Betrugsprävention

- Über Betrugsprävention mit IP-Tracking
  - Allgemeines zur Betrugsprävention
- Zusatzparameter für Betrugsprävention
  - Definitionen
  - Zusatzparameter bei Aufruf der Paygate Kreditkarten-Schnittstelle
  - Aufruf der Schnittstelle zur Bearbeitung einer Blacklist
    - BlackListInfo

Über Betrugsprävention mit IP-Tracking

Allgemeines zur Betrugsprävention

Das Paygate unterstützt verschiedene Verfahren zur Betrugsprävention. Dazu zählen die Anfrage bei Auskunfteien, die Kontrolle des Kartenherkunftslandes sowie Zahlungsgarantien für Kreditkarten.

Paygate

Ein Großteil aller Betrugsversuche kommt aus dem Ausland. Das kann das Herkunftsland und oft sogar die Stadt der IP-Adresse prüfen, die Ihr Kunde gerade nutzt. Wenn das Herkunftsland der IP-Adresse Ihres Kunden nicht Ihren Lieferländern entspricht oder nicht zum Land der Kreditkarte passt, kann das Paygate eine Warnung per E-Mail verschicken oder die Zahlung automatisch ablehnen.

Zudem finden 75% aller Betrugsversuche mit ausländischen Kreditkarten statt. Das Paygate kann deshalb die Kartenherkunft prüfen: Wenn Sie das Lieferland als Parameter übergeben, gibt das Paygate das Herkunftsland von Visa- und MasterCard-Kreditkarten zurück und sendet eine E-Mail, falls das Lieferland von der Kartenherkunft abweicht. Sie sollten dann dem Kunden erklären, warum das Kartenherkunftsland vom Lieferland abweicht, um Betrug zu vermeiden. Optional kann das Paygate solche Zahlungen sofort ablehnen.

Zusatzparameter für Betrugsprävention

Definitionen

Datenformate:

Format	Beschreibung
a	alphabetisch
as	alphabetisch mit Sonderzeichen
n	numerisch
an	alphanumerisch
ans	alphanumerisch mit Sonderzeichen
ns	numerisch mit Sonderzeichen
bool	Bool'scher Ausdruck (true oder false)
3	feste Länge mit 3 Stellen/Zeichen
..3	variable Länge mit maximal 3 Stellen/Zeichen
enum	Aufzählung erlaubter Werte
dttm	ISODateTime (JJJJ-MM-TTThh:mm:ss)

Abkürzungen:

Abkürzung	Beschreibung	Kommentar
CND	Bedingung (condition)	

M	Pflicht (mandatory)	Wenn ein Parameter Pflicht ist, dann muss er vorhanden sein
O	optional	Wenn ein Parameter optional ist, dann kann er vorhanden sein, ist aber nicht erforderlich
C	bedingt (conditional)	Wenn ein Parameter bedingt ist, dann gibt es eine Bedingungsregel, die angibt, ob er Pflicht oder optional ist

Hinweis: Bitte beachten Sie, dass die Bezeichnungen der Parameter in Groß- oder Kleinbuchstaben zurückgegeben werden können.

Zusatzparameter bei Aufruf der Paygate Kreditkarten-Schnittstelle

Die Betrugsprävention per IP-Tracking betrifft die Kreditkarten VISA und MasterCard über die Paygate-Schnittstellen payssl.aspx, paynow.aspx sowie direct.aspx.

Bezüglich der allgemeinen und sonstigen speziellen Parameter für die Ausführung einer Kreditkartenzahlung über die Schnittstellen payssl.aspx, paynow.aspx sowie direct.aspx beachten Sie bitte das Handbuch für Kreditkarten.

Hinweis: Die Funktionen der Betrugsprävention sind standardmäßig nicht freigeschaltet. Der Computop Vertrieb kann diese Funktionen bei Bedarf gerne für Sie freischalten.

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
IPAddr	ans..15	O	IP-Adresse. Damit kann das Paygate ermitteln, in welchem Land und welcher Stadt Ihr Kunde mit dem Internet verbunden ist (vgl. IPZone). Format 123.456.789.012
IPZone	ans..1100	O	Codes der Länder, aus denen Sie Bestellungen akzeptieren, dreistellig numerisch gemäß ISO 3166-1. Mehrere Länder durch Kommata trennen: **036,040,124**. Wenn Sie Länder in **IPZone** übergeben, prüft das Paygate, aus welchem Land die IP-Adresse Ihres Kunden stammt, ob es in Ihrer Länderliste enthalten ist und ob es mit dem Land der Kreditkarte (s.u.) übereinstimmt. Das Paygate übergibt das IP-Land auch an Ihren Shop (s.u.). Wenn das IP-Land nicht in Ihrer Liste ist oder nicht zur Kreditkarte passt, kann das Paygateeine Warnung per E-Mail senden oder Zahlungen ablehnen.
Zone	ans..1100	O	Codes der Länder, in denen Sie Kreditkarten akzeptieren, dreistellig numerisch oder alphanumerisch gemäß ISO 3166.1. Mehrere Länder durch Kommata trennen: 036,040,124. Wenn Sie Länder in Zone übergeben, prüft das Paygate, aus welchem Land die Kreditkarte (MasterCard, Visa) Ihres Kunden stammt und ob es in Ihrer Länderliste enthalten ist. Das Pay gate übergibt das Kartenland auch an Ihren Shop (s.u.). Wenn das Kartenland nicht in Ihrer Liste ist oder nicht zur IP-Adresse des Kunden passt, kann das Paygate eine Warnung per E-Mail senden oder Zahlungen ablehnen. Um Karten aus bestimmten Ländern abzulehnen (Negativliste), geben Sie vor dem Ländercode ein Ausrufezeichen an: !036,!040,!124. Bitte beachten Sie die Längenbegrenzung auf max. 1100 Zeichen.

