Heartland

Logo	
Info	Heartland
Typ	Zahlungen per Kreditkarte

- Einleitung
  - Acquirer und Verbindung
  - Integration mit Computop Paygate
  - Implementierung von 3-D Secure (2.x)
    - Allgemeine Hinweise zu 3-D Secure
    - 3-D Secure mit Computop Paygate
- Spezifische Parameter für Heartland
- Kreditkarten - Kreditkartenformular
  - Vereinfachtes Sequenz-Diagramm
  - Zahlungsanfrage
  - HTTP POST an URLSuccess / URLFailure / URLNotify
  - Kreditkartenzahlung mit separater Autorisierung
  - Erweitertes Sequenz-Diagramm
- Kreditkarten - Server-2-Server Integration
  - Server-2-Server Sequenzdiagramm
  - Initiierung der Zahlung
    - Aufruf-Elemente
    - Antwort-Elemente
    - versioningData
  - 3DS Methode
    - 3DS Methode: threeDSMethodURL
    - 3DS Method: Keine Issuer threeDSMethodURL
    - 3-D Secure Method Form Post
    - ACS Response Document
    - 3-D Secure Method Notification Form
  - Authentisierung
    - Karteninhaber-Challenge: Browser-Antwort
    - Browser Challenge-Antwort
      - Datenelemente

Einleitung

Acquirer und Verbindung

Computop Paygate unterstützt viele verschiedene Kreditkartenverbindungen zu verschiedenen Acquirern / Prozessoren mit unterschiedlichen Protokollen.

Hier finden Sie eine Übersicht aller unterschiedlichen Kreditkartenschnittstellen: Zahlungen per Kreditkarte.

Zusätzliche Funktionen (z.B. AVS (Address Verification Service), Rückerstattung, 3D Secure, ...) können von der spezifischen Integration und vom Acquirer abhängen.

Integration mit Computop Paygate

Allgemein bieten wir zwei verschiedene Möglichkeiten der Integration an:

	Zahlungsseite (payssl.aspx)	**Direkte Integration (direct.aspx)**
Handhabung von Kreditkartennummern (PAN)	• Wird direkt über die Zahlungsseite abgewickelt. • Kreditkartennummer, Ablaufdatum, CVV, ... werden im Zahlungsformular abgefragt • Sie kommen nicht mit dern PAN in Kontakt, was die Compliance zu PCI DSS deutlich vereinfacht. • Sie erhalten optional eine PseudoCardNumber (PcNr) als Paygate internen Token zur Repräsentation der PAN.	• Ihr System verarbeitet PAN direkt, sodass Sie "volle Kontrolle" haben. • Da Ihr System mit der Kreditkartennummer (PAN) in Kontakt kommt, unterliegt ihr System vollständig dem PCI-DSS-Fokus.
Handhabung von 3-D Secure	• Sie müssen nur KVP "MsgVer=2.0" hinzufügen, um anzuzeigen, dass Ihr System für 3-D Secure 2.x bereit ist • Der Rest (Weiterleitung an die Bank des Ausstellers zur Authentifizierung des Verbrauchers) wird von derPaygate Zahlungsseite abgewickelt.	• Sie müssen nur KVP "MsgVer=2.0" hinzufügen, um anzuzeigen, dass Ihr System für 3-D Secure 2.x bereit ist • Ihr System muss im Falle einer Verbraucherauthentifizierung eine Verbraucherumleitung zur Emittentenbank durchführen
Zusätzliche Daten	• Zusätzliche Daten können über zusätzliche JSON-Parameter übermittelt werden, z.B.: ◦ "credentialOnFile" (für wiederkehrende Zahlungen) ◦ Adressdaten (für AVS) ◦ 3-D Secure Richtliniendaten	

Shop-/System-Integration	• Die Zahlungsseite kann durch selbst erstellte Vorlagen an Ihre Firmenidentität angepasst werden (Logos, Farben, Positionen, ...). • Der Verbraucher wird auf die Zahlungsseite ***weitergeleitet***, um Kreditkartendaten (PAN, Ablaufdatum, CVV, ...) einzugeben. • Ihr Shop wird über das Paygate Notify über das Ergebnis der Zahlung im Prozess informiert.	• Ihr System hat volle Kontrolle über die Eingabefelder für Kreditkartendaten • Der Verbraucher wird nicht umgeleitet und Ihr System erhält das Ergebnis des API-Aufrufs über direkte Antwortwerte
Weitere Aktionen	• Nach dem Auslösen des Zahlungsvorgangs können Sie weitere Aktionen wie Buchung, Gutschrift/Rückerstattung, Stornierungen, ... starten. • Diese Aktionen beziehen sich auf einen vorherigen Zahlungsprozess, der durch eine PayID identifiziert wird – was völlig außerhalb vom PCI-DSS-Fokus liegt.	
Schlussfolgerung	Empfohlen für Standardintegrationen – aufgrund einfacher Integration und vereinfachter Compliance.. • Paygate übernimmt die PAN-Handhabung für Sie ***vereinfachte PCI DSS Handhabung***. • Sie können die Paygate Zahlungsseite mittels Vorlagen anpassen.	Empfohlen, wenn Sie die volle Kontrolle benötigen und keine Weiterleitung des Verbrauchers wünschen. • Ihr System befindet sich im vollen Geltungsbereich von PCI DSS.

Die nachfolgende Dokumentation gliedert sich daher immer in zwei Abschnitte:

- Integration über Zahlungsseite (Zahlungsformular)
  - mit allgemeinen Parametern zur Integration des Computop Paygate Zahlungsformulars
  - mit Parametern zur Anpassung des Zahlungsformulars
  - mit spezifischen Parametern für den gewünschten Acquirer / Prozessor
- Integration über (direkte) Server-2-Server-Integration
  - mit allgemeinen Parametern zur Integration des Computop Paygate Zahlungsformulars
  - mit spezifischen Parametern für den gewünschten Acquirer / Prozessor

Implementierung von 3-D Secure (2.x)

Allgemeine Hinweise zu 3-D Secure

3-D Secure ist ein Verfahren, das den Karteninhaber authentifiziert und sicherstellt, dass der Verbraucher, der die Kreditkartendaten verwendet, wirklich der Karteninhaber ist.

3-D Secure soll den Missbrauch von Kreditkartendaten verhindern – insbesondere im E-Commerce.

3-D Secure 1.x wurde implementiert und fragt den Karteninhaber typischerweise bei jeder Kartennutzung nach einem Passwort.

3-D Secure 2.x wurde implementiert, um:

- eine starke Kundenauthentifizierung (SCA) zu ermöglichen, indem sie den Karteninhaber mit 2 unabhängigen Faktoren dieser 3 Faktoren anthentifiziert:
  - etwas, das der Karteninhaber ***weiß***, z.B. ein Kennwort
  - etwas, das der Karteninhaber ***besitzt***, z.B. ein Gerät (wie ein Telefon, um einen Token per SMS zu empfangen oder ein anderes OTP, Token-Generator, ...)
  - etwas, das der Karteninhaber ***ist***, z.B. Biometrie (wie Fingerabdruck, Gesichts-ID, ...)
- eine nahtlose Authentisierung zu ermöglichen, wenn der Verbraucher nicht authentifiziert wird und nicht aufgefordert wird, sich selbst zu authentifizieren.

3-D Secure mit Computop Paygate

- Schema Browser Challenge-Antwort
- Beispiel Browser Challenge-Antwort
- Authentisierungs-Benachrichtigung
- Browser Challenge
- Challenge-Anfrage
- 3DS Challenge-Anfrage initialisieren - Beispiel
- Autorisierung
- Zahlungs-Benachrichtigung
- Browser Zahlungs-Antwort
- Datenelemente
- Schema
- Entschlüsseltes Objekt Data
- Beispiel für entschlüsseltes Objekt Data
- Buchung / Gutschrift / Storno
- Buchung

- Gutschrift mit Referenz
- Gutschrift ohne Referenz
- Storno
- Storno einer Autorisierungsverlängerung
- Kreditkartenzahlung über stationäre Terminals
- Storno von stationären Kreditkartenzahlungen
- PayNow
  - Silent Mode für Kreditkarten mit SSL und 3-D Secure-Verfahren
- Batch-Nutzung der Schnittstelle
  - Batch-Aufrufe und Antworten
  - Stopp von Autorisierungsverlängerungen

Bereiten Sie sich / Ihre Integration auf 3-D Secure 2.x ready vor – hier eine kurze Übersicht mit einigen technischen Details.

<table>
<tr><th></th><th>3-D Secure 1.x</th><th>3-D Secure 2.x</th><th>3-D Secure 2.x Beispiel</th></tr>
<tr><td colspan="4">Hängt von Ihrer Integration ab: Zahlungsformular ./. Server-2-Server</td></tr>
<tr><td>Zahlungsseite / Zahlungsformular</td><td>Ihre vorhandene Integration</td><td>Ergänzen Sie einfach den API-Parameter "MsgVer=2.0", der Rest wird automatisch erledigt vomComputop Paygate</td><td>Ergänzen Sie den Parameter "MsgVer=2.0" bei Ihrem bestehenden API-Aufruf für den Start des Zahlungsformulars.</td></tr>
<tr><td>URL-Verarbeitung</td><td>URLFailure und URLSuccess arbeiten mit http-GET</td><td>URLFailure und URLSuccess arbeiten mit http-POST (wegen der Datenmenge). Seien Sie bereit, beides (GET + POST) zu handhaben.</td><td></td></tr>
<tr><td>Server-2-Server Integration</td><td>Use KVP:<table><tr><td>CCNr</td><td>Kreditkartennummer (PAN)</td></tr><tr><td>CCExpiry</td><td>Ablaufdatum der Kreditkarte</td></tr><tr><td>CCCVC</td><td>Kreditkartenprüfnummer</td></tr><tr><td>CCBrand</td><td>Kreditkartenmarke</td></tr></table></td><td>Übergeben Sie die Kartendaten mittels "card"-JSON an die API</td><td>z.B.:<pre>{
    "securityCode": "569",
    "expiryDate": "202508",
    "cardholderName": "William Thomas",
    "number": "4111111111111111",
    "brand": "VISA"
}</pre>card=ewogICAgInNlY3VyaXR5Q29kZSI6ICI1NjkiLAogICAgImV4cGlyeURhdGUiOiAiMjAyNTA4IiwKICAgICJjYXJkaG9sZGVyTmFtZSI6ICJXaWxsaWFtIFRob21hcyIsCiAgICAibnVtYmVyIjogIjQxMTExMTExMTExMTExMTEiLAogICAgImJyYW5kIjogIlZJU0EiCn0=</td></tr>
<tr><td colspan="4">Für spezielle Anwendungsfälle finden Sie hier weitere Anwendungsbeispiele: 3DS 2.0 Händler-Anwendungsfälle</td></tr>
<tr><th>Anwendungsfall</th><th>3-D Secure 1.x</th><th>3-D Secure 2.x</th><th>3-D Secure 2.x Beispiel</th></tr>
</table>

<table>
<tr>
<td>Wiederkehrende Zahlungen (initial)</td>
<td>Nutzen Sie den Parameter "RTF=I".

Sie erhalten eventuell eine TransactionID als spezifische Transaktions-ID des Karten-Schemes.</td>
<td>Ändern Sie "RTF" zum Parameter "credentialOnFile"-JSON mit "recurring" und "initial=true".

Sie erhalten eventuell eine schemeReferenceID als spezifische Transaktions-ID des Karten-Schemes.</td>
<td>z.B.:

Recurring mit initial=true

<pre>{
    "type": {
        "recurring": {

"recurringFrequency": 30,

"recurringStartDate": "2021-09-14",

"recurringExpiryDate": "2022-09-14"
        }
    },
    "initialPayment": true
}</pre>
Das JSON muss Base64-codiert sein und dann als Wert für den Parameter credentialOnFile verwendet werden (Bitte beachten Sie, dass Sie den vollständigen Base64-codierten String verwenden einschließlich "=" am Ende.)

credentialOnFile=ewogICAgInR5cGUiOiB7CiAgICAgICAgInJlY3VycmluZyI6IHsKICAgICAgICAgICAgInJlY3VycmluZ0ZyZXF1ZW5jeSI6IDMwLAogICAgICAgICAgICAicmVjdXJyaW5nU3RhcnREYXRlIjogIjIwMjEtMDktMTQiLAogICAgICAgICAgICAicmVjdXJyaW5nRXhwaXJ5RGF0ZSI6ICIyMDIyLTA5LTE0IgogICAgICAgIH0KICAgIH0sCiAgICAiaW5pdGlhbFBheW1lbnQiOiB0cnVlCn0=</td>
</tr>
<tr>
<td>Wiederkehrende Zahlungen (nachfolgend)</td>
<td>Nutzen Sie den Parameter "RTF=R"

und übermitteln die TransactionID als spezifische Transaktions-ID des Karten-Schemes</td>
<td>Ändern Sie "RTF" zum Parameter "credentialOnFile"-JSON mit "recurring" und "initial=false"

und übermitteln die schemeReferenceID als spezifische Transaktions-ID des Karten-Schemes</td>
<td>z.B.

Recurring mit initial=false

<pre>{
    "type": {
        "recurring": {

"recurringFrequency": 30,

"recurringStartDate": "2021-09-14",

"recurringExpiryDate": "2022-09-14"
        }
    },
    "initialPayment": false
}</pre>
Nach der Base64-Codierung:

credentialOnFile=ewogICAgInR5cGUiOiB7CiAgICAgICAgInJlY3VycmluZyI6IHsKICAgICAgICAgICAgInJlY3VycmluZ0ZyZXF1ZW5jeSI6IDMwLAogICAgICAgICAgICAicmVjdXJyaW5nU3RhcnREYXRlIjogIjIwMjEtMDktMTQiLAogICAgICAgICAgICAicmVjdXJyaW5nRXhwaXJ5RGF0ZSI6ICIyMDIyLTA5LTE0IgogICAgICAgIH0KICAgIH0sCiAgICAiaW5pdGlhbFBheW1lbnQiOiBmYWxzZQp9</td>
</tr>
</table>

Vom Kunden ausgelöst (initial)	Nutzen Sie Parameter "RTF=E". Sie erhalten eventuell eine TransactionID als spezifische Transaktions-ID des Karten-Schemes.	Ändern Sie "RTF" zum Parameter "credentialOnFile"-JSON mit "CIT" und "initial=true". Sie erhalten eventuell eine schemeReferenceID als spezifische Transaktions-ID des Karten-Schemes.	z.B. **CIT (CustomerInitiated) mit initial=true** `{ "type": { "unscheduled": "CIT" }, "initialPayment": true }` Nach der Base64-Codierung (nochmal: vergessen Sie nicht das "=" am Ende; es muss Bestandteil des Wertes sein): credentialOnFile=ewogICAgInR5cGUiOiB7CiAgICAgICAgInVuc2NoZWR1bGVkIjogIkNJVCIKICAgIH0sCiAgICAiaW5pdGlhbFBheW1lbnQiOiB0cnVlCn0=
Vom Händler ausgelöst (nachfolgend)	Nutzen Sie Parameter "RTF=M" und übermitteln die TransactionID als spezifische Transaktions-ID des Karten-Schemes	Ändern Sie "RTF" zum Parameter "credentialOnFile"-JSON mit "MIT" und "initial=false" und übermitteln die schemeReferenceID als spezifische Transaktions-ID des Karten-Schemes	z.B. **MIT (MerchantInitiated) mit initial=false** `{ "type": { "unscheduled": "MIT" }, "initialPayment": false }` Nach der Base64-Codierung: credentialOnFile=ewogICAgInR5cGUiOiB7CiAgICAgICAgInVuc2NoZWR1bGVkIjogIk1JVCIKICAgIH0sCiAgICAiaW5pdGlhbFBheW1lbnQiOiBmYWxzZQp9
Adressverifizierungsdienst (AVS) (abhängig vom Acquirer / Prozessor)	Nutzen Sie die Parameter • AddrStreet • AddrStreetNr • AddrZip • AddrCity •	Ändern Sie die Adressdaten zu address"-JSON	z.B. **Adresse in JSON-Struktur geben** `{ "city": "New York", "country": { "countryA3": "USA" }, "addressLine1": { "street": "Park Avenue", "streetNumber": "270" }, "postalCode": "10017-2070", "state": "NY" }` billingAddress=ewogICAgImNpdHkiOiAiTmV3IFlvcmsiLAogICAgImNvdW50cnkiOiB7CiAgICAgICAgImNvdW50cnlBMyI6ICJVU0EiCiAgICB9LAogICAgImFkZHJlc3NMaW5lMSI6IHsKICAgICAgICAic3RyZWV0Ijogll BhcmsgQXZlbnVlliwKICAgICAgICAic3RyZWV0TnVtYmVyIjogIjI3MCIKICAgIH0sCiAgICAicG9zdGFsQ29kZSI6ICIxMDAxNy0yMDcwliwKICAgICJzdGF0ZSI6ICJOWSIKfQ==

Antrag für reibungslose Zahlungsabwicklung	• nicht unterstützt bei 3-D Secure 1.x • jede Zahlung wird authentisiert	Stellen Sie zusätzliche Daten bereit als JSON-KVP: JSON-Objekte	z.B.: **Kunden-Challenge explizit anfordern** `{ "challengePreference ": "mandateChallenge" }` Nach der Base64-Codierung (nochmal: vergessen Sie nicht das "=" am Ende; es muss Bestandteil des Wertes sein): threeDSPolicy=ewogICAgImNoYWxsZW5nZVByZWZlcmVuY2UgIjogIm1hbmRhdGVDaGFsbGVuZ2UiCn0=

Spezifische Parameter für Heartland

Für die Kreditkartenanbindung Heartland sind neben den oben beschriebenen allgemeinen Parametern noch nachstehende Parameter zusätzlich zu übergeben.

Hinweis: Aus Sicherheitsgründen lehnt das Paygate alle Zahlungsanfragen mit Formatfehlern ab. Bitte übergeben Sie deshalb bei jedem Parameter den korrekten Datentyp.

Die folgende Tabelle beschreibt die verschlüsselten Übergabeparameter, welche **zusätzlich** zu denen im Abschnitt "Allgemein per Formular" bzw. "Allgemein per Server-zu-Server" übergeben werden müssen:

Key	Format	CND	Beschreibung
RefNr	ns..30	M	Eindeutige Referenznummer des Händlers, welche als Auszahlungsreferenz in der entsprechenden Acquirer EPA-Datei angegeben wird. Bitte beachten Sie, ohne die Übergabe einer eigenen Auszahlungsreferenz können Sie die EPA-Transaktionen nicht zuordnen, zusätzlich kann das Computop Settlement File (CTSF) auch nicht zusätzlich angereichert werden. Es sind ausschließlich ASCII-Zeichen erlaubt. Sonderzeichen wie ("Umlaute", ...) sind nicht erlaubt und müssen ggf. durch ASCII-Zeichen ersetzt werden (z.B. ü ue, é e, ...).
			Kontaktdaten/Adressverifikation (AVS)
FirstName	ans..100	O	Vorname des Kunden
LastName	ans..100	O	Nachname des Kunden
AddrStreet	ans..128	O	Straßenname und Hausnummer
AddrZip	ans..20	O	Postleitzahl
AddrCity	ans..50	O	Ort
AddrState	a2	O	Code des Bundeslandes des Kunden
AddrCountryCode	a2/a3	M	Ländercode im Format ISO-3166-1, alphanumerisch 2-stellig oder 3-stellig

Zusätzliche Parameter für Kreditkartenzahlungen

Die folgende Tabelle beschreibt die Parameter, die das Paygate als Antwort zurückgibt:

diese Antwort-Parameter kommen zusätzlich zu den Standard-Parametern aus den Abschnitten "Allgemein per Formular" bzw. "Allgemein per Server-zu-Server"

es können jederzeit neue Parameter hinzugefügt bzw. die Reihenfolge geändert werden

die Parameter (z.B. MerchantId, RefNr) sollten nicht auf Groß-/Kleinschreibung geprüft werden

Key	Format	CND	Beschreibung
RefNr	ns..30	O	Eindeutige Referenznummer des Händlers, welche als Auszahlungsreferenz in der entsprechenden Acquirer EPA-Datei angegeben wird. Bitte beachten Sie, ohne die Übergabe einer eigenen Auszahlungsreferenz können Sie die EPA-Transaktionen nicht zuordnen, zusätzlich kann das Computop Settlement File (CTSF) auch nicht zusätzlich angereichert werden. Es sind ausschließlich ASCII-Zeichen erlaubt. Sonderzeichen wie ("Umlaute", ...) sind nicht erlaubt und müssen ggf. durch ASCII-Zeichen ersetzt werden (z.B. ü ue, é e, ...).
ErrorText	ans..128	O	Fehlertext vom nachgelagertem System, nur wenn dessen Rückgabe mit Computop Helpdesk abgesprochen ist.
CodeExt	ans..10	O	Nur wenn konfiguriert: externer Fehlercode (nachgelagertes System)
ApprovalCode	an6	O	Externer Genehmigungscode (nachgelagertes System). Nur vorhanden, wenn die Autorisierung erfolgreich war.
HpsTransactionID	n10	O	Von Heartland vergebene TransaktionsID: wird zurückgegeben, wenn die Autorisierung okay ist
HpsReferenceNumber	n12	O	Von Heartland vergebene ReferenceNumber: wird zurückgegeben, wenn die Autorisierung okay ist
Match	a1	O	Ergebnis der Adressprüfung: Der Parameter wird je nach Merchant-Konfiguration zurückgeliefert – als vereinfachter Match-Parameter oder wie von Heartland zurückgegeben; Details finden Sie hier: A3 AVS Match-Parameter

Zusätzliche Ergebnis-Parameter für Kreditkartenzahlungen

Kreditkarten - Kreditkartenformular

Bei Kartenzahlungen über bei Computop gehostete Formulare wird die Komplexität von 3-D Secure vollständig bei der Implementierung beim Händler entfernt.

Aus Sicht des Händlers unterscheidet sich die Sequenz nicht zwischen Zahlungen, die mit 3DS authentisiert sind, sowie nicht mit 3DS authentisierten Zahlungen, welche die Berücksichtigung zusätzlicher Parameter in Aufruf und Antwort erfordern.

Hinweis zum Cookie-/Session Handling

Bitte beachten Sie, dass einige Browser beim Rücksprung zu Ihrem Shop erforderliche Cookies blockieren könnten. Hier finden Sie weitere Informationen und verschiedene Lösungsansätze.

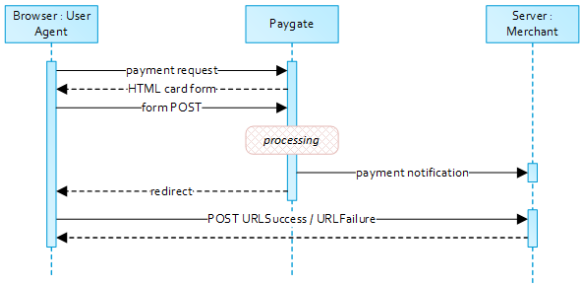
- Kreditkarten - Kreditkartenformular
  - Vereinfachtes Sequenz-Diagramm
  - Zahlungsanfrage
  - HTTP POST an URLSuccess / URLFailure / URLNotify
  - Kreditkartenzahlung mit separater Autorisierung
  - Erweitertes Sequenz-Diagramm

EMV 3-D Secure

Hinweise zum Cookie-/session-Handling

API Playground

Vereinfachtes Sequenz-Diagramm



Zahlungsanfrage

Zum Abruf eines Computop-Formulars für Kartenzahlungen übermitteln Sie bitte folgende Parameter über einen HTTP POST Aufruf an https://www.computop-paygate.com/payssl.aspx.

Hinweis: Aus Sicherheitsgründen lehnt das Paygate alle Zahlungsanfragen mit Formatfehlern ab. Bitte übergeben Sie deshalb bei jedem Parameter den korrekten Datentyp.

