



Payment Services

# Merchant Plug-In



## Spezifikation

Version 3.2



## Inhaltsverzeichnis

1	Einleitung.....	3
1.1	Zusammenfassung .....	3
1.2	Voraussetzungen .....	4
1.3	Teilnahme und Ergebnis der Authentifizierung .....	4
1.4	Haftungsumkehr und Risiken .....	5
1.5	Datensicherheit und PCI DSS .....	5
1.6	Formatangaben .....	5
2	Saferpay Payment Page und Merchant Plug-In .....	6
2.1	Übersicht .....	6
2.2	Prozessbeschreibung.....	7
2.3	Schnittstelle.....	8
3	Saferpay Authorization Interface und Merchant Plug-In.....	9
3.1	Übersicht .....	9
3.2	Prozessbeschreibung.....	10
4	Merchant Plug-In Schnittstellenbeschreibung.....	11
4.1	Abwicklung.....	11
4.2	Schritt 1: VerifyEnrollmentRequest.....	12
4.3	Schritt 2: Verify EnrollmentResponse.....	13
4.4	Schritt 3: Authentifizierung des Karteninhabers .....	14
4.5	Schritt 4: Prüfung der Authentifizierungsantwort.....	14
4.6	Schritt 5: Autorisationsanfrage .....	15
4.7	Schritt 6: Autorisationantwort .....	15
5	Saferpay Testkonto.....	16
6	Beispiele .....	17
6.1	Wichtiger Hinweis .....	17
6.2	C# mit der .NET LIB .....	17
6.3	Kommandozeilenaufrufe mit der Java LIB .....	19
6.4	Verwendung des https Interface.....	22
7	Kontakt.....	25
7.1	Saferpay Integration Team .....	25
7.2	Saferpay Support Team.....	25

## 1 Einleitung

Dieses Dokument beschreibt das „Saferpay Merchant Plug-In“ (MPI), das für 3-D Secure Transaktionen benötigt wird. Das MPI kann sowohl mit der Payment Page (PP), als auch in Kombination mit dem Saferpay Authorization Interface (AI) verwendet werden.

Das MPI wird für die Verfahren „Verified by Visa“ und „MasterCard SecureCode“ eingesetzt. Händler, die das 3-D Secure Verfahren anbieten, profitieren von der erhöhten Sicherheit bei der Kreditkartenakzeptanz und weniger Zahlungsausfällen durch die Haftungsumkehr („Liability Shift“). Es ist dabei nicht von Bedeutung, ob die Karteninhaber (KI) an dem Verfahren teilnehmen oder nicht.

### 1.1 Zusammenfassung

Das 3-D Secure Verfahren kann ausschließlich für Zahlungen im Internet eingesetzt werden. Der KI muss, sofern er an den Verfahren teilnimmt, sich während der Zahlung gegenüber seiner kartenausgebenden Bank (Issuer) ausweisen.

Zahlungen, die der Händler mit 3-D Secure abwickelt, sind speziell zu kennzeichnen. Nur wenn die entsprechenden Merkmale mit der Autorisation an die Kreditkartengesellschaft gesendet werden, gilt die Haftungsumkehr.

Das Saferpay MPI unterstützt die notwendigen Interaktionen und den sicheren Datenaustausch zwischen den beteiligten Systemen. Die Authentifizierung des KI erfolgt über ein Webformular, das der Issuer oder ein von ihm beauftragter Dienstleister hostet. Für eine 3-D Secure Authentifizierung benötigt der KI daher zwingend einen Internet Browser.

1. Der Händler sendet die Kreditkartendaten zusammen mit den relevanten Zahlungsdaten an Saferpay.
2. Saferpay prüft ob der KI an dem 3-D Secure Verfahren teilnimmt oder nicht. Nimmt er teil, muss er sich gegenüber seiner Bank authentifizieren. Falls nicht, wird die Zahlung ohne Authentifizierung durchgeführt.
3. Über den Internet Browser des KI wird die 3-D Secure Anfrage an die kartenausgebende Bank weitergeleitet. Der KI muss sich mit einem Passwort, Zertifikat oder einer anderen Methode ausweisen.
4. Das Ergebnis dieser Überprüfung (Authentifizierung) wird über den Internet Browser des Kunden zurück an Saferpay gesendet.
5. Saferpay prüft das Resultat und stellt sicher, dass keine Manipulation vorliegt. Die Zahlung kann fortgeführt werden, wenn die Authentifizierung erfolgreich verlaufen ist. Andernfalls wird die Zahlung mit dieser Karte abgebrochen.
6. Das Saferpay MPI liefert die notwendigen 3-D Secure Kennzeichen für die Autorisation der Kreditkartenzahlung zurück.

