Bundesanstalt für
Finanzdienstleistungsaufsicht

BaFin

Zahlungsdiensterichtlinie 2 (PSD2)

Informationsveranstaltung *IT-Aufsicht bei Banken*

Dr. Felix Reinshagen
Tobias Schmidt

Themen dieses Vortrags

- Hintergrund/Termine
- Meldung von Sicherheitsvorfällen
- Statistische Daten zu Betrugsfällen
- Maßnahmen zur Beherrschung operationeller und sicherheitsrelevanter Risiken
- Schnittstelle für den Zugang zum Zahlungskonto
- Starke Kundenauthentifizierung und Ausnahmen dazu
- Ausblick

Einschränkungen

BaFin

Nicht behandelt werden:

- Erlaubnisverfahren und laufende Aufsicht über Zahlungsinstitute
- Auswirkungen der PSD2 auf das Privatrecht
- Ausnahmen vom Anwendungsbereich

Stand von heute, vorbehaltlich:

- Deutsche Umsetzungsgesetzgebung
- Erlass der endgültigen RTS durch die EU-Kommission (Vetorecht von Rat und EU-Parlament)

PSD2 Hintergrund

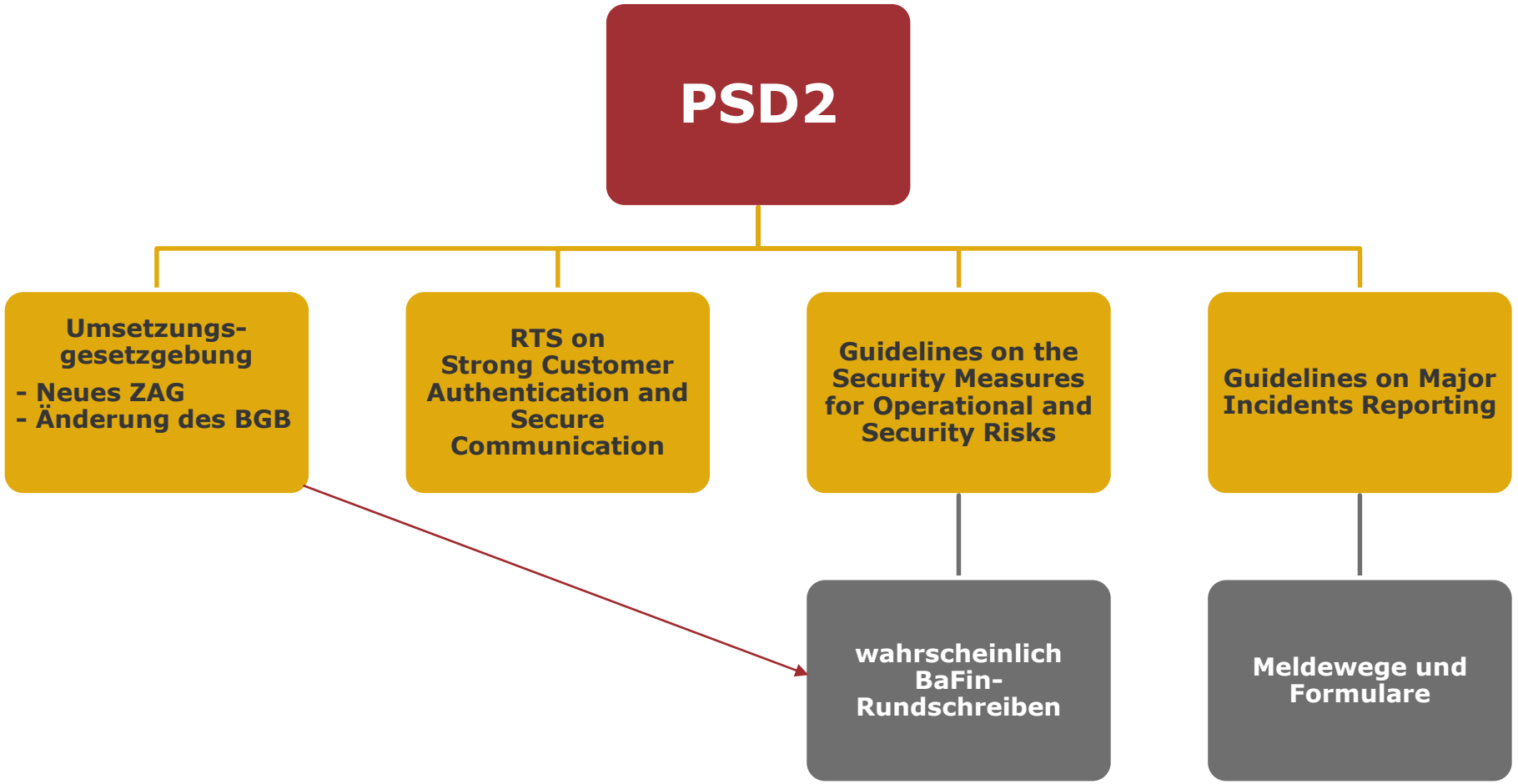
- Förderung von Innovationen im Zahlungsverkehr
- Erhöhung der Sicherheit im Zahlungsverkehr
- Stärkung des Verbraucherschutzes
- Inkrafttreten am 12.01.2016
- Umsetzung bis 13.01.2018
- EBA entwickelt insg. 6 technische Regulierungsstandards (RTS) und 5 Leitlinien zur PSD2

