DirectLink with 3-D Secure

ingenico
ePayments

Inhaltsverzeichnisses

1. 3-D Secure v1.0

1.1 Einleitung

Das 3-D Secure-Protokoll gestattet es, den Karteninhaber während des Kaufprozesses zu identifizieren. Der Karteninhaber muss während des Identifikationsprozesses mit dem Internet verbunden sein. Deshalb funktioniert 3-D Secure nicht für Callcenter- oder wiederkehrende Zahlungen.

Visa hat das Protokoll 3-D Secure unter dem Namen Verified By Visa implementiert, MasterCard unter dem Namen SecureCode, JCB unter dem Namen J-Secure und American Express unter dem Namen SafeKey.

Das Prinzip der Integration von DirectLink mit 3-D Secure ist, eine Zahlung im DirectLink-Modus zu initiieren und sie im e-Commerce-Modus zu beenden, wenn eine Authentifizierung des Karteninhabers verlangt wird.

Dieses Dokument beschreibt die Integration des Protokolls 3-D Secure in DirectLink. Weitere Informationen über DirectLink oder e-Commerce entnehmen Sie bitte der Dokumentation zu DirectLink oder e-Commerce.

1.2 Ablauf der 3-D-Transaktion über DirectLink

Der Transaktionsablauf umfasst folgende Schritte:

1. Sie senden uns für die Transaktion eine DirectLink-Anfrage mit einer Reihe von zusätzlichen Parametern (vgl. Zusätzliche Anfrageparameter).
2. Unser System empfängt die Kartennummer in Ihrer Anfrage und prüft online, ob die Karte im VISA-, Mastercard-, JCB- bzw. AmEx-Verzeichnis eingetragen ist (eingetragen bedeutet, dass eine Identifikation für die Kartennummer möglich ist, d. h. die Karte ist eine 3-D Secure-Karte).
3. Ist der Karteninhaber registriert, enthält die Antwort auf die DirectLink-Anfrage einen bestimmten Zahlungsstatus und HTML-Code, der an den Kunden zurückgegeben muss, um den Identifikationsprozess zu starten (vgl. Zusätzliche Rückgabefelder). Der Block aus HTML-Code startet automatisch den Identifikationsprozess zwischen dem Karteninhaber (Kunde) und seiner ausstellenden Bank.
4. Der Karteninhaber identifiziert sich selbst auf der Seite der ausstellenden Bank.
5. Unser System empfängt die Identifikationsantwort vom Aussteller.
6. Wenn die Identifikation erfolgreich war, übermittelt unser System die eigentliche Finanztransaktion an den Acquirer.
7. Das Ergebnis der globalen Identifikation und des Online-Autorisierungsvorgangs erhalten Sie über e-Commerce-Modus-Rückmeldungskanäle.

Anmerkungen:

- Ob die Haftungsumkehr gilt, hängt von Ihrem Acquirer-Vertrag ab. Daher empfehlen wir Ihnen, die Allgemeinen Geschäftsbedingungen Ihres Acquirers zu prüfen.
- Wenn der Karteninhaber nicht (in Schritt 3) registriert wurde, erhalten Sie die XML-Standardantwort mit dem Ergebnis des Online-Autorisierungsprozesses.
- Um die genauen Zahlungsstatus-/Fehlercodes (in Schritt 7) zu erhalten, müssen Sie die Online- oder Offline-Post-Sale-Rückmeldungen wie in der E-Commerce-Dokumentation beschrieben implementieren.