## 1.2 Voraussetzungen

Das Saferpay MPI kann sowohl über die Saferpay Client Library (LIB) für Java oder .NET, als auch über das Saferpay https Interface (HI) gesteuert werden.

Das Saferpay MPI muss für den Händler separat eingerichtet und aktiviert werden. Wichtig ist dabei die Registrierung des Händlers bei den teilnehmenden Kreditkartengesellschaften, die das Saferpay Team automatisch durchführt.

Eine passende Saferpay Lizenz- und Dienstleistungsvereinbarung wird vorausgesetzt.

Folgende Varianten stehen für den Einsatz des MPI zur Auswahl:

- Nutzung über die Saferpay Payment Page (PP) oder
- Nutzung in Kombination mit dem Saferpay Authorization Interface (AI)

### **Vertragliche Vereinbarung zwischen der Kreditkartengesellschaft und dem Händler:**

- Vertrag mit dem Acquirer über die Abwicklung von 3-D Secure Zahlungen "Verified by Visa" und / oder "MasterCard SecureCode". Bitte beachten Sie die Konditionen und Weisungen zur Haftungsumkehr!
- Die 3-D Secure Logos oder Trademarks sind auf der Web-Seite des Händlers, je nach Vereinbarung, anzuzeigen.

### **Webshop und Trademarks:**

- Beim Einsatz der Saferpay Payment Page muss sich der Händler nicht um die 3-D Secure Logos kümmern. Die notwendigen Symbole und Logos werden angezeigt, sobald das Saferpay MPI aktiviert wurde.
- Bei Nutzung des AI hat der Händler für die korrekte Anzeige der Logos oder Trademarks auf seiner Webseite zu sorgen. Bitte kontaktieren Sie Ihre Kreditkartengesellschaft, um weitere Details zu erfahren.

## 1.3 Teilnahme und Ergebnis der Authentifizierung

Für eine 3-D Secure Zahlung gibt es zwei Kennzeichnungsmöglichkeiten:

- I. Eine Zahlung mit erfolgter Authentifizierung des KI, in diesem Fall wird die Karte als „enrolled“ bezeichnet oder
- II. der KI nimmt an dem Verfahren nicht teil und die Zahlung wird als Karte „not enrolled“ gekennzeichnet.

Im Falle einer erfolgten Authentifizierung des KI muss bei der Autorisationsanfrage die MPI\_SESSIONID mitgesendet werden. Saferpay vervollständigt dann anhand der MPI\_SESSIONID die anderen, von der Kreditkartengesellschaft noch benötigten 3-D Secure Zahlungsdaten. Die MPI\_SESSIONID wird bei der VerifyEnrollment-Anfrage generiert und mit der Antwort übermittelt.

## 1.4 Haftungsumkehr und Risiken

An dieser Stelle möchten wir Sie als E-Commerce Händler darauf hinweisen, dass Sie sich an die Vereinbarungen und besonderen Regeln der Kreditkartengesellschaften halten müssen, um von der Haftungsumkehr profitieren zu können. Die Haftungsumkehr stellt keine Zahlungsgarantie dar, sondern unterliegt der Definition der Kreditkartengesellschaften.



**Es ist zwingend notwendig, dass die MPI\_SESSIONID bei der Autorisationsanfrage mitgesendet wird. Sollte diese Angabe fehlen oder den falschen Inhalt haben, entfällt die Haftungsumkehr!**



Falls Sie sich nicht sicher sind, welche Regeln oder Verfahrensweisen im Zusammenhang mit der Haftungsumkehr gelten, fragen Sie bitte Ihren Acquirer nach weiteren Details. Die vertraglichen Richtlinien für die Haftungsumkehr können sich zukünftig ändern.