Termine

12. Januar 2016	Inkrafttreten der Zweiten Zahlungsdienstrichtlinie (PSD2)
08. Februar 2017	Veröffentlichung des Regierungsentwurfs des deutschen PSD2-Umsetzungsgesetzes
23. Februar 2017	Veröffentlichung des endgültigen EBA-Entwurfs der RTS über Starke Kundenauthentifizierung und Sichere Kommunikation
13. Januar 2018 (voraussichtlich)	Inkrafttreten des deutschen Umsetzungsgesetzes, betrifft insbes. Regelungen über ▪ Meldung von Sicherheitsvorfällen und ▪ Beherrschung operationeller und sicherheitsrelevanter Risiken
Oktober 2018 (oder später)	Inkrafttreten der Regelungen über „Starke Kundenauthentifizierung“ und Drittzugang

PSD2

Verhältnis der Umsetzungsmaßnahmen



Guidelines on Major Incidents Reporting

(Meldung schwerwiegender Sicherheitsvorfälle)

Major Incidents Reporting

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: BaFin plant hierzu ein standardisiertes Meldeverfahren auf Basis der Melde- und Veröffentlichungsplattform (MVP)

- Neues Bewertungsschema für Sicherheitsvorfälle

Major Incidents Reporting

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
- Benachrichtigung der Zahlungsdienstenutzer in bestimmten Fällen
  - durch den Zahlungsdienstleister

Major Incidents Reporting
Definitionen

BaFin

Was ist ein schwerwiegender Sicherheitsvorfall im Zahlungsverkehr?

*"A singular event or a series of linked events which have or may have a **material adverse impact** on the integrity, availability, confidentiality, authenticity and/or continuity of **payment-related services.**"* (Guidelines Major Incidents Reporting, Konsultationsentwurf)

