Integration mit Ingenico ePayments DirectLink (Server-zu-Server)

Inhaltsverzeichnisses

1. Einleitung

DirectLink ermöglicht die Einrichtung speziell angepasster Verbindungen zwischen Ihren eigenen Applikationen und unserem System, so als wäre unser System einfach ein lokaler Server. Es bietet einen Programm-zu-Programm (Server-zu-Server) -Zugriff der Händlersoftware auf unsere Plattform für Zahlungen und Administration. Das Programm des Händlers interagiert dabei direkt und ohne menschlichen Eingriff mit unserer Remote-API.

Bei Verwendung von DirectLink gibt es keinen Kontakt zwischen unserem System und dem Kunden des Händlers. Der Händler sendet alle für die Zahlung erforderlichen Informationen in einer HTTPS Posting-Anfrage direkt an unser System. Unser System fragt die Finanztransaktion (synchron oder asynchron) beim betreffenden Akzeptanzpartner an und sendet dessen Antwort im XML-Format an den Händler zurück. Das Programm des Händlers liest die Antwort und setzt seine Verarbeitung fort.

Der Händler ist darum für die Sammlung und Speicherung sensibler Zahlungsdaten seiner Kunden verantwortlich. Er muss die Vertraulichkeit und Sicherheit dieser Daten durch verschlüsselte Web-Kommunikation und Sicherung seines Servers gewährleisten. Wenn der Händler keine sensiblen Daten wie beispielsweise Kartennummern speichern möchte, empfehlen wir die Nutzung der Alias-Option innerhalb seines Kontos (weitere Informationen hierzu finden Sie im Alias-Manager Integrationsleitfaden).

Der Händler kann neue Bestellungen verarbeiten, die Daten bestehender Bestellungen pflegen und den Status einer Bestellung mit DirectLink abfragen.

Auch wenn der Händler Anfragen mit DirectLink automatisiert hat, kann er die Historie einer Transaktion manuell im Back-Office einsehen. Hierzu kann er seinen Web-Browser verwenden oder einen Bericht herunterladen. Lesen Sie Informationen zur Konfiguration und Funktionalität des Administrator-Standortes bitte im Back-Office Anwenderhandbuch nach.

2. Allgemeine Vorgehensweisen und Sicherheitseinstellungen

Die folgenden allgemeinen Vorgehensweisen und Sicherheitskontrollen gelten für alle DirectLink-Anfragen: neue Bestellanfragen, Datenpflegeanfragen und Direktabrufe.

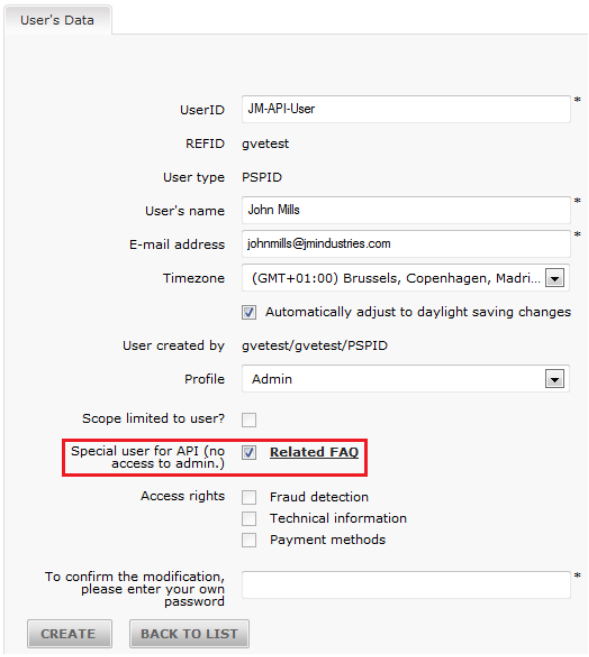
2.1 API-Benutzer

Ein API (Application Program Interface)-Benutzer wird benötigt, an den DirectLink-Anfragen gerichtet werden können.

Im Allgemeinen handelt es sich dabei um einen speziell erstellten Benutzer, der von einer Anwendung verwendet wird, um automatische Anfragen an die Zahlungsplattform zu richten.

Sie können in Ihrem Ingenico-Konto über „Konfiguration" > „Benutzer" einen API-Benutzer erstellen. Wählen Sie „Neuer Benutzer" und füllen Sie die Pflichtfelder aus.

Um den neuen Benutzer zu einem API-Benutzer zu machen, vergewissern Sie sich, dass Sie das Kästchen „Sonderbenutzer für API (Kein Zugriff auf Administration)" abhaken.



Wenn für einen API-Benutzer auch die verschiedenen Benutzerprofile zur Verfügung stehen, empfehlen wir Ihnen dringend, diesen Benutzer mit dem „Admin"-Profil zu konfigurieren.
Wenn Sie die Rechte für die Pflege von Transaktionen (Erstattungen, Abbruch, usw.) einschränken möchten, können Sie das Benutzerprofil noch zu z.B. „Kodierer" ändern.

Wenn Sie nicht sicher sind, empfehlen wir Ihnen, das „Admin"-Profil zu wählen; oder wechseln Sie zu den Benutzerprofilen (Benutzermanager) für mehr Informationen.

Das Passwort eines API-Benutzers muss nicht regelmäßig geändert werden. Das ist praktischer, wenn das Passwort fest in Ihrer Anwendung hinterlegt werden muss. Jedoch empfehlen wir, das Passwort von Zeit zu Zeit zu ändern.

Mehr Informationen über Benutzertypen und wie das Passwort des API-Benutzers geändert wird, finden Sie unter "Benutzertypen" (Benutzermanager).

2.2 Anfrageformat

Für neue Bestellanfragen, Datenpflegeanfragen und Direktabrufe muss der Händler die Anfragen mit bestimmten Parametern an bestimmte URLs senden. Die Parameter für Zahlung/Datenpflege/Abruf müssen in einer Posting-Anfrage wie folgt gesendet werden:

PSPID=value1&USERID=value2&PSWD=value3&...

Der Type/Subtyp zur Anzeige des Medientyps im Content-Type Entity-Header Feld der POST-Anfrage muss „application/x-www-form-urlencoded" lauten.

DirectLink arbeitet im Modus „eine Anfrage - eine Antwort". Jede Zahlung wird einzeln verarbeitet. Unser System handhabt individuelle Anfragen via DirectLink und kann synchron arbeiten (wenn diese Option technisch unterstützt wird). D. h. wir warten auf die Antwort der Bank, ehe wir eine XML-Antwort auf die Anfrage zurücksenden.

2.3 Sicherheit

Wenn wir auf unseren Servern eine Anfrage empfangen, prüfen wir das Verschlüsselungsniveau und die IP-Adresse, von der die Anfrage stammt.

2.3.1 Verschlüsselung

DirectLink baut auf einem robusten und sicheren Kommunikationsprotokoll auf. DirectLink API ist ein Instruktionsbestand, der über normale HTTPS Posting-Anfragen übermittelt wird.

