehr als zwei aufeinander folgende Wochen nicht mehr vorliegen.

Wer widerruft die Ausnahme?

- Die NCAs unter Mitteilung an die EBA.

Was ist dann zu tun?

- Die NCAs haben sicherzustellen, dass innerhalb von kürzester Zeit, aber vor Ablauf von zwei Wochen, die Anforderung an den Fall-Back-Mechanismus erfüllt werden.

RTS SCA SC

Communication Interface

BaFin

Die Rolle der NCAs

- **Überwachung der dedizierten Schnittstellen.**

  „Those interfaces, indicators and targets shall be monitored by the competent authorities and stress-tested."

- **Wie kann das aussehen?**

  „The Commision is promoting the set-up of a market group, composed of representatives from banks, PIS, AIS and PSU. This group will review the quality of dedicated communication interfaces. This follows up on the work carried out by the EURO Retail Payments Board on PIS."

BaFin

Strong Customer Authentication
(Starke Kundenauthentifizierung)

Art. 97 PSD2, § 55 ZAG (neu)

Starke Kundenauthentifizierung

BaFin

Wichtigste Änderungen gegenüber den Mindestanforderungen an die Sicherheit bei Internetzahlungen (MaSI):

- **Alle** elektronischen Zahlungen werden erfasst (z.B. auch am POS)
- Pflicht zur dynamischen Verknüpfung bei elektronischen Fernzahlungsvorgängen
- Die Ausnahmen von der SKA werden neu gefasst
  - Insbesondere: inhaltliche Anforderungen an die Transaktionsrisikoanalyse bei Kartenzahlungen im Internet

Starke Kundenauthentifizierung
Definition

BaFin

SKA ist eine Authentifizierung durch **zwei unabhängige**

Elemente der Kategorien:

- **Wissen** (etwas, das nur der Nutzer weiß),
- **Besitz** (etwas, das nur der Nutzer besitzt) oder
- **Inhärenz** (etwas, das der Nutzer ist)

Pflicht zur SKA ergibt sich direkt aus PSD2/ZAG (neu) .

Die „RTS on SCA" enthalten Detailvorschriften zur Ausgestaltung der SKA sowie die Ausnahmen von dieser Pflicht.

Starke Kundenauthentifizierung

Wann ist eine starke Kundenauthentifizierung erforderlich?

BaFin

SKA erforderlich, wenn der Zahler:

(1) online auf sein Zahlungskonto zugreift;

(2) einen elektronischen Zahlungsvorgang auslöst;

(3) über einen Fernzugang eine Handlung vornimmt, die das Risiko eines Betrugs im Zahlungsverkehr oder anderen Missbrauchs beinhaltet.

Starke Kundenauthentifizierung

Wann ist eine starke Kundenauthentifizierung erforderlich?

BaFin

Was ist mit Lastschriften?

- Lastschriften sind nicht erfasst. Die Zahlung wird hierbei durch den Zahlungsempfänger ausgelöst

Starke Kundenauthentifizierung

SKA mit „dynamischer Verknüpfung“

BaFin

Falls es sich bei (2) um einen elektronischen <u>Fern</u>zahlungsvorgang handelt:

- SKA erforderlich, die Elemente umfasst, die den Zahlungsvorgang dynamisch mit einem bestimmten Betrag und einem bestimmten Zahlungsempfänger verknüpfen
- Auswirkungen auf statische Verfahren wie die iTAN
- laut RTS ist es **nicht erforderlich**, dass der dynamische Authentifizierungscode direkt aus Betrag und Empfänger-IBAN erzeugt wird

Starke Kundenauthentifizierung

SKA mit „dynamischer Verknüpfung“

Was ist bei Sammelüberweisungen?

- Dynamische Verlinkung kann sich auf den Gesamtbetrag und die Gesamtheit der Empfänger beziehen (Art. 5 (3b))

Starke Kundenauthentifizierung
Ausnahmen

BaFin

Laut RTS:

- Zugang zu bestimmten Kontoumsätzen
  - Einschränkung: zwei(!) 90 Tage Fristen
- Vertrauenswürdige Empfänger (auf Liste)
- Wiederkehrende Zahlungen
- Zahlungen an mich selbst (beim selben ZDL)
- „Secure Corporate Payments“

Starke Kundenauthentifizierung
Ausnahmen

BaFin

Was sind „Secure Corporate Payments“?