SIX Card Solutions garantiert nicht für Zahlungen, Ansprüche oder Forderungen, auch werden keine technischen oder finanziellen Risiken abgedeckt. Die Risiken der Kartenakzeptanz werden nicht von SIX Card Solutions übernommen und sind nicht Bestandteil der angebotenen Dienste.

## 1.5 Datensicherheit und PCI DSS

Die Kreditkartenorganisationen haben das Sicherheitsprogramm PCI DSS (Payment Card Industry Data Security Standard) ins Leben gerufen, um Betrug mit Kreditkarten und deren Missbrauch vorzubeugen.

Bitte beachten Sie bei der Gestaltung des Zahlungsprozesses und dem Einsatz des Saferpay MPI die PCI DSS Richtlinien. Zusammen mit dem optionalen Dienst „Saferpay Secure Card Data“ können Sie die Zahlungsprozesse so sicher gestalten, dass keine Kreditkartennummern auf Ihren (Web)Servern verarbeitet, weitergeleitet oder gespeichert werden. Für weitere Informationen können Sie uns gerne kontaktieren.

## 1.6 Formatangaben

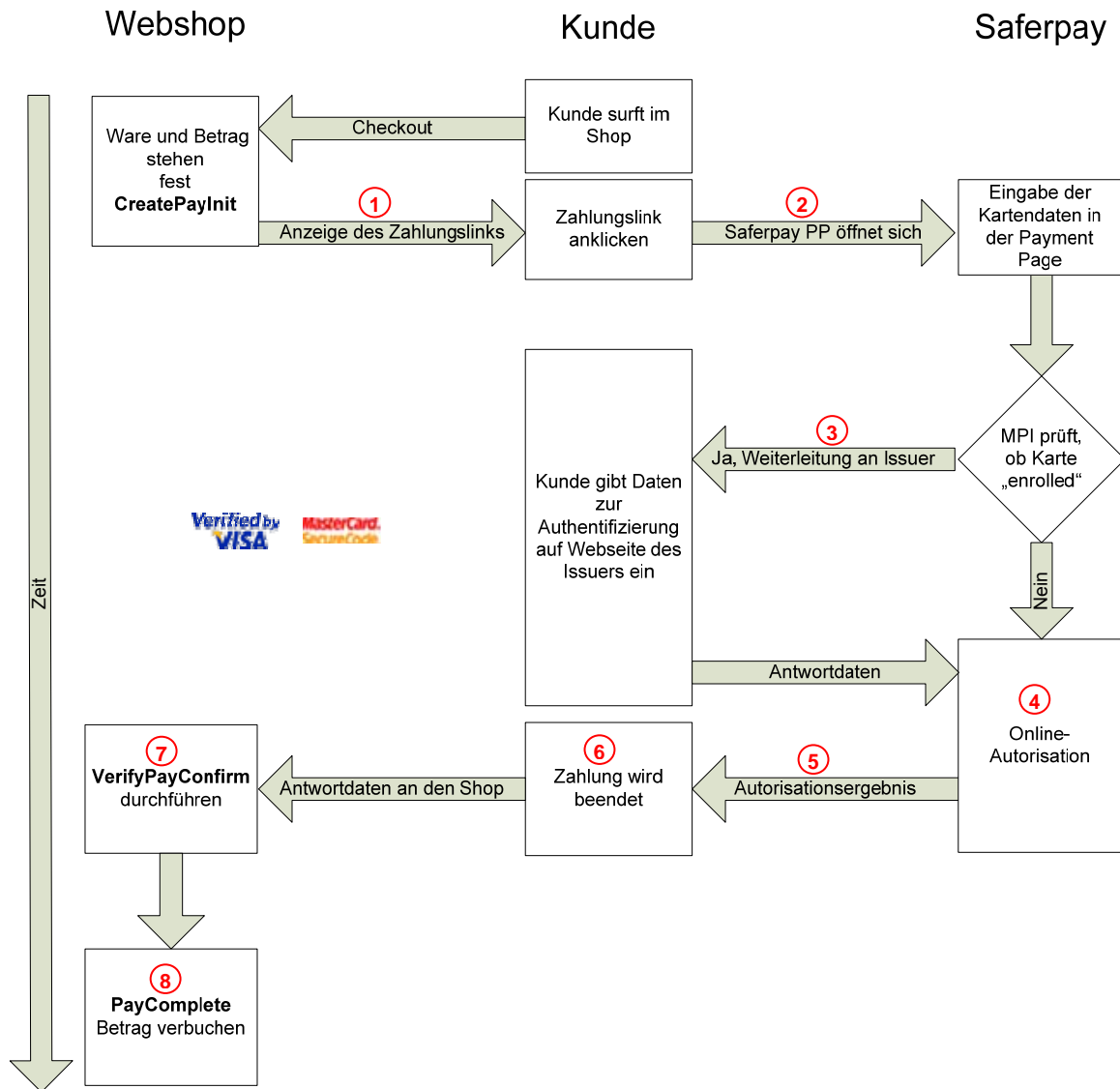
Folgende Abkürzungen für die Formatangaben werden in diesem Dokument verwendet:

- a Buchstaben (a - z, A - Z)
- n numerische Zeichen (0 - 9)
- an alphanumerische Zeichen (a - z, A - Z, 0 - 9)
- s Sonderzeichen (- ; / \ < > . =)
- ans alphanumerische und Sonderzeichen

## 2 Saferpay Payment Page und Merchant Plug-In

### 2.1 Übersicht

Die folgende Grafik zeigt den Ablauf einer Online Zahlung mit 3-D Secure-Verarbeitung über die Saferpay Payment Page:



## 2.2 Prozessbeschreibung

### Phase 1 – Angebot und Zahlungslink

- ① Sobald der Zahlungsbetrag feststeht kann der Webshop den Zahlungslink erzeugen (CreatePayInit). Beispielsweise könnte im Webshop auf der Bestellbestätigung der Zahlungslink in Form eines „Bezahlen“ Buttons dargestellt werden.
- ② Der Kunde klickt auf den „Bezahlen“ Button oder Link und die Saferpay Payment Page öffnet sich.

### Phase 2 – Überprüfung Karteninhaber

- ③ Der Kunde wählt die Kreditkarte für die Zahlungsabwicklung und gibt seine Kreditkartendaten ein. Falls der KI am 3-D Secure Verfahren teilnimmt, wird er an seine kartenausgebende Bank zur Authentifizierung weitergeleitet.

### Phase 3 – Autorisation

- ④ Nach erfolgreicher Authentifizierung des KI wird die Online Autorisation der Kreditkartenzahlung durchgeführt.
- ⑤ Saferpay zeigt das Ergebnis der Autorisation an .
- ⑥ Der Einkauf ist abgeschlossen, wenn die Payment Page geschlossen und der Kunde zum Webshop zurückgeleitet wurde.
- ⑦ Das Händlersystem prüft die Zahlungsbestätigung (VerifyPayConfirm) und speichert sie zusammen mit den Auftragsinformationen ab.

### Phase 4 – Buchung

- ⑧ Der Betrag wird verbucht (PayComplete).

Anmerkung: Das Verbuchen ist für den Tagesabschluss obligatorisch. Dieser berücksichtigt nur Transaktionen mit dem Status „Buchung“ und leitet diese zur Auszahlung an die Händlerbank weiter. Das Geld wird in Form einer Sammelposition dem Geschäftskonto des Händlers gutgeschrieben. Von der Kreditkartengesellschaft erhält der Händler eine Abrechnungsliste.

Der Tagesabschluss kann manuell oder automatisch ausgelöst werden.