Auf der Serverseite verwenden wir ein von Verisign bereitgestelltes Zertifikat. Die TLS-Verschlüsselung garantiert, dass Sie wirklich mit unseren Servern kommunizieren und dass die Daten in verschlüsselter Form übertragen werden. Ein clientseitiges TLS-Zertifikat ist nicht notwendig.

Wenn wir eine Anfrage erhalten, prüfen wir das Verschlüsselungsniveau. Wir erlauben dem Händler eine Verbindungsaufnahme mit uns nur im sicheren HTTPS-Modus unter Nutzung von TLS und wir raten dringend an, die neuesten und sichersten Versionen zu nutzen, welche gegenwärtig TLS 1.1 und 1.2 sind.

Anmerkung: Zum Zeitpunkt dieser Niederschrift unterstützen wir SSL v3 noch. Dieses Protokoll wird jedoch aufgrund bestimmter Anfälligkeiten auslaufen und letztendlich nicht mehr unterstützt werden.

2.3.2 IP-Adresse

Für jede Anfrage prüft unser System die IP-Adresse, von der die Anfrage kam, um sicherzustellen, dass die Anfragen wirklich vom Server des Händlers stammen. Im IP-Adressenfeld des Bereichs „Daten- und Ursprungsüberprüfung", Abschnitt „Überprüfungen für DirectLink" der Seite „Technische Informationen" Ihres Kontos müssen Sie die IP-Adressen oder IP-Adressbereiche der Server eintragen, die Ihre Anfragen an uns senden.

Wenn die IP-Adresse, von der die Anfrage stammt, im IP-Adressenfeld des Bereichs „Daten- und Ursprungsüberprüfung", Abschnitt „Überprüfungen für DirectLink", Seite „Technische Informationen" Ihres Kontos nicht angegeben ist, erhalten Sie die Fehlermeldung „unknown order/1/i". Die IP-Adresse, von der die Anfrage gesendet wurde, wird ebenfalls in dieser Fehlermeldung angezeigt.

2.3.3 Zusätzliche Sicherheit: SHA-Signatur

Für jede Bestellung erzeugt der Server des Händlers eine eindeutige Zeichenfolge, aus der mittels SHA1-, SHA-256- oder SHA-512-Algorithmus ein Hashcode generiert wird. Das Resultat dieses Hashvorgangs wird in der Bestellanfrage des Händlers an uns gesendet. Unser System rekonstruiert diesen Hashcode, um so die Datenintegrität der Bestellinformationen zu überprüfen, die an uns gesendet worden sind.

2.4 Auswertung der Antwort (Parsing)

Wir reagieren mit einer XML-Antwort auf Ihre Anfrage. Bitte sorgen Sie dafür, dass Ihre Systeme diese XML-Antwort mit größtmöglicher Toleranz auswerten (parsen). Vermeiden Sie beispielsweise Attributnamen, bei denen die Unterscheidung von Groß- und Kleinschreibung notwendig ist, schreiben Sie keine spezifische Reihenfolge für die in Antworten zurückgelieferten Attribute vor, sorgen Sie dafür, dass neue Attribute in der Antwort nicht zu Problemen führen, usw.

3. Neue Bestellungen anfragen

3.1 Anfrage-URL

- Die Anfrage-URL in der TESTUMGEBUNG lautet https://secure.ogone.com/ncol/test/orderdirect.asp.
- Die Anfrage-URL in der PRODUKTIVUMGEBUNG lautet https://secure.ogone.com/ncol/prod/orderdirect.asp.

Wichtig
Vergessen Sie nicht, in der Anfrage-URL die Zeichenfolge „test" durch „prod" zu ersetzen, wenn Sie auf Ihr reguläres Produktivkonto umstellen. Wenn Sie vergessen, die Anfrage-URL zu ändern und den regulären Betrieb mit realen Bestellungen aufnehmen, laufen Ihre Transaktionen weiter in die Testumgebung und werden nicht an die Akzeptanzpartner bzw. Banken gesendet.

3.2 Anfrageparameter

Die folgende Tabelle enthält die Anfrageparameter für das Senden einer neuen Bestellung:

Format: AN=alphanumerisch / N=numerisch, die maximal erlaubte Anzahl der Zeichen

Feld	Nutzung	Format	Pflicht
PSPID	Name Ihres Händlerkontos in unserem System.	AN, 30	Ja
ORDERID	Ihre eindeutige Bestellnummer (Händlerreferenz).	AN, 40	Ja
USERID	Name Ihres applikationsgebundenen (API-) Anwenders. Wie Sie einen API-Anwender anlegen, ist in der Benutzer ManagerDokumentation beschrieben.	AN, 20 (min 2)	Ja
PSWD	Passwort des API-Anwenders (USERID).	AN	Ja
AMOUNT	Zu zahlender Betrag, MULTIPLIZIERT MIT 100, da die Betragsangabe keine Dezimalstellen oder andere Trennzeichen enthalten darf.	N, 15	Ja
CURRENCY	Alphanumerischer Währungswert nach ISO, beispielsweise: EUR, USD, GBP, CHF, …	AN, 3	Ja
CARDNO	Karten-/Kontonummer.	AN, 21	Ja
ED	Ablaufdatum (MM/YY oder MMYY)	MM/YY or MMYY	Ja
COM	Beschreibung der Bestellung	AN, 100	Nein
CN	Name des Kunden	AN, 35	Nein
EMAIL	E-Mail-Adresse des Kunden.	AN, 50	Nein
SHASIGN	Signatur (gehashte Zeichenfolge) zur Authentifizierung der Daten (siehe SHA-Signatur).	AN, 128	Nein
CVC	Kartenverifikationscode. Je nach Kartenmarke entspricht der Verifikationscode einer 3- oder 4-stelligen Ziffernfolge auf der Vorder- oder Rückseite der Karte, einer Ausgabenummer, einem Beginndatum oder einem Geburtsdatum.	N, 5	Ja
ECOM_PAYMENT_ CARD_VERIFICATION	Identisch mit CVC	N, 5	Nein
OWNERADDRESS	Straße und Hausnummer des Kunden.	AN, 50	Nein
OWNERZIP	PLZ des Kunden	AN, 10	Nein
OWNERTOWN	Ortsname des Kunden	AN, 40	Nein
OWNERCTY	Land des Kunden, z. B. AT, DE, CH,	AN, 2	Nein
OWNERTELNO	Telefonnummer des Kunden.	AN, 30	Nein