- „Payment service providers shall be allowed not to apply strong customer authentication, in respect of **legal persons** initiating electronic payment transactions through the **use of dedicated payment processes** or **protocols** that are only made available to payers who are **not consumers**, where the competent authorities are satisfied that those processes or protocols guarantee at least **equivalent levels** of security to those provided for by Directive 2015/2366.”

Starke Kundenauthentifizierung

Ausnahmen

- **Fernzahlungsvorgänge**
  - maximal 30 Euro pro Zahlung
  - maximal 100 Euro kumulativ (alternativ: max. fünf Zahlungen)
- **Kontaktlose Zahlungen am POS**
  - maximal 50 Euro pro Zahlung
  - maximal 150 Euro kumulativ (alternativ: max. fünf Zahlungen)
- **Zahlungen von Verkehrs- oder Parkentgelten an „unbeaufsichtigten" Terminals**
  - keine quantitativen Grenzen

Starke Kundenauthentifizierung

Ausnahmen

BaFin

Transaktionsrisikoanalyse:

- ZDL kann je nach Risiko entscheiden, ob er SKA verlangt
- Zulässiger Höchstbetrag abhängig von Betrugsrate

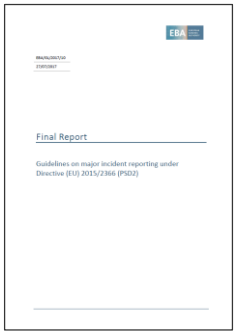
Höchst-betrag	Kartenbasierte Fernzahlungsvorgänge	Überweisungen
500 €	0,01 %	0,005 %
250 €	0,06 %	0,010 %
100 €	0,13 %	0,015 %

Starke Kundenauthentifizierung
Ausnahmen

Definition der Betrugsrate:

$$\frac{\text{Wert der betrügerischen Zahlungen der letzten 90 Tage}}{\text{Wert aller Zahlungen der letzten 90 Tage}}$$

- alle Zahlungen der betreffenden Kategorie, egal ob mit SKA oder nicht
- Rohwert der betrügerischen Zahlungen, unabhängig vom entstandenen Schaden
- Berechnung der Betrugsrate ist durch Wirtschaftsprüfer zu kontrollieren



Guidelines on Major Incident Reporting

(Meldung schwerwiegender Betriebs- und Sicherheitsvorfälle)

Art. 96 PSD2, § 54 ZAG (neu)

Major Incident Reporting

BaFin

Was ändert sich?

im Vergleich zu den „Mindestanforderungen an die Sicherheit von Internetzahlungen" (MaSI)

- Keine Beschränkung auf Internetzahlungen

  Schwerwiegende **Sicherheitsvorfälle** im Zahlungsverkehr sind zu melden

- Neue Meldeformulare: Standardisiertes Meldeverfahren auf Basis der Melde- und Veröffentlichungsplattform (MVP)

- Neues Bewertungsschema für Sicherheitsvorfälle

Major Incident Reporting

BaFin

Was ändert sich?

im Vergleich zu den „Mindestanforderungen an die Sicherheit von Internetzahlungen" (MaSI)

- Die BaFin muss maßgebliche Einzelheiten der Meldungen unverzüglich an die EBA und die EZB weiterleiten; bei Bedarf auch an andere deutsche Behörden.
- In bestimmten Fällen: Pflicht zur Benachrichtigung der Zahlungsdienstnutzer durch den Zahlungsdienstleister (vgl. § 54 Abs. 4 ZAG n.F.)

Major Incident Reporting
Definitionen

BaFin

Was ist ein Betriebs- oder Sicherheitsvorfall im Zahlungsverkehr?