Die folgende Tabelle beschreibt die verschlüsselten Übergabeparameter:

Key	REST	Format	CND	Beschreibung
MerchantID	BasicAuth. Username	ans..30	M	HändlerID, die von Computop vergeben wird. Dieser Parameter ist zusätzlich auch unverschlüsselt zu übergeben.

Key	REST	Format	CND	Beschreibung
msgver	---	ans..5	M	Computop Paygate Message-Version. Zulässige Werte: **Wert** – **Beschreibung** 2.0 – Mit 3-D Secure 2.x wurde eine Vielzahl zusätzlicher Daten (Browser-Information, Rechnungs-/Versand-Adresse, ...) erforderlich, um den Authentifizierungs-Prozess zu optimieren. Um diese Informationen zu handhaben, wurden die JSON-Objekte eingeführt. Der Parameter MsgVer zeigt an, dass diese Daten verwendet werden.

Key	REST	Format	CND	Beschreibung
ReqId	"requestId": "..."	ans..32	O	Um Doppelzahlungen (z.B. durch ETM) zu vermeiden, übergeben Sie einen alphanumerischen Wert, der Ihre Transaktion oder Aktion identifiziert und nur einmal vergeben werden darf. Falls die Transaktion oder Aktion mit derselben ReqID erneut eingereicht wird, führt das Computop Paygate keine Zahlung oder weitere Aktion aus, sondern gibt nur den Status der ursprünglichen Transaktion oder Aktion zurück. Bitte beachten Sie, dass das Computop Paygate für die erste initiale Aktion (Authentifizierung/Autorisierung) einen abgeschlossenen Transaktionsstatus haben muss. Dies gilt nicht für 3-D Secure Authentifizierungen, die durch einem Timeout beendet werden. Der Status 3-D Secure Timeout gilt nicht als abgeschlossener Status, bei dem ReqID-Funktionalität am Paygate nicht greift. Einreichungen mit identischer ReqID auf einen offenen Status werden regulär verarbeitet. **Hinweis:** Bitte beachten Sie, dass eine ReqID nur 12 Monate gültig ist, danach wird sie vom Paygate gelöscht.

Key	REST	Format	CND	Beschreibung
TransID	"transactionId": "..."	ans..64	M	Ihre eigene TransaktionsID, die für jede Zahlung eindeutig sein muss

Key	REST	Format	CND	Beschreibung
RefNr	"referenceNumber": "..."		O	Eindeutige Referenznummer des Händlers, welche als Auszahlungsreferenz in der entsprechenden Acquirer EPA-Datei angegeben wird. Bitte beachten Sie, ohne die Übergabe einer eigenen Auszahlungsreferenz können Sie die EPA-Transaktionen nicht zuordnen, zusätzlich kann das Computop Settlement File (CTSF) auch nicht zusätzlich angereichert werden. Informationen zum unterstützten Format finden Sie weiter unten in der zahlartspezifischen Beschreibung. Es sind ausschließlich ASCII-Zeichen erlaubt. Sonderzeichen wie ("Umlaute", ...) sind nicht erlaubt und müssen ggf. durch ASCII-Zeichen ersetzt werden (z.B. ü ue, é e, ...).

Key	REST	Format	CND	Beschreibung
MAC	---	an64	M	Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier: • HMAC-Authentisierung (Anfrage) • HMAC-Authentisierung (Notify)

Key	REST	Format	CND	Beschreibung
Amount	"amount": { "value": ...}	n..10	M	Betrag in der kleinsten Währungseinheit (z.B. EUR Cent). Bitte wenden Sie sich an den Computop Helpdesk, wenn Sie Beträge < 100 (kleinste Währungseinheit) buchen möchten.

Key	REST	Format	CND	Beschreibung
Currency	"amount": { "currency": "..."}	a3	M	Währung, drei Zeichen DIN / ISO 4217, z.B. EUR, USD, GBP. Hier eine Übersicht: A1 Währungstabelle

Key	REST	Format	CND	Beschreibung

Capture	"capture": {"auto": "Yes"} "capture": {"manual": "Yes"} "capture": ...	an..6	OM	Bestimmt Art und Zeitpunkt der Buchung (engl. Capture). **Buchungsart** / **Beschreibung** **AUTO** – Buchung sofort nach Autorisierung (Standardwert). **MANUAL** – Buchung erfolgt durch den Händler - in der Regel die Buchung zum Zeitpunkt der Warenauslieferung bzw. Leistungserbringung. **<Zahl>** – Verzögerung in Stunden bis zur Buchung (ganze Zahl; 1 bis 696).

Key	REST	Format	CND	Beschreibung
PayTypes	"payment": {"cardForm": { "payTypes": "..." }}	ans..256	O	Mit diesem Parameter können Sie die akzeptierten Schemes übersteuern, d.h. Sie können innerhalb dieses Parameters durch Pipe getrennt entscheiden, welche der verfügbaren Kreditkartenschemes angezeigt werden. Das Template muss diese Funktion unterstützen wie zum Beispiel das "Cards_v1". Beispiel: PayTypes=VISA|MasterCard
billingDescriptor	"billing": {"addressInfo": { "descriptor": "..." }}	ans..22	O	Eine Bezeichnung, die auf dem Kontoauszug des Karteninhbaers gedruckt wird. Beachten Sie bitte auch die zusätzliche Hinweise an anderer Stelle für weitere Informationen über Regeln und Vorschriften.
OrderDesc	"order": {"description": "..."}	ans..768	O	Beschreibung der gekauften Waren, Einzelpreise etc.
AccVerify	"payment": {"card": { "accountVerification": "..." }}	a3	O	Indikator für Anforderung einer Kontoverifizierung (alias Nullwert-Authorisierung). Bei einer angeforderten Kontoverifizierung ist der übermittelte Betrag optional und wird für die tatsächliche Zahlungstransaktion ignoriert (z.B. Autorisierung). Zulässiger Wert: • **Yes**
threeDSPolicy	"payment": {"card": { "threeDsPolicy": JSON }}	JSON	O	Objekt, das Authentisierungs-Richtlinien und Vorgaben für die Ausnahmenbehandlung festlegt
priorAuthenticationInfo	"payment": {"card": { "priorAuthenticationInfo": JSON }}	JSON	O	Das Objekt Prior Transaction Authentication Information enthält optionale Informationen über eine Authentisierung eines 3DS-Karteninhabers, die vor der aktuellen Transaktion erfolgt ist
accountInfo	"accountInfo": JSON	JSON	O	Das Objekt Kontoinformationen enthält optionale Informationen über das Kundenkonto beim Händler
billToCustomer	"billing": JSON	JSON	C	Der Kunde, dem die Waren und / oder Dienstleistungen in Rechnung gestellt werden. Für EMV 3DS erforderlich, sofern nicht Markt- oder Regionalmandate die Übermittlung dieser Informationen beschränken.
shipToCustomer	"shipping": JSON	JSON	C	Der Kunde, an den die Waren und / oder Dienstleistungen gesendet werden. Erforderlich, falls von billToCustomer abweichend.
billingAddress	"billing": {"addressInfo": JSON}	JSON	C	Rechnungsadresse. For EMV 3DS erforderlich (falls verfügbar), sofern nicht Markt- oder Regionalmandate die Übermittlung dieser Informationen beschränken.
shippingAddress	"shipping": {"addressInfo": JSON}	JSON	C	Lieferadresse. Falls von billingAddress abweichend; für EMV 3DS erforderlich (falls verfügbar), sofern nicht Markt- oder Regionalmandate die Übermittlung dieser Informationen beschränken.
credentialOnFile	"credentialOnFile": JSON	JSON	C	Objekt, das Art und Reihe von Transaktionen mittels Zahlungskonto-Zugangsdaten festlegt (z.B. Kontonummer oder Zahlungs-Token), die bei einem Händler für die Verarbeitung zukünftiger Einkäufe für einen Kunden gespeichert sind. Erforderlich, falls zutreffend.
merchantRiskIndicator	"riskIndicator": JSON	JSON	O	Der Händler-Risikoindikator enthält optionale Informationen über den bestimmten Einkauf des Kunden. Falls **`shippingAddress`** nicht vorhanden ist, ist es dringend empfohlen, das Merkmal **`shippingAddressIndicator`** mit einem entsprechenden Wert wie **`shipToBillingAddress`**, **`digitalGoods`** oder **`noShipment`** auszufüllen.
subMerchantPF	"subMerchantPaymentFacilitator": JSON	JSON	O	Objekt, das die Details des SubMerchant (Payment Facilitator) angibt. Wird ausschließlich von SafeCharge unterstützt.

Key	REST	Format	CND	Beschreibung

URLSuccess	"urls": {"success": "..."}	ans..256	M	Vollständige URL, die das Paygate aufruft, wenn die Zahlung erfolgreich war. Die URL darf nur über Port 443 aufgerufen werden. Diese URL darf keine Parameter enthalten: Um Parameter durchzureichen nutzen Sie stattdessen den Parameter UserData. **Allgemeine Hinweise:** • Wir empfehlen, den Parameter "response=encrypt" zu verwenden, um eine verschlüsselte Antwort von Paygate zu erhalten • Betrüger könnten das verschlüsselte DATA-Element kopieren, welches an URLFailure gesendet wurde, und betrügerisch dasselbe DATA an URLSuccess senden. Überprüfen Sie daher unbedingt den "code"-Wert des DATA-Elements. Nur eine Antwort mit "code=00000000" sollte als erfolgreich angesehen werden.

Key	REST	Format	CND	Beschreibung
URLFailure	"urls": {"failure": "..."}	ans..256	M	Vollständige URL, die das Paygateaufruft, wenn die Zahlung gescheitert ist. Die URL darf nur über Port 443 aufgerufen werden. Diese URL darf keine Parameter enthalten: Um Parameter durchzureichen nutzen Sie stattdessen den Parameter UserData. **Allgemeine Hinweise:** • Wir empfehlen, den Parameter "response=encrypt" zu verwenden, um eine verschlüsselte Antwort von Paygate zu erhalten • Betrüger könnten das verschlüsselte DATA-Element kopieren, welches an URLFailure gesendet wurde, und betrügerisch dasselbe DATA an URLSuccess/URLNotify senden. Überprüfen Sie daher unbedingt den "code"-Wert des DATA-Elements. Nur eine Antwort mit "code=00000000" sollte als erfolgreich angesehen werden.

Key	REST	Format	CND	Beschreibung
URLBack	"urls": {"cancel": "..."}	ans..256	O	Vollständige URL, die das Paygate aufruft, wenn der **Kunde auf Abbruch** klickt. Der Parameter "URLBack" kann • sowohl unverschlüsselt ans Paygate übermittelt werden (Kompabilitätsmodus) • als auch in den verschlüsselten Übergabeparametern (bevorzugte Variante) Wenn Sie Parameter/Werte in der URLBack übergeben möchten, so können Sie folgende Methode verwenden: `URLBack=https://your.shop.com/back.php?param1%3Dvalue1%26param2%3Dvalue3%26status%3Dcancelled` Wenn der Kunde auf Abbruch klickt, so wird die URL genauso aufgerufen, so dass Sie URL Decode verwenden können, um Parameter und Werte zu extrahieren.

Key	REST	Format	CND	Beschreibung
Response	---	a7	O	Die Status-Rückmeldung, die das Paygate an URLSuccess und URLFailure sendet, sollte verschlüsselt werden. Dazu übergeben Sie den Parameter Response=encrypt.

Key	REST	Format	CND	Beschreibung
URLNotify	"urls": {"notify": "..."}	ans..256	M	Vollständige URL, die das Paygate aufruft, um den Shop zu benachrichtigen. Die URL darf nur über Port 443 aufgerufen werden. Sie darf keine Parameter enthalten: Nutzen Sie stattdessen den Parameter UserData. **Allgemeine Hinweise:** • Wir empfehlen, den Parameter "response=encrypt" zu verwenden, um eine verschlüsselte Antwort von Paygate zu erhalten • Betrüger könnten das verschlüsselte DATA-Element kopieren, welches an URLFailure gesendet wurde, und betrügerisch dasselbe DATA an URLSuccess/URLNotify senden. Überprüfen Sie daher unbedingt den "code"-Wert des DATA-Elements. Nur eine Antwort mit "code=00000000" sollte als erfolgreich angesehen werden.

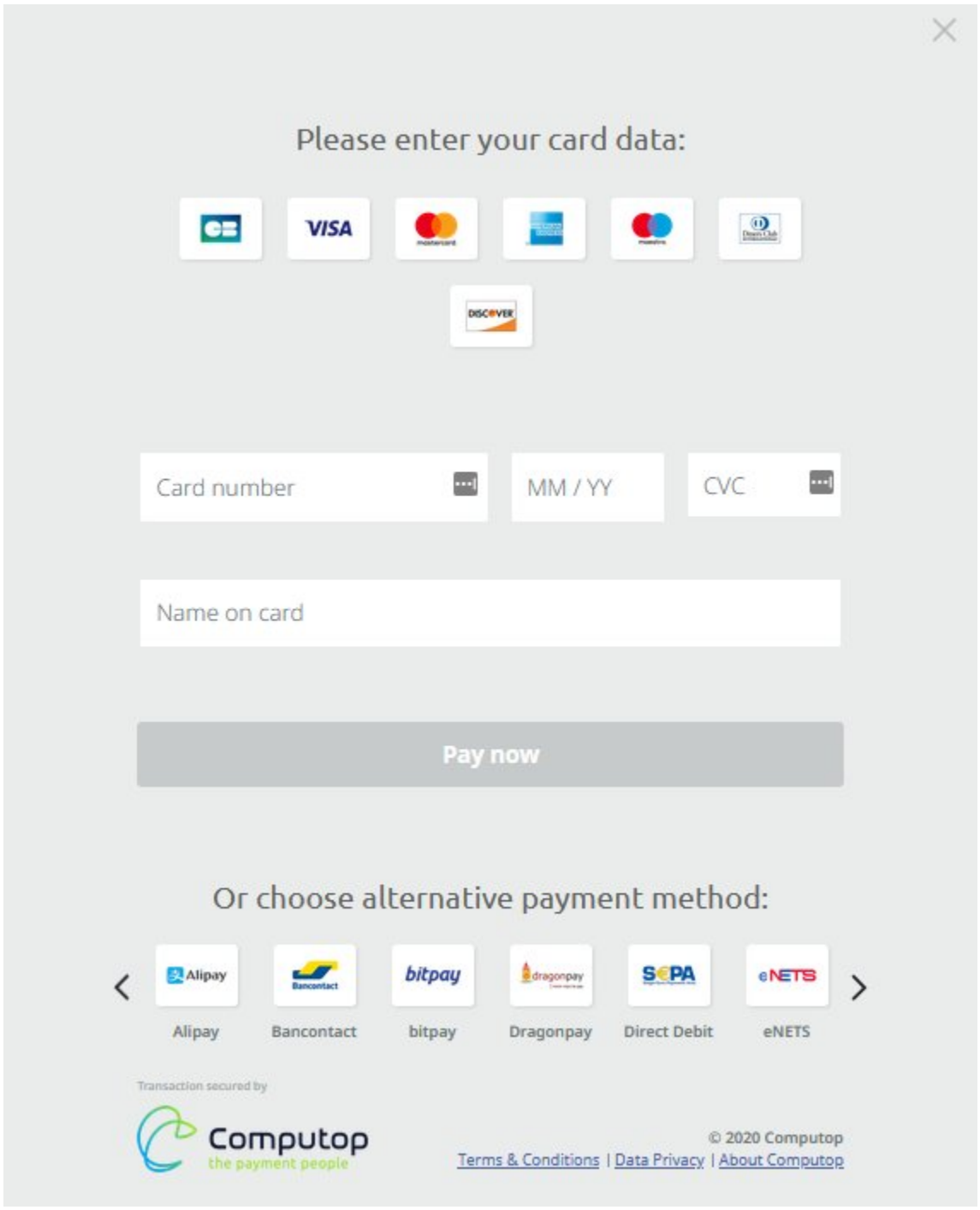
Key	REST	Format	CND	Beschreibung
UserData	"metadata[userData]": "..."	ans..1024	O	Wenn beim Aufruf angegeben, übergibt das Paygate die Parameter mit dem Zahlungsergebnis an den Shop.

Key	REST	Format	CND	Beschreibung
Plain	"metadata[plain]": "..."	ans..50	O	Ein einzelner Wert, der von Ihnen gesetzt werden kann, um Informationen wieder unverschlüsselt in der Antwort bzw. im Notify zurückzugeben, z.B. die MID. Da der "Plain"-Parameter Teil des verschlüsselten "Data" im Computop Paygate ist, ist dieser vor Manipulationen geschützt.

Key	REST	Format	CND	Beschreibung
Custom	"metadata": "..."	ans..1024	O	Der "Custom"-Parameter wird vor der Verschlüsselung an den Aufruf angehängt und ist Teil des verschlüsselten "Data" im Computop Paygate Aufruf. Dadurch ist der Wert gegen Manipulation geschützt. Der Custom-Wert wird dann in Klartext an die Computop Paygate-Antwort angehängt und dabei wird "|" durch "&" ersetzt. Dadurch können Sie einen Custom-Wert übergeben und bekommen mehrere Key-Value-Paare zu Ihrer eigenen Verwendung in der Antwort zurück. Hier finden Sie ein Beispiel: Custom

Key	REST	Format	CND	Beschreibung
expirationTime	"expirationTime": "..."	ans..19	O	Zeitstempel für den Endzeitpunkt der Transaktionsverarbeitung, Angabe in UTC. Format: YYYY-MM-ddTHH:mm:ss

Computop Paygate gibt in der Antwort ein HTML-Dokument zurück, welches das angeforderte Kartenzahlungsformular darstellt. Das Formular kann in die Checkout-Seite des Händlers integriert oder als selbständige Seite verwendet werden, auf die der Karteninhaber weitergeleitet wird.



Die Authentisierung des Karteninhabers sowie die Zahlungsautorisierung erfolgen, nachdem der Karteninhaber aller erforderlichen Kartendetails eingegeben und das Formular an das Computop Paygate übermittelt hat.

Hinweis: Falls Sie ein eigenes Zahlungsformular verwenden (Corporate Payment Page), achten Sie darauf, dass der Name des Karteninhabers auf dem Formular enthalten ist. Der Name das Karteninhabers wird auf den Paygate API-Parameter "CreditCardHolder" abgebildet. Das Feld Cardholder name darf keine Sonderzeichen enthalten und muss eine Mindestlänge von 2 Zeichen und eine Maximallänge von 45 Zeichen haben.

Wenn die Zahlung abgeschlossen ist, sendet das Computop Paygate eine Benachrichtigung an den Server des Händlers (d.h. **URLNotify**) und leitet den Browser an **URLSuccess** beziehungsweise **URLFailure** weiter.

Die per Blowfish verschlüsselten Parameter laut folgender Tabelle werden per **HTTP POST** an URLNotify und URLSuccess/URLFailure übertragen.

Hinweis: Bitte beachten Sie, dass der Aufruf der URLSuccess oder URLFailure bei einem Fallback zu 3-D Secure 1.0 mit GET stattfindet. Ihre Systeme sollten daher Parameter sowohl per GET als auch per POST entgegennehmen können.

Das Kreditkarten-Formular kann mittels eines eigenen Templates sehr stark angepasst werden.

Details hierzu finden Sie hier: Corporate PayPage und Templates

HTTP POST an URLSuccess / URLFailure / URLNotify

Die folgende Tabelle beschreibt die Ergebnis-Parameter, die das Paygate an Ihre **URLSuccess, URLFailure** und **URLNotify** übergibt. Wenn Sie den Parameter **Response=encrypt** angegeben haben, werden die folgenden Parameter mit Blowfish verschlüsselt an Ihr System übergeben:

es können jederzeit neue Parameter hinzugefügt bzw. die Reihenfolge geändert werden

die Parameter (z.B. MerchantId, RefNr) sollten nicht auf Groß-/Kleinschreibung geprüft werden

Key	Format	CND	Beschreibung
mid	ans..30	M	HändlerID, die von Computop vergeben wird

Key	Format	CND	Beschreibung
msgver	ans..5	M	Computop Paygate Message-Version. Zulässige Werte: **Wert** / **Beschreibung** 2.0 – Mit 3-D Secure 2.x wurde eine Vielzahl zusätzlicher Daten (Browser-Information, Rechnungs-/Versand-Adresse, ...) erforderlich, um den Authentifizierungs-Prozess zu optimieren. Um diese Informationen zu handhaben, wurden die JSON-Objekte eingeführt. Der Parameter MsgVer zeigt an, dass diese Daten verwendet werden.

Key	Format	CND	Beschreibung
PayID	an32	M	Vom Paygate vergebene ID für die Zahlung; z.B. zur Referenzierung in Batch-Dateien sowie im Capture- oder Credit-Request.

Key	Format	CND	Beschreibung
XID	an32	M	Vom Paygate vergebene ID für alle einzelnen Transaktionen (Autorisierung, Buchung, Gutschrift), die für eine Zahlung durchgeführt werden

Key	Format	CND	Beschreibung
TransID	ans..64	M	Ihre eigene TransaktionsID, die für jede Zahlung eindeutig sein muss

Key	Format	CND	Beschreibung
schemeReferenceID	ans..64	C	Spezifische Transaktions-ID des Kartenschemas, die für nachfolgende Zahlungen mit gespeicherten Zugangsdaten, verzögerte Autorisierungen und Wiedereinreichungen erforderlich ist. Pflicht: CredentialOnFile – initial false – unschedule MIT / recurring schemeReferenceID wird bei 3DS2-Zahlungsvorgängen zurückgegeben. Bei einem Fallback auf 3DS1 prüfen Sie bitte zusätzlich auf TransactionId. Die SchemeReferenceID ist eine eindeutige Kennung, die von den Kartenmarken generiert wird. In der Regel können Computop -Händler die SchemeReferenceIDs für Abonnements übergreifend verwenden, welche unter Verwendung eines anderen PSP / separater Paygate-MerchantID / separater Acquirer ContractID / Acquirer erstellt wurden.

Key	Format	CND	Beschreibung
refnr		O	Referenznummer vom Request

Status	a..20	M	Status der Transaction. Zulässige Werte: • **`Authorized`** • **`OK`** (Sale) • **`FAILED`** Im Fall von *nur-Authentisierung* ist der *Status* entweder **`OK`** oder **`FAILED`**.

Key	Format	CND	Beschreibung
Description	ans..1024	M	Nähere Beschreibung bei Ablehnung der Zahlung. Bitte nutzen Sie **nicht** den Parameter **Description, sondern** Code für die Auswertung des Transaktionsstatus!

Key	Format	CND	Beschreibung
Code	n8	M	Fehlercode gemäß Paygate Antwort-Codes (A4 Fehlercodes)

Key	Format	CND	Beschreibung
card	JSON	M	Kartendaten
ipinfo	JSON	O	Objekt mit IP-Informationen
threedsdata	JSON	M	Authentisierungsdaten
resultsresponse	JSON	C	Falls der Authentisierungsprozess eine Challenge des Karteninhabers enthalten hat, werden zusätzliche Informationen über das Ergebnis der Challenge bereitgestellt
externalPaymentData	JSON	O	Optionale Daten des Acquirers/Issuers/externen Dienstleisters für eine Autorisierung
TimeStamp	Date/Time	O	Zeitstempel dieser Aktion, wenn vom Computop Helpdesk aktiviert, z.B. 30.05.2023 08:47:57 oder 30.05.2023 10:03:01.633
CardHolder	ans..50	O	Name des Karteninhabers, wenn vom Computop Helpdesk aktiviert, z.B. Max Mustermann
bin	n..6	O	BIN der Kreditkarte, wenn vom Computop Helpdesk aktiviert, z.B. 40001
maskedpan	an..19	O	Maskierte Kreditkartennummer, wenn vom Computop Helpdesk aktiviert, z.B. 400001XXXXXX8323
cardinfo	JSON	O	JSON-Struktur, welche Informationen zur Kreditkarte bzw. dem Issuer enthält, wenn vom Computop Helpdesk aktiviert, z. B. {"BIN":"400001","Brand":"VISA","Product":"","Source":"CREDIT","Type":"","Country":{"A3":"USA","N3":"840"},"Issuer":""}
CCBrand	an..20	O	Brand / Karten-Scheme der Kreditkarte, z.B. VISA

Key	Format	CND	Beschreibung
PCNr	n16	O	Pseudo Card Number: Vom Computop Paygate generierte Zufallszahl, die eine reale Kreditkartennummer repräsentiert. Die Pseudokartennummer (PKN) beginnt mit 0, und die letzten 3 Stellen entsprechen denen der realen Kartennummer. Die PKN kann wie eine Kreditkartennummer für Autorisierung, Buchung und Gutschriften verwendet werden. PCNr ist ein **Antwortwert** von Computop Paygate und kann ebenfalls als CCNr im Request oder als Teil von card-JSON verwendet werden.