1.2.1 Zusätzliche Anfrageparameter

Neben den DirectLink-Standardparametern müssen auch folgende Informationen gesendet werden:

Feld	Beschreibung

Feld	Beschreibung
FLAG3D	Fester Wert: "Y" Weist unser System an, bei Bedarf 3-D Secure-Identifikation auszuführen.
HTTP_ACCEPT	Das Feld „Accept request header“ im Browser des Karteninhabers, mit dem angegeben wird, welche Medientypen für die Antwort angenommen werden können. Mit diesem Wert kontrolliert der Aussteller, ob der Browser des Karteninhabers mit dem Identifikationssystem des Ausstellers kompatibel ist. Zum Beispiel: Accept: */*
HTTP_USER_AGENT	Das Feld „User-Agent request-header“ im Browser des Karteninhabers mit Informationen über den User Agent, von dem die Anfrage ausgeht. Mit diesem Wert kontrolliert der Aussteller, ob der Browser des Karteninhabers mit dem Identifikationssystem des Ausstellers kompatibel ist. Zum Beispiel: User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0).
WIN3DS	Möglichkeit, dem Kunden die Identifikationsseite anzuzeigen. Mögliche Werte: • MAINW: Die Identifikationsseite im Hauptfenster anzeigen (Standardwert). • POPUP: Die Identifikationsseite in einem Popup-Fenster anzeigen und am Ende zum Hauptfenster zurückkehren. • POPIX: Die Identifikationsseite in einem Popup-Fenster anzeigen und im Popup-Fenster bleiben.
ACCEPTURL	URL der Webseite, die dem Kunden angezeigt wird, wenn die Zahlung autorisiert ist.
DECLINEURL	URL, an die der Kunde weitergeleitet wird, wenn die maximale Anzahl an fehlgeschlagenen Autorisierungsversuchen erreicht ist (Standardwert 10, er kann aber auf der Seite „Technische Informationen“, Registerkarte „Globale Transaktionsparameter“, Abschnitt „Zahlungswiederholungsversuche“ geändert werden).
EXCEPTIONURL	URL der Webseite, die dem Kunden angezeigt wird, wenn das Zahlungsergebnis unsicher ist.
PARAMPLUS	Feld zum Senden der verschiedenen Parameter und ihrer Werte, die in der Post-Sale-Anfrage oder in der endgültigen Weiterleitung zurückgegeben werden sollen.
COMPLUS	Feld zum Senden eines Wertes, der in der Post-Sale-Anfrage oder in der Ausgabe zurückgegeben werden soll.
LANGUAGE	Sprache des Kunden, zum Beispiel: "en_US"
Optional	
TP	Um das Layout der "order_A3DS"-Seite zu ändern, können Sie eine(n) Templatenamen/-URL mit diesem Parameter senden. e-Commerce: Dynamische Vorlage).

Für weitere Informationen siehe Transaction-feedback.

1.2.2 Zusätzliche Rückgabefelder

Wenn der Karteninhaber nicht registriert ist, wird die normale DirectLink-Antwort zurückgegeben. Wenn der Karteninhaber registriert ist, werden die folgenden (zusätzlichen) Felder zurückgegeben:

Field	Beschreibung
STATUS	Neuer Wert: "46" (Warten auf Identifikation)
HTML_ANSWER	BASE64-codierter HTML-Code zum Einfügen auf der HTML-Seite, die an den Kunden zurückgegeben wird. Dieser Tag wird als untergeordnetes Element des globalen XML-Tags <ncresponse> hinzugefügt. Das Feld HTML_ANSWER enthält HTML-Code, der in die HTML-Seite, die an den Kunden zurückgegeben wird, eingefügt werden muss. Dieser Code lädt automatisch die Identifikationsseite der ausstellenden Bank in einem Pop-up im Hauptfenster in Abhängigkeit vom Parameterwert WIN3DS. Damit es nicht zu Wechselwirkungen zwischen HTML-Tags im Inhalt des XML-Tags HTML_ANSWER mit dem übrigen XML-Code kommt, der als Antwort auf die DirectLink-Anfrage ausgegeben wird, wird der Inhalt von HTML_ANSWER vor Ausgabe der Antwort BASE64-codiert. Deshalb muss dieser Inhalt BASE64-decodiert werden, bevor er in die HTML-Seite, die an den Karteninhaber gesendet wird, eingefügt wird.