Feld	Nutzung	Format	Pflicht
OPERATION	Bestimmt den Typ der angefragten Transaktion. Sie können eine Standardoperation (Zahlungsprozedur) im Bereich „Globale Transaktionsparameter", Abschnitt „Standardoperationswert", auf der Seite „Technische Informationen" konfigurieren. Wenn Sie einen expliziten Operationswert in der Anfrage mitsenden, erhält dieser Vorrang vor dem Standardwert. Mögliche Werte: • RES: Anfrage für Autorisierung (Reservierung). • SAL: Anfrage für Direktbuchung (Verkauf). • RFD: Gutschrift ohne Verknüpfung mit einer vorhergehenden Zahlung, darum keine Datenpflegeoperation an einer bestehenden Transaktion (diese Funktionalität können Sie nur mit besonderer Erlaubnis Ihres Akzeptanzpartners nutzen). • PAU: Vorautorisierungsanfrage In Absprache mit Ihrem Acquirer können Sie diesen Operationskode verwenden, um zeitweise Beträge auf der Karte eines Kunden zu reservieren. Momentan (10/2015) steht Vorautorisierung allein für MasterCard-Transaktionen zur Verfügung und wird nur durch ausgewählte Acquirer unterstützt. Dieser Operationskode kann nicht als Standarteinstellung in Ihrem Ingenico ePayments-Konto ausgewählt werden. Sollten Sie versuchen, Vorautorisierungen für Transaktionen vorzunehmen, bei denen der Acquirer oder die Kartenmarke solche Vorautorisierung nicht unterstützt, werden diese Transaktionen nicht blockiert sondern wie normale Autorisierungen (=RES) ausgeführt.	A, 3	Ja
WITHROOT	Fügt ein Root-Element in Ihre XML-Antwort ein. Mögliche Werte: 'Y' oder leer.	Y or <empty>	Nein
REMOTE_ADDR	IP-Adresse des Kunden (nur für Betrugserkennungsmodul). Wenn für die IP-Adresse keine Prüfung des Absenderlandes erforderlich ist, senden Sie 'NONE'.	AN	Nein
RTIMEOUT	Zeitüberschreitung für die Transaktion (in Sekunden, Wert zwischen 30 und 90). **Wichtig**: Der hier angegebene Wert muss kleiner als der Zeitüberschreitungswert in Ihrem System sein!	N, 2	Nein
ECI	Electronic Commerce Indicator. Sie können einen ECI-Standardwert im Bereich „Globale Transaktionsparameter", Abschnitt „Standard-ECI-Wert" der Seite „Technische Informationen" festlegen. Wenn Sie in der Anfrage einen ECI-Wert senden, erhält dieser Vorrang vor dem ECI-Standardwert. Zulässige (numerische) Werte: 0 - Karte durch Lesegerät gezogen 1 - Manuelle Eingabe: Post-/ Telefon- Bestellung (MOTO) (ohne Vorlage der Karte) 2 - Wiederkehrende Zahlungen, von MOTO stammend 3 - Ratenzahlungen 4 - Manuelle Eingabe, Karte hat vorgelegen 7 - E-Commerce mit SSL-Verschlüsselung 9 - Wiederkehrend nach erster E-Commerce-Transaktion	N, 2	Nein

Weitere informationen zu diesen Feldern finden Sie in Ihrem Ingenico ePayments konto. Melden Sie sich einfach an und gehen Sie zu : Support > Integrations & Benutzerhandbucher > Technische Handbucher > Paramater Cookbook.

Die folgenden Parameter sind relevant i.B.a. auf Credentials-/Card-on-file (COF) - Regularien, welche von den Kreditkartenunternehmen Visa / MasterCard vorgegeben werden. Detaillierte Informationen zu deren Verwendung finden Sie im separaten Kapitel "Transaktionen mit gespeicherten Anmeldedaten abwickeln".

COF_INITIATOR	Credential-on-file initiator Mögliche Werte: • CIT: Eine vom Karteninhaber ausgelöste Transaktion • MIT: Eine vom Händler ausgelöste Transaktion	AN	Nein
COF_SCHEDULE	Credential-on-files geplant (oder außerplanmäßig) Mögliche Werte: • SCHED: Eine regelmäßige Transaktion • UNSCHED: Eine unregelmäßige Transaktion	AN	Nein
COF_TRANSACTION	Credential-on-file transaction Mögliche Werte: • FIRST: Die erste von einer Reihe von Transaktionen	AN	Nein

	• SUBSEQ: Weitere Reihen von Transaktionen		
COF_RECURRING_EXPIRY	Enddatum: Tag der letzten regelmäßigen Zahlung einer Serie	Datum JJJJMMTT (z.B. 20190914)	Nein
COF_RECURRING_FREQUENCY	Anzahl Tage welche zwischen regelmäßigen Zahlungen	numerisch zwischen 2 und 4 Stellen (z.B. 1, 031 oder 0031)	Nein

Die Liste der für die Sendung zulässigen Parameter kann für Händler länger sein, die in ihren Konten bestimmte Optionen aktiviert haben. Bitte lesen Sie in der betreffenden Dokumentation weitere Informationen über zusätzliche Parameter nach, die mit diesen Optionen verbunden sind.

Die folgenden Parameter sind in neuen Bestellungen obligatorisch:

- PSPID und USERID
- PSWD
- ORDERID
- AMOUNT (x100)
- CURRENCY
- CARDNO
- ED
- CVC
- OPERATION (der Operationscode ist nicht streng obligatorisch, aber dringend empfohlen).

3.3 Testseite

Ein Beispiel für eine Bestellanfrage (eine Testseite) finden Sie unter https://ogone.test.v-psp.com/ncol/test/testodl.asp.

3.4 Ausschluss spezifischer Zahlungsmethoden

Wenn Sie verhindern möchten, dass ein Kunde bestimmte Zahlungsverfahren nutzt, können Sie dazu einen bestimmten Parameter nutzen.

Dies ist insbesondere bei Unter-Marken nützlich, wenn Sie eine Marke (z. B. MasterCard) akzeptieren möchten, nicht aber eine ihrer Unter-Marken (z. B. Maestro).

Der Parameter ist wie folgt zu verwenden:

Feld	Verwendung
EXCLPMLIST	Liste der Zahlungsverfahren bzw. Kreditkartenmarken, getrennt durch Semikolon (;), die NICHT verwendet werden sollen.

Versucht ein Kunde, mit einer Karte zu bezahlen, die mit einem bestimmten Zahlungsverfahren bzw. einer (Unter-)Marke verknüpft ist, aber von Ihnen mittels Parameter EXCLPMLIST vom Gebrauch ausgeschlossen wurde, wird im Feld NCERRORPLUS die Fehlermeldung „Card number incorrect or incompatible“ („Falsche Kartennummer oder nicht zulässig“) zurückgesendet.

3.5 Bestellanforderungen mit 3-D Secure

Unser System unterstützt die Nutzung von 3-D Secure über DirectLink. Weitere Informationen zu diesem Feature finden Sie im Integrationsleitfaden für DirectLink mit 3-D Secure.

Wichtig

- Wenn Sie 3-D Secure mit DirectLink nutzen möchten, müssen Sie in Ihrem Konto die Option D3D aktiviert haben.
- Manche Acquirerbanken verlangen die Nutzung von 3-D Secure. Bitte klären Sie mit Ihrem Acquirer, ob dies bei Ihnen der Fall ist.