Key	Format	CND	Beschreibung
CCExpiry	n6	OC	In Verbindung mit PCNr: Ablaufdatum der Kreditkarte im Format YYYYMM (202207).

Key	Format	CND	Beschreibung
Plain	ans..50	O	Ein einzelner Wert, der von Ihnen gesetzt werden kann, um Informationen wieder unverschlüsselt in der Antwort bzw. im Notify zurückzugeben, z.B. die MID. Da der "Plain"-Parameter Teil des verschlüsselten "Data" im Computop Paygate ist, ist dieser vor Manipulationen geschützt.

Key	Format	CND	Beschreibung
Custom	ans..1024	O	Der "Custom"-Parameter wird vor der Verschlüsselung an den Aufruf angehängt und ist Teil des verschlüsselten "Data" im Computop Paygate Aufruf. Dadurch ist der Wert gegen Manipulation geschützt. Der Custom-Wert wird dann in Klartext an die Computop Paygate-Antwort angehängt und dabei wird "|" durch "&" ersetzt. Dadurch können Sie einen Custom-Wert übergeben und bekommen mehrere Key-Value-Paare zu Ihrer eigenen Verwendung in der Antwort zurück. Hier finden Sie ein Beispiel: Custom

Key	Format	CND	Beschreibung
UserData	ans..1024	O	Wenn beim Aufruf angegeben, übergibt das Paygate die Parameter mit dem Zahlungsergebnis an den Shop.

Key	Format	CND	Beschreibung
MAC	an64	M	Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier: • HMAC-Authentisierung (Anfrage) • HMAC-Authentisierung (Notify)

Kreditkartenzahlung mit separater Autorisierung

Für Kreditkartenzahlungen kann im Prozessablauf die ORDER von der anschließenden Autorisierung und nachfolgenden Schritten getrennt werden. Dazu wird die SSL-Kreditkartenzahlung zunächst per Formular oder Server-zu-Server-Anbindung wie in den voranstehenden Kapiteln dargestellt mit einem zusätzlichen Parameter initialisiert und dann über die Schnittstelle **authorize.aspx** per Server-zu-Server-Verbindung autorisiert. Zur Initialisierung rufen Sie folgende URL auf:

https://www.computop-paygate.com/payssl.aspx

Bei Server-zu-Server-Anbindung rufen Sie folgende URL auf:

https://www.computop-paygate.com/direct.aspx

Die folgende Tabelle beschreibt die verschlüsselten Übergabeparameter:

Key	REST	Format	CND	Beschreibung
TxType	"payment": {"card": { "transactionType": "..." }}	ans..20	M	Übergeben Sie „Order“, um eine Zahlung zu initialisieren und diese später über die Schnittstelle authorize.aspx zu autorisieren. Bitte beachten Sie, dass in Verbindung mit dem genutzten 3-D Secure-Verfahren eine separate Einstellung notwendig ist. Bitte wenden Sie sich hierzu direkt an Computop Helpdesk.

Zusatzparameter für Kreditkartenzahlung mit separater Autorisierung

Um eine zuvor mit TxType=Order initialisierte SSL-Kreditkartenzahlung zu autorisieren, rufen Sie folgende URL auf:

https://www.computop-paygate.com/authorize.aspx

Hinweis: Bitte beachten Sie, dass bei einer initialen Order keine KPN/CVC/CVV-Prüfung erfolgen kann. Für die folgende Reservierungsanfrage kann diese ID auch nicht weitergegeben werden.

Hinweis: Aus Sicherheitsgründen lehnt das Paygate alle Zahlungsanfragen mit Formatfehlern ab. Bitte übergeben Sie deshalb bei jedem Parameter den korrekten Datentyp.

Die folgende Tabelle beschreibt die verschlüsselten Übergabeparameter:

Key	REST	Format	CND	Beschreibung
MerchantID	BasicAuth.Username	ans..30	M	HändlerID, die von Computop vergeben wird. Dieser Parameter ist zusätzlich auch unverschlüsselt zu übergeben.

Key	REST	Format	CND	Beschreibung
PayID	"paymentId": "..."	an32	M	Vom Paygate vergebene ID für die Zahlung; z.B. zur Referenzierung in Batch-Dateien sowie im Capture- oder Credit-Request.

Key	REST	Format	CND	Beschreibung
TransID	"transactionId": "..."	ans..64	M	Ihre eigene TransaktionsID, die für jede Zahlung eindeutig sein muss

Key	REST	Format	CND	Beschreibung
Amount	"amount": { "value": ...}	n..10	M	Betrag in der kleinsten Währungseinheit (z.B. EUR Cent). Bitte wenden Sie sich an den Computop Helpdesk, wenn Sie Beträge < 100 (kleinste Währungseinheit) buchen möchten.

Key	REST	Format	CND	Beschreibung
Currency	"amount": { "currency": "..."}	a3	M	Währung, drei Zeichen DIN / ISO 4217, z.B. EUR, USD, GBP. Hier eine Übersicht: A1 Währungstabelle

Key	REST	Format	CND	Beschreibung
OrderDesc	"order": {"description": "..."}	ans..768	O	Beschreibung der gekauften Waren, Einzelpreise etc.

Key	REST	Format	CND	Beschreibung
MAC	---	an64	M	Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier: • HMAC-Authentisierung (Anfrage) • HMAC-Authentisierung (Notify)

Key	REST	Format	CND	Beschreibung
Capture	"capture": {"auto": "Yes"} "capture": {"manual": "Yes"} "capture": ...	an..6	OM	Bestimmt Art und Zeitpunkt der Buchung (engl. Capture). **Buchungsart** – **Beschreibung** **AUTO** – Buchung sofort nach Autorisierung (Standardwert). **MANUAL** – Buchung erfolgt durch den Händler - in der Regel die Buchung zum Zeitpunkt der Warenauslieferung bzw. Leistungserbringung. **<Zahl>** – Verzögerung in Stunden bis zur Buchung (ganze Zahl; 1 bis 696).

Parameter für Kreditkartenzahlungen über authorize.aspx

Die folgende Tabelle beschreibt die Parameter, die das Paygate als Antwort zurückgibt:

ℹ es können jederzeit neue Parameter hinzugefügt bzw. die Reihenfolge geändert werden

ℹ die Parameter (z.B. MerchantId, RefNr) sollten nicht auf Groß-/Kleinschreibung geprüft werden

Key	REST	Format	CND	Beschreibung
mid	"merchantId": "..."	ans..30	M	HändlerID, die von Computop vergeben wird

Key	REST	Format	CND	Beschreibung
PayID	"paymentId": "..."	an32	M	Vom Paygate vergebene ID für die Zahlung; z.B. zur Referenzierung in Batch-Dateien sowie im Capture- oder Credit-Request.

Key	REST	Format	CND	Beschreibung
XID	"xId": "..."	an32	M	Vom Paygate vergebene ID für alle einzelnen Transaktionen (Autorisierung, Buchung, Gutschrift), die für eine Zahlung durchgeführt werden

Key	REST	Format	CND	Beschreibung
TransID	"transactionId": "..."	ans..64	M	Ihre eigene TransaktionsID, die für jede Zahlung eindeutig sein muss

Key	REST	Format	CND	Beschreibung

Status	"status": "OK" "status": "FAILED"	a..50	M	OK (URLSuccess) oder FAILED (URLFailure)

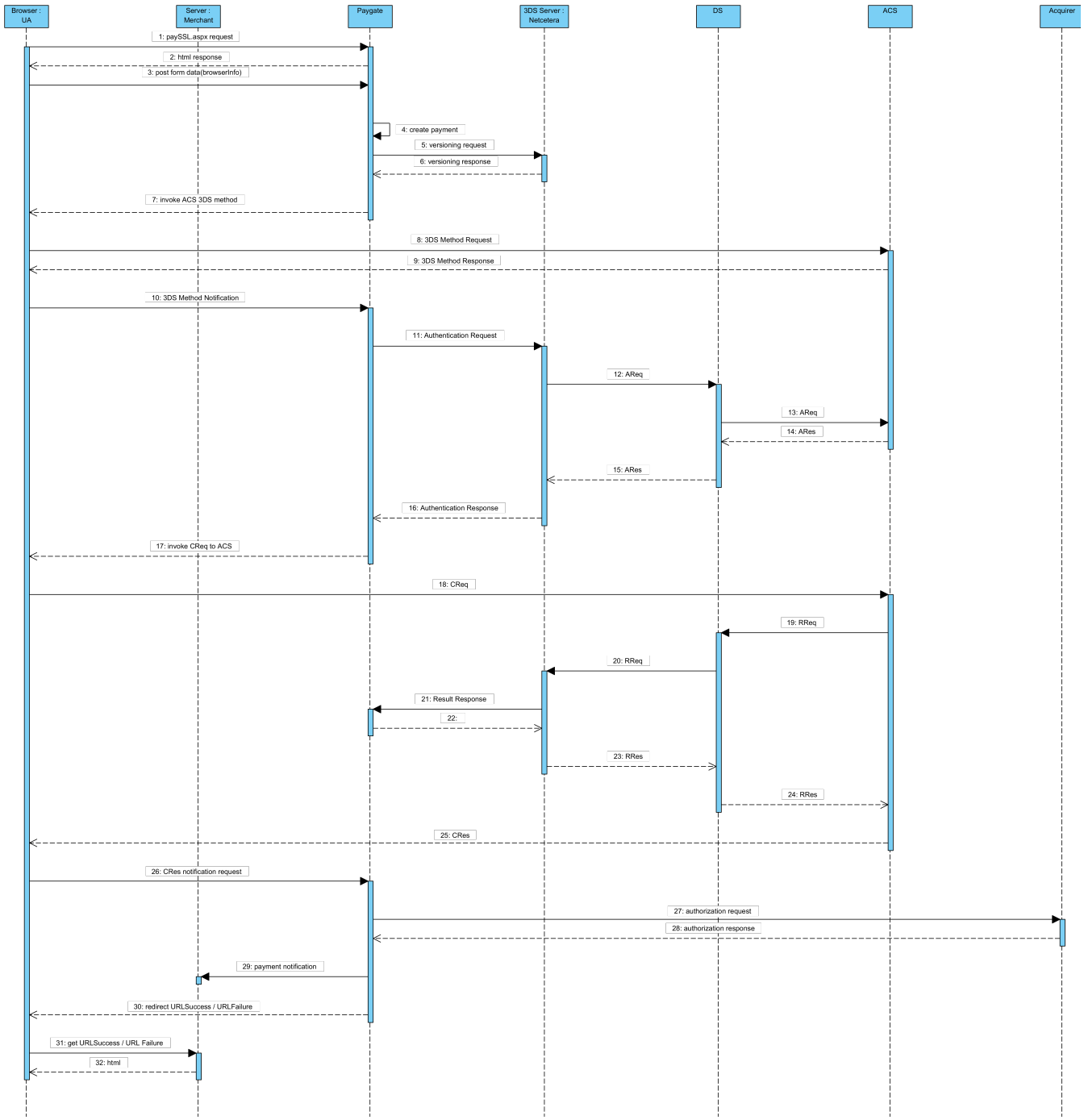
Key	REST	Format	CND	Beschreibung
Description	"description": "..."	ans..1024	M	Nähere Beschreibung bei Ablehnung der Zahlung. Bitte nutzen Sie **nicht** den Parameter **Description, sondern** Code für die Auswertung des Transaktionsstatus!

Key	REST	Format	CND	Beschreibung
Code	"code": ...	n8	M	Fehlercode gemäß Paygate Antwort-Codes (A4 Fehlercodes)

Key	Format	CND	Beschreibung
RefNr	"referenceNumber": "..."	O	Eindeutige Referenznummer des Händlers, welche als Auszahlungsreferenz in der entsprechenden Acquirer EPA-Datei angegeben wird. Bitte beachten Sie, ohne die Übergabe einer eigenen Auszahlungsreferenz können Sie die EPA-Transaktionen nicht zuordnen, zusätzlich kann das Computop Settlement File (CTSF) auch nicht zusätzlich angereichert werden. Informationen zum unterstützten Format finden Sie weiter unten in der zahlartspezifischen Beschreibung. Es sind ausschließlich ASCII-Zeichen erlaubt. Sonderzeichen wie ("Umlaute", ...) sind nicht erlaubt und müssen ggf. durch ASCII-Zeichen ersetzt werden (z.B. ü ue, é e, ...).

Ergebnis-Parameter für Kreditkartenzahlungen über authorize.aspx

Erweitertes Sequenz-Diagramm



Kreditkarten - Server-2-Server Integration

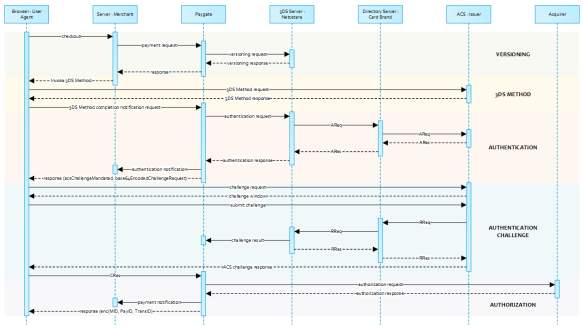
Eine 3DS 2.0 Zahlungssequenz kann aus den folgenden verschiedenen Aktivitäten bestehen:

- Versionierung
  - Anfrage von ACS- und DS-Protokol-Version(en), die mit dem Kartenkontenbereich korrespondieren sowie einer optionalen 3DS Method URL
- 3DS Methode
  - Verbindet den Browser des Karteninhabers mit dem ACS des Issuers, um zusätzliche Browserdaten zu erhalten
- Authentisierung

- Kreditkarten - Server-2-Server Integration
  - Server-2-Server Sequenzdiagramm
  - Initiierung der Zahlung
    - Aufruf-Elemente
    - Antwort-Elemente
    - versioningData
  - 3DS Methode

    - Übermittlung der Authentisierungs-Anfrage an den ACS des Issuers
- Challenge
    - Challenge des Karteninhabers, falls angeordnet
- Autorisierung
    - Autorisierung der authentisierten Transaktion beim Acquirer

Server-2-Server Sequenzdiagramm





Beachten Sie bitte, dass die Kommunikation zwischen Client und Access Control Server (ACS) über iFrames implementiert ist. Daher kommen die Antworten in einem HTML-Subdokument an und Sie können entsprechende Event-Listener in Ihrem Root-Dokument einrichten.

Alternativ könnten Sie alleinig auf die asynchronen Benachrichtigungen an ihr Backend vertrauen. In jenen Fällen müssen Sie eventuell Methoden wie Long Polling, SSE oder Websockets zum Update des Clients in Betracht ziehen.

- 3DS Methode: threeDSMethodURL
- 3DS Method: Keine Issuer threeDSMethodURL
- 3-D Secure Method Form Post
- ACS Response Document
- 3-D Secure Method Notification Form

- Authentisierung
    - Karteninhaber-Challenge: Browser-Antwort
    - Browser Challenge-Antwort
        - Datenelemente
        - Schema Browser Challenge-Antwort
        - Beispiel Browser Challenge-Antwort
    - Authentisierungs-Benachrichtigung
    - Browser Challenge
        - Challenge-An

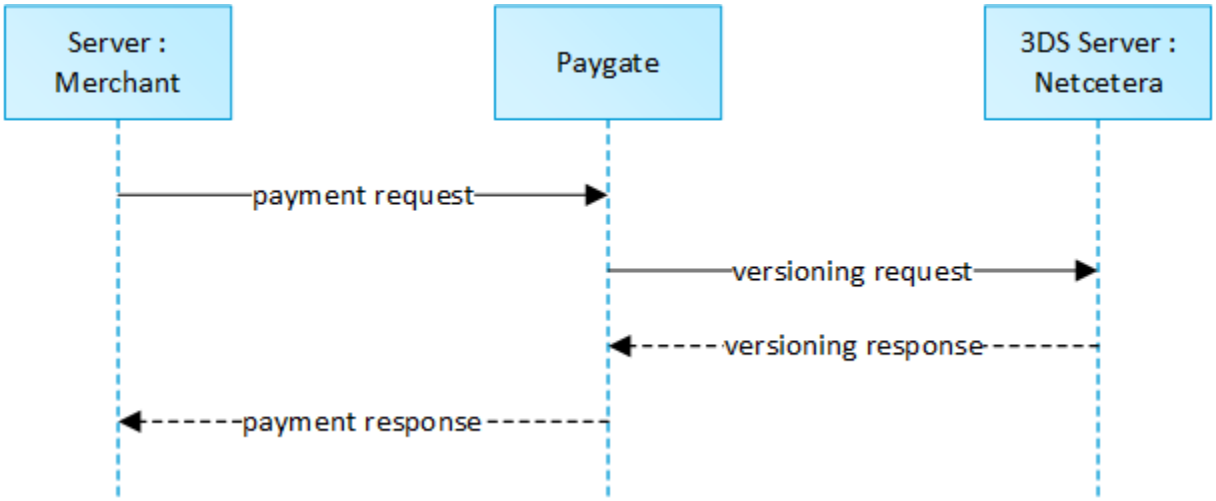
- frage
- 3DS Challenge-Anfrage initialisieren - Beispiel
  - Autorisierung
    - Zahlungs-Benachrichtigung
    - Browser Zahlungs-Antwort
      - Datenelemente
      - Schema
      - Entschlüsseltes Objekt Data
      - Beispiel für entschlüsseltes Objekt Data

EMV 3-D Secure

API Playground

Initiierung der Zahlung

Die anfängliche Anfrage an das Computop Paygate ist unabhängig vom zugrundeliegenden 3DS-Protokoll gleich.



Um eine Server-zu-Server 3-D Secure Kartenzahlungssequenz zu starten, senden Sie bitte folgende Schlüssel-Wert-Paare an https://www.computop-paygate.com/direct.aspx.

Aufruf-Elemente

Hinweis: Bei einer vom Händler initiierten, wiederkehrenden Zahlung sind die JSON-Objekte (außer credentialOnFile und card), die URLNotify und die TermURL keine Pflichtparameter, da kein 3D Secure und auch keine Risikobewertung durch die kartenausgebende Bank stattfindet und das Ergebnis der Zahlungsanfrage direkt in der Response mitgeteilt wird.

Key	REST	Format	CND	Beschreibung
MerchantID	BasicAuth. Username	ans..30	M	HändlerID, die von Computop vergeben wird. Dieser Parameter ist zusätzlich auch unverschlüsselt zu übergeben.
msgver	---	ans..5	M	Computop Paygate Message-Version. Zulässige Werte: **Wert** / **Beschreibung** 2.0 – Mit 3-D Secure 2.x wurde eine Vielzahl zusätzlicher Daten (Browser-Information, Rechnungs-/Versand-Adresse, ...) erforderlich, um den Authentifizierungs-Prozess zu optimieren. Um diese Informationen zu handhaben, wurden die JSON-Objekte eingeführt. Der Parameter MsgVer zeigt an, dass diese Daten verwendet werden.
TransID	"transactionId": "..."	ans..64	M	Ihre eigene TransaktionsID, die für jede Zahlung eindeutig sein muss
ReqId	"requestId": "..."	ans..32	O	Um Doppelzahlungen (z.B. durch ETM) zu vermeiden, übergeben Sie einen alphanumerischen Wert, der Ihre Transaktion oder Aktion identifiziert und nur einmal vergeben werden darf. Falls die Transaktion oder Aktion mit derselben ReqID erneut eingereicht wird, führt das Computop Paygate keine Zahlung oder weitere Aktion aus, sondern gibt nur den Status der ursprünglichen Transaktion oder Aktion zurück. Bitte beachten Sie, dass das Computop Paygate für die erste initiale Aktion (Authentifizierung/Autorisierung) einen abgeschlossenen Transaktionsstatus haben muss. Dies gilt nicht für 3-D Secure Authentifizierungen, die durch einem Timeout beendet werden. Der Status 3-D Secure Timeout gilt nicht als abgeschlossener Status, bei dem ReqID-Funktionalität am Paygate nicht greift. Einreichungen mit identischer ReqID auf einen offenen Status werden regulär verarbeitet. **Hinweis:** Bitte beachten Sie, dass eine ReqID nur 12 Monate gültig ist, danach wird sie vom Paygate gelöscht.
RefNr	"referenceNumber": "..."		O	Eindeutige Referenznummer des Händlers, welche als Auszahlungsreferenz in der entsprechenden Acquirer EPA-Datei angegeben wird. Bitte beachten Sie, ohne die Übergabe einer eigenen Auszahlungsreferenz können Sie die EPA-Transaktionen nicht zuordnen, zusätzlich kann das Computop Settlement File (CTSF) auch nicht zusätzlich angereichert werden. Informationen zum unterstützten Format finden Sie weiter unten in der zahlartspezifischen Beschreibung. Es sind ausschließlich ASCII-Zeichen erlaubt. Sonderzeichen wie ("Umlaute", ...) sind nicht erlaubt und müssen ggf. durch ASCII-Zeichen ersetzt werden (z.B. ü ue, é e, ...).
schemeReferenceID	"payment": {"card": { "schemeReferenceId": "..." }}	ans..64	C	Spezifische Transaktions-ID des Kartenschemas, die für nachfolgende Zahlungen mit gespeicherten Zugangsdaten, verzögerte Autorisierungen und Wiedereinreichungen erforderlich ist. Pflicht: CredentialOnFile – initial false – unschedule MIT / recurring schemeReferenceID wird bei 3DS2-Zahlungsvorgängen zurückgegeben. Bei einem Fallback auf 3DS1 prüfen Sie bitte zusätzlich auf TransactionId. Die SchemeReferenceID ist eine eindeutige Kennung, die von den Kartenmarken generiert wird. In der Regel können Computop-Händler die SchemeReferenceIDs für Abonnements übergreifend verwenden, welche unter Verwendung eines anderen PSP / separater Paygate-MerchantID / separater Acquirer ContractID / Acquirer erstellt wurden.
industrySpecificTxType	"payment": {"card": { "industrySpecificTransactionType": "..." }}	ans..20	C	Dieser Parameter ist erforderlich, wenn eine branchenspezifische Transaktion entsprechend dem Kartenmarken MIT-Framework (**M**erchant **I**nitiated **T**ransactions) verarbeitet wird. Der Parameter wird nur für bestimmte Use Cases verwendet, die unten beschrieben sind. Wird nur von Omnipay und GICC unterstützt. CB2A unterstützt nur den Wert Reauthorization

<table>
<tr><td></td><td></td><td></td><td></td><td>Zulässige Werte:
<table><tr><th>Wert</th><th>Beschreibung</th></tr><tr><td>Resubmission</td><td>Ein Händler führt eine erneute Einreichung durch, wenn er eine Autorisierung angefordert hat, diese aber aufgrund unzureichender Mittel abgelehnt wurde; die Waren oder Dienstleistungen wurden jedoch bereits an den Karteninhaber geliefert.

In solchen Szenarien können Händler den Antrag auf Beitreibung ausstehender Forderungen von Karteninhabern erneut einreichen.</td></tr><tr><td>Reauthorization</td><td>Ein Händler leitet eine erneute Autorisierung ein, wenn Abschluss oder Erfüllung der ursprünglichen Bestellung oder Dienstleistung die von Visa festgelegte Gültigkeitsdauer der Autorisierung überschreitet.