## 2.3 Schnittstelle

Neben den üblichen PayConfirm Feldern werden bei 3-D Secure Zahlungen zusätzlich folgende Parameter zurückgeliefert:

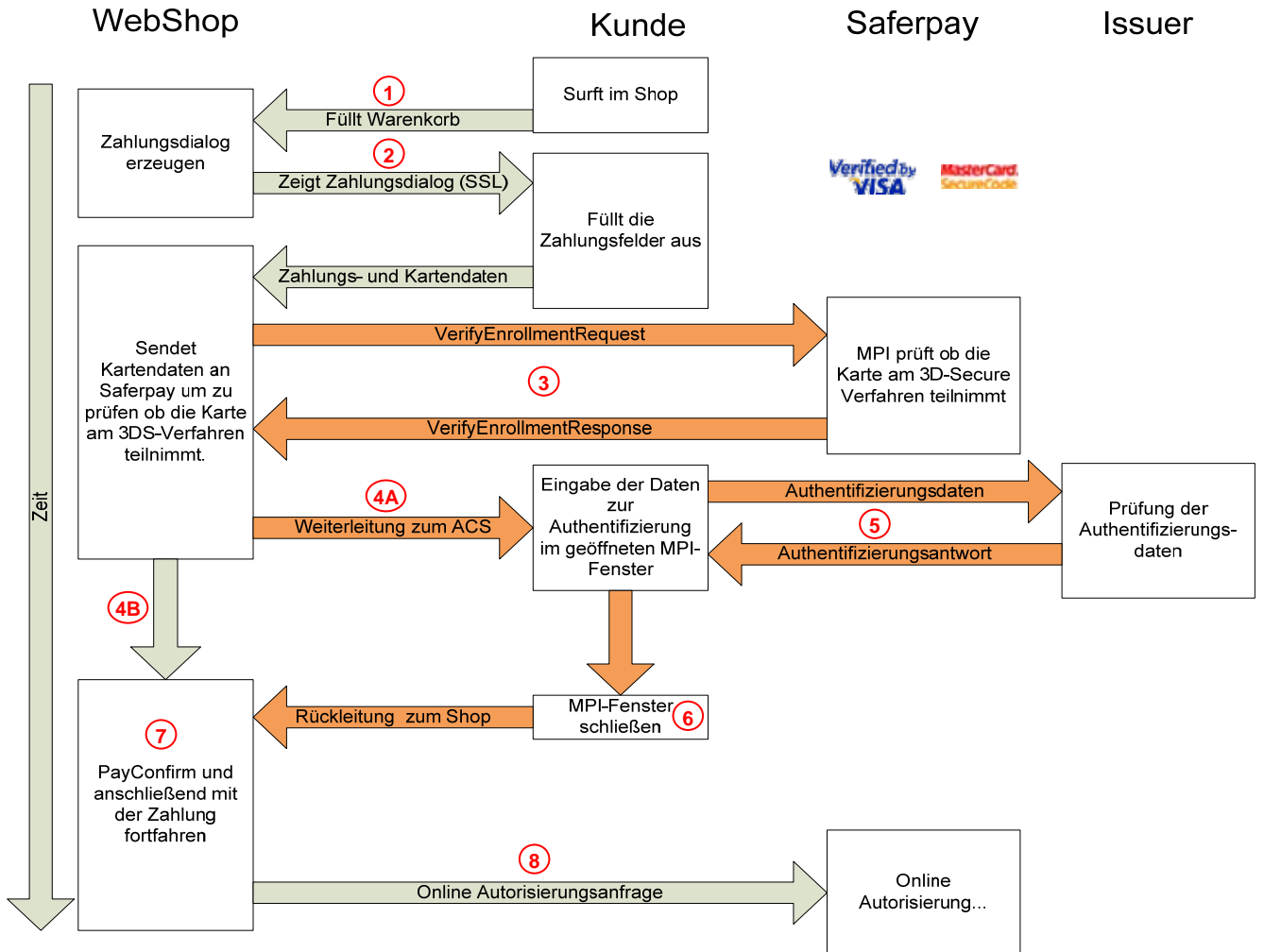
Parameter	Format	Beschreibung
MPI_SESSIONID	an[28]	Die Referenz auf die 3-D Secure Session. Diese Session-ID wird vom MPI generiert.
MPI_LIABILITYSHIFT	an[..3]	Zeigt dem Händlersystem an, ob für eine Zahlung eine Haftungsumkehr besteht oder nicht. Bitte beachten Sie, dass diese Angaben anhand des technischen 3-D Secure Protokolls erfolgen. Es sind die Ausnahmeregelungen Ihres Acquirers zu beachten, zum Beispiel ein Ausschluss bestimmter Kartenarten von der Haftungsumkehr. Werte: <i>yes</i> oder <i>no</i>
CAVV	ans[28]	<i>Optional</i> Cardholder Authentication Verification Value Im Falle einer MasterCard ist hier der UCAF-Wert enthalten. Saferpay benutzt unabhängig vom Kreditkartentyp den Wert CAVV.
ECI	n [1]	<i>Optional</i> Electronic Commerce Indicator Wird zur Kennzeichnung von 3-D Secure Transaktionen benötigt („Verified by Visa“, „MasterCard SecureCode“): 0 = Internet Zahlung ohne Haftungsumkehr 1 = 3-D Secure Zahlung mit Authentisierung 2 = 3-D Secure Zahlung, Karte nimmt am Verfahren nicht teil
XID	ans[28]	<i>Optional</i> 3-D Secure Transaction Identifier



