



PSD2 Praktischer Leitfaden

für E-Commerce-Transaktionen



Inhalt

Einführung	3
Starke Kundenauthentifizierung	4
Faktoren zur Authentifizierung	4
Umsetzungszeitraum	4
EMV 3D Secure	5
Vorteile des Upgrades auf die neueste Version von EMV 3D Secure	5
Haftungsumkehr	5
Wie funktioniert es	6
Was bedeutet dies für meine Kunden?	7
Was bedeutet es für mich als Händler?	7
Wie kann Elavon mich unterstützen?	7

Einführung

Die Zahlungsdiensterichtlinie (PSD2) der Europäischen Kommission fordert bei jeder E-Commerce-Transaktion die Anwendung der starken Kundenauthentifizierung (Strong Customer Authentication, SCA).

Von 2017 bis Ende 2018 stiegen allein in Großbritannien die Verluste durch Kartenbetrug um 19 %. Der hieraus entstandene Schaden betrug rund 760 Mio. Euro¹. Die PSD2 hat zum Ziel, Betrug im Zahlungsverkehr zu reduzieren und so die Sicherheit für Verbraucher und Unternehmen EU-weit zu erhöhen.

- Sie betrifft alle Unternehmen mit Sitz oder Kundenstamm im Europäischen Wirtschaftsraum (EWR), die Kartenzahlungen akzeptieren.
- Diese Gesetze führen Sicherheitsmaßnahmen ein, die als Zwei-Faktor-Authentifizierung bezeichnet werden, um die Sicherheit der Kunden bei Onlinezahlungen zu erhöhen. Dies ist eine branchenweite Änderung.
- Unternehmen müssen ihre Zahlungsinfrastruktur aktualisieren, um die Zwei-Faktor-Authentifizierung zu unterstützen. Damit erhalten alle am Ökosystem beteiligten Parteien verbesserte Daten, was zu qualitativ besseren Autorisierungsentscheidungen führt.
- Elavons SCA-Lösungen nutzen die neueste Technologie, um eine Risikoanalyse in Echtzeit zu ermöglichen, die Ihren Kunden ein reibungsloses Benutzererlebnis verschafft.
- Die erhöhten Sicherheits- und Kontrollstandards werden den Kunden direkt zugutekommen und ihr Vertrauen ins Online-Shopping erhöhen.



**Kartenbetrug kostete
die Unternehmen
im Jahr 2018
760 Mio. €¹.**

1. [statista.com/statistics/911873/value-of-losses-to-card-fraud-in-europe-by-country/](https://www.statista.com/statistics/911873/value-of-losses-to-card-fraud-in-europe-by-country/)



Starke Kundenauthentifizierung

Starke Kundenauthentifizierung bedeutet, dass Banken die Identität des Karteninhabers überprüfen müssen, bevor sie eine Transaktion genehmigen.

Um nachzuweisen, dass der Karteninhaber der tatsächliche Eigentümer der Karte ist, muss er seiner Bank auf Anfrage mindestens zwei von drei möglichen Faktoren zur Authentifizierung übermitteln.

Faktoren zur Authentifizierung

Diese können eine beliebige Kombination aus zwei der folgenden Optionen beinhalten:

Wissen – dies bezieht sich auf ein Merkmal, das nur der Karteninhaber und seine Bank kennen.

Ein Passcode oder eine einprägsame Information ist bereits die branchenübliche Methode, um diese Anforderung zu erfüllen.



Besitz – dies bezieht sich auf ein Merkmal, das der Karteninhaber besitzt und das von seiner Bank anerkannt wird.

Ein RFID-Transponder oder ein Telefon erfüllen automatisch diese Anforderung.



Persönliches – dies bezieht sich auf ein einzigartiges Merkmal des Karteninhabers, das von seiner Bank überprüfbar ist.

Fingerabdruck, Gesichts- und Spracherkennung oder Iris-Scan sind Beispiele für Merkmale, die durch die Weiterentwicklung der Technologie zunehmend genutzt werden.



Umsetzungszeitraum

Die Europäische Bankenaufsichtsbehörde (EBA) hat die Komplexität und die Herausforderungen bei der Umsetzung dieser Richtlinie im Umfeld des Zahlungsverkehrs erkannt und die ursprüngliche Frist verlängert. Die neue Frist für die Umsetzung der Richtlinie im E-Commerce in Europa ist der 31. Dezember 2020.