Es gibt zwei gängige Szenarien für die erneute Autorisierung:

• Geteilte oder verzögerte Lieferung be E-Commerce-Händlern. Eine Teillieferung liegt vor, wenn zum Zeitpunkt des Kaufs nicht alle bestellten Waren versandbereit sind. Erfolgt die Lieferung der Ware nach der von Visa festgelegten Gültigkeitsdauer der Autorisierung, führen E-Commerce-Händler eine separate Autorisierung durch, um sicherzustellen, dass Kundengelder verfügbar sind.

• Verlängerte Hotelaufenthaltens, Autovermietungen und Keuzfahrten. Eine erneute Autorisierung wird für Aufenthalte, Reisen und /oder Anmietungen verwendet, die über die von Visa festgelegte Gültigkeitsdauer der Autorisierung hinausgehen.</td></tr><tr><td>Delayed Charges</td><td>Verzögerte Gebühren dienen dazu, um eine zusätzliche Kontogebühr zu verarbeiten, nachdem die ursprünglichen Dienstleistungen erbracht und die entsprechende Zahlung verarbeitet wurde.</td></tr><tr><td>NoShow</td><td>Karteninhaber können mit ihren Visa-Karten eine garantierte Reservierung bei bestimmten Händlersegmenten vornehmen. Eine garantierte Reservierung stellt sicher, dass die Reservierung berücksichtigt wird und ermöglicht es einem Händler, eine No-Show-Transaktion durchzuführen, um dem Karteninhaber eine Strafe gemäß den Stornierungsbedingungen des Händlers zu berechnen. Hinweis: Für Händler, die tokenbasierte Zahlungsinformationen akzeptieren, um eine Reservierung zu garantieren, ist es zum Zeitpunkt der Reservierung erforderlich, einen CIT (Kontoverifizierungsservice) durchzuführen, um später eine No-Show-Transaktion durchführen zu können.</td></tr></table>
Hinweis: Das wird immer zusammen mit dem Parameter "schemeReferenceID" übermittelt. Bezüglich unterstützer Acquirer und Kartenmarken wenden Sie sich bitte an den Computop Helpdesk.</td></tr>
<tr><td>Amount</td><td>"amount": { "value": ...}</td><td>n..10</td><td>M</td><td>Betrag in der kleinsten Währungseinheit (z.B. EUR Cent). Bitte wenden Sie sich an den Computop Helpdesk, wenn Sie Beträge < 100 (kleinste Währungseinheit) buchen möchten.</td></tr>
<tr><td>Currency</td><td>"amount": { "currency": "..."}</td><td>a3</td><td>M</td><td>Währung, drei Zeichen DIN / ISO 4217, z.B. EUR, USD, GBP. Hier eine Übersicht: A1 Währungstabelle</td></tr>
<tr><td>card</td><td>"payment": {"card": JSON}</td><td>JSON</td><td>M</td><td>Kartendaten</td></tr>
<tr><td>Capture</td><td>"capture": {"auto": "Yes"}

"capture": {"manual": "Yes"}

"capture": ...</td><td>an..6</td><td>OM</td><td>Bestimmt Art und Zeitpunkt der Buchung (engl. Capture).
<table><tr><th>Buchungsart</th><th>Beschreibung</th></tr><tr><td>AUTO</td><td>Buchung sofort nach Autorisierung (Standardwert).</td></tr><tr><td>MANUAL</td><td>Buchung erfolgt durch den Händler - in der Regel die Buchung zum Zeitpunkt der Warenauslieferung bzw. Leistungserbringung.</td></tr><tr><td><Zahl></td><td>Verzögerung in Stunden bis zur Buchung (ganze Zahl; 1 bis 696).</td></tr></table></td></tr>
<tr><td>billingDescriptor</td><td>"billing": {"addressInfo": { "descriptor": "..." }}</td><td>ans..22</td><td>O</td><td>Ein auf dem Kontoauszug des Karteninhabers zu druckender Beschreiber. Beachten Sie bitte auch die andernorts gemachten zusätzlichen Hinweise für weitere Informationen über Regeln und Vorschriften.</td></tr>
<tr><td>OrderDesc</td><td>"order": {"description": "..."}</td><td>ans..768</td><td>O</td><td>Beschreibung der Bestellung</td></tr>
<tr><td>AccVerify</td><td>"payment": {"card": { "accountVerification": "..." }}</td><td>a3</td><td>O</td><td>Indikator zur Anforderung einer Konto-Verifizierung (alias Nullwert-Autorisierung). Wenn eine Konto-Verifizierung angefordert wird, ist der übermittelte Betrag optional und wird für die tatsächliche Zahlungstransaktion (d.h. Autorisierung) ignoriert.

Zulässige Werte:

• Yes</td></tr>
<tr><td>threeDSPolicy</td><td>"payment": {"card": { "threeDsPolicy": JSON }}</td><td>JSON</td><td>O</td><td>Objekt, dass die Authentisierungs-Richtlinien und Strategien zur Behandlung von Ausnahmen angibt</td></tr>
<tr><td>threeDSData</td><td>"payment": {"card": { "threeDSData": JSON }}</td><td>JSON</td><td>C</td><td>Objekt mit Details der Authentisierungsdaten, falls die Authentisierung durch Dritte oder durch den Händler durchgeführt wurde</td></tr>
<tr><td>priorAuthenticationInfo</td><td>"payment": {"card": { "priorAuthenticationInfo": JSON }}</td><td>JSON</td><td>O</td><td>Das Objekt Prior Transaction Authentication Information enthält optionale Informationen über eine 3-D Secure-Authentisierung eines Karteninhabers, die vor der aktuellen Transaktion erfolgt ist</td></tr>
<tr><td>browserInfo</td><td>"browserInfo": JSON</td><td>JSON</td><td>C</td><td>Exakte Browserinformationen sind nötig, um eine optimierte Nutzererfahrung zu liefern. Erforderlich für 3-D Secure 2.0 Transaktionen.</td></tr>
<tr><td>accountInfo</td><td>"accountInfo": JSON</td><td>JSON</td><td>O</td><td>Die Kontoinformationen enthalten optionale Informationen über das Kundenkonto beim Händler</td></tr>
<tr><td>billToCustomer</td><td>"billing": JSON</td><td>JSON</td><td>C</td><td>Der Kunde, dem die Waren und / oder Dienstleistungen in Rechnung gestellt werden. Erforderlich, sofern nicht Markt- oder regionale Mandate das Senden dieser Informationen beschränken.</td></tr>
<tr><td>shipToCustomer</td><td>"shipping": JSON</td><td>JSON</td><td>C</td><td>Der Kunde, an den die Waren und / oder Dienstleistungen gesendet werden. Erforderlich (falls verfügbar und von billToCustomer abweichend), sofern nicht Markt- oder regionale Mandate das Senden dieser Informationen beschränken.</td></tr>
<tr><td>billingAddress</td><td>"billing": {"addressInfo": JSON}</td><td>JSON</td><td>C</td><td>Rechnungsadresse. Erforderlich für 3-D Secure 2.0 (falls verfügbar), sofern nicht Markt- oder regionale Mandate das Senden dieser Informationen beschränken.</td></tr>
<tr><td>shippingAddress</td><td>"shipping": {"addressInfo": JSON}</td><td>JSON</td><td>C</td><td>Lieferadresse. Falls abweichend von billingAddress, erforderlich für 3-D Secure 2.0 (falls verfügbar), sofern nicht Markt- oder regionale Mandate das Senden dieser Informationen beschränken.</td></tr>
<tr><td>credentialOnFile</td><td>"credentialOnFile": JSON</td><td>JSON</td><td>C</td><td>Objekt, dass Art und Reihe der Transaktionen angibt, die unter Verwendung von beim Händler hinterlegten Zahlungsdaten (z.B. Kontonummer oder Zahlungs-Token) zur Verarbeitung künftiger Käufe eines Kunden erfolgen. Erforderlich, falls zutreffend.</td></tr>
<tr><td>merchantRiskIndicator</td><td>"riskIndicator": JSON</td><td>JSON</td><td>O</td><td>Der Händler-Risikoindikator enthält optionale Informationen über den bestimmten Einkauf des Kunden</td></tr>
<tr><td>subMerchantPF</td><td>"subMerchantPaymentFacilitator": JSON</td><td>JSON</td><td>O</td><td>Objekt, das die Details des SubMerchant (Payment Facilitator) angibt</td></tr>
</table>

				Wird ausschließlich von SafeCharge unterstützt.
TermURL	"payment": {"threeDSLegacy": { "termUrl": "..." }}	ans..256	C	Nur bei 3-D Secure: URL des Shops, die vom Access Control Server (ACS) der Bank aufgerufen wird, um das Ergebnis der Authentisierung zu übermitteln. Dabei übergibt die Bank per GET die Parameter **PayID**, **TransID**, **MerchantID** und per POST den Parameter **PAResponse** an die TermURL. Im Falle einer vom Händler initiierten wiederkehrenden Transaktion sind die JSON-Objekte (außer credentialOnFile und card), URLNotify und TermURL keine obligatorischen Parameter, da kein 3-D Secure und keine Risikobewertung durch die kartenausgebende Bank erfolgt und das Zahlungsergebnis direkt erfolgt innerhalb der Antwort zurückgegeben.
URLNotify	"urls": {"notify": "..."}	ans..256	C	Vollständige URL, die das Paygate aufruft, um den Shop zu benachrichtigen. Die URL darf nur über Port 443 aufgerufen werden. Sie darf keine Parameter enthalten: Nutzen Sie stattdessen den Parameter UserData. Im Falle einer vom Händler initiierten wiederkehrenden Transaktion sind die JSON-Objekte (außer credentialOnFile und card), URLNotify und TermURL keine obligatorischen Parameter, da kein 3-D Secure und keine Risikobewertung durch die kartenausgebende Bank erfolgt und das Zahlungsergebnis direkt erfolgt innerhalb der Antwort zurückgegeben. **Allgemeine Hinweise:** • Wir empfehlen, den Parameter "response=encrypt" zu verwenden, um eine verschlüsselte Antwort von Paygate zu erhalten • Betrüger könnten das verschlüsselte DATA-Element kopieren, welches an URLFailure gesendet wurde, und betrügerisch dasselbe DATA an URLSuccess/URLNotify senden. Überprüfen Sie daher unbedingt den "code"-Wert des DATA-Elements. Nur eine Antwort mit "code=00000000" sollte als erfolgreich angesehen werden.
UserData	"metadata [userData]": "..."	ans..1024	O	Wenn beim Aufruf angegeben, übergibt das Paygate die Parameter mit dem Zahlungsergebnis an den Shop.
MAC	---	an64	M	Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier: • HMAC-Authentisierung (Anfrage) • HMAC-Authentisierung (Notify)

Antwort-Elemente

Key	Format	CND	Beschreibung
mid	ans..30	M	HändlerID, die von Computop vergeben wird
PayID	an32	M	Vom Paygate vergebene ID für die Zahlung; z.B. zur Referenzierung in Batch-Dateien sowie im Capture- oder Credit-Request.
XID	an32	M	Vom Paygate vergebene ID für alle einzelnen Transaktionen (Autorisierung, Buchung, Gutschrift), die für eine Zahlung durchgeführt werden
TransID	ans..64	M	Ihre eigene TransaktionsID, die für jede Zahlung eindeutig sein muss
refnr		O	Referenznummer wie im Request angegeben
Status	a..20	M	Status der Transaktion. Zulässige Werte: • **`AUTHENTICATION_REQUEST`** • **`PENDING`** • **`FAILED`**
Description	ans..1024	M	Nähere Beschreibung bei Ablehnung der Zahlung. Bitte nutzen Sie **nicht** den Parameter **Description, sondern** Code für die Auswertung des Transaktionsstatus!
Code	n8	M	Fehlercode gemäß Paygate Antwort-Codes (A4 Fehlercodes)
UserData	ans..1024	O	Wenn beim Aufruf angegeben, übergibt das Paygate die Parameter mit dem Zahlungsergebnis an den Shop.
card	JSON	M	Kartendaten
versioningdata	JSON	M	Das Datenelement Card Range Data enthält Informationen, welche die jüngste vom ACS, der den Kartenbereich hostet, unterstützte EMV 3-D Secure-Version angeben. Es kann optional auch die ACS URL für die 3-D Secure Methode enthalten, falls vom ACS unterstützt, sowie die DS Start- und End-Protokoll-Versionen, die den Kartenbereich unterstützen.
threeDSLegacy	JSON	C	Objekt, dass die erforderlichen Datenelemente für die Konstruktion der Anfrage zur Zahler-Authentisierung im Falle eines **Fallbacks** auf 3-D Secure 1.0 enthält.

versioningData

Das Objekt **`versioningData`** gibt die EMV 3DS Protokoll-Versionen (d.h. 2.1.0 oder höher) an, die vom Access Control Server des Issuers unterstützt werden.

Wenn die entsprechenden Felder der Protokoll-Version NULL sind, bedeutet dies, dass der BIN-Bereich des Karten-Issuers nicht für 3DS 2.0 registriert ist und ein Fallback auf 3DS 1.0 für Transaktionen erforderlich ist, die unter den Geltungsbereich der PSD2 SCA fallen.

Achten Sie beim Zerlegen von **`versioningData`** bitte auch auf das Subelement **`errorDetails`**, das den Grund angibt, falls einige Felder nicht ausgefüllt sind (z.B. Ungültige Kontonumber des Karteninhabers übergeben, nicht verfügbare Kartenbereichsdaten, Fehler beo Codieren /Serialisieren der 3DS Methoden-Daten usw.)

BASEURL= https://www.computop-paygate.com/

```
{
        "threeDSServerTransID": "14dd844c-b0fc-4dfe-8635-366fbf43468c",
```

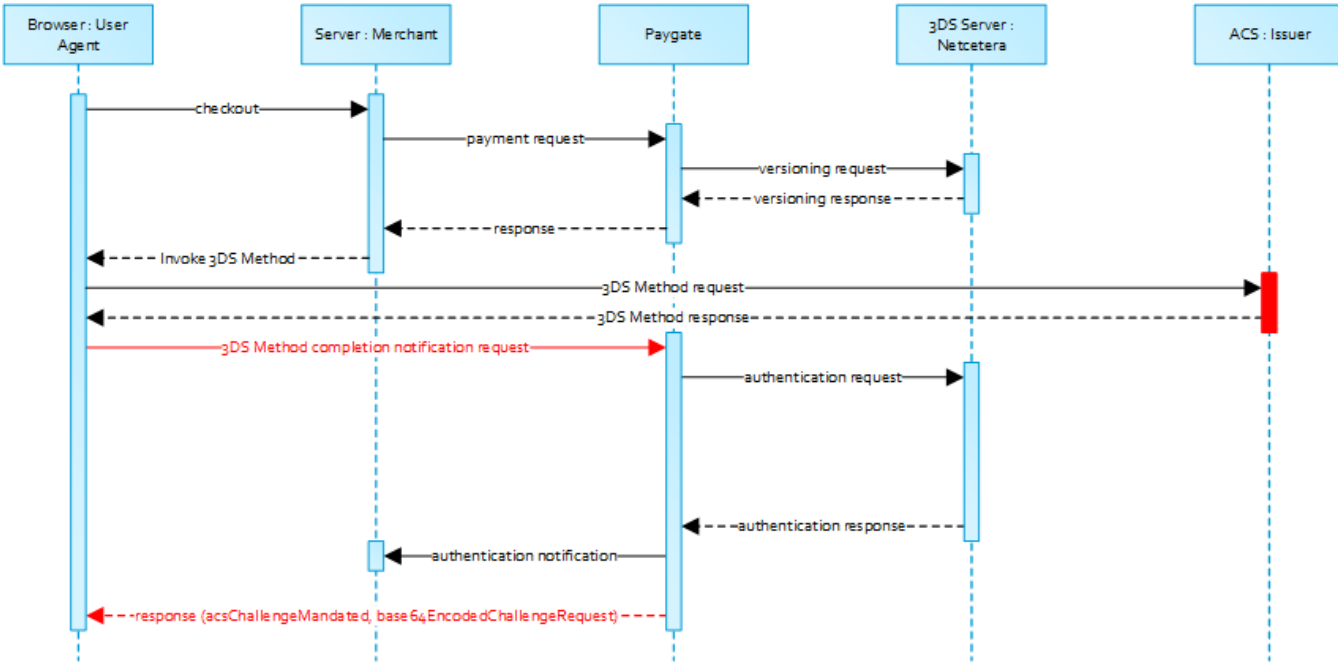
```
        "acsStartProtocolVersion": "2.1.0",
        "acsEndProtocolVersion": "2.1.0",
        "dsStartProtocolVersion": "2.1.0",
        "dsEndProtocolVersion": "2.1.0",
        "threeDSMethodURL": "http://www.acs.com/script",
        "threeDSMethodDataForm":
"eyJ0aHJlZURTTWV0aG9kTm90aWZpY2F0aW9uVVJMIjoiaHR0cHM6Ly93d3cuY29tcHV0b3AtcGF5Z2F0ZS5jb20vY2JUaHJlZURTLmFzcHg_YWN0aW9uPW10aGROdGZuIiwidGhyZWVEU1NlcnZlclRyYW5zSUQiOiIxNGRkODQ0Yy1iMGZjLTRkZmUtODYzNS0zNjZmYmY0MzQ2OGMifQ==",
        "threeDSMethodData": {
                "threeDSMethodNotificationURL": "BASEURL/cbThreeDS.aspx?action=mthdNtfn",
                "threeDSServerTransID": "14dd844c-b0fc-4dfe-8635-366fbf43468c"
        }
}
```


3DS Methode

Die 3DS Methode ermöglicht das Erfassen zusätzlicher Browserinformationen durch einen ACS vor Erhalt der Authensisierungsanfrage (AReq), um die Risikobeurteilung der Transaktion zu erleichtern. Die Unterstützung der 3DS Methode ist optional und liegt im Ermessen des Issuers.

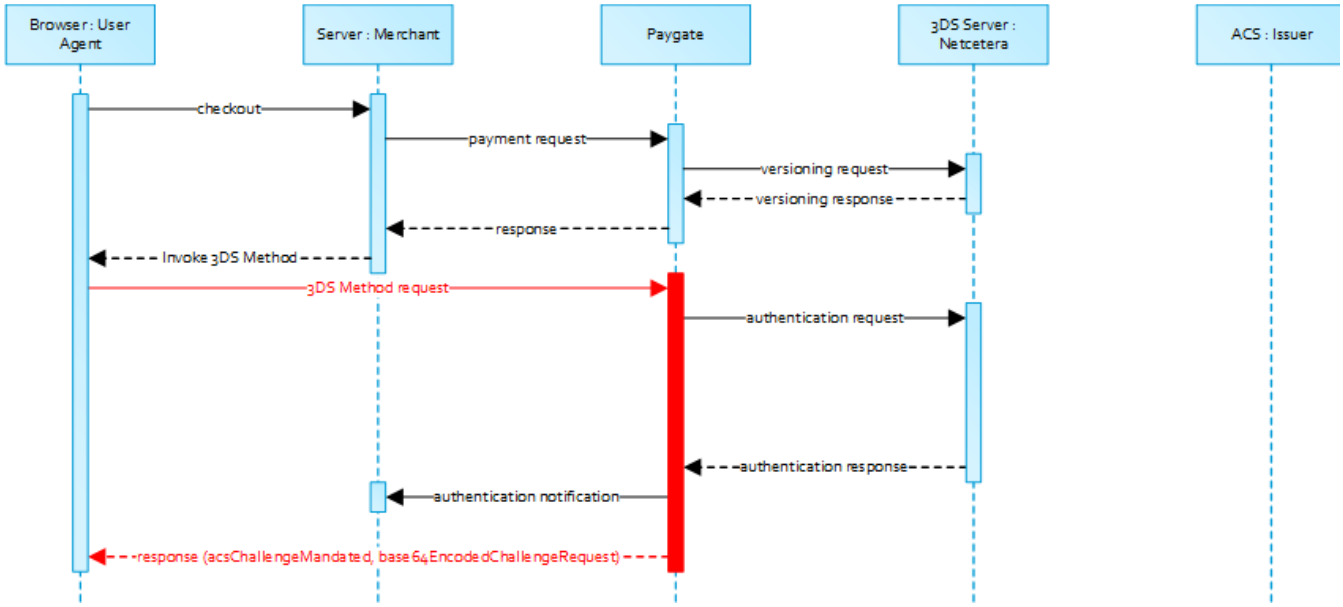
Das Objekt **`versioningData`** enthält einen Wert für **`threeDSMethodURL`**. Der Händler sollte die 3DS Methode über einen versteckten HTML-iFrame im Browser des Karteninhabers aufrufen und ein Formular mit einem Feld namens **`threeDSMethodData`** über HTTP POST an die ACS 3DS Methoden-URL senden.

3DS Methode: `threeDSMethodURL`



Beachten Sie bitte, dass die **`threeDSMethodURL`** vom Computop Paygate ausgefüllt wird, falls der Issuer die 3DS Methode nicht unterstützt. Der 3DS Methoden-Formular-Post wie unten dargestellt muss unabhängig davon ausgeführt werden, ob dies vom Issuer unterstützt wird. Das ist notwending, um die direkte Kommunikation zwischen dem Browser und dem Computop Paygate im Falle einer angeordneten Challenge oder eines reibungslosen Ablaufs zu erleichtern.

3DS Method: Keine Issuer `threeDSMethodURL`



3-D Secure Method Form Post

```
<form name="frm" method="POST" action="Rendering URL">
    <input type="hidden" name="threeDSMethodData" value="
eyJ0aHJlZURTU2VydmVyVHJhbnNJRCI6IjNhYzdjYWE3LWFhNDItMjY2My03OTFiLTJhYzA1YTU0MmM0YSIsInRocmVlRFNNZXRob2ROb
3RpZmljYXRpb25VUkwiOiJ0aHJlZURTTWV0aG9kTm90aWZpY2F0aW9uVVJMIn0">
</form>
```

Der ACS interagiert mit dem Browser des Karteninhabers über den HTML-iFrame und speichert dann die zutreffenden Werte mit der 3DS Server Transaction ID für die Verwendung, wenn eine nachfolgende Authentisierungs-Nachricht empfangen wird, welche die gleiche 3DS Server Transaction ID enthält.

> **Netcetera 3DS Web SDK**
>
> Sie können nach eigenem Ermessen die Operationen **`init3DSMethod`** oder **`createIframeAndInit3DSMethod`** vom nca3DSWebSDK verwenden, um die 3DS Methode zu initialisieren. Bitte beachten Sie dazu das Integrations-Handbuch unter https://mpi.netcetera.com/3dsserver/doc/current/integration.html#Web_Service_API.

Nachdem die 3DS Methode abgeschlossen ist, weist der ACS den Browser des Karteninhabers über das iFrame-Antwortdokument an, **`threeDSMethodData`** als ein verstecktes Formularfeld an die 3DS Method Notification URL zu übermitteln.

