BaFin

Starke Kundenauthentifizierung, sichere Schnittstellen und Meldepflichten

Umsetzung des Abschnitts 10 des neuen ZAG aus Sicht der BaFin

Felix Strassmair-Reinshagen
BaFin, Referat GIT 1

Inhaltsverzeichnis

Inhaltsverzeichnis

Überblick zum Stand der Umsetzung Wichtige Meilensteine

BaFin

12.01.2018	EBA-Leitlinien zu Sicherheitsmaßnahmen bezüglich der operationellen und sicherheitsrelevanten Risiken von Zahlungsdiensten
13.01.2018	Inkrafttreten des neuen ZAG
13.03.2018	Veröffentlichung der „RTS on SCA & CSC" als Delegierte Verordnung (EU) 2018/389 im EU-Amtsblatt
07.06.2018	BaFin Rundschreiben 08/2018 (BA) zur Meldung schwer-wiegender Zahlungssicherheitsvorfälle
13.06.2018	EBA Opinion zur RTS und Konsultation einer Leitlinie dazu
vsl. Q3 2018	EBA Leitlinien zur Meldung von Betrugsdaten
14.09.2019	Wirksamwerden der Delegierten Verordnung (EU) 2018/389

Überblick zum Stand der Umsetzung Erlaubnisverfahren

- Unternehmen, die vor dem 13.01.2018 ZAD oder KID erbracht hatte, und bis zum 13.04.2018 eine Antrag eingereicht haben, können bis Verfahrensabschluss erlaubnisfrei tätig sein (vgl. § 65 Abs. 5 ZAG)
- bisher:
  - 12 Erlaubnisanträge für die Erbringung von ZAD und KID
  - 13 Registrierungsanträge für Erbringung nur von KID
  - Verfahren laufen noch
- Unterlagen für das Antragsverfahren richten sich nach den „EBA-Leitlinien zur Zulassung und Eintragung gemäß PSD2“
- außerdem: alle CRR-Kreditinstitute und E-Geld-Institute bereits jetzt zur Erbringung von ZAD und KID berechtigt

Überblick zum Stand der Umsetzung Weitere Informationsquellen

- BaFin-Merkblatt - Hinweise zum Zahlungsdiensteaufsichtsgesetz (ZAG) vom 29.11.2017
- Folien der BaFin-Veranstaltung am 05.12.2017
- Aufsätze im BaFin-Journal 01/2018 und 06/2018
- EBA Single Rulebook Q&A-Tool seit 22.06.2018 auch für PSD2-Fragen freigeschaltet

Überblick zum Stand der Umsetzung EBA-Papiere

ZAG	EBA - Konkretisierung	Umsetzung in Deutschland	Übergangszeit
§ 53 I ZAG	EBA Guidelines on Security Measures	Erweiterung BAIT in Vorbereitung	MaSI
§ 54 I ZAG	EBA Guidelines on Major Incident Reporting	BaFin Rundschreiben 08/2018 (BA) zur Meldung schwer-wiegender Zahlungs-sicherheitsvorfälle	vorbei
§ 54 V	EBA Guidelines on Fraud Reporting (voraussichtlich Q3)	Wahrscheinlich BaFin-Rundschreiben	Meldung erst für Transaktionen ab 2019
§§ 48 – 52, § 55 ZAG	RTS on Strong Customer Authentication and Secure Communication	Als Delegierten Verordnung (EU) 2018/389 unmittelbar anwendbares Recht ab 14.09.2019	MaSI vgl. § 68 IV ZAG

Inhaltsverzeichnis

Starke Kundenauthentifizierung Begriffsklärung

BaFin

- 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)
- Die zwei abgefragten Elemente müssen aus unterschiedlichen Kategorien kommen.
- Auf der Zahlungskarte aufgedruckten Codes können **kein** Element der Kategorie Wissen sein.

Starke Kundenauthentifizierung Erforderlichkeit

- Gemäß § 55 Abs. 1 ZAG ist eine 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.

- Beim elektronischen Fernzahlungsvorgang zusätzlich „dynamische Verknüpfung“ notwendig (§ 55 Abs. 2 ZAG).

Starke Kundenauthentifizierung Gegenbeispiele zur Erforderlichkeit

BaFin

- Vom Zahlungsempfänger ausgelöste Zahlungen
  - Beispiel: Lastschriften (inklusive ELV)
  - Was ist bei Kreditkarten?
    - Vgl. EBA-Opinion Tz. 32
- Nicht elektronisch ausgelöste Zahlungen
  - Beispiel: Kreditkartenzahlung mit Unterschrift
- Kartenzahlung, bei denen einer der ZDL außerhalb des EWR sitzt.