Diese zusätzliche Zeit wird benötigt, um sicherzustellen, dass alle Beteiligten des Ökosystems (Banken, Zahlungsdienstleister, Gateway-Provider und Händler) in der Lage sind, sich mit den relevanten Werkzeugen zur vollständigen Umsetzung von PSD2 auszustatten. Sie sind verpflichtet, diese Frist einzuhalten und die Auswirkungen auf Ihre Kunden zu minimieren.

Händler sollten den Migrationszeitraum vollständig ausnutzen. Sie müssen weiterhin mit Ihren Lösungsanbietern und Lieferanten zusammenarbeiten, um sicherzustellen, dass die branchenüblichen EMV 3D Secure-Protokolle vorhanden sind, um eine Zwei-Faktor-Authentifizierung Ihrer Kunden durch deren Banken zu ermöglichen.

Die neue Frist für die Umsetzung der Richtlinie bei E-Commerce-Transaktionen in der EU ist der 31. Dezember 2020.



EMV 3D Secure

EMV 3D Secure ist das Standardprotokoll für SCA bei der Akzeptanz von Zahlungen über das Internet. Es hilft, die Betrugs- und Abbruchquoten beim Einkauf zu senken, indem es bestehende Daten nahtlos mit zusätzlichen Informationen ergänzt.

Die Aktualisierung auf die neueste Version gibt Ihnen als Händler mehr Flexibilität. Gleichzeitig sorgt es für die traditionelle Haftungsumkehr, die bei der Anwendung von EMV 3D Secure erwartet wird.

EMV 3D Secure	2.1	2.2
SCA für angeschlossene Geräte und Internethandel	✓	✓
Szenarien zur Authentifizierung ohne Bezahlung, wie etwa die Aufnahme von Zahlungskarten in Händler-Apps	✓	✓
Unterstützt alle verfügbaren SCA-Freistellungsarten		✓
Europaspezifische Szenarien zur Unterstützung von PSD2, wie etwa vertrauenswürdige Empfänger und delegierte Authentifizierung		✓
Biometrische Nutzererfahrung der Verbraucher		✓

Machen Sie sich bereit für die Authentifizierung mit der neuesten verfügbaren Version des EMV 3D Secure-Frameworks. Planen Sie zusammen mit Ihrem Gateway-Provider schon jetzt die Migration auf die neueste Version von EMV 3D Secure, da sie im Laufe des Jahres 2020 verfügbar sein wird.

Mit diesen Upgrades profitieren Sie von der größtmöglichen Anzahl an Freistellungsarten.



Vorteile des Upgrades auf die neueste Version von EMV 3D Secure

- Größeres Vertrauen der Karteninhaber in Transaktionen mit Ihrem Unternehmen
- Weniger Betrug und Rückbuchungen – Haftungsschutz
- Verhinderung von nicht authentifizierten abgelehnten Transaktionen
- Verbesserte risikobasierte Entscheidungen führen zu höheren Genehmigungsraten
- Volle Unterstützung aller verfügbaren Freistellungsarten und Zahlungsgerätearten

Haftungsumkehr

Sobald Sie EMV 3D Secure zur Authentifizierung nutzen, besteht für Ihr Unternehmen ein minimales Risiko der Rückbuchung.

Aktivierungsdaten für die Haftungsumkehr sind variabel, abhängig vom Gateway und der Region. Wenden Sie sich bitte an Ihren Gateway-Provider, um das für Sie gültige Datum zu erfahren.

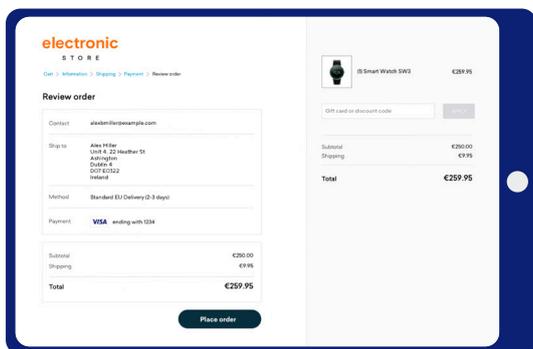


Wie funktioniert es

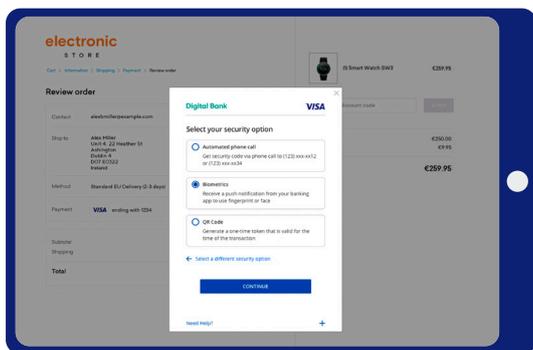


Was bedeutet dies für meine Kunden?