ACS Response Document

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8"/>
    <title>Identifying...</title>
</head>
<body>
<script>
    var tdsMethodNotificationValue =
'eyJ0aHJlZURTU2VydmVyVHJhbnNJRCI6ImUxYzFlYmViLTc0ZTgtNDNiMi1iMzg1LTJlNjdkMWFhY2ZhMiJ9';

    var form = document.createElement("form");
    form.setAttribute("method", "post");
    form.setAttribute("action", "notification URL");

    addParameter(form, "threeDSMethodData", tdsMethodNotificationValue);

    document.body.appendChild(form);
    form.submit();
```

```
    function addParameter(form, key, value) {
        var hiddenField = document.createElement("input");
        hiddenField.setAttribute("type", "hidden");
        hiddenField.setAttribute("name", key);
        hiddenField.setAttribute("value", value);
        form.appendChild(hiddenField);
    }
</script>
</body>
</html>
```

3-D Secure Method Notification Form

```
<form name="frm" method="POST" action="3DS Method Notification URL">
    <input type="hidden" name="threeDSMethodData" value="
eyJ0aHJlZURTU2VydmVyVHJhbnNJRCI6ImUxYzFlYmViLTc0ZTgtNDNiMi1iMzg1LTJlNjdkMWFhY2ZhMiJ9">
</form>
```

> Beachten SIe bitte, dass die **`threeDSMethodNotificationURL`** wie sie in den Base64-codierten **`threeDSMethodData`** eingebettet ist, auf das Computop Paygate weist und nicht verändert werden darf. Die Händler-Benachrichtigung wird an die URLNotify geliefert, wie sie in der Originalanfrage übermittelt oder für die MerchantID im Computop Paygate konfiguriert ist.

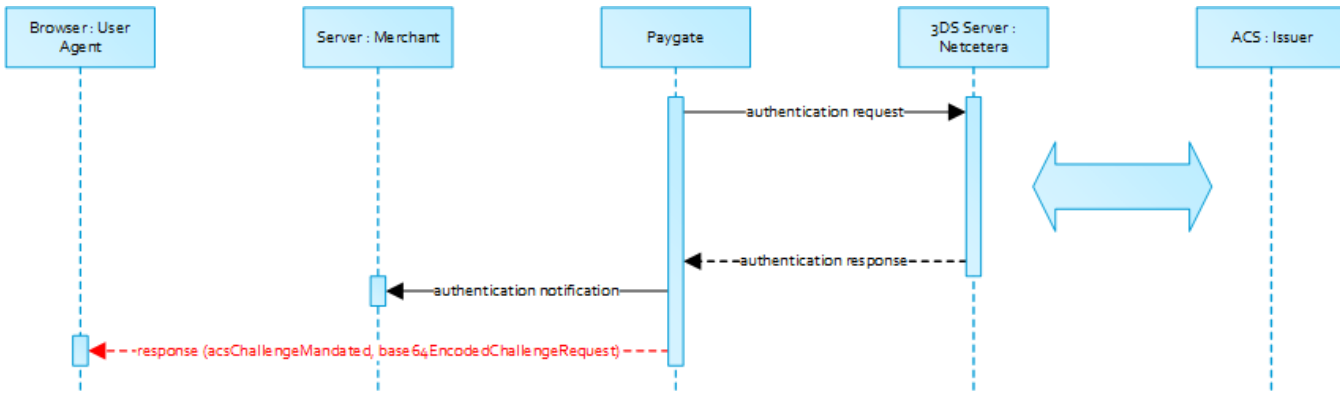
Authentisierung

Wenn die 3DS-Methode vom ACS des Issuers unterstützt wird und vom Händler aufgerufen wurde, setzt das Computop Paygate automatisch mit der Authentisierungsanfrage fort, nachdem die 3DS-Methode abgeschlossen ist (d.h. 3DS Methoden-Benachrichtigung).

Das Ergebnis der Authentisierung wird per HTTP POST an die **`URLNotify`** übertragen. Es kann anzeigen, dass der Karteninhaber authentisiert worden ist oder dass eine weitere Interaktion des Karteninhabers (d.h. Challenge) für den Abschluss der Authentisierung erforderlich ist.

Falls für den Karteninhaber eine Challenge für nötig angesehen ist, überträgt das Computop Paygate ein JSON-Objekt im Body der HTTP Browser-Antwort mit den Elementen **`acsChallengeMandated`**, **`challengeRequest`**, **`base64EncodedChallengeRequest`** und **`acsURL`**. Anderenfalls setzt das Computop Paygate in einem reibungslosen Ablauf automatisch fort und antwortet dem Browser des Karteninhabers, sobald die Autorisierung abgeschlossen ist.

Karteninhaber-Challenge: Browser-Antwort



Browser Challenge-Antwort

Datenelemente

Key	Format	CND	Beschreibung
acsChallengeMandated	boolean	M	Zeigt an, on eine Challenge für die Autorisierung einer Transaktion wegen lokaler/regionaler Vorschriften oder anderer Variablen nötig ist:

			• true Challenge ist obligatorisch wegen lokaler/regional Vorschriften • false Challenge ist nicht obligatorisch wegen lokaler/regional Vorschriften, wird aber von ACS als **nötig angesehen**
challengeRequest	object	M	Objekt Challenge-Anfrage
base64EncodedChallengeRequest	string	M	Base64-codiertes Objekt Challenge-Anfrage
acsURL	string	M	Vollständige URL des ACS, die für das Posten der Challenge-Anfrage verwendet werden soll

Schema Browser Challenge-Antwort

```
{
        "$schema": "http://json-schema.org/draft-07/schema#",
        "type": "object",
        "properties": {
                "acsChallengeMandated": {"type": "boolean"},
                "challengeRequest": {"type": "object"},
                "base64EncodedChallengeRequest": {"type": "string"},
                "acsURL": {"type": "string"}
        },
        "required": ["acsChallengeMandated", "challengeRequest", "base64EncodedChallengeRequest",
"acsURL"],
        "additionalProperties": false
}
```

Beispiel Browser Challenge-Antwort

```
{
        "acsChallengeMandated": false,
        "challengeRequest": {
                "threeDSServerTransID": "8a880dc0-d2d2-4067-bcb1-b08d1690b26e",
                "acsTransID": "d7c1ee99-9478-44a6-b1f2-391e29c6b340",
                "messageType": "CReq",
                "messageVersion": "2.1.0",
                "challengeWindowSize": "01",
                "messageExtension": [
                        {
                                "name": "emvcomsgextInChallenge",
                                "id": "tc8Qtm465Ln1FX0nZprA",
                                "criticalityIndicator": false,
                                "data": "messageExtensionDataInChallenge"
                        }
                ]
        },
        "base64EncodedChallengeRequest": "base64-encoded-challenge-request",
        "acsURL": "acsURL-to-post-challenge-request"
}
```

Authentisierungs-Benachrichtigung

Die Datenelemente der Authentisierungs-Benachrichtigung stehen in folgender Tabelle.

Key	Format	CND	Beschreibung
mid	ans..30	M	HändlerID, die von Computop vergeben wird
PayID	an32	M	Vom Paygate vergebene ID für die Zahlung; z.B. zur Referenzierung in Batch-Dateien sowie im Capture- oder Credit-Request.
TransID	ans..64	M	Ihre eigene TransaktionsID, die für jede Zahlung eindeutig sein muss
Code	n8	M	Fehlercode gemäß Paygate Antwort-Codes (A4 Fehlercodes)
MAC	an64	M	Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier: • HMAC-Authentisierung (Anfrage) • HMAC-Authentisierung (Notify)

authenticationResponse	JSON	M	Antwort-Objekt als Rückgabe zur Authentisierungs-Anfrage beim ACS

Browser Challenge

Wenn eine Challenge für nötig angesehen wird (siehe challengeRequest), erfolgt die Browser Challenge im Browser des Karteninhabers. Zum Erzeugen einer Challenge ist es erforderlich, den Wert **`base64EncodedChallengeRequest`** über ein HTML-iFrame an die ACS URL zu posten.

Challenge-Anfrage

```
<form name="challengeRequestForm" method="post" action="acsChallengeURL">
        <input type="hidden" name="creq" value="
ewogICAgInRocmVlRFNTZXJ2ZXJUcmFuc0lEIjogIjhhODgwZGMwLWQyZDItNDA2Ny1iY2IxLWIwOGQxNjkwYjI2ZSIsCiAgICAiYWNzV
HJhbnNJRCI6ICJkN2MxZWU5OS05NDc4LTQ0YTYtYjFmMi0zOTFlMjljNmIzNDAiLAogICAgIm1lc3NhZ2VUeXBlIjogIkNSZXEiLAogIC
AgIm1lc3NhZ2VWZXJzaW9uIjogIjIuMS4wIiwKICAgICJjaGFsbGVuZ2VXaW5kb3dTaXplIjogIjAxIiwKICAgICJtZXNzYWdlRXh0ZW5
zaW9uIjogWwoJCXsKCQkJIm5hbWUiOiAiZW12Y29tc2dleHRJbkNoYWxsZW5nZSIsCgkJCSJpZCI6ICJ0YzhRdG00NjVMbjFGWDBuWnBy
QSIsCgkJCSJjcml0aWNhbGl0eUluZGljYXRvciI6IGZhbHNlLAoJCQkiZGF0YSI6ICJtZXNzYWdlRXh0ZW5zaW9uRGF0YUluQ2hhbGxl
mdlIgoJCX0KICAgIF0KfQ==">
</form>
```

Sie können die Operationen **`init3DSChallengeRequest`** oder **`createIFrameAndInit3DSChallengeRequest`** aus dem nca3DSWebSDK verwenden, um die Challenge-Nachricht an den Browser des Karteninhabers zu übermitteln.

3DS Challenge-Anfrage initialisieren - Beispiel

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <script src="nca-3ds-web-sdk.js" type="text/javascript"></script>
    <title>Init 3-D Secure Challenge Request - Example</title>
</head>
<body>
<!-- This example will show how to initiate Challenge Reqeuests for different window sizes. -->
<div id="frameContainer01"></div>
<div id="frameContainer02"></div>
<div id="frameContainer03"></div>
<div id="frameContainer04"></div>
<div id="frameContainer05"></div>
<iframe id="iframeContainerFull" name="iframeContainerFull" width="100%" height="100%"></iframe>

<script type="text/javascript">
    // Load all containers
    iFrameContainerFull = document.getElementById('iframeContainerFull');
    container01 = document.getElementById('frameContainer01');
    container02 = document.getElementById('frameContainer02');
    container03 = document.getElementById('frameContainer03');
    container04 = document.getElementById('frameContainer04');
    container05 = document.getElementById('frameContainer05');


    // nca3DSWebSDK.init3DSChallengeRequest(acsUrl, creqData, container);
    nca3DSWebSDK.init3DSChallengeRequest('http://example.com', 'base64-encoded-challenge-request',
iFrameContainerFull);

    // nca3DSWebSDK.createIFrameAndInit3DSChallengeRequest(acsUrl, creqData, challengeWindowSize,
frameName, rootContainer, callbackWhenLoaded);
    nca3DSWebSDK.createIFrameAndInit3DSChallengeRequest('http://example.com', 'base64-encoded-challenge-
request', '01', 'threeDSCReq01', container01);
    nca3DSWebSDK.createIFrameAndInit3DSChallengeRequest('http://example.com', 'base64-encoded-challenge-
request', '02', 'threeDSCReq02', container02);
    nca3DSWebSDK.createIFrameAndInit3DSChallengeRequest('http://example.com', 'base64-encoded-challenge-
request', '03', 'threeDSCReq03', container03);
    nca3DSWebSDK.createIFrameAndInit3DSChallengeRequest('http://example.com', 'base64-encoded-challenge-
request', '04', 'threeDSCReq04', container04);
    nca3DSWebSDK.createIFrameAndInit3DSChallengeRequest('http://example.com', 'base64-encoded-challenge-
request', '05', 'threeDSCReq05', container05, () => {
        console.log('Iframe loaded, form created and submitted');
    });
```

```
</script>

</body>
</html>
```

Sobald die Challenge des Karteninhabers abgeschlossen, abgebrochen oder per Zeitüberschreitung beendet ist, weist der ACS den Browser an, die Ergebnisse per Post an die in der Challenge-Anfrage angegebene Benachrichtigungs-URL zu senden und eine Ergebnis-Anfrage (RReq) über den Directory Server an den 3DS Server zu senden.

Beachten Sie bitte, dass die in der Challenge-Anfrage übergebene Benachrichtigungs-URL auf das Computop Paygate zeigt und nicht verändert werden darf.

Autorisierung

Nachdem die erfolgreiche Authentisierung des Karteninhabers oder der Nachweis der versuchten Authentisierung/Verifizierung bereitgestellt ist, setzt das Computop Paygate die Zahlungsautorisierung automatisch fort.

Falls die Authentisierung des Karteninhabers nicht erfolgreich war oder der Nachweise der versuchten Authentisierung/Verifizierung nicht bereitgestellt werden kann, setzt das Computop Paygate nicht mit einer Autorisierungsanfrage fort.

In beiden Fällen liefert das Paygate eine Benachrichtigung mit dem Ergebnis der Authentifizierung an die vom Händler angegebene **`URLNotify`** mit den Datenelementen gemäß nachstehender Tabelle.

Zahlungs-Benachrichtigung

Key	Format	CND	Beschreibung
mid	ans..30	M	HändlerID, die von Computop vergeben wird

Key	Format	CND	Beschreibung
msgver	ans..5	M	Computop Paygate Message-Version. Zulässige Werte: **Wert** / **Beschreibung** 2.0 – Mit 3-D Secure 2.x wurde eine Vielzahl zusätzlicher Daten (Browser-Information, Rechnungs-/Versand-Adresse, ...) erforderlich, um den Authentifizierungs-Prozess zu optimieren. Um diese Informationen zu handhaben, wurden die JSON-Objekte eingeführt. Der Parameter MsgVer zeigt an, dass diese Daten verwendet werden.

Key	Format	CND	Beschreibung
PayID	an32	M	Vom Paygate vergebene ID für die Zahlung; z.B. zur Referenzierung in Batch-Dateien sowie im Capture- oder Credit-Request.

Key	Format	CND	Beschreibung
XID	an32	M	Vom Paygate vergebene ID für alle einzelnen Transaktionen (Autorisierung, Buchung, Gutschrift), die für eine Zahlung durchgeführt werden

Key	Format	CND	Beschreibung
TransID	ans..64	M	Ihre eigene TransaktionsID, die für jede Zahlung eindeutig sein muss

Key	Format	CND	Beschreibung
schemeReferenceID	ans..64	C	Spezifische Transaktions-ID des Kartenschemas, die für nachfolgende Zahlungen mit gespeicherten Zugangsdaten, verzögerte Autorisierungen und Wiedereinreichungen erforderlich ist. Pflicht: CredentialOnFile – initial false – unschedule MIT / recurring schemeReferenceID wird bei 3DS2-Zahlungsvorgängen zurückgegeben. Bei einem Fallback auf 3DS1 prüfen Sie bitte zusätzlich auf TransactionId. Die SchemeReferenceID ist eine eindeutige Kennung, die von den Kartenmarken generiert wird. In der Regel können Computop -Händler die SchemeReferenceIDs für Abonnements übergreifend verwenden, welche unter Verwendung eines anderen PSP / separater Paygate-MerchantID / separater Acquirer ContractID / Acquirer erstellt wurden.

Key	Format	CND	Beschreibung
TrxTime	an21	M	Zeitstempel der Transaktion im Format DD.MM.YYYY HH:mm:ssff

Status	a..20	M	Status der Transaktion. Zulässige Werte: • **`Authorized`** • **`OK`** (Sale) • **`PENDING`** • **`FAILED`** Im Falle von **nur Authentisierung** ist der **Status** entweder **`OK`** oder **`FAILED`** .

Key	Format	CND	Beschreibung
Description	ans..1024	M	Nähere Beschreibung bei Ablehnung der Zahlung. Bitte nutzen Sie **nicht** den Parameter **Description, sondern** Code für die Auswertung des Transaktionsstatus!

Key	Format	CND	Beschreibung
Code	n8	M	Fehlercode gemäß Paygate Antwort-Codes (A4 Fehlercodes)

Key	Format	CND	Beschreibung
MAC	an64	M	Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier: • HMAC-Authentisierung (Anfrage) • HMAC-Authentisierung (Notify)

Key	Format	CND	Beschreibung
card	JSON	M	Kartendaten
ipinfo	JSON	O	Objekt mit IP-Informationen
threedsdata	JSON	M	Authentisierungsdaten
resultsresponse	JSON	C	Falls der Authentisierungsprozess eine Challenge des Karteninhabers enthalten hat, werden zusätzliche Informationen über das Ergebnis der Challenge bereitgestellt
externalPaymentData	JSON	O	Optionale Daten des Acquirers/Issuers/externen Dienstleisters für eine Autorisierung

Key	Format	CND	Beschreibung
PCNr	n16	O	Pseudo Card Number: Vom Computop Paygate generierte Zufallszahl, die eine reale Kreditkartennummer repräsentiert. Die Pseudokartennummer (PKN) beginnt mit 0, und die letzten 3 Stellen entsprechen denen der realen Kartennummer. Die PKN kann wie eine Kreditkartennummer für Autorisierung, Buchung und Gutschriften verwendet werden. PCNr ist ein **Antwortwert** von Computop Paygate und kann ebenfalls als CCNr im Request oder als Teil von card-JSON verwendet werden.

Browser Zahlungs-Antwort

Zusätzlich werden nachstehende Datenelemente im JSON-Format im Body der HTTP-Antwort zum Browser des Karteninhabers übertragen. Beachten Sie bitte, dass die Datenelemente (d.h. **`MID`**, **`Len`**, **`Data`**) base64-codiert sind.

Datenelemente

Key	Format	CND	Beschreibung
mid	ans..30	M	HändlerID, die von Computop vergeben wird
Len	integer	M	Länge des unverschlüsselten Strings **`Data`**
Data	string	M	Blowfish-verschlüsselter String, der ein JSON-Objekt mit **`MID`** , **`PayID`** und **`TransID`** enthält

Schema

```
{
        "$schema": "http://json-schema.org/draft-07/schema#",
        "type": "object",
        "properties": {
                "MID": {
                        "type": "string"
```

```
                },
                "Len": {
                        "type": "integer"
                },
                "Data": {
                        "type": "string"
                }
        },
        "required": ["MID", "Len", "Data"],
        "additionalProperties": false
}
```

Händler sollten diese Datenelemente zur Entschlüsselung und für den Abgleich mit der Zahlungs-Benachrichtigung am ihren Server weiterleiten. Basierend auf dem Zahlungsergebnis kann der Händler-Server eine entsprechende Antwort an den Browser des Karteninhabers senden (z.B. Erfolgsseite).

Entschlüsseltes Objekt Data

Key	Format	CND	Beschreibung
mid	ans..30	M	HändlerID, die von Computop vergeben wird
PayID	an32	M	Vom Paygate vergebene ID für die Zahlung; z.B. zur Referenzierung in Batch-Dateien sowie im Capture- oder Credit-Request.
TransID	ans..64	M	Ihre eigene TransaktionsID, die für jede Zahlung eindeutig sein muss

Beispiel für entschlüsseltes Objekt Data

```
MID=YourMID&PayID=PayIDassignedbyPlatform&TransID=YourTransID
```


- Buchung / Gutschrift / Storno
  - Buchung
  - Gutschrift mit Referenz
  - Gutschrift ohne Referenz
  - Storno
  - Storno einer Autorisierungsverlängerung
  - Kreditkartenzahlung über stationäre Terminals
  - Storno von stationären Kreditkartenzahlungen
- PayNow
  - Silent Mode für Kreditkarten mit SSL und 3-D Secure-Verfahren
- Batch-Nutzung der Schnittstelle
  - Batch-Aufrufe und Antworten
  - Stopp von Autorisierungsverlängerungen

Hinweise zum Cookie-/session-Handling

Buchung / Gutschrift / Storno

Buchung

Buchungen sind über eine Server-zu-Server-Kommunikation möglich. Um eine Buchung (Capture) über eine Server-zu-Server-Verbindung auszuführen, verwenden Sie bitte folgende URL:

https://www.computop-paygate.com/capture.aspx

Hinweis: Bitte beachten Sie die Reservierungs- / Autorisierungsfristen Ihres Acquirers (siehe AGBs), damit Sie als Händler sicherstellen, dass die Abbuchungen in der korrekten Frist an unserem Paygate eingereicht werden.

Hinweis: Aus Sicherheitsgründen lehnt das Paygate alle Zahlungsanfragen mit Formatfehlern ab. Bitte übergeben Sie deshalb bei jedem Parameter den korrekten Datentyp.

Die folgende Tabelle beschreibt die verschlüsselten Übergabeparameter:

Key	REST	Format	CND	Beschreibung
MerchantID	BasicAuth. Username	ans..30	M	HändlerID, die von Computop vergeben wird. Dieser Parameter ist zusätzlich auch unverschlüsselt zu übergeben.
PayID	"paymentId": "..."	an32	M	Vom Paygate vergebene ID für die Zahlung; z.B. zur Referenzierung in Batch-Dateien sowie im Capture- oder Credit-Request.
TransID	"transactionId": "..."	ans..64	M	TransaktionsID, die für jede Zahlung eindeutig sein muss Bitte beachten Sie bei einigen Anbindungen die abweichenden Formate, die bei den spezifischen Parametern angegeben sind.
RefNr	"referenceNumber": "..."	ns..30	C	Eindeutige Referenznummer des Händlers, welche als Auszahlungsreferenz in der entsprechenden Acquirer EPA-Datei angegeben wird. Bitte beachten Sie, ohne die Übergabe einer eigenen Auszahlungsreferenz können Sie die EPA-Transaktionen nicht zuordnen, zusätzlich kann das Computop Settlement File (CTSF) auch nicht zusätzlich angereichert werden. (nicht bei EVO Payments, bei CardComplete im Format an..25, bei Cofidis im Format n..15, bei Omnipay im Format ns..15, bei RBI im Format ns..20) Es sind ausschließlich ASCII-Zeichen erlaubt. Sonderzeichen wie ("Umlaute", ...) sind nicht erlaubt und müssen ggf. durch ASCII-Zeichen ersetzt werden (z.B. ü ue, é e, ...).
Amount	"amount": { "value": ...}	n..10	M	Betrag in der kleinsten Währungseinheit (z.B. EUR Cent). Bitte wenden Sie sich an den Computop Helpdesk, wenn Sie Beträge < 100 (kleinste Währungseinheit) buchen möchten.
Currency	"amount": { "currency": "..."}	a3	M	Währung, drei Zeichen DIN / ISO 4217, z.B. EUR, USD, GBP. Hier eine Übersicht: A1 Währungstabelle
MAC	---	an64	M	Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier: • HMAC-Authentisierung (Anfrage) • HMAC-Authentisierung (Notify)
ReqId	"requestId": "..."	ans..32	O	Um Doppelzahlungen (z.B. durch ETM) zu vermeiden, übergeben Sie einen alphanumerischen Wert, der Ihre Transaktion oder Aktion identifiziert und nur einmal vergeben werden darf. Falls die Transaktion oder Aktion mit derselben ReqID erneut eingereicht wird, führt das Computop Paygate keine Zahlung oder weitere Aktion aus, sondern gibt nur den Status der ursprünglichen Transaktion oder Aktion zurück. Bitte beachten Sie, dass das Computop Paygate für die erste initiale Aktion (Authentifizierung/Autorisierung) einen abgeschlossenen Transaktionsstatus haben muss. Dies gilt nicht für 3-D Secure Authentifizierungen, die durch einem Timeout beendet werden. Der Status 3-D Secure Timeout gilt nicht als abgeschlossener Status, bei dem ReqID-Funktionalität am Paygate nicht greift. Einreichungen mit identischer ReqID auf einen offenen Status werden regulär verarbeitet. **Hinweis:** Bitte beachten Sie, dass eine ReqID nur 12 Monate gültig ist, danach wird sie vom Paygate gelöscht.
FinishAuth	"finishAuth": "..."	a1	C	Nur bei ETM: Übergeben Sie den Wert <Y>, um bei Teilbuchungen die Autorisierungserneuerung oder die Reservierung des Restbetrages zu stoppen. Bitte nutzen Sie den Parameter nur, wenn Sie die Zusatzfunktion ETM (Erweitertes Transaktions-Managament) nutzen. (Nicht bei Clearhaus)
Textfeld1	"cardHolder": { "name": "..."}	ans..30	O	Karteninhaber-Information: Name (Nicht bei Clearhaus) Für Banksys: Name des Händlers. Bei VISA-Transaktionen sind bis zu 25 Zeichen erlaubt, bei MasterCard nur bis zu 22.
Textfeld2	"cardHolder": { "city": "..."}	ans..30	O	Karteninhaber-Information: Ort (Nicht bei Clearhaus) Für Banksys: Ort des Händlers. Der Wert wird nach 13 Zeichen abgeschnitten.
CHDesc	---	ans..22	OC	Nur bei Clearhaus: Text, der auf der Kreditkartenabrechnung angezeigt wird. Nur ASCII druckbare Zeichen von 0x20 bis 0x7E

Parameter für Buchungen von Kreditkartenzahlungen

Die folgende Tabelle beschreibt die Parameter, die das Paygate als Antwort zurückgibt:

ℹ es können jederzeit neue Parameter hinzugefügt bzw. die Reihenfolge geändert werden

ℹ die Parameter (z.B. MerchantId, RefNr) sollten nicht auf Groß-/Kleinschreibung geprüft werden

Key	REST	Format	CND	Beschreibung
mid	"merchantId": "..."	ans..30	M	HändlerID, die von Computop vergeben wird
PayID	"paymentId": "..."	an32	M	Vom Paygate vergebene ID für die Zahlung; z.B. zur Referenzierung in Batch-Dateien sowie im Capture- oder Credit-Request.
XID	"xId": "..."	an32	M	Vom Paygate vergebene ID für alle einzelnen Transaktionen (Autorisierung, Buchung, Gutschrift), die für eine Zahlung durchgeführt werden
TransID	"transactionId": "..."	ans..64	M	Transaktionsnummer des Händlers. Bitte beachten Sie bei einigen Anbindungen die abweichenden Formate, die bei den spezifischen Parametern angegeben sind.