1.2.3 Anmerkungen

Testkarten

Mit den folgenden Testkarten können Sie eine registrierte 3-D Secure-Karte in unserer Testumgebung simulieren:

Marke	Kartenummer	Ablaufdatum	Passwort
VISA	4000000000000002	Beliebiges Datum in der Zukunft	1111
MasterCard	5300000000000006	Beliebiges Datum in der Zukunft	11111
American Express	371449635311004	Beliebiges Datum in der Zukunft	11111

Falsche Identifikation

Wenn eine Transaktion wegen einer fehlerhaften Identifikation blockiert ist, hat die Transaktion das Ergebnis:

STATUS = 0

NCSTATUS = 5

NCERROR = 40001134

2. 3-D Secure v2.1 (Verfügbar in TEST)

2.1 Introduction

Im Jahr 2013 veröffentlichte die Europäische Kommission einen Vorschlag für die überarbeitete Version der Richtlinie über Zahlungsdienste (PSD2) zur Vereinfachung der Zahlungsabwicklung und Erstellung von Regeln und Vorschriften für Zahlungsdienste in der EU. Dort wurde auch die Notwendigkeit einer neuen Version von 3D Secure v2.1 erkannt.

Die größte Änderung besteht darin, dass Sie als Händler aufgefordert werden, mehr Daten zu teilen: Die Emittenten verlangen nach Datenpunkten zur Verbesserung der Genauigkeit ihrer Entscheidung, was letztendlich zu einem reibungslosen Szenario führt, aber Sie sind an der vordersten Front, um die Daten zu erfassen. Der 3DS v2-Ansatz zur Risikobewertung ist effektiver, erfordert jedoch eine Änderung des gesamten Ökosystems, sodass Sie die Daten an den Emittenten weitergeben können.

Die Kreditkartenunternehmen haben mit der Einführung dieser neuen Richtlinie außerdem ihre 3DS-Logos aktualisiert. Da Sie Ihre eigene Zahlungsseite erstellen, sollten Sie dafür sorgen, dass Sie diese neuen Logos Ihrer Zahlungsseite hinzufügen (Visa / Mastercard / JCB /…).

2.2 Ablauf der 3-D-Transaktion über DirectLink

Der Transaktionsfluss umfasst die folgenden Schritte:

1. Sie senden uns eine DirectLink-Anfrage für die Transaktion mit einer Reihe zusätzlicher Parameter.

Diese Parameter können aus drei Sätzen bestehen:

a. Erforderliche Parameter, die auf der Zahlungsseite erfasst werden müssen, auf der der Karteninhaber die Kartendaten eingibt.

Parameter	Beschreibung	Format	Verpflichtend
browserAcceptHeader	Exakter Inhalt des von HTTP akzeptierten Headers, die vom Browser des Karteninhabers an den Händler gesendet werden.*	Länge: variabel, maximal 2.048 Zeichen Datentyp: String Gültiger Wert: Wenn die Gesamtlänge des vom Browser gesendeten akzeptierten Headers 2.048 Zeichen überschreitet, schneidet der 3DS-Server den überschüssigen Teil ab.	Ja
browserColorDepth	Wert, der die Bittiefe der Farbpalette für die Anzeige von Bildern in Bit pro Pixel darstellt. Wird vom Karteninhaber-Browser unter Verwendung der Bildschirmfarbeigenschaft ‚Tiefe' abgerufen.	Datentyp: String Gültige Werte: 1 = 1 Bit 4 = 4 Bit 8 = 8 Bit 5 = 15 Bit 16 = 16 Bit 24 = 24 Bit 32 = 32 Bit 48 = 48 Bit	Ja
browserJavaEnabled	Boolescher Wert, ob der Karteninhaber-Browser Java ausführen kann. Der Wert wird vom Attribut „Navigator-Java aktiviert" zurückgegeben.	Datentyp: Boolescher Wert Gültige Werte: true false	Ja

