BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

PSD2 in der Aufsichtspraxis
– Erste Bilanz und Ausblick –

Dr. Felix Strassmair-Reinshagen,
Referat GIT 1

Dr. Markus Burkow,
Referat GIT 2

Inhalt

GIT 1 – Sicherheit und Wettbewerb im Zahlungsverkehr

Dr. Strassmair-Reinshagen

- Starke Kundenauthentifizierung
  - Eckpunkte
  - Nachfrist für Kartenzahlung im Internet
- Zugang für Dritte Zahlungsdienstleister
  - Eckpunkte
  - Übergang in die neue API-Welt

GIT 2 - Operative Aufsicht über Zahlungsinstitute und E-Geld-Institute

Dr. Burkow

- Aktuelle Situation
- Nicht technische Neuerungen durch PSD 2 und ZAG
- technische Neuerungen durch PSD 2 und ZAG
- Zahlungsinstitutsregister (BaFin/EBA)
- Fazit und Ausblick

Starke Kundenauthentifizierung (SKA) Begriffsklärung

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)

… resultieren in der Generierung eines „Authentication Code“

> Die zwei abgefragten Elemente müssen aus unterschiedlichen Kategorien kommen.

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.

Starke Kundenauthentifizierung
Gegenbeispiele zur Erforderlichkeit

- Vom Zahlungsempfänger ausgelöste Zahlungen
  - Beispiel: Lastschriften (auch bei online erteilten Mandaten)
    siehe BaFin Mitteilung vom 17.04.2019 und EBA Q&A 2019_4664
  - „Merchant Initiated Transactions" im Kreditkartenbereich (aber Mandat ist SKA-pflichtig)
- Kartenzahlung, bei denen einer der Zahlungsdienstleister außerhalb des EWR sitzt
- Telefonbanking, MOTO-Transaktionen

Starke Kundenauthentifizierung
Beispiele für (un)zulässige Verfahren

Beispiele für grundsätzlich zulässige Lösungen

- Passwort und SMS-TAN
- Am POS: Chipkarte und PIN

Nicht als Elemente geeignet

- iTAN-Listen (weder Wissen noch Besitz)
- Aufgedruckte Kartendaten (weder Wissen noch Besitz)
- 3-D Secure-Transaktionsdaten (nicht als Inhärenz geeignet)

Starke Kundenauthentifizierung
Ausnahmen gemäß der Delegierten Verordnung 2018/389

- Kontaktlose Zahlungen am POS
- Unbeaufsichtigte Terminals für Verkehrsnutzungsentgelte und Parkgebühren
- Vom Zahler als vertrauenswürdig eingestufte Empfänger
- Wiederkehrende Zahlungsvorgänge
- Zahlungen an die eigene Person (beim selben Zahlungsdienstleister)
- Kleinbetragszahlungen bei elektronischen Fernzahlungsvorgängen
- Zahlungsmethoden mit hohem Sicherheitsniveau, zu denen nur Unternehmen zugelassen sind
- Durch eine Transaktionsrisikoanalyse als „risikoarm“ klassifizierte Zahlungen
- Zugriff auf Kontostand und Umsätze der vergangenen 90 Tage

Starke Kundenauthentifizierung
Nachfrist für Kartenzahlungen im Internet

- Anlass: Fehlende Vorbereitung durch die Zahlungsempfänger (*Merchants)*
- BaFin wird vorerst nicht beanstanden, wenn bestimmte Zahlungen ohne SKA durchgeführt werden
  - Gilt nur für „kartengebundene elektronische Fernzahlungsvorgänge“; erstreckt sich nicht auf sonstige Fälle von SKA
  - BaFin will Enddatum EU-weit abstimmen
  - Gespräch mit Händlerverbänden am 04.09.2019

Zugang für Dritte Zahlungsdienstleister Berechtigte

Für wen muss der Zugang bereitgestellt werden?

- Zahlungsauslösedienstleister (ZAD)
- Kontoinformationsdienstleister (KID)
- Drittkartenemittenten (DKE)

Wer ist berechtigt, auf den Zugang zuzugreifen?