3.6 Aufteilung Kredit/Debit

Die Funktionalität zur Aufteilung von VISA und MasterCard in ein Debit- und ein Kreditkarten-Zahlungsverfahren erlaubt es Ihnen, Ihren Kunden diese Programme als zwei unterschiedliche Zahlungsverfahren anzubieten (z. B. VISA Debit und VISA Kredit). Sie können auch entscheiden, nur eines der Teilverfahren für beide Marken zu akzeptieren.

Um die Aufteilung von Kredit- und Debit-Karten via DirectLink zu nutzen, müssen Sie den Parameter CREDITDEBIT in die verborgenen Felder aufnehmen, die Sie an die Seite orderdirect.asp senden (und daher auch in die SHA-IN-Berechnung einschließen!).

Feld	Format
CREDITDEBIT	"C": credit card (Kreditkarte) "D": debit card (Debitkarte)

Zugehörige Fehlermeldung: Wenn ein Käufer das Debitkarten-Zahlungsverfahren auswählt, aber die Nummer einer Kreditkarte eingibt, wird ein Fehler zurückgemeldet: „Wrong brand/Payment method was chosen“ (Falsche Marke/falsches Zahlungsverfahren ausgewählt).

Wenn die Zahlung mit dem Parameter CREDITDEBIT erfolgreich verarbeitet worden ist, wird der gleiche Parameter auch in der XML-Rückmeldung zurückgegeben bzw. kann mit einem Direct Query angefordert werden. Lauten die eingereichten Parameterwerte C bzw. D, ist der zurückgemeldete Wert "CREDIT" bzw. "DEBIT".

Sie finden diese Rückmeldungswerte in der Transaktionsübersicht über „View transactions“ (Transaktionen anzeigen) und „Financial history“ (Zahlungshistorie) sowie in den Berichten, die Sie nachfolgend herunterladen.

Konfiguration in Ihrem Konto

Die Aufteilungsfunktion kann auch in Ihrem Ingenico ePayments-Konto pro Zahlungsverfahren aktiviert und konfiguriert werden. Weitere Informationen finden Sie unter Split Credit/Debit Cards.

3.7 Transaktionen mit gespeicherten Anmeldedaten abwickeln

Bei der Credential-on-File-Transaktion (COF) werden bereits vom Händler gespeicherte, vorhandene Kreditkartendetails verwendet, um die Zahlung abzuwickeln. Bevor eine COF-Transaktion ausgelöst wird, muss der Karteninhaber zuerst den Händler autorisieren, die Kartendetails zu speichern. Credential-on-File (COF) wird hauptsächlich für wiederkehrende Zahlungen angewandt und gibt an, ob die Zahlung vom Karteninhaber oder Händler ausgelöst wird.

Es gibt zwei Arten von COF-Transaktionen: eine vom Karteninhaber ausgelöste Transaktion (CIT) oder eine vom Händler ausgelöste Transaktion (MIT). Eine vom Karteninhaber ausgelöste Transaktion (CIT) muss immer zuerst stattfinden, bevor eine vom Händler ausgelöst werden kann.

Bei der vom Karteninhaber ausgelöste Transaktion (CIT) ist der Karteninhaber an der Transaktion beteiligt und authentifiziert die Transaktion persönlich, z. B. durch eine Unterschrift, eine 3D Secure-Anwendung oder der Vorlage von IDs.

Beispiel für eine vom Karteninhaber ausgelöste Transaktion (CIT):

Ein Karteninhaber kauft ein Zugticket online und bezahlt es. Er/Sie zahlt mit seiner/ihrer Kreditkarte und wird aufgefordert, die Zahlung zu authentifizieren und zu autorisieren. Gleichzeitig wird der Karteninhaber auch gefragt, ob er/sie die Kreditkarteninformationen im Zusammenhang mit dieser Zahlung speichern möchte. Wenn der Karteninhaber zustimmt, kann diese Information dann in zukünftigen, vom Händler ausgelösten Transaktionen wiederverwendet werden.
Einer vom Händler ausgelöste Transaktion (MIT) geht voraus, dass der Karteninhaber eine Transaktion ausgelöst und zuvor eine Dauerbestellung für gekaufte Waren und Dienstleistungen vereinbart hat. Der Karteninhaber muss dabei nicht an der Transaktion beteiligt sein.

Beispiel für eine vom Händler ausgelöste Transaktion (MIT):

Ein Händler kann automatisch eine Transaktion auslösen, um die Zahlung eines Karteninhabers für ein monatliches Zeitschriftenabonnement zu erfüllen.

In Übereinstimmung mit den von Visa und MasterCard für die Credential-on-file-Transaktion (COF) festgelegten Regeln müssen neue Parameter gesendet werden, um die COF-Transaktion zu bestimmen

Betroffen, wenn:

- Sie ein Alias verwenden
- Sie planen, wiederkehrende Transaktionen (regelmäßig oder nicht) auszulösen, nachdem Sie zum ersten Mal eine vom Karteninhaber ausgelöste Transaktion (CIT) ausgelöst haben

Erforderliche Aktion

Diese Parameter werden standardmäßig in einer DirectLink Transaktion verwendet:

Parameter-Werte COF_INITIATOR-COF_TRANSACTION-COF_SCHEDULE	Beschreibung
CIT-FIRST-UNSCHED	Gilt, wenn ein Alias verwendet oder erstellt wird
CIT-FIRST-SCHED	Gilt für eine erste regelmäßige Zahlung/ein Abonnement
MIT-SUBSEQ-UNSCHED	Gilt für wiederkehrende Zahlung
MIT-SUBSEQ-SCHED	Gilt für Ratenzahlung

Die Standardwerte werden markiert, wenn Sie keine Parameter hinzufügen. Wenn Sie sie jedoch ändern möchten, können Sie diese Standardwerte mit neuen Parametern überschreiben. Vergessen Sie nicht, die SHA-Signatur neu zu berechnen (klicken Sie **hier**, um weitere Informationen zur SHA-Signatur zu erhalten.)

Parameter	Werte	Beschreibung
COF_INITIATOR	CIT	Eine vom Karteninhaber ausgelöste Transaktion
	MIT	Eine vom Händler ausgelöste Transaktion
COF_SCHEDULE	SCHED	Eine regelmäßige Transaktion
	UNSCHED	Eine unregelmäßige Transaktion
COF_TRANSACTION	FIRST	Die erste von einer Reihe von Transaktionen
	SUBSEQ	Weitere Reihen von Transaktionen
COF_RECURRING_EXPIRY	Datum JJJJMMTT (z.B. 20190914)	Enddatum: Tag der letzten regelmäßigen Zahlung einer Serie
COF_RECURRING_FREQUENCY	numerisch zwischen 2 und 4 Stellen (z.B. 1, 031 oder 0031)	Anzahl Tage welche zwischen regelmäßigen Zahlungen

4. Rückmeldung zur Bestellung

Unser Server sendet als Rückmeldung zur Anfrage eine XML-Antwort:

Beispiel einer XML-Antwort auf eine Bestellanfrag

```
<?xml version="1.0"?>

<ncresponse orderID="99999" PAYID="1111111" NCSTATUS="0" NCERROR="" NCERRORPLUS="" ACCEPTANCE="12345" STATUS="5" ECI="7" amount="125" currency="EUR" PM="CreditCard" BRAND="VISA"/>
```

Die folgende Tabelle enthält eine Attributliste zum ncresponse-tag:

Feld	Nutzung
ACCEPTANCE	Vom Akzeptanzpartner zurückgesendeter Akzeptanzwert.
amount	Betrag der Bestellung (nicht mit 100 multipliziert)
BRAND	Kartenmarke oder vergleichbare Informationen für andere Zahlungsmethoden.
currency	Währung der Bestellung.
ECI	Electronic Commerce Indicator.
NCERROR	Fehlerwert.
NCERRORPLUS	Erklärung des Fehlercodes.
NCSTATUS	Transaktionsstatus.
orderID	Ihre Bestellnummer.
PAYID	Bezahlungs-ID als Referenz in unserem System.
PM	Zahlungsmethode.
STATUS	Transaktionsstatus.