? **Wann liegt ein „material impact" vor?**

Major Incidents Reporting

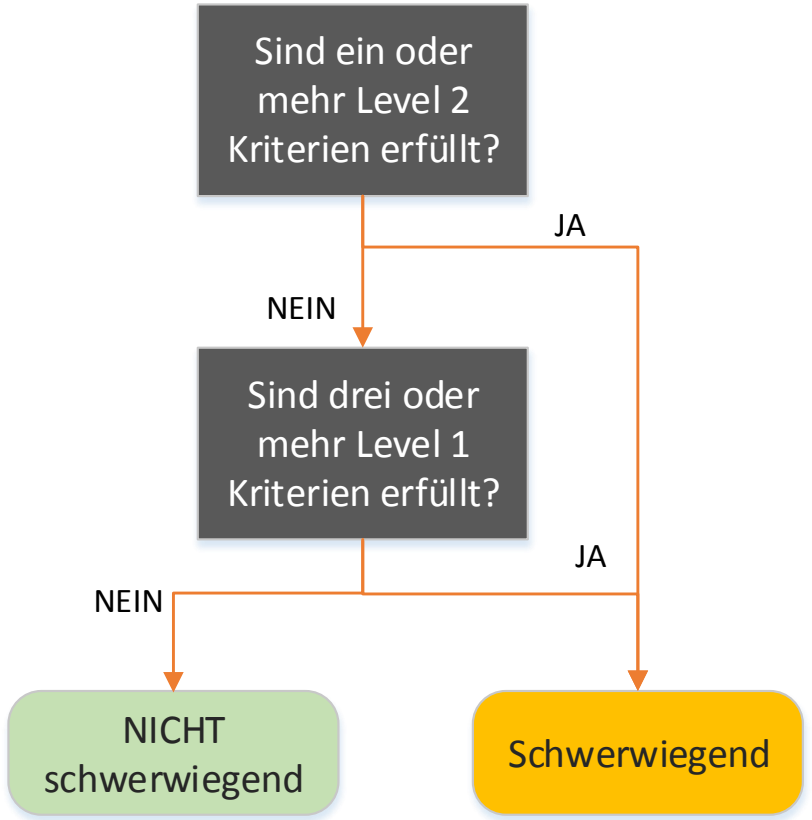
Bewertungskriterien

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

Major Incidents Reporting

Bewertungskriterien

Kriterium	Level 1	Level 2
Betroffene Transaktionen	> 10 % des üblichen Transaktionsvolumens und > EUR 100.000	> 25 % des üblichen Transaktionsvolumens oder > EUR 1.000.000
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 % Tier-1 Kapital*, 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 Incidents Reporting

BaFin

Was ändert sich NICHT?

- BaFin als Meldeempfänger von schwerwiegenden Zahlungssicherheitsvorfällen
- Grundsätzlicher Inhalt von Meldungen (Schäden, Beschreibung, Ursache)
- Meldung durch zentrale IT-Dienstleister möglich
- Konsolidierte Meldungen bei gleicher Ursache und Auswirkungen möglich (sog. *„aggregated reporting“*)

Statistische Daten zu Betrugsfällen

Betrugsstatistiken

- Gemäß Art. 96 Abs. 6 PSD2 sind die ZDL verpflichtet, mindestens einmal jährlich Betrugsstatistiken an die nationale Aufsicht zu liefern
- Inhalt und Form dieser Statistiken werden wahrscheinlich durch weitere EBA-Leitlinie geregelt
- Arbeiten haben gerade erst begonnen

Guidelines on the security measures for operational and security risks

Was können Sie erwarten?

- Die derzeitigen Arbeiten der EBA bauen stark auf den aus den MaSI bekannten Anforderungen auf (allerdings durch PSD2 nun Erweiterung über die von der MaSI betroffenen Internetzahlungen hinaus; bspw. auch POS-Zahlungen erfasst).
- Anforderungen an Kundeninformation und –kommunikation

  Zu großen Teilen bereits in der PSD2 enthalten
- Konsultation bevorstehend

RTS on Strong Customer Authentication and Secure Communication

(RTS SCA SC)

RTS SCA SC


Wissen
Mobile Payments
InhärenzRTSPayment Accounts
Exemption Threshold Value
Strong Customer Authentication
Contactless
Regulierung
API
Qualified Certificates
Digitale Signaturen
Dedicated interface
Account Information Services
Secure Communication
Payment Initiation Services
Kanaltrennung
Vollharmonisierung
eIDAS
Kreditkarten
Screen Scraping
Innovation
Wettbewerb
Sicherheit
Besitz

RTS SCA SC

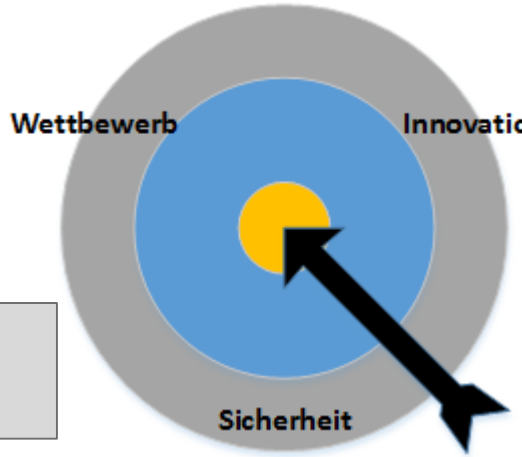
Sicherheit vs. Wettbewerb vs. Innovation

EU-Bankenaufsicht blockiert strengere Regeln bei Online-Zahlungen
Süddeutsche, 10.02.2017:

„Die Europäische Bankenaufsicht (EBA) blockiert einen besseren Verbraucherschutz beim Einkaufen im Internet."

„Die Banken haben sich offenbar erfolgreich bei der EBA für ihre Interessen eingesetzt."

„Der Europäischer Zentralbank zufolge ist der Betrug bei elektronischen Zahlungen in den vergangenen Jahren massiv gestiegen."



Kampf um die Kreditkarte
FAZ, 16.02.2017:

„..die Frage ob es mehr Sicherheit beim Bezahlen mit Kreditkarte überhaupt braucht."