Starke Kundenauthentifizierung Ausnahmen gemäß VO 2018/389

- Kontaktlose Zahlungen
- Unbeaufsichtigte Terminals für Verkehrsnutzungsentgelte und Parkgebühren
- Vom Zahler als vertrauenswürdig eingestufte Empfänger
- Wiederkehrende Zahlungsvorgänge
- Zahlungen an die eigene Person (beim selben Zahlungsdienstleister)
- Kleinbetragszahlungen
- Zahlungsmethoden mit hohem Sicherheitsniveau, zu denen nur Unternehmen zugelassen sind
- Transaktionsrisikoanalyse
- Abrufen von Kontostand und Umsätzen der letzten 90 Tage

(Details siehe Art. 10 ff. der VO (EU) 2018/389)

Starke Kundenauthentifizierung Beispiel einer Ausnahme

BaFin

Fernzahlungsvorgänge über Kleinbeträge (Art. 16)

- A: Betrag Zahlung maximal 30 Euro
- B: Betrag der vorheriger Fernzahlungsvorgänge seit der letzten SKA maximal 100 Euro
- C: Zahl der vorheriger Fernzahlungsvorgänge seit der letzten SKA maximal fünf

Zahlung ohne SKA zulässig, wenn gilt:

A und (B oder C)

Starke Kundenauthentifizierung Transaktionsrisikoanalyse

BaFin

- Ausnahme kann vom Zahlungsdienstleister (ZDL) des Zahlers aber auch vom ZDL des Zahlungs-empfängers genutzt werden (aber letztes Wort beim ZDL des Zahlers)
- Berechnung der Betrugsrate erfolgt immer für den ZDL (nicht etwa gesondert für einzelne Händler)
- Was geht in die Berechnung der Betrugsrate ein?
  - Vgl. EBA-Opinion Tz. 46

Inhaltsverzeichnis

Zugang für Dritte Zahlungsdienstleister Berechtigte

BaFin

Für wen muss der Zugang bereitgestellt werden?

- Zahlungsauslösedienstleister (ZAD)
- Kontoinformationsdienstleister (KID)
- ZDL, die kartengebundene Zahlungsinstrumente ausgeben

(Zahlungsinstitute mit Zulassung für die jeweiligen Geschäfte sowie CRR-Kreditinstitute und E-Geld-Institute.)

Zugang für Dritte Zahlungsdienstleister
Formen der Bereitstellung

Drei Optionen für kontoführende ZDL:

- Modifizierte Kundenschnittstelle
  (Art. 30 und 31)
- Dedizierte Schnittstelle mit Notfall-Mechanismus
  (Art. 30, 32 und 33 Abs. 1 - 5)
- Dedizierte Schnittstelle mit Befreiung vom Notfall-Mechanismus durch die BaFin
  (Art. 30, 32 und 33 Abs. 1 - 3, sowie 6 - 7)

Zugang für Dritte Zahlungsdienstleister Zeitplan

Meilensteine für eine dedizierte Schnittstelle mit Befreiung wirksam ab dem 14.09.2019

- 14.03.2019 Bereitstellung einer Testumgebung (Art. 30 Abs. 5)
- 14.06.2019 Beginn des Markttests (Art. 33 Abs. 6 lit c)
- 14.09.2019 Zugriffe von Drittdienstleistern laufen nur noch über die dedizierte Schnittstelle

Zugang für Dritte Zahlungsdienstleister
Welche Daten erhält ein ZAD?

BaFin

Antwort ergibt sich aus Art. 36 Abs. 1 lit. b und c:

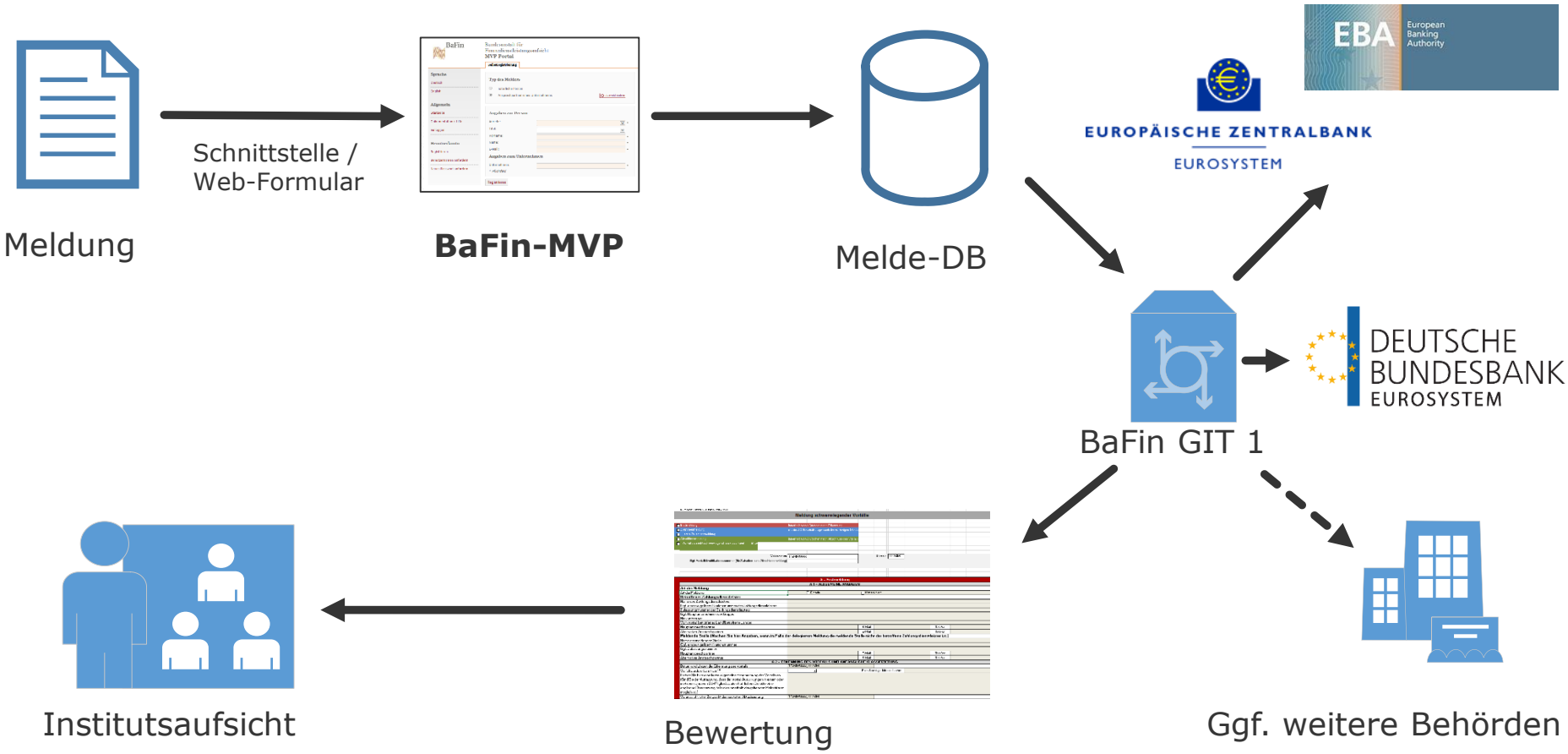
- Alle Informationen, die auch der Zahlungsdienstnutzer über die Auslösung und Ausführung einer Zahlung erhält
  - Unterschiede zwischen Systemen mit Echtzeit- bzw. Batchverarbeitung
- Bestätigung über die Verfügbarkeit eines Geldbetrages
  - Art. 36 Abs. 1 lit. c nicht nur auf kartenausgebende ZDL anwendbar

Inhaltsverzeichnis

Meldung von Sicherheitsvorfälle Grundlagen

- Pflicht zur Meldung schwerwiegender Sicherheits-vorfälle ergibt sich aus § 54 Abs. 1 ZAG
- BaFin-Rundschreiben 08/2018 (BA) vom 07.06.2018 definiert, welche Vorfälle meldepflichtig sind und bestimmt den Inhalt der Meldungen
- Meldungen sind (ausschließlich) über das Fachverfahren „PSD2-Zahlungssicherheitsvorfälle“ auf der BaFin-MVP abzugeben
- Bitte nicht mehr das MaSI-Formular verwenden!

Meldung von Sicherheitsvorfälle Meldeverarbeitung



Meldung von Sicherheitsvorfälle
Nicht meldepflichtige Vorfälle

BaFin

Folgende Vorfälle sollten beispielsweise als **nicht** meldepflichtig betrachtet werden:

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

Inhaltsverzeichnis

Leitlinien über Sicherheitsmaßnahmen Umsetzung in Deutschland

BaFin

- Konkretisieren § 53 Abs. 1 ZAG; angelehnt an die MaSI
- Veröffentlichung der deutschen Fassung im Januar 2018; BaFin hat „intends to comply" erklärt
- Viele Überschneidungen mit dem BaFin-Rundschreiben 10/2017 (BA) - Bankaufsichtliche Anforderungen an die IT (BAIT)
- Deshalb derzeitige Planung: Aufnahme der zusätzlichen Anforderungen in die BAIT
- Anwendung auf die ZAG-Institute klären
- Nach Umsetzung dieser Leitlinien und Ablauf des 14.09.2019 werden die MaSI aufgehoben

Inhaltsverzeichnis

Meldung von Betrugsdaten Grundlagen

- Gemäß § 54 Abs. 5 ZAG sind die ZDL verpflichtet, mindestens einmal jährlich Betrugsstatistiken an die BaFin zu liefern
- BaFin hat aggregierte Daten an EBA und EZB weiterzuleiten
- Inhalt und Gliederung dieser Statistiken soll durch eine weitere, „own-initiative" EBA-Leitlinien geregelt werden
- Harmonisierung mit Novelle der EZB-Verordnung zur Zahlungsverkehrsstatistik (soweit wie sinnvoll)

Meldung von Betrugsdaten Umsetzung

- Erster Entwurf im August 2017 veröffentlicht; endgültige Leitlinie wahrscheinlich in Q3/2018
- Umsetzung in Deutschland voraussichtlich als BaFin-Rundschreiben
- Enge Zusammenarbeit mit dem Markt, um einen reibungslosen Start zu gewährleisten
- Übergangszeit für den Aufbau des Berichtswesens (erst Transaktionen ab 2019 zu melden)

Vielen Dank für Ihre Aufmerksamkeit