Die Attributliste kann bei Händlern länger sein, die in ihren Konten bestimmte Optionen (z. B. Betrugserkennungsmodul) aktiviert haben. Bitte lesen Sie in der betreffenden Dokumentation weitere Informationen über zusätzliche Rückmeldungsattribute nach, die mit dieser Option verbunden sind.

4.1 Duplicate request

If you request processing for an already existing (and correctly processed) orderID, our XML response will contain the PAYID corresponding to the existing orderID, the ACCEPTANCE given by the acquirer in the previous processing, STATUS “0” and NCERROR “50001113”.

5. Direkte Datenpflege: Pflege bestehender Bestellungsdaten

Eine direkte Datenpflegeanfrage von ihrer Applikation aus ermöglicht Ihnen:

- Eine Kontobelastung (Zahlung) einer autorisierten
- Bestellung automatisch vorzunehmen (anstatt manuell im Back-Office)
- Autorisierung einer Bestellung zu stornieren
- Autorisierung einer Bestellung zu erneuern oder eine bezahlte Bestellung wieder gutzuschreiben.

5.1 Datenpflege-Anfrage

5.1.1 Anfrage-URL

- Die Anfrage-URL in der TESTUMGEBUNG lautet https://ogone.test.v-psp.com/ncol/test/maintenancedirect.asp.
- Die Anfrage-URL in der PRODUKTIVUMGEBUNG lautet https://secure.ogone.com/ncol/prod/maintenancedirect.asp.

Wichtig

Vergessen Sie nicht, in der Anfrage-URL die Zeichenfolge „test" durch „prod" zu ersetzen, wenn Sie auf Ihr reguläres PRODUKTIVKONTO umstellen. Wenn Sie vergessen, die Anfrage-URL zu ändern und den regulären Betrieb mit realen Bestellungen aufnehmen, laufen Ihre Datenpflege-Transaktionen weiter in die Testumgebung und werden nicht an die Akzeptanzpartner bzw. Banken gesendet.

5.1.2 Anfrageparameter

Die folgende Tabelle enthält die obligatorische Aufforderung Parameter zur Durchführung einer Wartungsarbeit:

Feld	Nutzung
AMOUNT	Betrag der Bestellung, mit 100 multipliziert. Nur obligatorisch, wenn der Betrag in der Datenpflegeanfrage sich von dem in der Originalautorisierung unterscheidet. Wir empfehlen jedoch, den Betrag immer anzugeben. Unser System prüft, ob der Betrag in der Datenpflegeanfrage nicht zu hoch im Vergleich zum Betrag in der Originalautorisierung bzw. -zahlung ist.
OPERATION	Mögliche Werte: • REN: Erneuerung der Autorisierung, wenn die Originalautorisierung nicht mehr gültig ist. • DEL: Löschung der Autorisierung. Die Transaktion bleibt dabei für mögliche nachfolgende Datenpflegeoperationen geöffnet. • DES: Löschung der Autorisierung. Die Transaktion wird nach diesem Vorgang geschlossen. • SAL: Teilweise Kontobelastung (Zahlung). Die Transaktion bleibt für eine mögliche weitere Kontobelastung geöffnet. • SAS: (Letzte) teilweise oder vollständige Kontobelastung (Zahlung). Nach dieser Kontobelastung wird die Transaktion für weitere Kontobelastungen geschlossen. • RFD: Teilweise Gutschrift (einer bezahlten Bestellung). Die Transaktion bleibt für mögliche weitere Gutschriften geöffnet. • RFS: (Letzte) teilweise oder vollständige Gutschrift (einer bezahlten Bestellung). Nach dieser Gutschrift wird die Transaktion geschlossen. Bitte beachten Sie bei DEL und DES, dass nicht alle Akzeptanzpartner das Löschen einer Autorisierung unterstützen. Wenn Ihr Akzeptanzpartner DEL/DES nicht unterstützt, können wir dennoch die Löschung der Autorisierung im Back-Office simulieren.
ORDERID	Sie können die PAYID oder die orderID zur Identifikation der Originalbestellung senden. Wir empfehlen die Verwendung der PAYID.
PAYID	
PSPID	Anmeldedaten: PSPID und (API) USERID mit dem zur USERID gehörenden Passwort
PSWD	
USERID	
SHASIGN	Mit dem Secure Hash Algorithmus gehashte Zeichenfolge (siehe SHA-IN-Signatur)

5.1.3 Testseite

Ein Beispiel für eine direkte Datenpflegeanfrage (eine Testseite) finden Sie unter: https://ogone.test.v-psp.com/ncol/test/testdm.asp

5.2 Datenpflege-Antwort

Beispiel einer XML-Antwort auf eine direkte Datenpflegeanfrage:

<?xml version="1.0"?>

<ncresponse orderID="99999" PAYID="1111111" PAYIDSUB="3" NCSTATUS="0" NCERROR="" NCERRORPLUS="" ACCEPTANCE="12345" STATUS="91" amount="125" currency="EUR"/>

Die folgende Tabelle enthält eine Attributliste zum ncresponse-tag:

Feld	Nutzung
ACCEPTANCE	Vom Akzeptanzpartner zurückgesendeter Akzeptanzwert.

Feld	Nutzung
AMOUNT	Betrag der Bestellung (nicht mit 100 multipliziert).
CURRENCY	Währung der Bestellung.
NCERROR	Fehlerwert.
NCERRORPLUS	Erklärung des Fehlercodes.
NCSTATUS	Erste Ziffer von NCERROR.
ORDERID	Ihre Bestellnummer
PAYID	Bezahlungs-ID als Referenz in unserem System.
PAYIDSUB	Die PAYID der angewendeten Datenpflegeoperation auf Historien-Ebene
STATUS	Transaktionsstatus.

Weitere technische Einzelheiten zu diesen Feldern finden Sie im Parameter Cookbook.
Die Standardattribute des ncresponse-tags sind identisch mit denen der XML-Antwort auf eine neue Bestellung mit Ausnahme des zusätzlichen Attributs PAYIDSUB.