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

Zugang für Dritte Zahlungsdienstleister
Formen der Bereitstellung

Kundenschnittstelle		**Dedizierte Schnittstelle (API)**	
ohne Identifizierung	mit Identifizierung	mit „Fallback“	ohne „Fallback“ mit Befreiung vom Notfallmechanismus
X	✓	✓	✓
	Art. 30, 31 RTS	Art. 30, 32 und 33 Abs. 1 - 5 RTS	Art. 30, 32 und 33 Abs. 1 - 3, sowie 6 - 7 RTS

Zugang für Dritte Zahlungsdienstleister
Identifizierung beim Zugriff

- Identifizierungspflicht des Drittdienstleisters gilt bei allen drei Bereitstellungsformen (auch beim *„Fallback“*)
- Nutzung qualifizierter Zertifikate auf Basis der eIDAS-Verordnung
- Beantragung bei einem qualifizierten Vertrauensdiensteanbieter
- Zugang zum Zahlungskonto erfolgt aber mit den Zugangsdaten des Kunden

Testphase

Artikel 30 Absatz 5 (RTS) / Leitlinie 6.5 (Guidelines)

- Verbindungs- und Funktionstest
  - Stabile und sichere Verbindung
  - Zertifikatshandling (Testzertifikate)
  - Fehlermeldungen
  - ZAD/KID/DKE Funktionalität
  - Zugriff auf Authentifizierungsverfahren
- Schnittstellendokumentation
  - Zusammenfassung auf Webseite
  - Vollständige Dokumentation auf Anfrage
- Konsolidierte Testumgebung bei Institutsverbünden und Gruppen

- Voraussetzung für Teilnahme an der Testphase: Antrag (Registrierung/Erlaubnis) eingereicht

Marktbewährungsphase

Art. 33 Absatz 6 Buchstabe c (RTS) / Leitlinie 7 (Guidelines)

- Zeitdauer: mind. drei Monate
- Umfangreiche Nutzung durch TPPs (Wide Usage)
- Echtdaten / Echtzertifikate
- Kann parallel zur Testphase erfolgen

eIDAS Zertifikate:

1. für elektronische Siegel (QSEALs) *oder*
2. für Website-Authentifizierung (QWACS)

Vorgabe durch kontoführendes Institut

Bewertung durch BaFin

Zentrale Aspekte

- Bereitstellung aller geforderten Funktionalitäten
- Ergebnisse der Testphase
- Ergebnisse der Marktbewährungsphase
- Performance und Verfügbarkeit
- Umgang mit aufgetretenen Problemen
- Keine Beeinträchtigungen („Obstacles“)

Zugang für Dritte Zahlungsdienstleister Befreiungsverfahren gemäß Art. 33 Abs. 6 RTS

- Befreiung erfolgt auf der Ebene des einzelnen ZDL (nicht direkt auf der Ebene der API-Initiativen)