Zusatzparameter für Betrugsprävention bei 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	Format	CND	Beschreibung
Zone	a..7	O	Falls bei der Anfrage Ländercodes in **Zone** übergeben wurden, gibt das Paygate den Ländercode der Kreditkarte oder "UNKNOWN" zurück
IPZone	a..7	O	Falls bei der Anfrage IP-Länder in **IPZone** übergeben wurden, gibt das Paygate den Ländercode der IP-Adresse oder "UNKNOWN" zurück
IPZoneA2	a..7	O	Falls bei der Anfrage **IPZone** übergeben wurde, gibt das Paygate den zweistelligen Ländercode der IP-Adresse oder "UNKNOWN" zurück (DE=Deutschland, FR=Frankreich etc.)
IPState	a..32	O	Falls bei der Anfrage **IPZone** übergeben wurde, gibt das Paygate das Bundesland zurück, aus der die IP-Adresse Ihres Kunden stammt
IPCity	a..32	O	Falls bei der Anfrage **IPZone** übergeben wurde, gibt das Paygate die Stadt zurück, aus der die IP-Adresse Ihres Kunden stammt

IPLongitude	n..20	O	Falls bei der Anfrage **IPZone** übergeben wurde, gibt das Paygate den geographischen Längengrad (Fließkomma, dezimal) des Internet-Einwahlknotens Ihres Kunden zurück
IPLatitude	n..20	O	Falls bei der Anfrage **IPZone** übergeben wurde, gibt das Paygate den geographischen Breitengrad (Fließkomma, dezimal) des Internet-Einwahlknotens Ihres Kunden zurück
fsStatus	ans..9	OC	Nur über direct.aspx, nur bei EVO Payments International: ACCEPT=Kein Verdacht auf Kartenbetrug, DENY=Abweisen empfohlen, CHALLENGE=Prüfung empfohlen, NOSCORE= keine Risikobewertung, ENETFP=Ausnahmefehler im Netzwerk, ERROR=Fehler im Rechenzentrum, ETMOUT=Timeout
fsCode	n4	OC	Nur über direct.aspx, nur bei EVO Payments International: Handlungsempfehlung: <0000> keine Bewertung, <0100> annehmen, <0150> immer annehmen, <0200> ablehnen, <0250> immer ablehnen, <0300> verdächtig, <0330> überprüfen, <0400> verdächtig ReD-Blacklist, <0500> fragwürdig, <0600> fragwürdig ReD-Blacklist, <0700> Schwellwert überschritten, <0800> ungewöhnliches Nutzungsmuster, <901> interner ebitGuard-Fehler, <902> Formatfehler

Zusätzliche Ergebnisparameter für Betrugsprävention bei Kreditkartenzahlungen

Aufruf der Schnittstelle zur Bearbeitung einer Blacklist

Um einen Blacklist-Eintrag über eine Server-zu-Server-Verbindung anzulegen, zu lesen, zu aktualisieren oder zu löschen, rufen Sie folgende URL auf:

https://www.computop-paygate.com/BlackList.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.
MAC	an64	M	Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier: • HMAC-Authentisierung (Anfrage) • HMAC-Authentisierung (Notify)
EventToken	enum	M	Abkürzung der auszuführender Aktion: <Create>, <Read>, <Update> oder <Delete>
BlackListInfo	ans..1024	M	Information über den Blacklist-Eintrag als JSON-String im Base64-Format. Siehe Tabelle BlackListInfo unten.

Key	Format	CND	Description	Beschreibung
MAC	an64	M	Hash Message Authentication Code (HMAC) with SHA-256 algorithm. Details can be found here: • HMAC Authentication (Request) • HMAC Authentication (Notify)	Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier: • HMAC-Authentisierung (Anfrage) • HMAC-Authentisierung (Notify)

Key	Format	CND	Description	Beschreibung
EventToken	enum	M	Abbreviation of the action to be done: <Create>, <Read>, <Update> or <Delete>	Abkürzung der auszuführender Aktion: <Create>, <Read>, <Update> oder <Delete>
BlackListInfo	ans..1024	M	Information about the blacklist entry as JSON string in the Base64 format. See table BlackListInfo below.	Information über den Blacklist-Eintrag als JSON-String im Base64-Format. Siehe Tabelle BlackListInfo unten.