„…vergleichsweise wenige Betrugsfälle…"

„Im Jahr 2015 gab es lediglich etwa 23.000 Betrugsfälle, die mit Kreditkarten im Zusammenhang standen."

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*

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

BaFin

Screen Scraping verboten?

```
<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>
```

JEIN

- Das kontoführende Institut muss einen PSD2-konformen Zugang zu den Online-Konten ihrer Kunden bereitstellen
  - **Möglichkeit A:** Dediziertes Interface (API)
  - **Möglichkeit B:** „Klassische" Online-Banking-Website +
    - Identifizierungsmöglichkeit für PIS/AIS/PIISP
    - Adressatenkonforme Informationsbereitstellung

Zugang nur über PSD2-konformes „Communication Interface"

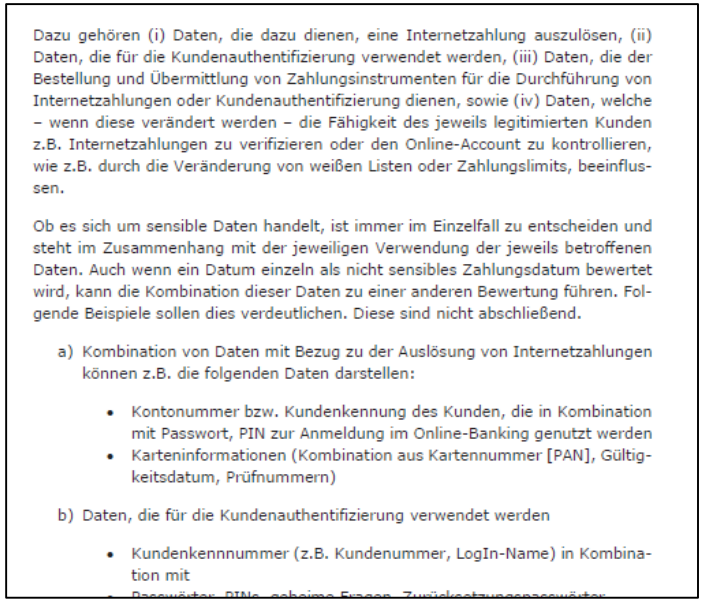
Nicht funktionale Anforderungen

- Testmöglichkeit (inkl. Support)
  - Verbindungstest und funktionaler Test
- Gleiche Performanz und Verfügbarkeit wie die Kundenschnittstelle
  - Umfassendes Monitoring durch kontoführendes Institut
  - Muss vom kontoführenden Institut nachgewiesen werden können
  - **Meldepflicht** ggü. der BaFin bei Verletzung der Anforderung
- „Same Level of contingency measures" (Notfallplanung)
  - Einbeziehung der Schnittstelle in die üblichen Business-Continuity- und Disaster-Recovery-Pläne

Was sind „sensitive payment data“ (sensible Zahlungsdaten)

- Es kommt auf den Kontext an!
- Keine abschließende Definition (im Sinne einer Liste)
- Risiko eines Zahlungsbetrugs falls Vertraulichkeit nicht sichergestellt
- S. MaSI FAQs, S. 3 – 5

Nicht sensible Zahlungsdaten im Sinne der PSD2 müssen ggf. aber auch geschützt werden!



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

Häufige Fragen zum Rundschreiben 4/2015 (BA) – MaSI, vom 24.06.2016

Strong Customer Authentication

Starke Kundenauthentifizierung (SKA)

Starke Kundenauthentifizierung

BaFin

Wichtigste Änderungen gegenüber den 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

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 bzw. neuem ZAG. Die RTS werden Detailvorschriften zur Ausgestaltung der SKA sowie die Ausnahmen von dieser Pflicht enthalten.

Starke Kundenauthentifizierung

Wann ist eine starke Kundenauthentifizierung erforderlich?

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.

Was ist mit Lastschriften?

Starke Kundenauthentifizierung

SKA mit „dynamischer Verknüpfung“

Falls es sich bei (2) um einen elektronischen **Fern**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-Entwurf der EBA ist es **nicht erforderlich**, dass der dynamische Authentifizierungscode direkt aus Betrag und Empfänger-IBAN erzeugt wird

Was ist bei Sammelüberweisungen?

Starke Kundenauthentifizierung

Ausnahmen -1-

BaFin

Laut **EBA-Entwurf** der RTS:

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

Starke Kundenauthentifizierung

Ausnahmen -2-

- 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 -3-

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 -4-

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

Ausblick