"A singular event or a series of linked events unplanned by the payment service provider which has or will probably have an adverse impact on the integrity, availability, confidentiality, authenticity and/or continuity of payment-related services."
(Guidelines on major incident reporting under PSD2)

? **Wann ist ein solcher Vorfall schwerwiegend?**

Major Incident Reporting
Bewertungskriterien

BaFin

Quantitativ	Qualitativ
Betroffene Transaktionen	Hohe interne Eskalationsstufe (über Standardreporting hinaus)
Betroffene Kunden	Auswirkungen auf weitere Zahlungsdienstleister oder Infrastrukturen
Ausfallzeit	Reputationsschaden
Wirtschaftlicher Schaden	

Major Incident Reporting

Bewertungskriterien - Schwellenwerte

BaFin

1x Hoch

oder

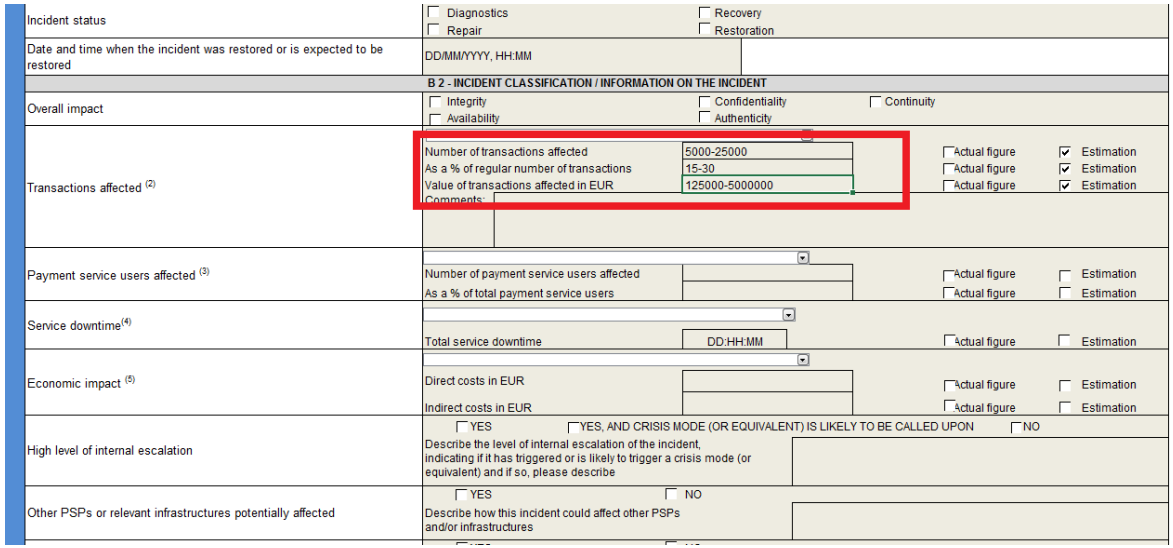
3 x Niedrig

Meldepflicht

Kriterium	Niedrige Schwelle	Hohe Schwelle
Betroffene Transaktionen	**> 10 % des üblichen Transaktionsvolumens und** **> EUR 100.000**	**> 25 % des üblichen Transaktionsvolumens oder** **> EUR 5.000.000**
Betroffene Kunden	**> 5.000 und** **> 10 % der Kunden des ZDLs**	**> 50.000 oder** **> 25 % der Kunden des ZDLs**
Ausfallzeit	**> 2 Stunden**	**-**
Wirtschaftlicher Schaden	**-**	**> max (0,1 % des Kernkapitals; EUR 200.000)** **oder** **> EUR 5.000.000**
Hohe interne Eskalationsstufe	**Ja**	**Ja, und interne Einstufung als "Krise"**
Auswirkungen auf weitere Zahlungsdienstleister oder Infrastrukturen	**Ja**	**-**
Reputationsschaden	**Ja**	**-**

Major Incident Reporting
Zukünftiger Meldeprozess

- Delegierte Meldung durch IT-Dienstleister möglich
- Konsolidierte Meldungen bei gleicher Ursache und Auswirkungen möglich