Parameter	Beschreibung	Format	Verpflichtend
browserLanguage	Wert, der die Browser-Sprache wie in IETF BCP47 definiert darstellt. Aus dem Attribut „Navigatorsprache“ zurückgegeben.	JSON-Datentyp: String Länge: variabel, 1–8 Zeichen	Ja
browserScreenHeight	Gesamthöhe des Karteninhaber-Bildschirms in Pixeln. Der Wert wird vom Attribut „Bildschirmhöhe“ wiedergegeben.	Datentyp: Int Zwischen 0 und 999999	Ja
browserScreenWidth	Gesamtbreite des Karteninhaber-Bildschirms in Pixeln. Der Wert wird vom Attribut „Bildschirmbreite“ wiedergegeben.	Datentyp: Int Zwischen 0 und 999999	Ja
browserTimeZone	Zeitunterschied zwischen UTC-Zeit und Ortszeit des Karteninhaber-Browsers in Minuten.	Datentyp: Int Zwischen -720 und 840	Ja
browserUserAgent	Genauer Inhalt des HTTP-Benutzeragent-Headers. *	Datentyp: String Länge: variabel, maximal 2.048 Zeichen Hinweis: Wenn die Gesamtlänge des vom Browser gesendeten Benutzeragents 2.048 Zeichen überschreitet, schneidet der 3DS-Server den überschüssigen Teil ab.	Ja

*HTTP_ACCEPT und HTTP_USER_AGENT müssen nicht mit browserAcceptHeader und browserUserAgent gesendet werden, da wir sie sonst mit den Browserparametern füllen.

Hinweis: Bitte vergessen Sie nicht, die Parameter in Ihrer SHA-Signatur zu berechnen.

Sie können den folgenden Javascript-Code verwenden, um diese Parameter zu erfassen.

```
<script type="text/javascript" language="javascript">

function createHiddenInput(form, name, value)
{
var input = document.createElement("input");
input.setAttribute("type", "hidden");
input.setAttribute("name", name);
input.setAttribute("value", value);
form.appendChild(input);
}

var myCCForms = document.getElementsByName("MyForm");
if (myCCForms != null && myCCForms.length > 0)
{
var myCCForm = myCCForms[0];
createHiddenInput(myCCForm, "browserColorDepth", screen.colorDepth);
createHiddenInput(myCCForm, "browserJavaEnabled", navigator.javaEnabled());
```

```
createHiddenInput(myCCForm, "browserLanguage", navigator.language);
createHiddenInput(myCCForm, "browserScreenHeight", screen.height);
createHiddenInput(myCCForm, "browserScreenWidth", screen.width);
createHiddenInput(myCCForm, "browserTimeZone", new Date().getTimezoneOffset());
}
</script>
```

b. Zusätzliche benötigte Parameter (vgl. Zusätzliche Anfrageparameter).

c. Empfohlene Parameter (Liste der Parameter) die, wenn gesendet, sich positiv auf die Transaktions-Conversion-Rate auswirken. Basierend auf den in diesen Parametern enthaltenen Informationen kann ein potenzieller reibungsloser Authentifizierungsablauf stattfinden. Dabei muss sich der Karteninhaber nicht mehr authentifizieren und daher wird ein schnellerer Abschluss der Transaktion erwartet. Wenn jedoch keiner dieser Parameter angegeben wird, findet die normale Umleitung in Bezug auf die Authentifizierung statt.

Obwohl diese Parameter optional sind, wird jedoch von den großen Kartenanbietern dringend empfohlen, dass die folgenden Parameter in Ihrer Anfrage enthalten sein sollten, da dadurch die Chancen für einen reibungslosen Fluss steigen.

ECOM_BILLTO_POSTAL_CITY
ECOM_BILLTO_POSTAL_COUNTRYCODE
ECOM_BILLTO_POSTAL_STREET_LINE1
ECOM_BILLTO_POSTAL_STREET_LINE2
ECOM_BILLTO_POSTAL_STREET_LINE3
ECOM_BILLTO_POSTAL_POSTALCODE
REMOTE_ADDR
CN
EMAIL

Unser System empfängt die Kartennummer in Ihrer Anfrage und prüft online, ob die Karte im VISA-, Mastercard-, JCB- bzw. AmEx-Verzeichnis eingetragen ist (eingetragen bedeutet, dass eine Identifikation für die Kartennummer möglich ist, d. h. die Karte ist eine 3-D Secure-Karte).