5.3 Doppelte Anfrage

Geht eine Datenpflegeanfrage für die gleiche Bestellung zweimal ein, wird die zweite theoretisch mit der Fehlermeldung „50001127" (Bestellung nicht autorisiert) abgelehnt, weil die erste erfolgreiche Transaktion den Bestellstatus geändert hat.

6. Direktabruf: Bestellstatus abrufen

Eine Direktabruf-Abfrage von Ihrer Applikation ermöglicht Ihnen, den Status einer Bestellung automatisch abzurufen (anstatt manuell im Back-Office). Sie können immer nur eine Zahlung gleichzeitig abrufen und erhalten nur in begrenztem Umfang Informationen über die Bestellung.

Wenn Sie weitere Details über die Bestellung benötigen, können Sie die Transaktion im Back-Office aufrufen oder einem manuellen bzw. automatischen Dateidownload vornehmen (siehe hierzu Transaktionen Ansehen und **Advanced Batch** Integrationsleitfaden).

6.1 Abruf-Anfrage

6.1.1 Anfrage-URL

- Die Anfrage-URL in der TESTUMGEBUNG lautet https://ogone.test.v-psp.com/ncol/test/querydirect.asp.
- Die Anfrage-URL in der PRODUKTIVUMGEBUNG lautet https://secure.ogone.com/ncol/prod/querydirect.asp.

Wichtig

Vergessen Sie nicht, in der Anfrage-URL die Zeichenfolge „test" durch „prod" zu ersetzen, wenn Sie auf Ihr reguläres PRODUKTIVKONTO umstellen.

6.1.2 Anfrageparameter

Die folgende Tabelle enthält die obligatorischen Anfrageparameter für die Durchführung eines Direktabrufs:

Feld	Nutzung
ORDERID	Sie können die PAYID oder die ORDERID zur Identifikation der Originalbestellung senden. Wir empfehlen die Verwendung der PAYID.
PAYID	
PAYIDSUB	Sie können die ID der Historien-Ebene angeben, wenn Sie die PAYID zur Identifikation der Originalbestellung verwenden (optional).
PSPID	Anmeldedaten: PSPID und (API) USERID mit dem zur USERID gehörenden Passwort
PSWD	
USERID	

6.1.3 Testseite

Ein Beispiel für eine Direktabruf-Anfrage (eine Testseite) finden Sie unter: https://ogone.test.v-psp.com/ncol/test/testdq.asp.

6.2 Abruf-Antwort

Unser Server sendet als Rückmeldung zur Anfrage eine XML-Antwort:

Beispiel einer XML-Antwort auf eine Direktabruf-Anfrage:

<?xml version="1.0"?>
<ncresponse orderID="99999" PAYID="1111111" PAYIDSUB="3" NCSTATUS="0" NCERROR="" NCERRORPLUS="" ACCEPTANCE="12345" STATUS="9" ECI="7" amount="125" currency="EUR" PM="CreditCard" BRAND="VISA" CARDNO="XXXXXXXXXXXX1111" IP="212.33.102.55"/>

Die folgende Tabelle enthält eine Attributliste des ncresponse-tags:

Feld	Nutzung
ACCEPTANCE	Vom Akzeptanzpartner zurückgesendeter Akzeptanzwert.
amount	Betrag der Bestellung (nicht mit 100 multipliziert).
BRAND	Kartenmarke oder vergleichbare Informationen für andere Zahlungsmethoden.
CARDNO	Maskierte Kartennummer.
currency	Währung der Bestellung.
ECI	Electronic Commerce Indicator.
IP	IP-Adresse des Kunden, wie von unserem System in einer 3-Ebenen-Integration ermittelt oder uns vom Händler in einer 2-Ebenen-Integration gesendet.
NCERROR	Fehlerwert.
NCERRORPLUS	Erklärung des Fehlercodes.
NCSTATUS	Erste Ziffer von NCERROR.

Feld	Nutzung
orderID	Ihre Bestellnummer.
PAYID	Zahlungsreferenz in unserem System.
PAYIDSUB	Die PAYID der angewendeten Datenpflegeoperation auf Historien-Ebene.
PM	Zahlungsmethode.
STATUS	Transaktionsstatus

Die Standardattribute des ncresponse-tags sind identisch mit denen für die XML-Antwort auf eine neue Bestellung mit Ausnahme der zusätzlichen Attribute PAYIDSUB, CARDNO und IP.

Die Attributliste kann bei Händlern länger sein, die in ihren Konten bestimmte Optionen (z. B. das Betrugserkennungsmodul) aktiviert haben. Bitte lesen Sie in der Dokumentation der betreffenden Option weitere Informationen über zusätzliche Antwortattribute nach, die mit dieser Option verbunden sind.

6.2.1 Mit e-Commerce verarbeitete Transaktionen

Wenn die Transaktion, deren Status Sie abrufen möchten, mit e-Commerce verarbeitet wurde, erhalten Sie die folgenden zusätzlichen Attribute (vorausgesetzt, Sie haben mit der ursprünglichen e-Commerce Transaktion diese Felder gesendet).

Feld	Nutzung
COMPLUS	Ein Wert, den Sie in der Antwort zurückgesendet bekommen wollten.
(paramplus Inhalt)	The parameters and their values you wanted to have returned

Beispiel einer XML-Antwort auf den Direktabruf bezüglich einer e-Commerce-Transaktion:

<ncresponse orderID="99999" PAYID="1111111" PAYIDSUB="3" NCSTATUS="0" NCERROR="" NCERRORPLUS="" ACCEPTANCE="12345" STATUS="9" amount="125" currency="EUR" PM="CreditCard" BRAND="VISA" CARDNO="XXXXXXXXXXXX1111" IP="212.33.102.55" **COMPLUS="12345678912345678912345678 9" SessionID="126548354" ShopperID="73541312"**/>

6.3 Mögliche rückgemeldete Statuszustände

Das Feld STATUS enthält den Status der Transaktion. Eine vollständige Liste der möglichen Statuszustände finden Sie im Back-Office: Support > Integrations & Benutzerhandbücher > Benutzerhandbücher > Liste der Status- und Fehlermeldungen.

Nur der folgende Status bezieht sich speziell auf den Abruf selbst:

Status	NCERROR	NCSTATUS	Description
88			Der Abruf an querydirect.asp ist fehlgeschlagen.

6.4 Direktabruf als Fallback

Die Antwortzeit für die Anfrage bezüglich einer DirectLink Transaktion beträgt generell nur wenige Sekunden. Einige Akzeptanzpartner haben jedoch möglicherweise längere Antwortzeiten.

Wenn Sie innerhalb von 30 Sekunden keine Antwort von unserem System erhalten haben, können Sie eine Anfrage an querydirect.asp senden, die den Status der gerade an orderdirect.asp gesendeten Transaktion abruft. Wenn Sie eine sofortige Antwort erhalten, die für die Transaktion einen noch nicht abgeschlossenen Status meldet, liegen eventuell Probleme auf Akzeptanzpartnerseite vor.