Status	"status": "OK" "status": "FAILED"	a..50	M	OK (URLSuccess) oder FAILED (URLFailure)
Description	"description": "..."	ans..1024	M	Nähere Beschreibung bei Ablehnung der Zahlung. Bitte nutzen Sie **nicht** den Parameter **Description, sondern** Code für die Auswertung des Transaktionsstatus!
Code	"code": ...	n8	M	Fehlercode gemäß Paygate Antwort-Codes (A4 Fehlercodes)
RefNr	"referenceNumber": "..."	ns..30	C	Eindeutige Referenznummer des Händlers, welche als Auszahlungsreferenz in der entsprechenden Acquirer EPA-Datei angegeben wird. Bitte beachten Sie, ohne die Übergabe einer eigenen Auszahlungsreferenz können Sie die EPA-Transaktionen nicht zuordnen, zusätzlich kann das Computop Settlement File (CTSF) auch nicht zusätzlich angereichert werden. (nicht bei EVO Payments, bei Card Complete im Format an..25, bei Omnipay im Format ns..15, bei RBI im Format ns..20) Es sind ausschließlich ASCII-Zeichen erlaubt. Sonderzeichen wie ("Umlaute", ...) sind nicht erlaubt und müssen ggf. durch ASCII-Zeichen ersetzt werden (z.B. ü ue, é e, ...).
Aid	"authorizationId": "..."	n6	OC	Nur bei Card Complete: von Card Complete zurückgegebene Autorisierungs-ID
Amount	"amountValue": "..."	n..10	OC	Nur bei Clearhaus: Betrag in der kleinsten Währungseinheit (z.B. EUR Cent) Sollte der tatsächliche Betrag vom angefragten Betrag abweichen, wird dieser zurückgegeben. Nur bei MasaPay: Betrag muss gleich dem ursprünglich autorisierten Betrag sein.
CodeExt	"externalErrorCode": "..."	n5	OC	Nur bei Clearhaus: Nur wenn konfiguriert: externer Fehlercode (nachgelagertes System). Nur bei MasaPay: Format ans..10, Fehlercode von MasaPay.
ErrorText	"errorText": "..."	ans.128	OC	Nur bei Clearhaus: Detaillierte Clearhaus Fehlermeldung. Nur bei MasaPay: Format ans..128, Detaillierte MasaPay Fehlermeldung. Wird nur bei Status=FAILED zurückgegeben. Nutzung nur in Abstimmung mit Computop Helpdesk möglich.
TransactionID	"clearhausTransactionId": "..."	ans36	OC	Nur bei Clearhaus: Transaktionsnummer von Clearhaus
GuWID	"wirecardTransactionId": "..."	ans..22	O	Nur bei Wirecard: TransaktionsID des Acquirers
TID	"cofidisTransactionId": "..."	n..15	M	Nur bei Cofidis: Wenn RefNr übergeben wurde, wird dieser Wert zurückgegeben. Anderenfalls werden die ersten 15 Stellen der TransactionID zurückgegeben.

Ergebnis-Parameter für Buchungen von Kreditkartenzahlungen

Gutschrift mit Referenz

Gutschriften sind über eine Server-zu-Server-Kommunikation möglich. Das Paygate erlaubt einerseits Gutschriften, die sich auf eine vorher über das Paygate getätigte Buchung beziehen, andererseits können Sie Gutschriften ohne Bezugstransaktion ausführen. Dieses Kapitel beschreibt die Abwicklung von Gutschriften mit Bezugstransaktion. Wenn Sie sich bei einer Gutschrift auf eine Buchung beziehen, dann ist die Höhe der Gutschrift auf die Höhe der vorangegangen Buchung beschränkt.

Um eine Gutschrift (Credit) mit Referenztransaktion auszuführen, verwenden Sie bitte folgende URL:

https://www.computop-paygate.com/credit.aspx

Hinweis: Aus Sicherheitsgründen lehnt das Paygate alle Zahlungsanfragen mit Formatfehlern ab. Bitte übergeben Sie deshalb bei jedem Parameter den korrekten Datentyp.

Die folgende Tabelle beschreibt die verschlüsselten Übergabeparameter:

Key	REST	Format	CND	Beschreibung
MerchantID	BasicAuth.Username	ans..30	M	HändlerID, die von Computop vergeben wird. Dieser Parameter ist zusätzlich auch unverschlüsselt zu übergeben.

PayID	"paymentId": "..."	an32	M	Vom Paygate vergebene ID für die Zahlung; z.B. zur Referenzierung in Batch-Dateien sowie im Capture- oder Credit-Request.
TransID	"transactionId": "..."	ans..64	M	TransaktionsID, die für jede Zahlung eindeutig sein muss Bitte beachten Sie bei einigen Anbindungen die abweichenden Formate, die bei den spezifischen Parametern angegeben sind.
Amount	"amount": { "value": ...}	n..10	M	Betrag in der kleinsten Währungseinheit (z.B. EUR Cent). Bitte wenden Sie sich an den Computop Helpdesk, wenn Sie Beträge < 100 (kleinste Währungseinheit) buchen möchten.
Currency	"amount": { "currency": "..."}	a3	M	Währung, drei Zeichen DIN / ISO 4217, z.B. EUR, USD, GBP. Hier eine Übersicht: A1 Währungstabelle
MAC	---	an64	M	Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier: • HMAC-Authentisierung (Anfrage) • HMAC-Authentisierung (Notify)
RefNr	"referenceNumber": "..."	ns..30	C	Eindeutige Referenznummer des Händlers, welche als Auszahlungsreferenz in der entsprechenden Acquirer EPA-Datei angegeben wird. Bitte beachten Sie, ohne die Übergabe einer eigenen Auszahlungsreferenz können Sie die EPA-Transaktionen nicht zuordnen, zusätzlich kann das Computop Settlement File (CTSF) auch nicht zusätzlich angereichert werden. (nicht bei EVO Payments, Nur bei CardComplete, bei Clearhaus (ns..30, optional, nur ASCII druckbare Zeichen von 0x20 bis 0x7E), bei RBI (ns..20, optional), bei MasaPay (ns..30, optional), bei Cofidis (n..15, optional).) Hinweis: Für CAPN sind mehrere Teilgutschriften am selben Tag zulässig. Bitte beachten Sie, dass für jede Teilgutschrift eine separate eindeutige RefNr erforderlich ist. Es sind ausschließlich ASCII-Zeichen erlaubt. Sonderzeichen wie ("Umlaute", ...) sind nicht erlaubt und müssen ggf. durch ASCII-Zeichen ersetzt werden (z.B. ü ue, é e, ...).
OrderDesc	"orderDescription": "..."	ans..768	O	Beschreibung der gutgeschriebenen Artikel, Einzelpreise, Händlerkommentar etc. (Nicht bei Clearhaus)
ReqId	"requestId": "..."	ans..32	O	Um Doppelzahlungen (z.B. durch ETM) zu vermeiden, übergeben Sie einen alphanumerischen Wert, der Ihre Transaktion oder Aktion identifiziert und nur einmal vergeben werden darf. Falls die Transaktion oder Aktion mit derselben ReqID erneut eingereicht wird, führt das Computop Paygate keine Zahlung oder weitere Aktion aus, sondern gibt nur den Status der ursprünglichen Transaktion oder Aktion zurück. Bitte beachten Sie, dass das Computop Paygate für die erste initiale Aktion (Authentifizierung/Autorisierung) einen abgeschlossenen Transaktionsstatus haben muss. Dies gilt nicht für 3-D Secure Authentifizierungen, die durch einem Timeout beendet werden. Der Status 3-D Secure Timeout gilt nicht als abgeschlossener Status, bei dem ReqID-Funktionalität am Paygate nicht greift. Einreichungen mit identischer ReqID auf einen offenen Status werden regulär verarbeitet. **Hinweis:** Bitte beachten Sie, dass eine ReqID nur 12 Monate gültig ist, danach wird sie vom Paygate gelöscht.
Textfeld1	"cardHolder": { "name": "..."}	ans..30	O	Karteninhaber-Information: Name (Nicht bei Clearhaus) Für Banksys: Name des Händlers. Bei VISA-Transaktionen sind bis zu 25 Zeichen erlaubt, bei MasterCard nur bis zu 22.
Textfeld2	"cardHolder": { "city": "..."}	ans..30	O	Karteninhaber-Information: Ort (Nicht bei Clearhaus) Für Banksys: Ort des Händlers. Der Wert wird nach 13 Zeichen abgeschnitten.
CHDesc	---	ans..22	OC	Nur bei Clearhaus: Text, der auf der Kreditkartenabrechnung angezeigt wird. Nur ASCII druckbare Zeichen von 0x20 bis 0x7E
TID	"safeChargeTransactionId": "..."	ans..30	OC	Nur bei SafeCharge: TransaktionsID der gutzuschreibenden Buchung, falls der Händler eine bestimmte Buchung gutschreiben möchte. Wenn der Parameter nicht angegeben ist, wird die letzte Buchung gutgeschrieben.
				Zusätzliche Parameter bei Anbindung Wirecard (für Visa Direct)
refundType	"wirecardConnection": { "refundType": "p2p"} "wirecardConnection": { "refundType": "md"} "wirecardConnection": { "refundType": "acc2acc"} "wirecardConnection": { "refundType": "ccBill"} "wirecardConnection": { "refundType": "fd"}	enum	C	Art der Gutschrift. Mögliche Werte: “p2p”, “md”, “acc2acc”. “ccBill”, “fd”
receiverFirstName	"wirecardConnection": {"receiver": { "firstName": "..." }}	an..12	C	Vorname des Empfängers. Pflicht bei grenzüberschreitenden Transaktionen.
receiverLastName	"wirecardConnection": {"receiver": { "lastName": "..." }}	an..12	C	Nachname des Empfängers. Pflicht bei grenzüberschreitenden Transaktionen.
sender	"wirecardConne	n..12	C	Kontonnummer des Senders.

AccountNumber	ction": {"sender": { "accountNumber": "..." }}			Mastercard: Pflicht. Visa: Pflicht, wenn die RefNr leer ist.
senderFirstName	"wirecardConnection": {"sender": { "firstName": "..." }}	an..12	C	Vorname des Senders. Mastercard: Pflicht. Visa: Pflicht für US-Inlandstransaktionen und grenzüberschreitende Zahlungen.
senderLastName	"wirecardConnection": {"sender": { "lastName": "..." }}	an..12	C	Nachname des Senders. Mastercard: Pflicht. Visa: Optional.
senderAddrStreet	"wirecardConnection": {"sender": { "street": "..." }}	an..25	C	Straßenname des Senders. Mastercard: Optional. Visa: Pflicht für US-Inlandstransaktionen und grenzüberschreitende Zahlungen.
senderAddrStreetNr	"wirecardConnection": {"sender": { "streetNumber": "..." }}	an..25	C	Haunsummer des Senders. Mastercard: Optional. Visa: Pflicht für US-Inlandstransaktionen und grenzüberschreitende Zahlungen.
senderAddrCity	"wirecardConnection": {"sender": { "city": "..." }}	an..32	C	Ort des Senders. Mastercard: Optional. Visa: Pflicht für US-Inlandstransaktionen und grenzüberschreitende Zahlungen.
senderAddrState	"wirecardConnection": {"sender": { "stateCode": "..." }}	a2	C	Bundesland des Senders. Mastercard: Pflicht, wenn senderAddrCountry=US oder Canada. Visa: Pflicht für US-Inlandstransaktionen und grenzüberschreitende Zahlungen.
senderAddrCountry	"wirecardConnection": {"sender": { "countryCode": "..." }}	a2	C	Land des Senders. Mastercard: Optional. Visa: Pflicht, wenn das Land US ist, und bei grenzüberschreitende Zahlungen.

Parameter für Gutschrift von Kreditkartenzahlungen

Die folgende Tabelle beschreibt die Parameter, die das Paygate als Antwort zurückgibt:

ℹ es können jederzeit neue Parameter hinzugefügt bzw. die Reihenfolge geändert werden

ℹ die Parameter (z.B. MerchantId, RefNr) sollten nicht auf Groß-/Kleinschreibung geprüft werden

Key	REST	Format	CND	Beschreibung
mid	"merchantId": "..."	ans..30	M	HändlerID, die von Computop vergeben wird
PayID	"paymentId": "..."	an32	M	Vom Paygate vergebene ID für die Zahlung; z.B. zur Referenzierung in Batch-Dateien sowie im Capture- oder Credit-Request.
XID	"xId": "..."	an32	M	Vom Paygate vergebene ID für alle einzelnen Transaktionen (Autorisierung, Buchung, Gutschrift), die für eine Zahlung durchgeführt werden
TransID	"transactionId": "..."	ans..64	M	Transaktionsnummer des Händlers. Bitte beachten Sie bei einigen Anbindungen die abweichenden Formate, die bei den spezifischen Parametern angegeben sind.
Status	"status": "OK" "status": "FAILED"	a..50	M	OK (URLSuccess) oder FAILED (URLFailure)
Description	"description": "..."	ans..1024	M	Nähere Beschreibung bei Ablehnung der Zahlung. Bitte nutzen Sie **nicht** den Parameter **Description, sondern** Code für die Auswertung des Transaktionsstatus!
Code	"code": ...	n8	M	Fehlercode gemäß Paygate Antwort-Codes (A4 Fehlercodes)
Aid	"authorizationId": "..."	n6	OC	Nur bei Card Complete: von Card Complete zurückgegebene Autorisierungs-ID
RefNr	"referenceNumber": "..."	an..25	OC	Eindeutige Referenznummer des Händlers, welche als Auszahlungsreferenz in der entsprechenden Acquirer EPA-Datei angegeben wird. Bitte beachten Sie, ohne die Übergabe einer eigenen Auszahlungsreferenz können Sie die EPA-Transaktionen nicht zuordnen, zusätzlich kann das Computop Settlement File (CTSF) auch nicht zusätzlich angereichert werden.

				Nur bei Card Complete, bei Clearhaus (ans..30, nur ASCII druckbare Zeichen von 0x20 bis 0x7E), bei RBI (ns..20, optional), bei MasaPay (ns..30, optional), bei Cofidis (n..15, optional). Es sind ausschließlich ASCII-Zeichen erlaubt. Sonderzeichen wie ("Umlaute", ...) sind nicht erlaubt und müssen ggf. durch ASCII-Zeichen ersetzt werden (z.B. ü ue, é e, ...).
Amount	"amountValue": "..."	n..10	OC	Nur bei Clearhaus: Betrag in der kleinsten Währungseinheit (z.B. EUR Cent) Sollte der tatsächliche Betrag vom angefragten Betrag abweichen, wird dieser zurückgegeben. Nur bei MasaPay: Betrag muss gleich dem ursprünglich autorisierten Betrag sein.
CodeExt	"externalErrorCode": "..."	n5	OC	Nur bei Clearhaus: Nur wenn konfiguriert: externer Fehlercode (nachgelagertes System). Nur bei MasaPay: Format ans..10, Fehlercode von MasaPay.
ErrorText	"errorText": "..."	ans.128	OC	Nur bei Clearhaus: Detaillierte Clearhaus Fehlermeldung. Nur bei MasaPay: Format ans..128, Detaillierte MasaPay Fehlermeldung. Wird nur bei Status=FAILED zurückgegeben. Nutzung nur in Abstimmung mit Computop Helpdesk möglich.
TransactionID	"clearhausTransactionId": "..."	ans36	OC	Nur bei Clearhaus: Transaktionsnummer von Clearhaus

Ergebnis-Parameter für Gutschrift von Kreditkartenzahlungen

Gutschrift ohne Referenz

Das Paygate kann für Sie Gutschriften ausführen, die sich nicht auf eine vorherige Buchung beziehen. In diesem Fall muss die Gutschrift als komplett neue Zahlungstransaktion an das Paygate übergeben werden. Um die beschriebene Zusatzfunktion nutzen zu können, nehmen Sie bitte mit dem Computop Helpdesk Kontakt auf.

Hinweis: Bitte beachten Sie, dass Gutschriften ohne Bezug auf eine vorherige Buchung bei Ihrem Acquirer höhere Kosten verursachen. Wenn Sie häufig keinen Bezug auf die Buchung nehmen können, sollten Sie dies mit Ihrem Acquirer abstimmen.

Um eine Gutschrift (Credit) ohne Referenztransaktion über eine Server-zu-Server-Verbindung auszuführen, verwenden Sie bitte folgende URL:

https://www.computop-paygate.com/creditex.aspx

Hinweis: Aus Sicherheitsgründen lehnt das Paygate alle Zahlungsanfragen mit Formatfehlern ab. Bitte übergeben Sie deshalb bei jedem Parameter den korrekten Datentyp.

Die folgende Tabelle beschreibt die verschlüsselten Übergabeparameter:

Key	Format	CND	Beschreibung
MerchantID	ans..30	M	HändlerID, die von Computop vergeben wird. Dieser Parameter ist zusätzlich auch unverschlüsselt zu übergeben.
TransID	ans..64	M	TransaktionsID, die für jede Zahlung eindeutig sein muss Bitte beachten Sie bei einigen Anbindungen die abweichenden Formate, die bei den spezifischen Parametern angegeben sind.
Amount	n..10	M	Betrag in der kleinsten Währungseinheit (z.B. EUR Cent). Bitte wenden Sie sich an den Computop Helpdesk, wenn Sie Beträge < 100 (kleinste Währungseinheit) buchen möchten.
Currency	a3	M	Währung, drei Zeichen DIN / ISO 4217, z.B. EUR, USD, GBP. Hier eine Übersicht: A1 Währungstabelle
MAC	an64	M	Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier: • HMAC-Authentisierung (Anfrage) • HMAC-Authentisierung (Notify)
RefNr	ns..30	C	Eindeutige Referenznummer des Händlers, welche als Auszahlungsreferenz in der entsprechenden Acquirer EPA-Datei angegeben wird. Bitte beachten Sie, ohne die Übergabe einer eigenen Auszahlungsreferenz können Sie die EPA-Transaktionen nicht zuordnen, zusätzlich kann das Computop Settlement File (CTSF) auch nicht zusätzlich angereichert werden. (nicht bei EVO Payments, Nur bei CardComplete, bei Clearhaus (ns..30, optional, nur ASCII druckbare Zeichen von 0x20 bis 0x7E), bei RBI (ns..20, optional), bei MasaPay (ns..30, optional), bei Cofidis (n..15, optional).) Es sind ausschließlich ASCII-Zeichen erlaubt. Sonderzeichen wie ("Umlaute", ...) sind nicht erlaubt und müssen ggf. durch ASCII-Zeichen ersetzt werden (z.B. ü ue, é e, ...).

OrderDesc	ans..768	O	Beschreibung der gutgeschriebenen Artikel, Einzelpreise, Händlerkommentar etc. (Nicht bei Clearhaus)
ReqId	ans..32	O	Um Doppelzahlungen (z.B. durch ETM) zu vermeiden, übergeben Sie einen alphanumerischen Wert, der Ihre Transaktion oder Aktion identifiziert und nur einmal vergeben werden darf. Falls die Transaktion oder Aktion mit derselben ReqID erneut eingereicht wird, führt das Computop Paygate keine Zahlung oder weitere Aktion aus, sondern gibt nur den Status der ursprünglichen Transaktion oder Aktion zurück. Bitte beachten Sie, dass das Computop Paygate für die erste initiale Aktion (Authentifizierung/Autorisierung) einen abgeschlossenen Transaktionsstatus haben muss. Dies gilt nicht für 3-D Secure Authentifizierungen, die durch einem Timeout beendet werden. Der Status 3-D Secure Timeout gilt nicht als abgeschlossener Status, bei dem ReqID-Funktionalität am Paygate nicht greift. Einreichungen mit identischer ReqID auf einen offenen Status werden regulär verarbeitet. **Hinweis:** Bitte beachten Sie, dass eine ReqID nur 12 Monate gültig ist, danach wird sie vom Paygate gelöscht.
CCNr	n..19	M	Kreditkartennummer für Kreditkarten-Zahlungen. Es kann wahlweise übergeben werden: • entweder die richtige Kreditkartennummer (PAN) • oder die Pseudokartennummer, welche Sie zuvor in einer Paygate-Antwort als PCNr erhalten haben. Mit 3-D Secure 2.x wird die CCNr (PAN oder PCNr) im card-JSON gesendet. Wir empfehlen die Verwendung der "Hosted Payment Page" oder des Kreditkartenformular (PaySSL) sowie Übergabe der PCNr zur vereinfachten PCI DSS Zertifizierung.
CCCVC	n..4	O	Kartenprüfnummer: Die letzten 3 Ziffern auf dem Unterschriftsfeld der Kreditkarte. Bei American Express 4 Ziffern.
CCExpiry	n6	M	Ablaufdatum der Kreditkarte im Format YYYYMM, z.B. 202507
CCBrand	a..22	M	Kreditkartenmarke. Bitte beachten Sie die Schreibweise gemäß Tabelle der Kreditkartenmarken!
OrderDesc	ans..768	MC	Nicht bei Clearhaus: Beschreibung der gutgeschriebenen Artikel, Einzelpreise, Händlerkommentar etc.
UserData	ans..1024	OC	Nur bei Clearhaus: Wenn beim Aufruf angegeben, übergibt das Paygate die Parameter mit dem Zahlungsergebnis an den Shop
Textfeld1	ans..30	O	Nicht bei Clearhaus: Karteninhaber-Information: Name Für Banksys: Name des Händlers. Bei VISA-Transaktionen sind bis zu 25 Zeichen erlaubt, bei MasterCard nur bis zu 22.
Textfeld2	ans..30	O	Nicht bei Clearhaus: Karteninhaber-Information: Ort Für Banksys: Ort des Händlers. Der Wert wird nach 13 Zeichen abgeschnitten.
CHDesc	ans..34	OC	Nur bei Clearhaus, Format ans..22: Text, der auf der Kreditkartenabrechnung angezeigt wird. Nur ASCII druckbare Zeichen von 0x20 bis 0x7E Nur bei Credorax: Text, der auf der Kreditkartenabrechnung angezeigt wird. Diese Funktion muss von Credorax freigeschalten werden und folgenden Aufbau haben. 1) merchant DBA Name (bis zu 20 Zeichen) 2) Stern 3) zusätzlicher Text (bis zu 13 Zeichen). z.B. Computop *Test Dieser Wert kann alternativ vom Computop Helpdesk fest hinterlegt werden.
CreditCardHolder	an..255	MC	Nur bei Credorax, ECPCC: Name des Karteninhabers
Email	ans..64	MC	Nur bei Credorax, ECPCC: E-Mail-Adresse des Kunden
IPAddr	ans..15	OC	Nur bei Credorax, ECPCC: IP-Adresse des Kunden
PaymentOfWinnings	ans..4	OC	Beim Acquirer EMS (Omnipay) kann der Händler hiermit CFT-Gutschriften steuern. Übergeben Sie PaymentOfWinnings=True, um einen Gewinn gutzuschreiben, anstatt nur einen eingezahlten Betrag zurückzuerstatten.
PaymentAddData	JSON	C	Nur bei OmniPay: Zusätzliche Daten, wenn PaymentOfWinnings=True
TransactionID	an..150	M	Zusätzliche Referenznummer
			Weitere Adressparameter bei der Anbindung ECPCC
DateOfBirth	n8	O	Geburtsdatum des Kunden im Format YYYYYMMDD