2. Basierend auf der Systemverzeichnisantwort werden zwei potenzielle Flüsse erwartet, wenn der Karteninhaber registriert wird (in 3D Secure), wobei zu berücksichtigen ist, ob die zusätzlichen Parameter in **1.c** (Empfohlene Parameter-Liste der Parameter) oben angegeben wurden:

2.1. **Ein reibungsloser Fluss:** Der Karteninhaber muss sich nicht physisch authentifizieren, da die Authentifizierung im Hintergrund ohne Eingabe erfolgt. In diesem Fall erfolgt die Haftungsschicht bei der ausstellenden Bank.
Ein problematischer Fluss: Der Karteninhaber muss sich weiter ausweisen.

ie Antwort auf die **DirectLink**-Anfrage enthält einen bestimmten Zahlungsstatus und einen HTML-Code. Dieser muss an den Kunden zurückgegeben werden, um den Identifikationsprozess zu starten (siehe Zusätzliche Rückgabefelder). Der HTML-Code-Block startet automatisch den Identifikationsprozess zwischen dem Karteninhaber (Kunden) und seiner ausstellenden Bank.

er Karteninhaber identifiziert sich selbst auf der Seite der ausstellenden Bank.

Jnser System empfängt die Identifikationsantwort vom Aussteller.

Wenn die Identifikation erfolgreich war, übermittelt unser System die eigentliche Finanztransaktion an den Acquirer.

3. Das Ergebnis der globalen Identifikation und des Online-Autorisierungsvorgangs erhalten Sie über e-Commerce-Modus-Rückmeldungskanäle.

2.2.1 Zusätzliche Anfrageparameter

Neben den DirectLink-Standardparametern müssen auch folgende Informationen gesendet werden:

Feld	Beschreibung
FLAG3D	Fester Wert: "Y" Weist unser System an, bei Bedarf 3-D Secure-Identifikation auszuführen.
HTTP_ACCEPT	Das Feld „Accept request header“ im Browser des Karteninhabers, mit dem angegeben wird, welche Medientypen für die Antwort angenommen werden können. Mit diesem Wert kontrolliert der Aussteller, ob der Browser des Karteninhabers mit dem Identifikationssystem des Ausstellers kompatibel ist. * Zum Beispiel: Accept: */*
HTTP_USER_AGENT	Das Feld „User-Agent request-header“ im Browser des Karteninhabers mit Informationen über den User Agent, von dem die Anfrage ausgeht. Mit diesem Wert kontrolliert der Aussteller, ob der Browser des Karteninhabers mit dem Identifikationssystem des Ausstellers kompatibel ist. * Zum Beispiel: User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0).
WIN3DS	Möglichkeit, dem Kunden die Identifikationsseite anzuzeigen. Mögliche Werte: • MAINW: Die Identifikationsseite im Hauptfenster anzeigen (Standardwert). • POPUP: Die Identifikationsseite in einem Popup-Fenster anzeigen und am Ende zum Hauptfenster zurückkehren. • POPIX: Die Identifikationsseite in einem Popup-Fenster anzeigen und im Popup-Fenster bleiben.
ACCEPTURL	URL der Webseite, die dem Kunden angezeigt wird, wenn die Zahlung autorisiert ist.
DECLINEURL	URL, an die der Kunde weitergeleitet wird, wenn die maximale Anzahl an fehlgeschlagenen Autorisierungsversuchen erreicht ist (Standardwert 10, er kann aber auf der Seite „Technische Informationen“, Registerkarte „Globale Transaktionsparameter“, Abschnitt „Zahlungswiederholungsversuche“ geändert werden).
EXCEPTIONURL	URL der Webseite, die dem Kunden angezeigt wird, wenn das Zahlungsergebnis unsicher ist.
PARAMPLUS	Feld zum Senden der verschiedenen Parameter und ihrer Werte, die in der Post-Sale-Anfrage oder in der endgültigen Weiterleitung zurückgegeben werden sollen.
COMPLUS	Feld zum Senden eines Wertes, der in der Post-Sale-Anfrage oder in der Ausgabe zurückgegeben werden soll.
LANGUAGE	Sprache des Kunden, zum Beispiel: "en_US"
Optional	
TP	Um das Layout der "order_A3DS"-Seite zu ändern, können Sie eine(n) Templatenamen/-URL mit diesem Parameter senden. e-Commerce: Dynamische Vorlage).