Wenn Sie nach 10 Sekunden noch keine Antwort auf den Direktabruf erhalten haben, liegen eventuell Probleme auf unserer Seite vor. Sie können diese Anfrage an querydirect.asp alle 30 Sekunden wiederholen, bis Sie feststellen, dass eine Antwort innerhalb von 10 Sekunden bei Ihnen eintrifft.

Bitte beachten Sie:

1. Dieses Prüfsystem kann nur dann Probleme auf unserer Seite anzeigen, wenn gleichzeitig eine Prüfung auf Ihrer Seite sicherstellt, dass die Anfragen Ihre Server korrekt verlassen.
2. Ein Problem auf unserer Seite ist nicht notwendigerweise durch einen Systemausfall begründet, sondern kann auch das Ergebnis langer Antwortzeiten aufgrund von Datenbankproblemen sein.
3. Bitte nutzen Sie diese Prüfmöglichkeiten mit Zurückhaltung, um ein Dauerbelastung unserer Server mit derartigen Anfragen zu vermeiden. Andernfalls sind wir eventuell gezwungen, Ihren Zugriff auf die Seite querydirect.asp zu sperren.

Wichtig

Um unser System vor unnötiger Überlastung zu schützen, unterbinden wir Prüfungen der Systemverfügbarkeit, die mit dem Senden vorgetäuschter Transaktionen oder systematischer Anfragen sowie mit systematischen Anfragen verbunden sind, die für jede Transaktion eine Transaktionsrückmeldung erfordern.

7. Datenschutzrichtlinie-Anforderung

Nach Artikel 12, 13 und 14 DSGVO ist der Datenverantwortliche verpflichtet, seine Endkunden über die zukünftige Verarbeitung ihrer persönlichen Daten zu informieren. Diese Informationen sollten auf der Grundlage der Art der für eine bestimmte Transaktion einzugebenden persönlichen Daten (z.B.: gewählte Zahlungsmethode, Controller/Verarbeiter, Acquirer, Betrug) spezifiziert werden. Das Ergebnis sollte zum Zeitpunkt der Datenerhebung verfügbar und sichtbar sein und dem Karteninhaber mit einer druckbaren und herunterladbaren Version angeboten werden. Gemäß der Datenschutz-Grundverordnung (DSGVO) müssen Sie Ihren Kunden vor deren Transaktionsbestätigung diese Informationen darlegen. Diese Informationen sind idealerweise auf derselben Seite anzuzeigen, auf der Ihre Kunden ihre Kreditkarten-/Kontoangaben eingeben.
Mit der folgenden Anfrage nach der Datenschutzrichtlinie erhalten Sie alle Informationen, die Sie Ihren Kunden für die Einhaltung der Datenschutz-Grundverordnung (DSGVO) über unsere Dienstleistungen anzeigen müssen.

7.1 Abruf-Anfrage

7.1.1 Query-Anforderung

• Die URL-Anforderung in der TEST-Umgebung ist https://secure.ogone.com/ncol/test/privacy-policy.asp

• Die URL-Anforderung in der PRODUKTIONS-Umgebung ist https://secure.ogone.com/ncol/prod/privacy-policy.asp

„Test“ in "Prod“ ändern

Ersetzen Sie „Test“ durch „Prod“ in der URL-Anforderung, wenn Sie zu Ihre Produktivkonto wechseln.

7.1.2 Anforderungsparameter

In der folgenden Tabelle sind die obligatorischen Anforderungsparameter aufgelistet, die Ihren Kunden hinsichtlich der Nutzung ihrer Datenschutzinformationen übermittelt werden:

Feld	Format	Beschreibung
USERID	Zeichenfolge	Ihr API-Benutzer
PSWD	Zeichenfolge	Ihr API-Benutzer-Password
PSPID	Zeichenfolge	Ihre Konto-PSPID
BRAND	String (e.g. Visa)	Optional: Zahlungsmethode Marke Sie können dieses Feld mehrmals übermitteln, um das Ergebnis mehrerer Marken zugleich zu erhalten. • Wird keine Marke übermittelt entspricht dies der Übermittlung aller Ihrer aktiven Marken • Leere/fehlerhaft formatierte Marken werden ignoriert
LANGUAGE	ISO 639-1: Zwei-Buchstaben-Codes (z.B. FR)	Optional: Die Sprache, in der Sie den Text erhalten möchten. Wenn nicht angegeben, wird der Text in der ursprünglich eingestellten Sprache des Händlers angezeigt.

7.1.3 Testseite

Sie können direkte Query-Anforderungen hier testen: https://secure.ogone.com/ncol/test/privacy-policy.asp

7.2 Abruf-Antwort

Im Folgenden finden Sie ein Verzeichnis von XML-Elementen und die zurückübermittelten XML-Antwortbeispiele für verschiedene Ergebnisse.

Name	Format	Beschreibung
Response	Complex	Root node, always present
Response.Status	String, possible values : Success, SuccessWithWarnings, Error	Always present
Response.Body	Complex	Present only when Response.Status = Success or SuccessWithWarnings
Response.Body.Html	String / html	Empty if Response.Status = SuccessWithWarnings & Response.Warnings.Warning.Code = NoContent
Response.Errors	Complex	Present only when Response.Status = Error
Response.Errors.Error	Complex	Can occur multiple times inside an <Errors> node
Response.Warnings	Complex	Present only when Response.Status = SuccessWithWarnings or Error
Response.Warnings.Warning	Complex	Occurs multiple times inside a <Warnings> node
Response.Errors.Error.Code Response.Warnings.Warning.Code	String, possible values : •Inside an <Error> node : Unauthorized, InternalServerError •Inside a <Warning> node : NoContent	Always present in an <Error> or <Warning> node
Response.Errors.Error.Message Response.Warnings.Warning.Message	String	Optional

Wird Ihnen Response.Status=Error ausgegeben, beziehen Sie sich bitte auf den Response.Errors.Error, um den Fehler zu beheben.
Im Folgenden zwei erfolgreiche Beispiele:

1. Beispiel einer XML-Antwort für einen Erfolg mit Warnungen. Wird zurückgegeben, wenn keine Datenschutzinformationen dem Kunden offengelegt werden müssen.

```
<?xml version="1.0" encoding="utf-8"?>
 <Response>
    <Status>SuccessWithWarnings</Status>
    <Warnings>
        <Warning>
            <Code>NoContent</Code>
        </Warning>
    </Warnings>
    <Body>
        <Html/>
    </Body>
 </Response>
```

2. Beispiel einer XML-Antwort für einen Erfolg mit Inhalt. Das Beispiel zeigt eine in 2 Bereiche aufgeteilte Anzeige.

```
<?xml version="1.0" encoding="utf-8"?>
<Response>
    <Status>Success</Status>
    <Body>
        <Html><![CDATA[<ul><li><h2>Title 1</h2><p>Content 1</p></li><li><h2>Title 2 (VISA, American Express)
        </h2><p>Content 2</p></li></ul>]]></Html>
    </Body>
</Response>
```

8. PM-Ausnahmen

Bei bestimmten Zahlungsmethoden weichen die Parameterwerte von den Kreditkarten-Standardwerten ab.