Phone	n..32	O	Telefonnummer des Kunden
FirstName	ans..255	M	Vorname des Kunden
LastName	ans..255	M	Nachname des Kunden
AddrStreet	ans..255	O	Straßenname
AddressAddition	ans..255	O	Adresszusatz
AddrZip	an..9	O	Postleitzahl
AddrCity	ans..255	O	Ort
AddrState	a2	O	Code des Bundeslandes des Kunden
AddrCountryCode	a2	M	Ländercode im Format ISO-3166-1, alphanumerisch 2-stellig
sdFirstName	ans..255	O	Vorname in der Lieferanschrift
sdLastName	ans..255	O	Nachname in der Lieferanschrift
sdStreet	ans..255	O	Straßenname der Lieferanschrift
sdAddressAddition	ans..255	O	Adresszusatz der Lieferanschrift
sdZIPCode	an..9	O	Postleitzahl der Lieferanschrift
sdCity	ans..255	O	Ort der Lieferanschrift
sdState	a2	O	Code des Bundeslandes der Lieferanschrift
sdCountryCode	a2	O	Ländercode der Lieferanschrift im Format ISO-3166-1, alphanumerisch 2-stellig
			Weitere Adressparameter bei der Anbindung Kalixa
IPAddr	ans..15	M	IP-Adresse des Kunden
BrowserSessionID	ans..64	M	SessionID des Kunden
CreditCardHolder	ans..100	M	Name des Karteninhabers
CustomerID	an..20	M	Kundennummer: Nummer zur Identifizierung des Kunden
Name	ans..100	C	Benutzername des Kunden
FirstName	ans..100	C	Vorname des Kunden
LastName	ans..100	C	Nachname des Kunden
Email	ans..64	C	E-Mail-Adresse des Kunden
Language	a2	C	Sprache des Kunden gemäß ISO, alphanumerisch 2-stellig
sdFirstName	ans..100	C	Vorname in der Lieferanschrift
sdLastName	ans..100	C	Nachname in der Lieferanschrift
sdStreet	ans..200	C	Straßenname der Lieferanschrift
sdStreetNr	ans..5	C	Hausnummer der Lieferanschrift

sdZIP Code	an..20	C	Postleitzahl der Lieferanschrift
sdCity	ans..40	C	Ort der Lieferanschrift
sdState	a2	C	Code des Bundeslandes der Lieferanschrift
sdCountryCode	a2	C	Ländercode der Lieferanschrift im Format ISO-3166-1, alphanumerisch 2-stellig
			Weitere Adressparameter bei der Anbindung Vantiv
bdFirstName	ans..25	O	Vorname in der Rechnungsadresse
bdLastName	ans..25	O	Nachname in der Rechnungsadresse
bdStreet	ans..35	O	Straßenname in der Rechnungsadresse Bitte beachten Sie, dass bdStreet und bdStreetNr zusammen maximal 34 Zeichen haben dürfen. bdStreet und bdStreetNr werden mit einem Leerzeichen getrennt zusammengefügt und gemeinsam weitergeleitet. Der Gesamtinhalt wird nach 35 Zeichen abgeschnitten.
bdStreetNr	ans..35	O	Hausnummer in der Rechnungsadresse Bitte beachten Sie, dass bdStreet und bdStreetNr zusammen maximal 34 Zeichen haben dürfen. bdStreet und bdStreetNr werden mit einem Leerzeichen getrennt zusammengefügt und gemeinsam weitergeleitet. Der Gesamtinhalt wird nach 35 Zeichen abgeschnitten.
bdStreet2	ans..35	O	Adresszusatz in der Rechnungsadresse
bdZIP Code	ans..20	O	Postleitzahl in der Rechnungsadresse
bdCity	ans..35	O	Ort in der Rechnungsadresse
bdState	ans..30	O	Staat/Land in der Rechnungsadresse
bdCountryCode	a2	O	Ländercode der Rechnungsadresse im Format ISO-3166-1, alphanumerisch 2-stellig
bdMail	ans..100	O	E-Mail in der Rechnungsadresse
bdPhone	ans..20	O	Telefonnummer in der Rechnungsanschrift

Parameter für Gutschrift von Kreditkartenzahlungen ohne Bezug

Die folgende Tabelle beschreibt die Parameter, die das Paygate als Antwort zurückgibt:

es können jederzeit neue Parameter hinzugefügt bzw. die Reihenfolge geändert werden

die Parameter (z.B. MerchantId, RefNr) sollten nicht auf Groß-/Kleinschreibung geprüft werden

Key	Format	CND	Beschreibung
mid	ans..30	M	HändlerID, die von Computop vergeben wird

Key	Format	CND	Beschreibung
PayID	an32	M	Vom Paygate vergebene ID für die Zahlung; z.B. zur Referenzierung in Batch-Dateien sowie im Capture- oder Credit-Request.

Key	Format	CND	Beschreibung
XID	an32	M	Vom Paygate vergebene ID für alle einzelnen Transaktionen (Autorisierung, Buchung, Gutschrift), die für eine Zahlung durchgeführt werden

Key	Format	CND	Beschreibung
TransID	ans..64	M	Transaktionsnummer des Händlers. Bitte beachten Sie bei einigen Anbindungen die abweichenden Formate, die bei den spezifischen Parametern angegeben sind.

Key	Format	CND	Beschreibung
Status	a..50	M	OK (URLSuccess) oder FAILED (URLFailure)

Key	Format	CND	Beschreibung
Description	ans..1024	M	Nähere Beschreibung bei Ablehnung der Zahlung. Bitte nutzen Sie **nicht** den Parameter **Description, sondern** Code für die Auswertung des Transaktionsstatus!

Key	Format	CND	Beschreibung
Code	n8	M	Fehlercode gemäß Paygate Antwort-Codes (A4 Fehlercodes)

Key	Format	CND	Beschreibung
AID	n6	OC	Nur bei Card Complete: von Card Complete zurückgegebene Autorisierungs-ID
RefNr	an..25	OC	Nur bei Card Complete: Falls eine RefNr übermittelt wurde, wird sie wieder zurückgegeben. Es sind ausschließlich ASCII-Zeichen erlaubt. Sonderzeichen wie ("Umlaute", ...) sind nicht erlaubt und müssen ggf. durch ASCII-Zeichen ersetzt werden (z.B. ü ue, é e, ...).
Amount	n..10	OC	Nur bei Clearhaus: Betrag in der kleinsten Währungseinheit (z.B. EUR Cent) Sollte der tatsächliche Betrag vom angefragten Betrag abweichen, wird dieser zurückgegeben.
CodeExt	n5	OC	Nur bei Clearhaus: Nur wenn konfiguriert: externer Fehlercode (nachgelagertes System)
ErrorText	ans..128	OC	Nur bei Clearhaus: Detaillierte Clearhaus Fehlermeldung. Wird nur bei Status=FAILED zurückgegeben. Nutzung nur in Abstimmung mit dem Computop Helpdesk möglich.
UserData	ans..1024	OC	Nur bei Clearhaus: Wenn beim Aufruf angegeben, übergibt das Paygate die Parameter mit dem Zahlungsergebnis an den Shop
TransactionID	ans36	OC	Nur bei Clearhaus: Transaktionsnummer von Clearhaus
PaymentSenderReference	an..19	C	Nur bei Omnipay: Referenznummer des Acquirers, die zur Identifikation der Zahlungstransaktion verwendet wird. Sie kann für MasterCard Payment of winnings Transaktionen zurückgegeben werden, wenn die erforderlichen zusätzlichen Parameter übergeben worden sind.

Ergebnis-Parameter für Gutschrift von Kreditkartenzahlungen ohne Bezug

Storno

Eine Kreditkartenautorisierung senkt das Kartenlimit des Kunden. Um das Limit wieder freizugeben, kann das Paygate eine Autorisierung stornieren. Verwenden Sie dazu die folgende URL:

https://www.computop-paygate.com/reverse.aspx

Hinweis: Die Reverse.aspx macht nicht nur Autorisierungen, sondern IMMER DEN LETZTEN TRANSAKTIONSSCHRITT rückgängig! Falls die letzte Transaktion eine Buchung war, löst die Reverse.aspx z.B. eine Gutschrift aus. Es ist daher größte Vorsicht geboten, und die Nutzung erfolgt auf eigene Gefahr. Wir empfehlen, vor Nutzung der Reverse.aspx den Transaktionsstatus mit der Inquire.aspx prüfen.

Hinweis: Aus Sicherheitsgründen lehnt das Paygate alle Zahlungsanfragen mit Formatfehlern ab. Bitte übergeben Sie deshalb bei jedem Parameter den korrekten Datentyp.

Die folgende Tabelle beschreibt die verschlüsselten Übergabeparameter:

Key	REST	Format	CND	Beschreibung
MerchantID	BasicAuth. Username	ans..30	M	HändlerID, die von Computop vergeben wird. Dieser Parameter ist zusätzlich auch unverschlüsselt zu übergeben.
PayID	"paymentId": "..."	an32	M	Vom Paygate vergebene ID für die Zahlung; z.B. zur Referenzierung in Batch-Dateien sowie im Capture- oder Credit-Request.
TransID	"transactionId": "..."	ans..64	M	TransaktionsID, die für jede Zahlung eindeutig sein muss Bitte beachten Sie bei einigen Anbindungen die abweichenden Formate, die bei den spezifischen Parametern angegeben sind.
Amount	"amount": { "value": ...}	n..10	M	Betrag in der kleinsten Währungseinheit (z.B. EUR Cent). Bitte wenden Sie sich an den Computop Helpdesk, wenn Sie Beträge < 100 (kleinste Währungseinheit) buchen möchten.

Currency	"amount": { "currency": "..."}	a3	M	Währung, drei Zeichen DIN / ISO 4217, z.B. EUR, USD, GBP. Hier eine Übersicht: A1 Währungstabelle
MAC	---	an64	M	Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier: • HMAC-Authentisierung (Anfrage) • HMAC-Authentisierung (Notify)
RefNr	"referenceNumber": "..."	ans..30	OC	Eindeutige Referenznummer des Händlers, welche als Auszahlungsreferenz in der entsprechenden Acquirer EPA-Datei angegeben wird. Bitte beachten Sie, ohne die Übergabe einer eigenen Auszahlungsreferenz können Sie die EPA-Transaktionen nicht zuordnen, zusätzlich kann das Computop Settlement File (CTSF) auch nicht zusätzlich angereichert werden. Nur bei Clearhaus (nur ASCII druckbare Zeichen von 0x20 bis 0x7E), bei MasaPay. Es sind ausschließlich ASCII-Zeichen erlaubt. Sonderzeichen wie ("Umlaute", ...) sind nicht erlaubt und müssen ggf. durch ASCII-Zeichen ersetzt werden (z.B. ü ue, é e, ...).
ReqId	"requestId": "..."	ans..32	O	Um Doppelzahlungen (z.B. durch ETM) zu vermeiden, übergeben Sie einen alphanumerischen Wert, der Ihre Transaktion oder Aktion identifiziert und nur einmal vergeben werden darf. Falls die Transaktion oder Aktion mit derselben ReqID erneut eingereicht wird, führt das Computop Paygate keine Zahlung oder weitere Aktion aus, sondern gibt nur den Status der ursprünglichen Transaktion oder Aktion zurück. Bitte beachten Sie, dass das Computop Paygate für die erste initiale Aktion (Authentifizierung/Autorisierung) einen abgeschlossenen Transaktionsstatus haben muss. Dies gilt nicht für 3-D Secure Authentifizierungen, die durch einem Timeout beendet werden. Der Status 3-D Secure Timeout gilt nicht als abgeschlossener Status, bei dem ReqID-Funktionalität am Paygate nicht greift. Einreichungen mit identischer ReqID auf einen offenen Status werden regulär verarbeitet. **Hinweis:** Bitte beachten Sie, dass eine ReqID nur 12 Monate gültig ist, danach wird sie vom Paygate gelöscht.

Parameter für Storno von Kreditkartenzahlungen

Die folgende Tabelle beschreibt die Parameter, die das Paygate als Antwort zurückgibt:

es können jederzeit neue Parameter hinzugefügt bzw. die Reihenfolge geändert werden

die Parameter (z.B. MerchantId, RefNr) sollten nicht auf Groß-/Kleinschreibung geprüft werden

Key	REST	Format	CND	Beschreibung
mid	"merchantId": "..."	ans..30	M	HändlerID, die von Computop vergeben wird
PayID	"paymentId": "..."	an32	M	Vom Paygate vergebene ID für die Zahlung; z.B. zur Referenzierung in Batch-Dateien sowie im Capture- oder Credit-Request.
XID	"xId": "..."	an32	M	Vom Paygate vergebene ID für alle einzelnen Transaktionen (Autorisierung, Buchung, Gutschrift), die für eine Zahlung durchgeführt werden
TransID	"transactionId": "..."	ans..64	M	Transaktionsnummer des Händlers. Bitte beachten Sie bei einigen Anbindungen die abweichenden Formate, die bei den spezifischen Parametern angegeben sind.
Status	"status": "OK" "status": "FAILED"	a..50	M	OK (URLSuccess) oder FAILED (URLFailure)
Description	"description": "..."	ans..1024	M	Nähere Beschreibung bei Ablehnung der Zahlung. Bitte nutzen Sie **nicht** den Parameter **Description, sondern** Code für die Auswertung des Transaktionsstatus!
Code	"code": ...	n8	M	Fehlercode gemäß Paygate Antwort-Codes (A4 Fehlercodes)
RefNr	"referenceNumber": "..."	an..25	OC	Eindeutige Referenznummer des Händlers, welche als Auszahlungsreferenz in der entsprechenden Acquirer EPA-Datei angegeben wird. Bitte beachten Sie, ohne die Übergabe einer eigenen Auszahlungsreferenz können Sie die EPA-Transaktionen nicht zuordnen, zusätzlich kann das Computop Settlement File (CTSF) auch nicht zusätzlich angereichert werden. Nur bei Card Complete, bei Clearhaus (ans..30, nur ASCII druckbare Zeichen von 0x20 bis 0x7E), bei MasaPay (ns..30). Es sind ausschließlich ASCII-Zeichen erlaubt. Sonderzeichen wie ("Umlaute", ...) sind nicht erlaubt und müssen ggf. durch ASCII-Zeichen ersetzt werden (z.B. ü ue, é e, ...).
AID	"authorizationId": "..."	n6	OC	Nur bei Card Complete: von Card Complete zurückgegebene Autorisierungs-ID
CodeExt	"externalErrorCode": "..."	n5	OC	Nur bei Clearhaus: Nur wenn konfiguriert: externer Fehlercode (nachgelagertes System) Nur bei MasaPay: Format ans..10, Fehlercode von MasaPay
		ans.128	OC	Nur bei Clearhaus: Detaillierte Clearhaus Fehlermeldung.

ErrorText	"errorText": "..."			Nur bei MasaPay: Format ans..128, Detaillierte MasaPay Fehlermeldung. Wird nur bei Status=FAILED zurückgegeben. Nutzung nur in Abstimmung mit dem Computop Helpdesk möglich.
TransactionID	"clearhausTransactionId": "..."	ans36	OC	Nur bei Clearhaus: Transaktionsnummer von Clearhaus

Ergebnis-Parameter für Storno von Kreditkartenzahlungen

Storno einer Autorisierungsverlängerung

Eine Kreditkartenautorisierung ist nur 7 bis 30 Tage gültig. Um Ihren Zahlungsanspruch bei längeren Lieferzeiten zu erhalten, erlaubt das Paygate die automatische Wiederholung der Autorisierung. Auch bei Ratenzahlung oder Teillieferungen ist die Wiederholung der Autorisierung wichtig, weil bei Teilbuchungen der Restbetrag ungültig wird.

Wenn Sie die Autorisierungsverlängerung nutzen, verlängert das Paygate Ihre Autorisierungen, bis die Zahlung komplett gebucht wurde. Unterdessen bleibt das Kartenlimit des Kunden um den autorisierten Betrag reduziert. Um das Kartenlimit freizugeben, zum Beispiel weil der Auftrag nicht vollständig lieferbar ist, müssen Sie die Autorisierungsverlängerung explizit mit folgender URL stoppen:

https://www.computop-paygate.com/cancelAuth.aspx

Hinweis: Mit CancelAuth wird nur die Wiederholung der Autorisierung beendet. Wenn Sie das Kartenlimit des Kunden freigeben wollen, nutzen Sie bitte ein Storno der Autorisierung (siehe oben).

Hinweis: Aus Sicherheitsgründen lehnt das Paygate alle Zahlungsanfragen mit Formatfehlern ab. Bitte übergeben Sie deshalb bei jedem Parameter den korrekten Datentyp.

Die folgende Tabelle beschreibt die verschlüsselten Übergabeparameter:

Key	Format	CND	Beschreibung
MerchantID	ans..30	M	HändlerID, die von Computop vergeben wird. Dieser Parameter ist zusätzlich auch unverschlüsselt zu übergeben.
PayID	an32	M	Vom Paygate vergebene ID für die Zahlung; z.B. zur Referenzierung in Batch-Dateien sowie im Capture- oder Credit-Request.
TransID	ans..64	M	ID des Händlers zur Identifizierung des zu stornierenden Zahlungsvorgangs
MAC	an64	M	Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier: • HMAC-Authentisierung (Anfrage) • HMAC-Authentisierung (Notify)

Parameter zur Stornierung einer Autorisierungsverlängerung

Die folgende Tabelle beschreibt die Parameter, die das Paygate als Antwort zurückgibt:

es können jederzeit neue Parameter hinzugefügt bzw. die Reihenfolge geändert werden

die Parameter (z.B. MerchantId, RefNr) sollten nicht auf Groß-/Kleinschreibung geprüft werden

Key	Format	CND	Beschreibung
mid	ans..30	M	HändlerID, die von Computop vergeben wird
PayID	an32	M	Vom Paygate vergebene ID für die Zahlung; z.B. zur Referenzierung in Batch-Dateien sowie im Capture- oder Credit-Request.
TransID	ans..64	M	Transaktionsnummer des Händlers.
Status	a..50	M	OK (URLSuccess) oder FAILED (URLFailure)
Description	ans..1024	M	Nähere Beschreibung bei Ablehnung der Zahlung. Bitte nutzen Sie **nicht** den Parameter **Description, sondern** Code für die Auswertung des Transaktionsstatus!
Code	n8	M	Fehlercode gemäß Paygate Antwort-Codes (A4 Fehlercodes)

Ergebnis-Parameter bei Stornierung einer Autorisierungsverlängerung

Kreditkartenzahlung über stationäre Terminals

Um eine Kreditkartenzahlung über ein stationäres Terminal (POS: Point of Sale) auszuführen, verwenden Sie bitte folgende URL:

https://www.computop-paygate.com/stationary.aspx

Hinweis: Aus Sicherheitsgründen lehnt das Paygate alle Zahlungsanfragen mit Formatfehlern ab. Bitte übergeben Sie deshalb bei jedem Parameter den korrekten Datentyp.

Die folgende Tabelle beschreibt die verschlüsselten Übergabeparameter:

Key	Format	CND	Beschreibung
MerchantID	ans..30	M	HändlerID, die von Computop vergeben wird. Dieser Parameter ist zusätzlich auch unverschlüsselt zu übergeben.
Amount	n..10	M	Betrag in der kleinsten Währungseinheit (z.B. EUR Cent). Bitte wenden Sie sich an den Computop Helpdesk, wenn Sie Beträge < 100 (kleinste Währungseinheit) buchen möchten.
Currency	a3	M	Währung, drei Zeichen DIN / ISO 4217, z.B. EUR, USD, GBP. Hier eine Übersicht: A1 Währungstabelle
MAC	an64	M	Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier: • HMAC-Authentisierung (Anfrage) • HMAC-Authentisierung (Notify)
TransID	ans..64	M	Ihre eigene TransaktionsID, die für jede Zahlung eindeutig sein muss
RefNr	ns..30	O	Eindeutige Referenznummer des Händlers, welche als Auszahlungsreferenz in der entsprechenden Acquirer EPA-Datei angegeben wird. Bitte beachten Sie, ohne die Übergabe einer eigenen Auszahlungsreferenz können Sie die EPA-Transaktionen nicht zuordnen, zusätzlich kann das Computop Settlement File (CTSF) auch nicht zusätzlich angereichert werden. **Das Format muss vorher mit Computop Helpdesk abgestimmt werden!**
CCNr	n..16	M	Kreditkartennummer mind. 12stellig numerisch ohne Leerzeichen
CCCVC	n..4	O	Kartenprüfnummer: Die letzten 3 Ziffern auf dem Unterschriftsfeld der Kreditkarte. Bei American Express 4 Ziffern.
CCExpiry	n6	M	Ablaufdatum der Kreditkarte im Format YYYYMM, z.B. 201707
CCBrand	a..22	M	Kreditkartenmarke. Bitte beachten Sie die Schreibweise gemäß Tabelle der Kreditkartenmarken!
Track2	ans..80	M	Hexadezimale Daten auf Spur 2 der Kreditkarte
Track3	ans..80	M	Hexadezimale Daten auf Spur 3 der Kreditkarte
OrderDesc	ans..768	M	Beschreibung der gekauften Waren, Einzelpreise etc.
Capture	an..6	OM	Bestimmt Art und Zeitpunkt der Buchung (engl. Capture). **AUTO** – Buchung sofort nach Autorisierung (Standardwert). **MANUAL** – Buchung erfolgt durch den Händler - in der Regel die Buchung zum Zeitpunkt der Warenauslieferung bzw. Leistungserbringung. **<Zahl>** – Verzögerung in Stunden bis zur Buchung (ganze Zahl; 1 bis 696).
ReqId	ans..32	O	Um Doppelzahlungen (z.B. durch ETM) zu vermeiden, übergeben Sie einen alphanumerischen Wert, der Ihre Transaktion oder Aktion identifiziert und nur einmal vergeben werden darf. Falls die Transaktion oder Aktion mit derselben ReqID erneut eingereicht wird, führt das Computop Paygate keine Zahlung oder weitere Aktion aus, sondern gibt nur den Status der ursprünglichen Transaktion oder Aktion zurück. Bitte beachten Sie, dass das Computop Paygate für die erste initiale Aktion (Authentifizierung/Autorisierung) einen abgeschlossenen Transaktionsstatus haben muss. Dies gilt nicht für 3-D Secure Authentifizierungen, die durch einem Timeout beendet werden. Der Status 3-D Secure Timeout gilt nicht als abgeschlossener Status, bei dem ReqID-Funktionalität am Paygate nicht greift. Einreichungen mit identischer ReqID auf einen offenen Status werden regulär verarbeitet. **Hinweis:** Bitte beachten Sie, dass eine ReqID nur 12 Monate gültig ist, danach wird sie vom Paygate gelöscht.

Parameter für Kreditkartenzahlungen über stationäre Terminals

Die folgende Tabelle beschreibt die Parameter, die das Paygate als Antwort zurückgibt:

es können jederzeit neue Parameter hinzugefügt bzw. die Reihenfolge geändert werden

die Parameter (z.B. MerchantId, RefNr) sollten nicht auf Groß-/Kleinschreibung geprüft werden

Key	Format	CND	Beschreibung
mid	ans..30	M	HändlerID, die von Computop vergeben wird
PayID	an32	M	Vom Paygate vergebene ID für die Zahlung; z.B. zur Referenzierung in Batch-Dateien sowie im Capture- oder Credit-Request.
XID	an32	M	Vom Paygate vergebene ID für alle einzelnen Transaktionen (Autorisierung, Buchung, Gutschrift), die für eine Zahlung durchgeführt werden
Code	n8	M	Fehlercode gemäß Paygate Antwort-Codes (A4 Fehlercodes)
Description	ans..1024	M	Nähere Beschreibung bei Ablehnung der Zahlung. Bitte nutzen Sie **nicht** den Parameter **Description, sondern** Code für die Auswertung des Transaktionsstatus!
TransID	ans..64	M	Transaktionsnummer des Händlers
TID	n..20	M	In der Regel neunstellige Terminalnummer
AuthCode	ans..6	M	Autorisierungscode des Acquirers
Status	a..50	M	AUTHORIZED oder FAILED. Nur bei Sale-Transaktionen lautet der Status OK.