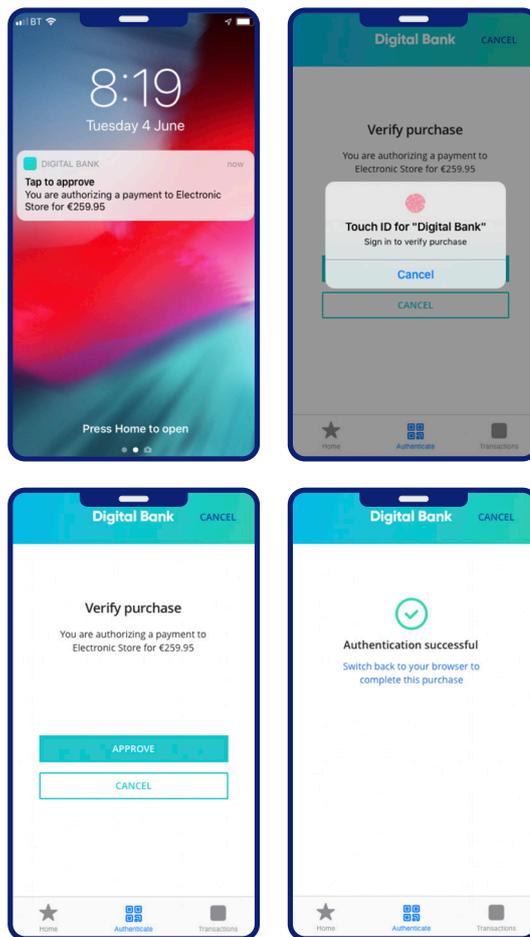
1. Ein Kunde möchte mit seinem PC, Laptop, Mobiltelefon oder einem anderen Gerät einen Onlinekauf tätigen und geht auf Ihre Kassen-Seite.



2. Um die Transaktion abzuschließen, kann er seine Verifizierungsmethode wählen oder der bevorzugten Methode seines Kartenausstellers folgen.



3. Er muss nur die Anweisungen befolgen, um seinen Kauf abzuschließen.



Was bedeutet es für mich als Händler?

Mit den neuen Regeln erfordern die meisten Online-Transaktionen eine verbesserte SCA - ganz im Gegensatz zu heute, wo Sie SCA wahlweise anwenden können oder nicht.

Wir empfehlen Ihnen, die neueste Version von EMV 3D Secure so bald wie möglich zu verwenden.

Setzen Sie sich mit Ihrem Gateway-Provider in Verbindung,

um die neueste Version von EMV 3D Secure einzuführen.



Wie kann Elavon mich unterstützen?

Elavon ist für seine technischen Fähigkeiten und soliden Geschäftspraktiken bekannt. Wir sind international stark vertreten und zeichnen uns durch technische Integration und Compliance aus. Wir arbeiten weiterhin mit den Kartenorganisationen und den Kartenausstellern zusammen, um die Einhaltung von PSD2 zu gewährleisten.

Profitieren Sie von unserem Fachwissen und unseren Beratungsleistungen im Zahlungswesen.

Sie können sich darauf verlassen, dass wir Sie mit erstklassigen Lösungen und Beratung unterstützen.

Noch Fragen? Ihr Elavon Kundenberater ist gerne für Sie da.

We make it possible. You make it happen.

 (069) 517 09 969

 [elavon.de](https://www.elavon.de)



Elavon Financial Services DAC, Sitz der Gesellschaft: Loughlinstown, Co. Dublin, Irland. Registriert in Irland unter der Nr. 418442.
Verwaltungsrat: Craig Gifford, Andrew Hastings, Shailesh Kotwal, Declan Lynch, Troy Remington, Adrian Wrafter, James Walker, Stephen Groarke. Niederlassung Deutschland: Lyoner Str. 36, 60528 Frankfurt.
Amtsgericht Frankfurt/M. HRB 81245.
Zuständige Aufsichtsbehörden: Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Central Bank of Ireland.
Y3604V10120