Incident status	☐ Diagnostics ☐ Repair	☐ Recovery ☐ Restoration	
Date and time when the incident was restored or is expected to be restored	DD/MM/YYYY, HH:MM		
B 2 - INCIDENT CLASSIFICATION / INFORMATION ON THE INCIDENT			
Overall impact	☐ Integrity ☐ Availability	☐ Confidentiality ☐ Authenticity	☐ Continuity
Transactions affected [2]	Number of transactions affected	5000-25000	☐ Actual figure ☑ Estimation
	As a % of regular number of transactions	15-30	☐ Actual figure ☑ Estimation
	Value of transactions affected in EUR	125000-5000000	☐ Actual figure ☑ Estimation
	Comments:		
Payment service users affected [3]	Number of payment service users affected		☐ Actual figure ☐ Estimation
	As a % of total payment service users		☐ Actual figure ☐ Estimation
Service downtime [4]	Total service downtime	DD:HH:MM	☐ Actual figure ☐ Estimation
Economic impact [5]	Direct costs in EUR		☐ Actual figure ☐ Estimation
	Indirect costs in EUR		☐ Actual figure ☐ Estimation
High level of internal escalation	☐ YES ☐ YES, AND CRISIS MODE (OR EQUIVALENT) IS LIKELY TO BE CALLED UPON ☐ NO		
	Describe the level of internal escalation of the incident, indicating if it has triggered or is likely to trigger a crisis mode (or equivalent) and if so, please describe		
Other PSPs or relevant infrastructures potentially affected	☐ YES ☐ NO		
	Describe how this incident could affect other PSPs and/or infrastructures		

Quelle: EBA Guidelines on Major Incident Reporting

Major Incident Reporting
Klarstellungen

BaFin

24/7 Reporting?

- JEIN!
- Vorfälle sind grundsätzlich **vier Stunden nach Entdeckung** zu melden.
- Aufbau eines 24/7 PSD2-Vorfallüberwachungszentrums ist keine Anforderung der Guidelines!

Major Incident Reporting
Klarstellungen

BaFin

Was ist nicht zu melden?

- Gesprengter Geldautomat
- Geplante Ausfallzeiten (Wartungsfenster)
- Einzelner Phishing-Angriff
- Einzelne Brute-Force-Angriffe durch Scriptkiddies

Schwellenwerte beachten

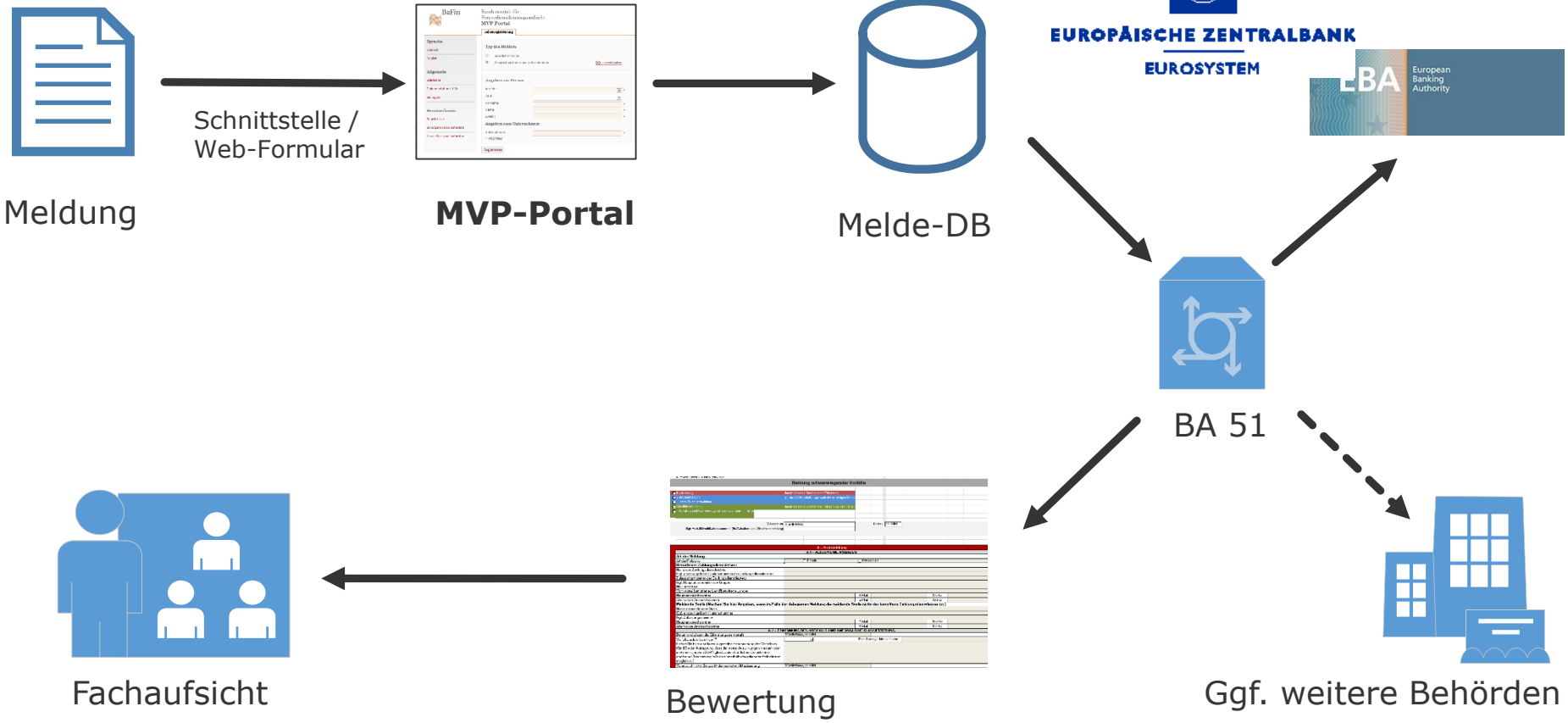
Kriterium	Niedrige Schwelle	Hohe Schwelle
Betroffene Transaktionen	> 10 % des üblichen Transaktionsvolumens und > EUR 100.000	> 25 % des üblichen Transaktionsvolumens oder > EUR 5.000.000
Betroffene Kunden	> 5.000 und > 10 % der Kunden des ZDLs	> 50.000 oder > 25 % der Kunden des ZDLs
Ausfallzeit	> 2 Stunden	-
Wirtschaftlicher Schaden	-	> max (0,1 % des Kern-kapitals; EUR 200.000) oder > EUR 5.000.000
Hohe interne Eskalationsstufe	Ja	Ja, und interne Einstufung als "Krise"
Auswirkungen auf weitere Zahlungsdienstleister oder Infrastrukturen	Ja	-
Reputationsschaden	Ja	-

