BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

Aufsicht über die Sicherheit im Zahlungsverkehr nach dem neuen ZAG

Tobias Schmidt
Felix Strassmair-Reinshagen
Referat GIT 1

Inhaltsübersicht

Überblick zum Stand der Umsetzung

Starke Kundenauthentifizierung

Zugang für Dritte Zahlungsdienstleister

Inhaltsübersicht

Wichtige Meilensteine der Umsetzung

12.12.2017	EBA-Leitlinien zu Sicherheitsmaßnahmen bezüglich der operationellen und sicherheitsrelevanten Risiken von Zahlungsdiensten (englische Fassung) veröffentlicht
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 schwerwiegender Zahlungssicherheitsvorfälle
13.06.2018	EBA Opinion zur RTS und Konsultation einer Leitlinie dazu
22.06.2018	Freischaltung des EBA Single Rulebook Q&A-Tools auch für PSD2-Fragen
18.07.2018	EBA Leitlinien zur Meldung von Betrugsdaten (englische Fassung)
14.09.2019	Wirksamwerden der Delegierten Verordnung (EU) 2018/389 sowie Inkrafttreten der §§ 45 – 52, 55 ZAG

Erlaubnisverfahren für Unternehmen, die ZAD oder KID erbringen

- Unternehmen, die vor dem 13.01.2018 ZAD oder KID erbracht hatten, und bis zum 13.04.2018 einen Antrag eingereicht haben, können bis Verfahrensabschluss erlaubnisfrei tätig sein (vgl. § 65 Abs. 5 ZAG)
- aktueller Stand:
  - 13 Erlaubnisanträge für die Erbringung von ZAD und KID
  - 14 Registrierungsanträge für Erbringung nur von KID
  - eine Erlaubnis für ZAD und KID bereits erteilt
- 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

Umsetzung der EBA-Maßnahmen in Deutschland

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 schwerwiegender Zahlungssicherheitsvorfälle	Rundschreiben seit dem 07.06.2018 in Kraft
§ 54 V ZAG	EBA Guidelines on Fraud Reporting	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)

Inhaltsübersicht

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)

Die zwei abgefragten Elemente müssen aus unterschiedlichen Kategorien kommen.

Auf der Zahlungskarte aufgedruckte Codes können kein Element der Kategorie Wissen sein.

- Auswirkung auf Kartenzahlungen im Internet!

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 **Fern**zahlungsvorgang zusätzlich „dynamische Verknüpfung“ notwendig (§ 55 Abs. 2 ZAG).

Starke Kundenauthentifizierung
Gegenbeispiele zur Erforderlichkeit

Vom Zahlungsempfänger ausgelöste Zahlungen

- Beispiel: Lastschriften (inklusive ELV)
- Was ist bei Kreditkarten?
  - Vgl. EBA-Opinion Tz. 32; weitere Klärung im Q&A-Prozess

Nicht elektronisch ausgelöste Zahlungen

- Beispiel: Kreditkartenzahlung mit Unterschrift

Kartenzahlung, bei denen einer der ZDL außerhalb des EWR sitzt.

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
- **Transaktionsrisikoanalyse**
- abrufen von Kontostand und Umsätzen der vergangenen 90 Tage

Starke Kundenauthentifizierung
Beispiel Kleinbetragsausnahme gemäß Art. 16 RTS

Fernzahlungsvorgänge über Kleinbeträge (Art. 16 RTS)

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

Zahlung ohne SKA zulässig, wenn gilt:

A und (B oder C)

Starke Kundenauthentifizierung
Transaktionsrisikoanalyse

Anwendungsbeispiel für kartengebundene elektronische Fernzahlungsvorgänge

Drei Optionen für den ZDL:
Nutzung für Zahlungen mit Betrag:

- von 0 € bis 500 €: Betrugsrate max. 0,01 %
- von 0 € bis 250 €: Betrugsrate max. 0,06 %
- von 0 € bis 100 €: Betrugsrate max. 0,13 %

Berechnung der Betrugsrate erfolgt immer für den ZDL (nicht etwa gesondert für einzelne Händler)

Inhaltsübersicht

Zugang für Dritte Zahlungsdienstleister Berechtigte

Für wen muss der Zugang bereitgestellt werden?

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

(Zahlungsinstitute mit Zulassung für die jeweiligen Geschäfte sowie 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
Befreiungsverfahren gemäß Art. 33 Abs. 6 RTS

EBA erarbeitet im Moment Leitlinien dazu (Konsultation endete am 13.08.2018)