Ergebnis-Parameter für Kreditkartenzahlungen über stationäre Terminals

Storno von stationären Kreditkartenzahlungen

Um die Buchung einer Kreditkartenzahlung über ein stationäres Terminal zu stornieren, verwenden Sie bitte folgende URL:

https://www.computop-paygate.com/stationary_rev.aspx

Hinweis: Aus Sicherheitsgründen lehnt das Paygate alle Zahlungsanfragen mit Formatfehlern ab. Bitte übergeben Sie deshalb bei jedem Parameter den korrekten Datentyp.

Die folgende Tabelle beschreibt die verschlüsselten Übergabeparameter:

Key	Format	CND	Beschreibung
MerchantID	ans..30	M	HändlerID, die von Computop vergeben wird. Dieser Parameter ist zusätzlich auch unverschlüsselt zu übergeben.
PayID	an32	M	Vom Paygate vergebene ID für die Zahlung; z.B. zur Referenzierung in Batch-Dateien sowie im Capture- oder Credit-Request.
XID	an32	M	Vom Paygate vergebene ID für alle einzelnen Transaktionen (Autorisierung, Buchung, Gutschrift), die für eine Zahlung durchgeführt werden
TransID	ans..64	M	ID des Händlers zur Identifizierung des zu stornierenden Zahlungsvorgangs
MAC	an64	M	Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier: • HMAC-Authentisierung (Anfrage) • HMAC-Authentisierung (Notify)

Parameter zur Stornierung von Kreditkartenzahlungen über stationäre Terminals

Die folgende Tabelle beschreibt die Parameter, die das Paygate als Antwort zurückgibt:

es können jederzeit neue Parameter hinzugefügt bzw. die Reihenfolge geändert werden

die Parameter (z.B. MerchantId, RefNr) sollten nicht auf Groß-/Kleinschreibung geprüft werden

Key	Format	CND	Beschreibung

mid	ans..30	M	HändlerID, die von Computop vergeben wird
PayID	an32	M	Vom Paygate vergebene ID für die Zahlung; z.B. zur Referenzierung in Batch-Dateien sowie im Capture- oder Credit-Request.
TransID	ans..64	M	Transaktionsnummer des Händlers.
Status	a..50	M	OK (URLSuccess) oder FAILED (URLFailure)
Code	n8	M	Fehlercode gemäß Paygate Antwort-Codes (A4 Fehlercodes)

Ergebnis-Parameter bei Stornierung von Kreditkartenzahlungen über stationäre Terminals

PayNow

Silent Mode für Kreditkarten mit SSL und 3-D Secure-Verfahren

PayNow verbindet die Vorteile von Paygate-Formularen und Server-zu-Server-Verbindungen: Im Unterschied zum Paygate-Formular, wo durch den Aufruf von **payssl.aspx** das Formular vom Paygate-Server geladen wird, muss bei PayNow das Formular vom Händlersystem bereitgestellt werden. Das Formular verwendet dieselben Parameter, wie hier nachfolgend beschrieben.

Im Unterschied zum Paygate-Formular werden die Parameter nicht wie beim Aufruf der payssl.aspx als URL-Parameter übergeben, sondern als Formular-Eingabeparameter. Im Übrigen können beim Aufruf der PayNow.aspx die gleichen Parameter wie bei der PaySSL.aspx verwendet werden.

⚠ Bitte beachten Sie, dass der Aufruf der URLSuccess oder URLFailure bei einem Fallback zu 3-D Secure 1.0 mit GET stattfindet. Ihre Systeme sollten daher Parameter sowohl per GET als auch per POST entgegennehmen können.

Paygate-Formular	PayNow

payssl.aspx?MerchantID=[mid]&Len=[len]&Data=[data]	`<form action=paynow.aspx>`
	`  <input type="hidden" name="MerchantID" value=[mid]>`
	`  <input type="hidden" name="Len" value=[len]>`
	`  <input type="hidden" name="Data" value=[data]>`
	`  :`
	`</form>`

Die Kreditkartendaten müssen mit folgenden Parametern an paynow.aspx übermittelt werden:

Key	Format	CND	Beschreibung
CCNr	n..19	M	Kreditkartennummer für Kreditkarten-Zahlungen. Es kann wahlweise übergeben werden: • entweder die richtige Kreditkartennummer (PAN) • oder die Pseudokartennummer, welche Sie zuvor in einer Paygate-Antwort als PCNr erhalten haben. ℹ Mit 3-D Secure 2.x wird die CCNr (PAN oder PCNr) im card-JSON gesendet. ℹ Wir empfehlen die Verwendung der "Hosted Payment Page" oder des Kreditkartenformular (PaySSL) sowie Übergabe der PCNr zur vereinfachten PCI DSS Zertifizierung.
CCCVC	n3	O	Kartenprüfnummer: Die letzten 3 Ziffern auf dem Unterschriftsfeld der Kreditkarte
CCExpiry	n6	M	Ablaufdatum der Kreditkarte im Format YYYYMM, z.B. 201807
CCBrand	a..22	M	Kreditkartenmarke. Bitte beachten Sie die Schreibweise gemäß Tabelle der Kreditkartenmarken!

PayNow-Parameter für 3-D Secure-Verfahren

Nachdem der Kunde seine Kreditkartendaten eingegeben hat, werden die Zahlungsdaten an die PayNow-Seite übertragen, wo die weitere Zahlungsabwicklung inkl. 3- D Secure stattfindet. Die Formulardaten müssen direkt an die PayNow-Seite übertragen werden und dürfen nicht an das Händlersystem übermittelt werden! Auch dürfen keine PCI-relevanten Daten als zusätzliche Eingabeparameter an die PayNow-Seite übermittelt werden!

Batch-Nutzung der Schnittstelle

Grundsätzliche Informationen zur Arbeit mit Batch-Dateien sowie zu deren Aufbau erfahren Sie im separaten Handbuch zum Batchmanager. Im Batch-Verfahren sind nicht alle Funktionen verfügbar, die für die Online-Schnittstelle verfügbar sind.

Batch-Aufrufe und Antworten

Dieses Kapitel beschreibt die Parameter, die Sie im Datensatz (**Record**) für die Ausführung einer Kreditkartenzahlung übergeben müssen und welche Informationen Sie der Antwort-Datei über den Status des Zahlungsvorgangs entnehmen können.

Hinweis: Bitte beachten Sie die Reservierungs- / Autorisierungsfristen Ihres Acquirers (siehe AGBs), damit Sie als Händler sicherstellen, dass die Abbuchungen in der korrekten Frist an unserem Paygate eingereicht werden.

Hinweis: Im Batch-Verfahren sind nicht alle Funktionen der Online-Schnittstelle verfügbar.

Bei den Batch-Aufrufen ist die verwendete Batch-Version zu unterscheiden, wovon die optionalen Parameter abhängen. Alle mit „2.“ beginnen Versionsbezeichnungen betreffen Aufrufe für einen Konzern. Das bedeutet, innerhalb einer Batch-Datei mit einer bestimmten MerchantID können auch Transaktionen anderer Händler mit einer abweichenden Sub-MID übertragen werden.

Für die Anbindungen ECPCC, GMO, Kalixa und SafeCharge beschränken sich die möglichen Actions auf Capture, Credit und Reverse.

Folgende Tabelle gibt eine Übersicht der pro Aktion jeweils möglichen Batch-Versionen und ihrer Besonderheiten:

Action	Version	Beschreibung
Authorize	1.2 / 2.2	mit textfeld1, textfeld2, RTF, cardholder, transactionID, schemeReferenceID
	1.21 / 2.21	mit textfeld1, textfeld2, RTF, approvalcode, cardholder, transactionID, schemeReferenceID
	1.3 / 2.3	mit CVC, transactionID, schemeReferenceID
	1.5 / 2.5	mit CVC, Zone
Capture	1.2 / 2.2	mit textfeld1, textfeld2
	1.21 / 2.21	mit textfeld1, textfeld2, approvalcode
	1.4 / 2.4	mit Stopp der Autorisierungsverlängerung (FinishAuth)
CaptureEx	1.3 / 2.3	mit CVC
Credit	1.2 / 2.2	mit textfeld1, textfeld2
	1.21 / 2.21	mit textfeld1, textfeld2
	1.4 / 2.4	mit Stopp der Autorisierungsverlängerung (FinishAuth)
CreditEx	1.2 / 2.2	mit textfeld1, textfeld2
	1.21 / 2.21	mit textfeld1, textfeld2
	1.3 / 2.3	mit textfeld1, textfeld2
Sale	1.2 / 2.2	mit textfeld1, textfeld2, RTF, cardholder, transactionID, schemeReferenceID
	1.21 / 2.21	mit textfeld1, textfeld2, RTF, approvalcode, cardholder, transactionID, schemeReferenceID
	1.3 / 2.3	mit CVC, textfeld1, textfeld2, transactionID, schemeReferenceID
	1.5 / 2.5	mit CVC, Zone
Reverse	1.x / 2.x	Standardversion

Beschreibung der möglichen Batch-Versionen

Der Aufbau für eine Kreditkartenzahlung in einer einzureichenden Batch-Datei sieht folgendermaßen aus:

```
HEAD,<MerchantID>,<Date>,<Version>
CC,Authorize,<Amount>,<Currency>,<TransID>,(<RefNr>),<CCBrand>,<CCNr|PCNr>,[<CCCVC>],<CCExpiry>,
<OrderDesc>[,<textfeld1>,<textfeld2>,<RTF>,<approvalcode>,<cardholder>,<Zone>,<transactionID>,
<schemeReferenceID>]
CC,Capture,<Amount>,<Currency>,<TransID>,(<RefNr>),<PayID>,[<FinishAuth,<textfeld1>,<textfeld2>,
<approvalcode>]
CC,Sale,<Amount>,<Currency>,<TransID>,(<RefNr>),<CCBrand>,<CCNr|PCNr>,[<CCCVC>],<CCExpiry>,<OrderDesc>[,
<textfeld1>,<textfeld2>,<RTF>,<approvalcode>,<cardholder>,<Zone>,<transactionID>,<schemeReferenceID>]]
CC,Credit,<Amount>,<Currency>,<TransID>,(<RefNr>),<PayID>[,<FinishAuth>,<textfeld1>,<textfeld2>]
CC,CreditEx,<Amount>,<Currency>,<TransID>,(<RefNr>),<CCBrand>,<CCNr|PCNr>,[<CCCVC>],<CCExpiry>,
<OrderDesc>[,<textfeld1>,<textfeld2>]
CC,Reverse,<Amount>,<Currency>,<TransID>,(<RefNr>),<PayID>
FOOT,<CountRecords>,<SumAmount>
```

Beispiel für Batch-Versionen:

Version 1.2

```
CC,Sale,<Amount>,<Currency>,<TransID>,(<RefNr>),<CCBrand>,<CCNr|PCNr>,<CCExpiry>,<OrderDesc>
CC,Sale,<Amount>,<Currency>,<TransID>,(<RefNr>),<CCBrand>,<CCNr|PCNr>,<CCExpiry>,<OrderDesc>,<textfeld1>,
<textfeld2>,<RTF>,<cardholder>,<transactionID>,<schemeReferenceID>
```

Version 1.21

```
CC,Sale,<Amount>,<Currency>,<TransID>,(<RefNr>),<CCBrand>,<CCNr|PCNr>,<CCExpiry>,<OrderDesc>,<textfeld1>,
<textfeld2>,<RTF>,<approvalcode>,<cardholder>,<transactionID>,<schemeReferenceID>
```

Version 1.3

```
CC,Sale,<Amount>,<Currency>,<TransID>,(<RefNr>),<CCBrand>,<CCNr|PCNr>,<CCCVC>,<CCExpiry>,<OrderDesc>,
<textfeld1>,<textfeld2>,<transactionID>,<schemeReferenceID>
```

Version 1.5

```
CC,Sale,<Amount>,<Currency>,<TransID>,(<RefNr>),<CCBrand>,<CCNr|PCNr>,<CCCVC>,<CCExpiry>,<OrderDesc>,
<Zone>
```

Beispiel für Master-MID-Funktion:

```
HEAD,[Master]MerchantID,Date,2.x
Type,Action,[Slave]MID,Amount,Currency,TransID,Data (depends on Action)
FOOT,CountRecords,SumAmount
```

Die folgende Tabelle beschreibt die einzelnen Felder und Werte, die im Datensatz (Record) innerhalb der Batch-Datei verwendet werden:

Key	Format	CND	Beschreibung
Type	a..11	M	HEAD für Header, FOOT für Footer, CC für Kreditkarte
Action	a..20	M	Der Action-Parameter definiert die Art der Transaktion: Authorize (Autorisierung) Capture (Buchung)

			Sale (Verkauf) Credit (Gutschrift) CreditEx (Gutschrift ohne vorherige Buchung; bitte stimmen sie sich hierzu vorher mit dem **Computop Helpdesk** ab) Reverse (Storno)
Amount	n..10	M	Betrag in der kleinsten Währungseinheit (z.B. EUR Cent). Bitte wenden Sie sich an den Computop Helpdesk, wenn Sie Beträge < 100 (kleinste Währungseinheit) buchen möchten.
Currency	a3	M	Währung, drei Zeichen DIN / ISO 4217, z.B. EUR, USD, GBP. Hier eine Übersicht: A1 Währungstabelle
PayID	an32	M	Vom Paygate vergebene ID für die Zahlung; z.B. zur Referenzierung in Batch-Dateien sowie im Capture- oder Credit-Request.
TransID	ans..64	M	TransaktionsID, die für jede Zahlung eindeutig sein muss. Bitte beachten Sie bei einigen Anbindungen die abweichenden Formate, die bei den spezifischen Parametern angegeben sind.
RefNr	ns..30	O	Eindeutige Referenznummer des Händlers, welche als Auszahlungsreferenz in der entsprechenden Acquirer EPA-Datei angegeben wird. Bitte beachten Sie, ohne die Übergabe einer eigenen Auszahlungsreferenz können Sie die EPA-Transaktionen nicht zuordnen, zusätzlich kann das Computop Settlement File (CTSF) auch nicht zusätzlich angereichert werden. Es sind ausschließlich ASCII-Zeichen erlaubt. Sonderzeichen wie ("Umlaute", ...) sind nicht erlaubt und müssen ggf. durch ASCII-Zeichen ersetzt werden (z.B. ü ue, é e, ...).
OrderDesc	ans..127	O	Beschreibung der gekauften Waren, Einzelpreise etc.
CCBrand	a..22	C	Kreditkartenmarke. Bitte beachten Sie die Schreibweise gemäß Tabelle der Kreditkartenmarken!
CCNr	n..16	C	Kreditkartennummer mind. 12stellig numerisch ohne Leerzeichen. Optional können Sie auch eine Pseudokartennummer (PKN) übergeben
PCNr	n16	O	Pseudo Card Number: Vom Computop Paygate generierte Zufallszahl, die eine reale Kreditkartennummer repräsentiert. Die Pseudokartennummer (PKN) beginnt mit 0, und die letzten 3 Stellen entsprechen denen der realen Kartennummer. Die PKN kann wie eine Kreditkartennummer für Autorisierung, Buchung und Gutschriften verwendet werden. PCNr ist ein **Antwortwert** von Computop Paygate und kann ebenfalls als CCNr im Request oder als Teil von card-JSON verwendet werden.
CCExpiry	n6	OC	In Verbindung mit PCNr: Ablaufdatum der Kreditkarte im Format YYYYMM (202207).
CCCVC	n..4	O	Kartenprüfnummer in Version 1.3: Bei Visa und MasterCard die letzten 3 Ziffern auf dem Unterschriftsfeld der Kreditkarte. Bei American Express 4 Ziffern.
FinishAuth	ans1	O	Version=1.4: Wenn Sie die Autorisierungsverlängerung nutzen, stoppen Sie die Wiederholung mit dem Wert Y im Feld FinishAuth bei Capture oder Credit. Beispiel: Sie buchen eine Teillieferung. Der Rest der Bestellung ist nicht lieferbar. Daher übergeben Sie beim Capture der Teilbuchung im Feld FinishAuth Y, damit das **Paygate** den Restbetrag nicht wieder autorisiert. Beachten Sie dazu auch den folgenden Abschnitt zum **Stopp von Autorisierungsverlängerungen**.

Beschreibung der Felder im Datensatz von Batch-Dateien

Der Record-Bereich in der Antwort-Datei zu Batch-Transaktionen sieht folgendermaßen aus:

```
HEAD,<MerchantID>,<Date>,<Version>
CC,Authorize,<Amount>,<Currency>,<TransID>,(<RefNr>),<PayID>,<CCBrand>,<CCNr|PCNr>,[<CCCVC>],<CCExpiry>,
<OrderDesc>[,<textfeld1>,<textfeld2>,<RTF>,<approvalcode>,<cardholder>,<Zone>,<transactionID>,
<schemeReferenceID>],<Status>,<Code>
CC,Capture,<Amount>,<Currency>,<TransID>,(<RefNr>),<PayID>[<textfeld1>,<textfeld2>,<approvalcode>],
<Status>,<Code>
CC,AuthSplit,<Amount>,<Currency>,<TransID>,(<RefNr>),<PayID>,FAILED,<Code>,<Description>,[<PCNr>]
CC,Renewal,<Amount>,<Currency>,<TransID>,(<RefNr>),<PayID>,FAILED,<Code>,<Description>,[<PCNr>]
CC,Sale,<Amount>,<Currency>,<TransID>,(<RefNr>),<PayID>,<CCBrand>,<CCNr|PCNr>,[<CCCVC>],<CCExpiry>,
<OrderDesc>[,<textfeld1>,<textfeld2>,<RTF>,<approvalcode>,<cardholder>,<Zone>,<transactionID>,
<schemeReferenceID>],<Status>,<Code>
CC,Credit,<Amount>,<Currency>,<TransID>,(<RefNr>),<PayID>[,<FinishAuth>,<textfeld1>,<textfeld2>],
<Status>,<Code>
CC,CreditEx,<Amount>,<Currency>,<TransID>,(<RefNr>),<CCBrand>,<CCNr|PCNr>,[<CCCVC>],<CCExpiry>,
<OrderDesc>[,<textfeld1>,<textfeld2>],<Status>,<Code>
CC,Reverse,<Amount>,<Currency>,<TransID>,(<RefNr>),<PayID>,<Status>,<Code>
FOOT,<CountRecords>,<SumAmount>
```

Beispiel für Batch-Versionen:

Version 1.2

```
CC,Sale,<Amount>,<Currency>,<TransID>,(<RefNr>),<CCBrand>,<CCNr|PCNr>,<CCExpiry>,<OrderDesc>,<Status>,
<Code>
CC,Sale,<Amount>,<Currency>,<TransID>,(<RefNr>),<CCBrand>,<CCNr|PCNr>,<CCExpiry>,<OrderDesc>,<textfeld1>,
<textfeld2>,<RTF>,<cardholder>,<transactionID>,<schemeReferenceID>,<Status>,<Code>
```

Version 1.21

```
CC,Sale,<Amount>,<Currency>,<TransID>,(<RefNr>),<CCBrand>,<CCNr|PCNr>,<CCExpiry>,<OrderDesc>,<textfeld1>,
<textfeld2>,<RTF>,<approvalcode>,<cardholder>,<transactionID>,<schemeReferenceID>,<Status>,<Code>
```

Version 1.3

```
CC,Sale,<Amount>,<Currency>,<TransID>,(<RefNr>),<CCBrand>,<CCNr|PCNr>,<CCCVC>,<CCExpiry>,<OrderDesc>,
<textfeld1>,<textfeld2>,<transactionID>,<schemeReferenceID>,<Status>,<Code>
```

Version 1.5

```
CC,Sale,<Amount>,<Currency>,<TransID>,(<RefNr>),<CCBrand>,<CCNr|PCNr>,<CCCVC>,<CCExpiry>,<OrderDesc>,
<Zone>,<Status>,<Code>
```

Die folgende Tabelle beschreibt die Antwort-Parameter, die der Batch-Manager im Record-Bereich zu jeder Transaktion speichert (hier nicht erklärte Standardparameter wie etwa <TransID> oder <RefNR> und Aufrufparameter werden unverändert zum Aufruf wieder zurückgegeben und sind vorstehend beschrieben):

Key	Format	CND	Beschreibung
Action	a..20	M	Der Action-Parameter definiert die Art der Transaktion wie Capture (Buchung) oder Credit (Gutschrift) – siehe oben.
PayID	an32	M	Vom Paygate vergebene ID für die Zahlung; z.B. zur Referenzierung in Batch-Dateien sowie im Capture- oder Credit-Request.
Status	a..50	M	OK oder FAILED
Code	n8	M	Fehlercode gemäß Paygate Antwort-Codes (A4 Fehlercodes)
PCNr	n16	O	Pseudo Card Number: Vom Computop Paygate generierte Zufallszahl, die eine reale Kreditkartennummer repräsentiert. Die Pseudokartennummer (PKN) beginnt mit 0, und die letzten 3 Stellen entsprechen denen der realen Kartennummer. Die PKN kann wie eine Kreditkartennummer für Autorisierung, Buchung und Gutschriften verwendet werden. PCNr ist ein **Antwortwert** von Computop Paygate und kann ebenfalls als CCNr im Request oder als Teil von card-JSON verwendet werden.

Beschreibung der Ergebnis-Parameter im Datensatz von Batch-Dateien

Stopp von Autorisierungsverlängerungen

Mit einer Kreditkartenautorisierung erwerben Sie einen Zahlungsanspruch. Allerdings verfällt eine Autorisierung nach spätestens 30 Tagen oder auch, wenn Sie einen Teilbetrag buchen, zum Beispiel weil mehrere Teillieferungen nötig sind. Um Ihren Zahlungsanspruch in solchen Fällen wiederherzustellen, kann das Paygate eine verfallene Autorisierung automatisch wiederholen.

Falls eine Bestellung nicht lieferbar ist oder vom Kunden storniert wurde, ist es **sehr wichtig**, dass Sie die automatischen Autorisierungen stoppen. Andernfalls wird das Kartenlimit Ihres Kunden dauerhaft reduziert, weil das Paygate die Karte Ihres Kunden immer wieder neu belastet.

Im Normalfall stoppt das Paygate die Autorisierungsverlängerung, wenn der autorisierte Betrag komplett gebucht wurde. Sie können die Autorisierungsverlängerung in der Batch-Version 1.4 aber auch manuell stoppen, indem Sie den Zahlungsstatus ändern. Zu diesem Zweck reichen Sie in Ihrer Batch-Datei eine Buchung ein, deren Betrag unter dem zulässigen Limit liegt. Da das Paygate Kreditkartenbuchungen unter 1,00 Euro ablehnt, ändert sich der Zahlungsstatus bei geringeren Beträgen auf FAILED. Das Paygate wird diese Autorisierung deshalb nicht weiter verlängern. Ein entsprechender Capture-Eintrag mit 0,05 EUR sieht beispielsweise so aus:

```
CC,Capture,5,EUR,BestNr.0815,Rg.Nr.5180,a86dga4310d24453acd6f8a3112a769,y
```

Da der Betrag von 5 Cent unter dem Mindestbetrag von 1,00 Euro liegt, lehnt das Paygate die Buchung mit der Fehlermeldung MinValue ab. Die Zahlung erhält dann den Status FAILED, so dass die Autorisierungsverlängerung gestoppt wird.