Major Incident Reporting
Englische Beschreibung

A - Initial report						
A 1 - GENERAL DETAILS						
Type of report						
Type of report	☐ Individual	☐ Consolidated				
Affected payment service provider (PSP)						
PSP name						
PSP unique identification number, if relevant						
PSP authorisation number						
Head of group, if applicable						
Home country						
Country / countries affected by the incident						
Primary contact person		Email		Telephone		
Secondary contact person		Email		Telephone		
Reporting entity (complete this section if the reporting entity is not the affected PSP in case of delegated reporting)						
Name of the reporting entity						
Unique identification number, if relevant						
Authorisation number, if applicable						
Primary contact person		Email		Telephone		
Secondary contact person		Email		Telephone		
A 2 - INCIDENT DETECTION and INITIAL CLASSIFICATION						
Date and time of detection of the incident	DD/MM/YYYY, HH:MM					
The incident was detected by [1]		If other, please explain:				
Please, provide a short and general description of the incident (should you deem the incident to have an impact in other EU Member States(s), and if feasible within the applicable reporting deadlines, please provide a translation in English)						
What is the estimated time for the next update?	DD/MM/YYYY, HH:MM					

Quelle: EBA Guidelines on Major Incident Reporting

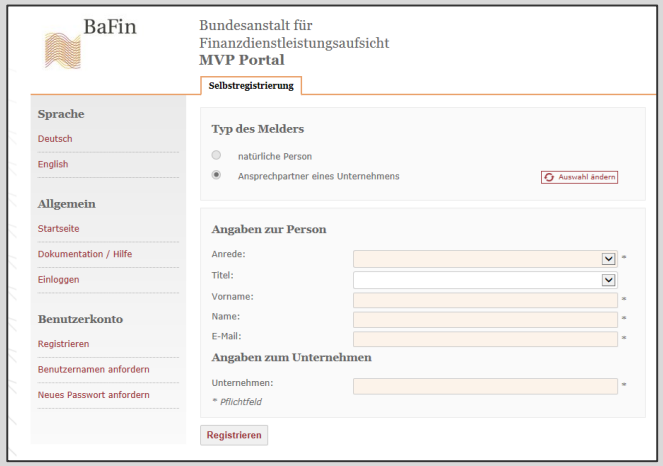
Major Incident Reporting
Zukünftiger Meldeprozess