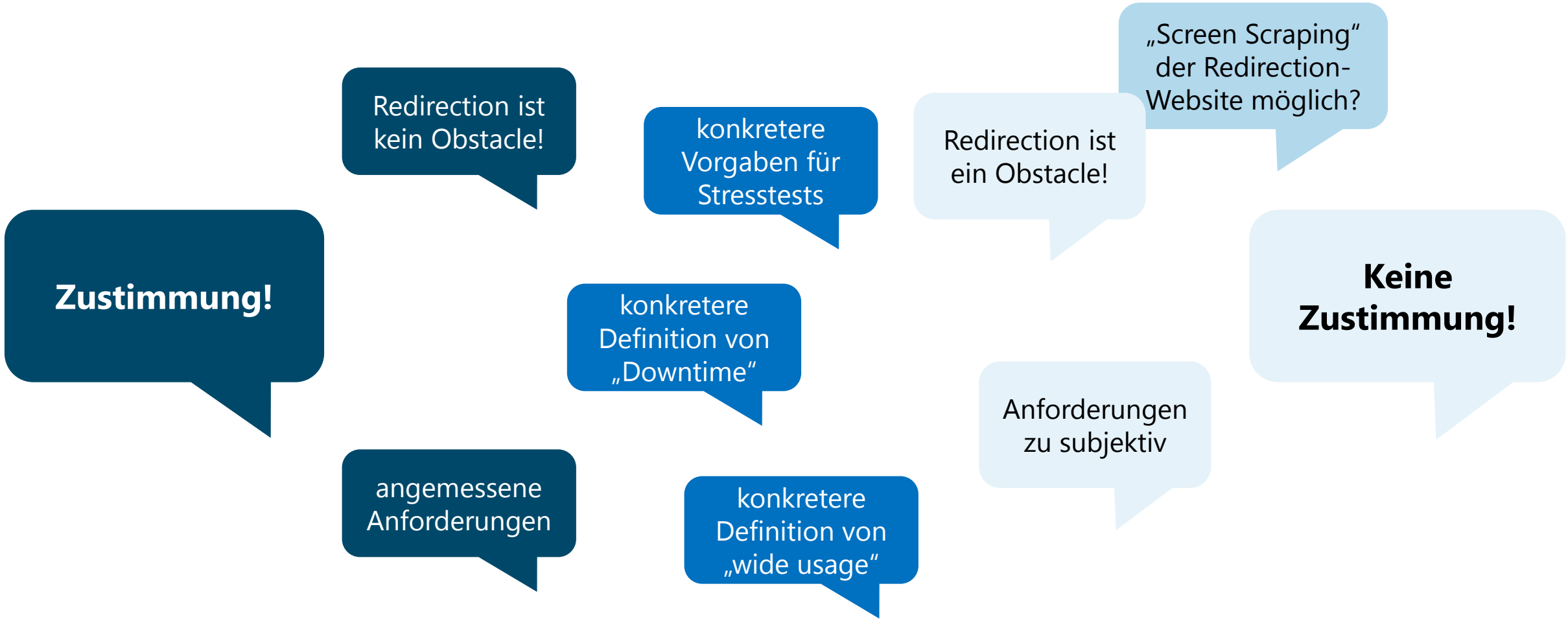
Befreiung erfolgt auf der Ebene des einzelnen ZDL (nicht direkt auf der Ebene der API-Initiativen)

➔ BaFin plant vereinfachte Verfahren für Verbünde und Gruppen

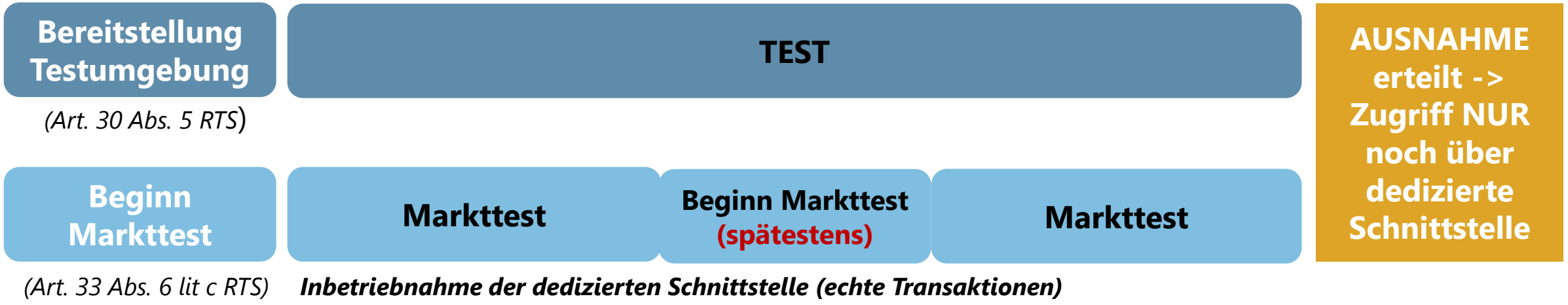
BaFin wird weitere Informationen zum Antragsprozess bereitstellen

Finalisierung der Guidelines sollte nicht zu Verzögerungen führen

Konsultationsergebnisse



Zugang für Dritte Zahlungsdienstleister
Zeitplan



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
- es gelten die Regeln dieser Anbieter
- Zugang zum Zahlungskonto erfolgt aber mit den Zugangsdaten des Kunden

Zugang für Dritte Zahlungsdienstleister
Welche Daten erhält ein ZAD?

Antwort ergibt sich aus Art. 36 Abs. 1 lit. b und c RTS (vgl. EBA Opinion Tz. 22 ff.)

Alle Informationen, die auch der Zahlungsdienstnutzer über die Auslösung und Ausführung einer Zahlung erhält

- bei Echtzeitverarbeitung: Antwort, ob Zahlung ausgeführt wurde
- hilfsweise (bei Batchverarbeitung): Bestätigung über die Verfügbarkeit eines Geldbetrages
- höchst hilfsweise: weitere Zahlungskontodaten

Zugang für Dritte Zahlungsdienstleister
Welche Daten erhält ein KID?

- Informationen von bezeichneten Zahlungskonten und damit in Zusammenhang stehenden Zahlungsvorgängen
- Andere Konten sowie Wertpapierdepots sind nicht erfasst
- Informationen über die Identität des Zahlungsdienstnutzers (z. B. Adresse, Geburtsdatum, Steuer-ID) sind nicht erfasst (EBA Opinion Tz. 27)

Quelle: Eigenes Foto des Autors