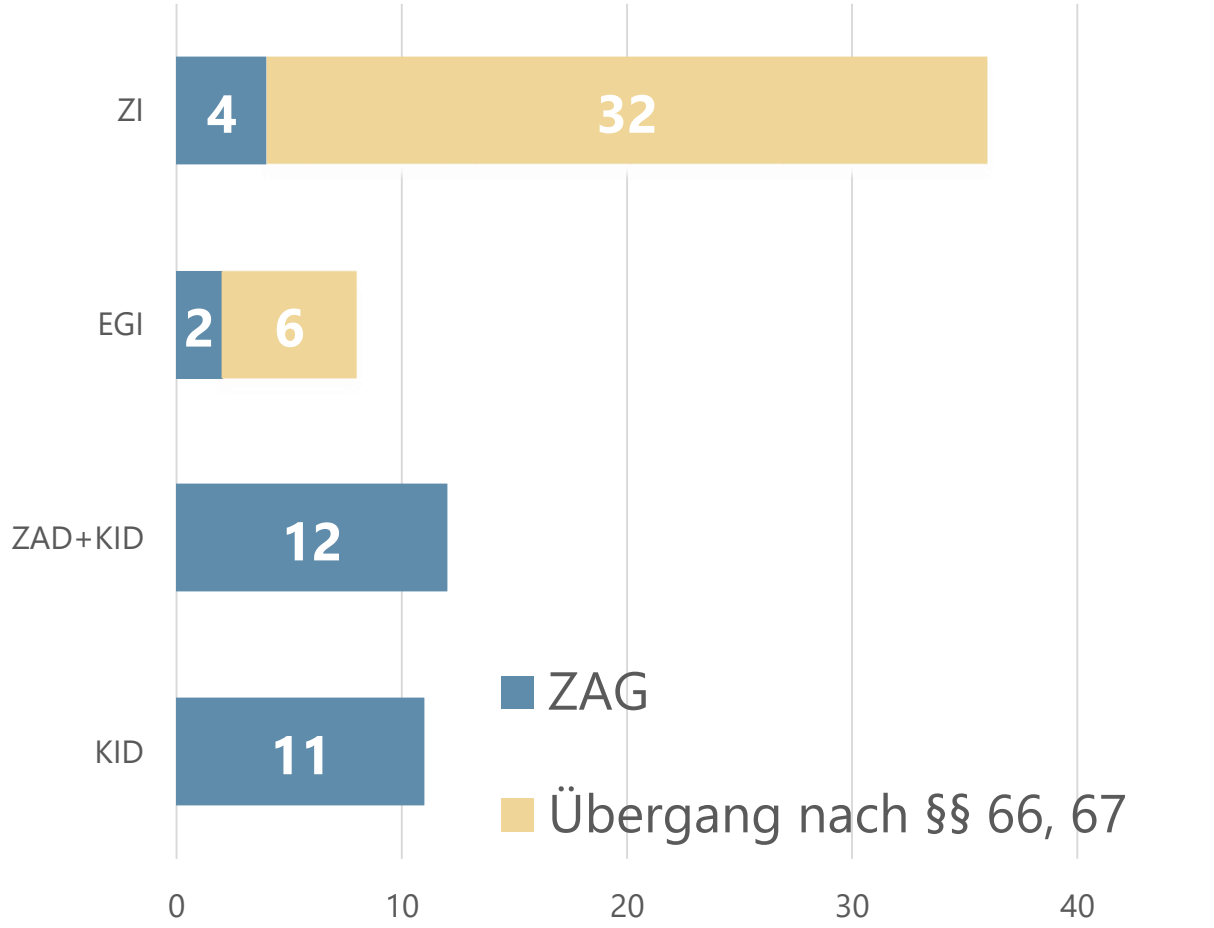
  ➔ vereinfachte Verfahren für ZDL, die den selben technischen Dienstleister verwenden
- BaFin stellt Antragsformular bereit (am 15.03.19 veröffentlicht)
- **Zentrale Forderung:** (Dedizierte) Zugangsschnittstelle darf keine Beeinträchtigungen („Obstacles“) beeinhalten
- Aktuell ca. 30 Befreiungsverfahren

Zugang für Dritte Zahlungsdienstleister
Aktuelle Entwicklungen

- BaFin-Schreiben vom 14.08.2019
  - Funktionale und operative Mängel bei einzelnen Schnittstellen
  - Keine erfolgreiche Marktbewährung bei den meisten Schnittstellen
  - unwahrscheinlich, dass die meisten Befreiungsanträge am 14.09.2019 positiv beschieden werden können
- BaFin-Workshop am 10.09.2019
  - Entscheidung offener Auslegungsfragen
  - Aufsichtliche Erwartungshaltung zum Stichtag 14.09.2019
  - Weitere Schritte für einen reibungslosen Übergang auf PSD2-konforme Schnittstellen

GIT 2 - Operative Aufsicht über Zahlungsinstitute und E-Geld-Institute

- Erlaubnis-/Registrierungsanträge
- Laufende Aufsicht: 67 Institute
  - „klassische“ Zahlungsinstitute (§ 1 Abs. 1 Satz 2 Nr. 1-6 ZAG)
  - E-Geld (§ 1 Abs. 2 Satz 2 ZAG)
  - ZAD + KID (§ 1 Abs. 1 Satz 2 Nr. 7+8 ZAG)
  - KID (§ 1 Abs. 1 Satz 2 Nr. 8 ZAG)
- Wechselstuben (4 ZI + 7 Sortengeschäft)
- Passporting (EWR) 500+