Parameter für Aufruf der Blacklist-Bearbeitung

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
MAC	an64	M	Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier: • HMAC-Authentisierung (Anfrage) • HMAC-Authentisierung (Notify)
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!
BlackListInfo	ans..1024	C	Information über den Blacklist-Eintrag als JSON-String im Base64-Format, wenn Status=OK. Siehe Tabelle BlackListInfo unten.

Key	Format	CND	Description	Beschreibung
MAC	an64	M	Hash Message Authentication Code (HMAC) with SHA-256 algorithm. Details can be found here: • HMAC Authentication (Request) • HMAC Authentication (Notify)	Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier: • HMAC-Authentisierung (Anfrage) • HMAC-Authentisierung (Notify)

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

Key	Format	CND	Description	Beschreibung
Description	ans..1024	M	Further details in the event that payment is rejected. Please **do not** use the **Description but** the Code parameter for the transaction status analysis!	Nähere Beschreibung bei Ablehnung der Zahlung. Bitte nutzen Sie **nicht** den Parameter **Description, sondern** Code für die Auswertung des Transaktionsstatus!

Key	Format	CND	Description	Beschreibung
BlackListInfo	ans..1024	C	Information about the blacklist entry as JSON string in the Base64 format, if Status=OK. See table BlackListInfo below.	Information über den Blacklist-Eintrag als JSON-String im Base64-Format, wenn Status=OK. Siehe Tabelle BlackListInfo unten.

Ergebnisparameter für Aufruf der Blacklist-Bearbeitung

BlackListInfo

Folgende Tabelle beschreibt das Objekt BlackListInfo für EventToken Insert:

Key	Format	CND	Beschreibung
Category	enum	M	Kategorie <EDD> für Lastschrift oder <CC> für Kreditkarte
Number	ans..64	M	IBAN, wenn Category=EDD Kreditkartennummer, wenn Category=CC
BIC	ans..32	C	BIC, wenn Category=EDD

Parameter für Blacklist-Bearbeitung, EventToken Insert

Folgende Tabelle beschreibt das Objekt BlackListInfo für EventToken Update:

Key	Format	CND	Beschreibung
BlockID	an..32	M	Eindeutige BlockID
LockActive	bool	M	Definiert, ob der Eintrag gesperrt werden soll oder nicht. Gesperrt: <True> Entsperrt: <False>

Parameter für Blacklist-Bearbeitung, EventToken Update

Folgende Tabelle beschreibt das Objekt BlackListInfo für EventToken Delete:

Key	Format	CND	Beschreibung
BlockID	an..32	M	Eindeutige BlockID

Parameter für Blacklist-Bearbeitung, EventToken Delete

Folgende Tabelle beschreibt das Objekt BlackListInfo, das das Paygate als Antwort zurückgibt:

Key	Format	CND	Beschreibung
BlockID	an..32	M	Eindeutige BlockID
mid	ans..30	M	HändlerID, die von Computop vergeben wird
Category	enum	M	Kategorie <EDD> für Lastschrift oder <CC> für Kreditkarte
Number	ans..64	M	IBAN, wenn Category=EDD Kreditkartennummer, wenn Category=CC
BIC	ans..32	C	BIC, wenn Category=EDD
MAC	an64	M	Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier: • HMAC-Authentisierung (Anfrage) • HMAC-Authentisierung (Notify)
LockActive	bool	M	Definiert, ob der Eintrag gesperrt werden soll oder nicht. Gesperrt: <True> Entsperrt: <False>
Created	dttm	M	Zeit des Anlegens (YYYY-MM-DD hh:mm:ss)
Changed	dttm	M	Zeit der Änderung (YYYY-MM-DD hh:mm:ss)

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

Key	Format	CND	Description	Beschreibung
Category	enum	M	Category <EDD> for direct debit or <CC> for credit card	Kategorie <EDD> für Lastschrift oder <CC> für Kreditkarte
Number	ans..64	M	IBAN, if Category=EDD Credit card number, if Category=CC	IBAN, wenn Category=EDD Kreditkartennummer, wenn Category=CC
BIC	ans..32	C	BIC, if Category=EDD	BIC, wenn Category=EDD

Key	Format	CND	Description	Beschreibung
MAC	an64	M	Hash Message Authentication Code (HMAC) with SHA-256 algorithm. Details can be found here: • HMAC Authentication (Request) • HMAC Authentication (Notify)	Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier: • HMAC-Authentisierung (Anfrage) • HMAC-Authentisierung (Notify)

Key	Format	CND	Description	Beschreibung
LockActive	bool	M	Defines, if the entry should by blocked or not. Blocked: <True> Unlocked: <False>	Definiert, ob der Eintrag gesperrt werden soll oder nicht. Gesperrt: <True> Entsperrt: <False>

Created	dttm	M	Time of creation (YYYY-MM-DD hh:mm:ss)	Zeit des Anlegens (YYYY-MM-DD hh:mm:ss)
Changed	dttm	M	Time of modification (YYYY-MM-DD hh:mm:ss)	Zeit der Änderung (YYYY-MM-DD hh:mm:ss)

Ergebnisparameter für Blacklist-Bearbeitung