Major Incident Reporting
MVP-Portal

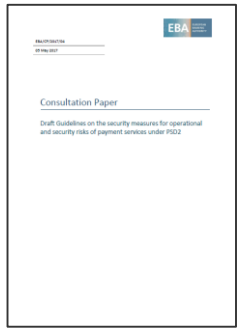
MVP-Portal der BaFin

1. Selbstregistrierung erforderlich!
2. Freischaltung für Meldeverfahren „PSD2-Zahlungssicherheitsvorfälle“
3. Ggf. separate Freischaltung für Testverfahren



Meldungen (ab 13.01.2018)

1. Nutzung eines Web-Formulars
2. XML Datei-Upload
3. SOAP Webservice Schnittstelle



Guidelines on the security measures for operational and security risks

Art. 95 PSD2, § 53 ZAG (neu)

Guidelines on Security Measures

Aktueller Stand

- Konsultation abgeschlossen; Finalisierung erfolgt
- Endgültige Fassung sehr wahrscheinlich noch dieses Jahr
- Angelehnt an MaSI, aber erweiterter Anwendungsbereich
- Aufsichtliche Übergangszeiten

Guidelines on Security Measures
Konsultation

BaFin

- Ergebnisse der Konsultation:
  - High level requirements vs. detailed requirements
  - Fehlende Definitionen / unklare Anforderungen
  - Zu strenge Anforderungen (Testen von Sicherheitsmaßnahmen, BCP,…)
  - Information Sharing (Verpflichtend?)
- *Nun aber ein Blick hinein…*

Guidelines on Security Measures

Risikomanagement

BaFin

Operational and security risk management framework

"…identify, measure, monitor and manage the range of risks stemming from the payment-related activities of the PSP and to which the PSP is exposed to"

- Risikoidentifizierung
- Sicherheitsleitlinie
- Outsourcing
- Zertifizierungen alleine nicht ausreichend

Guidelines on Security Measures

Three lines of defence vs. *defence in depth*

BaFin

Three lines of defence

- 1.) Operatives Management der Risiken
- 2.) Steuerung und Überwachung (Informationssicherheitsbeauftragter)
- 3.) Prüfungs- und Beratungsinstanz (Interne Revision)

Defence-in-depth

- *Aufbau mehrerer "Sicherheitsnetze"*
- *Vier-Augen Prinzip, Firewall + Intrusion Detection System, Starke Authentifizierung,…*

Guidelines on Security Measures

Business Continuity Management

BaFin

- Business Impact Analyse
- Contingency and Business Continuity Plan

  für die identifizierten Zahlungsverkehrsprozesse
- Szenario-basiert, auch unwahrscheinliche Szenarien

  berücksichtigen; aber keine Weltuntergangsszenarien
- Regelmäßige Tests um Anwendung im Notfall sicherzustellen

Guidelines on Security Measures

Testing of Security Measures

BaFin

- Test-Framework für Sicherheitsmaßnahmen
- Ziel: Robuste/Stabile und effektive Sicherheitsmaßnahmen
- Schwachstellen- und Penetrationstests
- Für kritische Systeme mind. jährliche Tests

Guidelines on Fraud Reporting

Statistische Daten zu Betrugsfällen

Betrugsstatistiken

Grundlagen

- Gemäß § 54 Abs. 5 ZAG n.F. sind die ZDL verpflichtet, mindestens einmal jährlich Betrugsstatistiken an die BaFin zu liefern
- BaFin hat aggregierte Daten an EBA und EZB weiterzuleiten
- Inhalt und Form dieser Statistiken soll durch eine weitere, „freiwillige" EBA-Leitlinie geregelt werden
- Erster Entwurf im August 2017 veröffentlicht; aktuell wertet EBA die Antworten aus der Konsultation dazu aus
- Endgültige Leitlinie wahrscheinlich im März 2018
- Umsetzung voraussichtlich als BaFin-Rundschreiben; Übergangszeit für den Aufbau des Berichtswesens

Ausblick

Vielen Dank für Ihre Aufmerksamkeit

WICHTIGE LINKS

Registrierung MVP-Portal

https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_170914_Meldepflicht_sicherheitsvorfaelle.html?nn=9021442