*HTTP_ACCEPT und HTTP_USER_AGENT müssen beim Senden von browserAcceptHeader und browserUserAgent nicht gesendet werden.

Für weitere Informationen siehe Transaction-feedback.

2.2.2 Zusätzliche Rückgabefelder

Wenn der Karteninhaber nicht registriert ist, wird die normale DirectLink-Antwort zurückgegeben. Wenn der Karteninhaber registriert ist, werden die folgenden (zusätzlichen) Felder zurückgegeben:

Field	Beschreibung
STATUS	Neuer Wert: "46" (Warten auf Identifikation)
HTML_ANSWER	BASE64-codierter HTML-Code zum Einfügen auf der HTML-Seite, die an den Kunden zurückgegeben wird. Dieser Tag wird als untergeordnetes Element des globalen XML-Tags <ncresponse> hinzugefügt. Das Feld HTML_ANSWER enthält HTML-Code, der in die HTML-Seite, die an den Kunden zurückgegeben wird, eingefügt werden muss. Dieser Code lädt automatisch die Identifikationsseite der ausstellenden Bank in einem Pop-up im Hauptfenster in Abhängigkeit vom Parameterwert WIN3DS. Damit es nicht zu Wechselwirkungen zwischen HTML-Tags im Inhalt des XML-Tags HTML_ANSWER mit dem übrigen XML-Code kommt, der als Antwort auf die DirectLink-Anfrage ausgegeben wird, wird der Inhalt von HTML_ANSWER vor Ausgabe der Antwort BASE64-codiert. Deshalb muss dieser Inhalt BASE64-decodiert werden, bevor er in die HTML-Seite, die an den Karteninhaber gesendet wird, eingefügt wird.

2.2.3 Anmerkungen

Testkarten

Mit den folgenden Testkarten können Sie eine registrierte 3-D Secure-Karte in unserer Testumgebung simulieren:

Reibungsloser Fluss Marke	Kartenummer	Ablaufdatum
VISA	4186455175836497	Beliebiges Datum in der Zukunft
Mastercard	5137009801943438	Beliebiges Datum in der Zukunft
American Express	375418081197346	Beliebiges Datum in der Zukunft

Problematischer Fluss Marke	Kartenummer	Ablaufdatum
VISA	4874970686672022	Beliebiges Datum in der Zukunft
Mastercard	5130257474533310	Beliebiges Datum in der Zukunft
American Express	379764422997381	Beliebiges Datum in der Zukunft

Hinweis: Weitere Testkartennummern können hier heruntergeladen werden

Falsche Identifikation

Wenn eine Transaktion wegen einer fehlerhaften Identifikation blockiert ist, hat die Transaktion das Ergebnis:

STATUS = 0

NCSTATUS = 5

NCERROR = 40001134

2.3 Ausschlüsse und Ausnahmen für 3DsV2

2.3.1 3DSv2 und Ausschlüsse

Mit der Einführung von 3DSv2 wird die Authentifizierung der Karteninhaber im Allgemeinen obligatorisch, wie in der Zweiten Zahlungsdiensterichtlinie der EU (2015/2366 PSD2) festgelegt. Trotzdem werden einige Transaktionen von dieser Regel ausgeschlossen, wenn eines der folgenden Szenarien gilt:

- Bestellung per E-Mail/telefonische Bestellung
- One leg journey - Der PSP (der Acquirer) des/der Zahlungsempfängers/Zahlungsempfängin oder der PSP (die Hausbank) des/der Zahlenden befindet sich außerhalb des EWR
- Übertragbare Prepaid-Karten mit Guthaben von bis zu 150€ (Artikel 63)
- MIT - vom Händler initiierte Transaktionen

2.3.2 SCA und 3DS reibungsloser / Challenge-Flow

Teil dieser neuen Regelung ist die Strong Customer Authentication (SCA). Dies beinhaltet die Möglichkeit, dass der Herausgeber (die Bank des Karteninhabers) zusätzliche Angaben vom Karteninhaber erfragt. In einem solchen Szenario führt der Authentifizierungsprozess zu einem Challenge-Flow (erfordert vom Karteninhaber eine aktive Authentifizierung) und nicht zu einem reibungslosen Flow (erfordert keine Authentifizierung durch den Karteninhaber).
Wir bieten unseren Händlern allerdings die Möglichkeit, den bevorzugten Flow anzugeben. Dies kann durch die Übermittlung zusätzlicher Parameter erreicht werden, die vom Herausgeber zur Risikobewertung verwendet werden. Je nach Entscheidung des Herausgebers kann ein reibungsloser Flow stattfinden. In einigen Szenarien könnte 3DS sogar völlig übersprungen werden, wenn bestimmte Ausnahmen gelten

2.3.3 Angabe des bevorzugten Flows

Zur Angabe der Präferenz für einen reibungslosen Flow während der Authentifizierungsanforderung kann der Händler den zusätzlichen Parameter Mpi.threeDSRequestorChallengeIndicator senden. Je nach Einschätzung des Betrugsrisikos durch den Händler können spezifische Werte gesendet werden (z. B. für eine geringe Risikobewertung: 02, für ein erhöhtes Betrugsrisiko: 03)

Parameter	Werte	Obligatorisch / Optional
Mpi.threeDSRequestorChallengeIndicator	01 = Kein Präferenz 02 = Keine Abfrage angefordert 03 = Keine Abfrage angefordert; Händlerpräferenz 04 = Abfrage angefordert: Mandat	Obligatorisch (falls ein Flow bevorzugt wird)

Der Händler kann zusätzlich die Möglichkeit eines reibungslosen Flow / Umwandlungssatzes durch Senden weiterer optionaler Felder erhöhen.

2.3.4 Ausnahmen von 3DS

Bei einigen Transaktionen kann der Händler möglicherweise 3DS überspringen (was zu einem reibungslosen Flow führt) und sich direkt für die Autorisierung entscheiden. Dieser Prozess beschränkt sich auf Transaktionen, die entweder von SCA ausgeschlossen werden (wie oben beschrieben) oder die von spezifischen Ausnahmen profitieren können. Diese Ausnahmen müssen Teil einer Vereinbarung zwischen dem Händler und seinem Erwerber sein. In einem Szenario wie diesem gibt der Händler an, dass er den Authentifizierungsprozess überspringen

möchte, indem er diese zusätzlichen Parameter sendet:

Parameter	Werte	Obligatorisch / Optional
FLAG3D	N = Überspringen des 3DS-Authentifizierungsprozesses	Obligatorisch (falls 3DS übersprungen werden soll)
3DS_EXEMPTION_INDICATOR	Angabe einer Begründung für das Überspringen von 3DS. Die numerischen Werte können je nach Transaktion zutreffend sein 03 = Herausgeber TRA* 04 = Ausnahme für einen geringen Betrag 05 = Händler/Erwerber TRA* 06 = Auf die weiße Liste setzen 07 = Unternehmen 08 = Verspäteter Versand 09 = Delegierte Authentifizierung (zertifiziertes Wallet)	Obligatorisch (falls 3DS übersprungen werden soll)

* Analyse des Transaktionsrisikos

Es bleibt jedoch dem Herausgeber überlassen, ob ein Authentifizierungsprozess stattfinden muss. Falls der Herausgeber auf 3DS besteht, wird die Transaktion abgelehnt.