Neuerungen durch PSD2 und ZAG

(organisatorische Aspekte)

- Sicherheitskonzepte
- Notfallstrategien
- Risikobewertung
- Berichtswege
- Arbeitsanweisungen
- Registrierung als KID
- Proportionalität
- Berufshaftpflichtversicherung (ZAD u. KID) (EBA/GL/2017/08)

EBA GL 2017/09 Leitlinie zur Zulassung und Eintragung gemäß PSD2 : IT-Anforderungen

- Sicherheitsvorfälle und sicherheitsbezogene Kundenbeschwerden
- Zugang zu sensiblen Zahlungsdaten
- Geschäftsfortführung im Krisenfall
- Statistische Daten
- Sicherheitsstrategie

Neuerungen durch PSD2 und ZAG

(technische Aspekte)

- Technisches Verständnis der Datenflüsse (Geschäftsmodell)
- Sensible Zahlungsdaten, Überwachungsinstrumente
- TOM zur Betrugsprävention, Risikominderungsmaßnahmen
- Berechtigungs- und Rollenkonzepte
- Verschlüsselung und Tokenisierung
- IT-Landschaft inkl. Backup-Strukturen

EBA GL 2017/09: IT-Anforderungen ZI (KID)

- GL 9.1 (7.1): a) und f)
- GL 10.1 (8.1): a), b), c), g) und h)
- GL 11.1 (9.1): a), c) und e)
- GL 12.1 (----): a), b), c) und e)
- GL 13.1 (10.1): a) bis g)

Register

ZAG Instituts-Register nach §§ 43, 44 ZAG (BaFin)

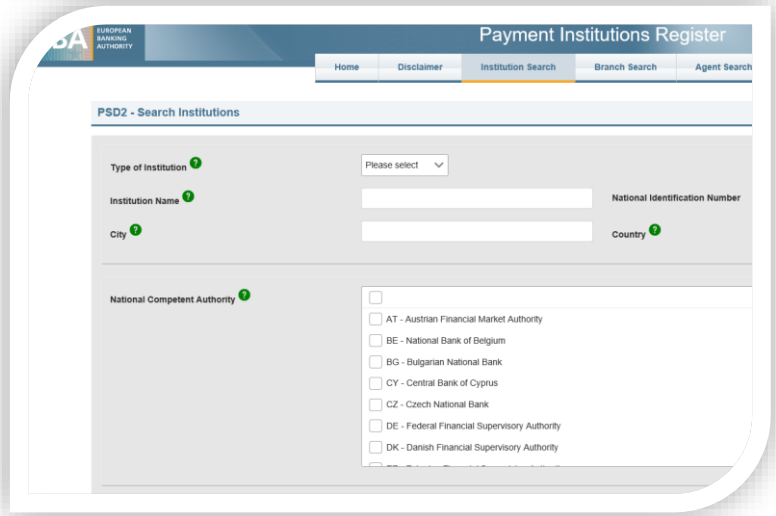
bafin.de -> Publikationen & Daten -> Datenbanken

- ZI + EGI + ZAD + KID (CSV/XML Export)
- „Erteilt am“ Datum
- Tägliches Update
- Voraussetzung für eIDAS Zertifikate

Payment-Institution-Register (EBA)

https://euclid.eba.europa.eu/register/pir/search

- Synchronisation mit BaFin-ZAG-Register
- Ausnahmen (Exclusions)
- 24 Stunden Update (automatisiert)



Fazit und Ausblick

- Starke Kundenauthentifizierung
- Zugang für Dritte Zahlungsdienstleister
- Laufende Aufsicht von 70+ Institute
- Neue Anträge 40+
- Neuerungen durch PSD 2 und ZAG (organisatorisch & technisch)
- Weiterentwicklung der Register

Ausblick:

- IT-Prüfung
- Technische Umsetzung (API, 2FA, etc.)
- Ausbau der Register
- Neue Geschäftsmodelle
- Technische Neuerungen