8.1 Direct Debits

8.1.1 Direct Debits AT

Die folgende Tabelle enthält die spezifischen Parameterwerte, die eine Übertragung von Direct Debits AT Transaktionen via DirectLink erlauben.

Format: AN=alphanumerisch / N=numerisch, die maximal erlaubte Anzahl der Zeichen

Feld	Beschreibung	Format/Wert
CARDNO	Bankkontonummer	AN, 21 Format: XXXXXXXXXXBLZYYYYY XXXXXXXXXX: Kontonummer, numerisch, 11 Stellen. YYYYY: Bankleitzahl, 5 Stellen.
CN	Name des Karteninhabers	AN, 35
ED	Verfallsdatum	„99/99“ oder „9999“
OPERATION	Operationscode (Auszuführende Aktion)	A, 3 Mögliche Werte: • RES: Autorisierung (Reservierung) • SAL/SAS: Geld vom Bankkonto abbuchen • RFD/RFS: Gutschrift auf das Bankkonto (*)
OWNERADDRESS	Anschrift des Kontoinhabers	AN, 50
OWNERTOWN	Wohnort des Bankkontoinhabers	AN, 40
OWNERZIP	Kontoinhabers Postleitzahl	AN, 10
PM	Zahlungsmethode	AN, 25 “Direct Debits AT”

(* Falls die Gutschrift Option verfügbar und aktiv ist, und DTAUS-Gutschrift verfügbar ist)

8.1.2 Direct Debits DE (ELV)

(* Falls die Gutschrift Option verfügbar und aktiv ist, und DTAUS-Gutschrift verfügbar ist)
Die folgende Tabelle enthält die spezifischen Parameterwerte, welche die Übertragung von ELV-Transaktionen über DirectLink (not Wirecard/Billpay).

Format: AN=alphanumerisch / N=numerisch, die maximal erlaubte Anzahl der Zeichen

Feld	Beschreibung	Format/Wert	Obligatorisch
CARDNO	Bankkontonummer	IBAN: alphanumerische Zeichen ODER Bankkontonummer + BLZ. Format: XXXXXXXXXBLZYYYYYYYY XXXXXXXXX: Kontonummer, numerisch, 1 bis 10 Stellen. YYYYYYYY: Bankleitzahl), 8 Stellen.	J
CN	Name des Bankkontoinhabers	AN, 35	J
ED	Verfallsdatum	„99/99“ oder „9999“	J
MANDATEID	Eindeutige Auftragsreferenz. Telego: Ohne Angabe übernimmt die Plattform die ORDERID oder PAYID Note: Ohne Angabe erstellt easycash einen Wert.	Telego: AN, 35 / Zeichensatz: “A-Z a-z 0-9 Leerzeichen /-?:().,'+” Ohne Angabe übernimmt die Plattform die ORDERID oder PAYID Easycash: Format: AN, 27 / Zeichensatz: “A-Z a-z 0-9 Leerzeichen /-?:().,'+” Note: Ohne Angabe erstellt easycash einen Wert.	N
OPERATION	Operationscode (Auszuführende Aktion)	A, 3 Mögliche Werte: • RES: Autorisierung • SAL/SAS: Einzug von Geld vom Bankkonto • RFD/RFS: Erstattung von Geld (*)	N

Note: Diese Felder können in der DirectLink XML-Antwort zurückgegeben werden und müssen in die SHA-IN-Berechnung eingeschlossen werden (optional auch SHA-OUT).
(* Falls die Gutschrift Option verfügbar und aktiv ist, und DTAUS-Gutschrift verfügbar ist)

8.1.3 Direct Debits NL

Die folgende Tabelle enthält die spezifischen Parameterwerte, welche die Übertragung von Bankeinzug NL-Transaktionen (Direct Debits NL) über DirectLink ermöglichen.

Format: AN=alphanumerisch / N=numerisch, die maximal erlaubte Anzahl der Zeichen

Feld	Beschreibung	Format/Wert
CARDNO	Bankkontonummer	Reguläre holländische Kontonummer: max. 10 alphanumerische Zeichen (falls weniger, links mit Nullen auffüllen). ODER IBAN-Kontonummer: max. 35 alphanumerische Zeichen (SEPA)
CN	Name des Bankkontoinhabers	AN, 35
ED	Verfallsdatum	„99/99“ oder „9999“
OPERATION	Operationscode (Auszuführende Aktion)	A, 3 Mögliche Werte: • SAL or SAS: Einzug von Geld vom Bankkonto • RFD or RFS: Gutschrift von Geld auf das Bankkonto (Erstattung)
OWNERTOWN	Stadt des Bankkontoinhabers	AN, 40
PM	Zahlungsmethode	AN, 25 “Direct Debits NL”
Nur relevant für SEPA-Transaktionen (*):		
BIC	Bankidentifikationscode.	AN, 11
MANDATEID	Eindeutige Auftragsreferenz. Note: Ohne Angabe wird die ORDERID verwendet.	AN, 35 Keine Leerzeichen; darf nicht mit einem Schrägstrich "/" beginnen oder enden, und darf keine zwei aufeinanderfolgende Schrägstriche enthalten.
SEQUENCETYPE	Typs der Bankeinzugstransaktion Note: Ohne Angabe wird die Transaktion als einmalig („OOFF“) betrachtet.	Mögliche Werte zur Angabe des Typs der Bankeinzugstransaktion (AN, 4): • "FRST": Erste Sammlung einer Reihe von Bankeinzugsanweisungen • "RCUR": Bankeinzugsanweisungen, wobei die Autorisierung des Debitors für reguläre, vom Kreditor eingeleitete Bankeinzugstransaktionen verwendet wird • "FNAL": Letzte Sammlung einer Serie von Bankeinzugsansweisungen (danach kann dieselbe MandateID nicht mehr verwendet werden) • "OOFF": Bankeinzugsanweisung, wobei die Autorisierung des Debitors zur Einleitung einer einzelnen Bankeinzugstransaktion verwendet wird
SIGNDATE	Datum, an dem der Auftrag vom Kunden unterschrieben wurde. Note: Ohne Angabe wird das Transaktionsdatum verwendet	JJJJMMTT

(*SEPA: Single Euro Payments Area)

Hinweis: Diese Felder können in der DirectLink XML-Antwort zurückgegeben werden und müssen in die SHA-IN-Berechnung (optional auch SHA-OUT) eingeschlossen werden.

8.2 PM nur mit Datenpflege möglich über DirectLink

Bei bestimmten (nicht mit Kreditkarten verbundenen) Zahlungsmethoden können Sie keine neuen Transaktionen via DirectLink senden. Sie haben jedoch die Möglichkeit, bestimmte Datenpflegeanfragen via DirectLink zu senden. Dies ist der Fall bei: PostFinance Card, PostFinance e-finance, PayPal Express Checkout und TUNZ. Beim Senden einer Datenpflegeanfrage müssen PM/BRAND/CARDNO/ED nicht angegeben werden. Damit ist es auch nicht erforderlich, bestimmte Werte für diese Zahlungsmethoden zu senden.