### 3 Saferpay Authorization Interface und Merchant Plug-In

#### 3.1 Übersicht

Die folgende Grafik zeigt den Ablauf einer Online Zahlung mit 3-D Secure-Verarbeitung in Kombination mit dem Saferpay Authorization Interface (AI) und dem Saferpay MPI:



## 3.2 Prozessbeschreibung

### Phase 1 – Angebot und Zahlung

- ① Der Kunde füllt den Warenkorb im Shop und geht zur Kasse. Der Webserver zeigt ein Dialogfenster, in dem der Kunde seine Zahlungsdaten eingibt.
- ② Der Kunde gibt seine Kreditkartendaten ein. Die Daten dürfen ausschließlich SSL verschlüsselt vom Webserver entgegen genommen werden.

### Phase 2 – Überprüfung Karteninhaber

- ③ Der Webserver prüft, ob der KI am 3-D Secure Verfahren teilnimmt oder nicht. Er sendet die Kartendaten an das Saferpay MPI und nimmt die Antwort entgegen.
- ④A Bei Teilnahme am 3-D Secure Verfahren wird der KI durch Aufruf des MPI\_PA\_LINK aus dem Shop zum Access Control Server (ACS) mit der Authentifizierungsseite seines Issuers geleitet. Der Aufruf kann zum Beispiel durch ein JavaScript gesteuert werden.
- ④B Nimmt der KI nicht 3-D Secure Verfahren teil, fährt der Webserver mit dem Zahlungsprozess ohne 3-D Secure Authentifizierung fort(→ weiter mit ⑧).
- ⑤ Die vom KI eingegebenen Daten werden vom Issuer geprüft und das Ergebnis der Authentifizierung ans MPI-Fenster zurück gegeben.
- ⑥ Durch das Schließen des Saferpay MPI-Fensters wird der KI zurück zum Webshop geleitet.
- ⑦ Der Webserver prüft das Ergebnis der Authentifizierung (VerifyPayConfirm) und speichert die MPI\_SESSIONID zur weiteren Verwendung ab.

### Phase 3 – Autorisation

- ⑧ Der Webserver übermittelt die Autorisationsanfrage. Falls vorhanden (bei Visa und MasterCard der Regelfall), muss die Autorisationsanfrage mit der MPI\_SESSIONID ergänzt werden. Anhand des ECI-Wertes in der Autorisationsantwort kann die Haftungsumkehr geprüft werden.  
**Hinweis:** Nicht alle Verarbeiter können die Haftungsumkehr während der Autorisation überprüfen und diese gegebenenfalls schon mit der Autorisationsantwort ausschließen (ECI=0). Fragen Sie bei Bedarf direkt bei Ihrem Verarbeiter nach, ob dieser dazu in der Lage ist.

### Phase 4 – Buchung

- ⑨ Nicht auf dem Schaubild, aber analog zur Payment Page muss der Betrag für den Tagesabschluss verbucht werden (PayComplete).  
Nach dem Tagesabschluss wird jede verbuchte Zahlung zur Händlerbank übersendet und zur Ausführung gebracht. Der Tagesabschluss kann manuell oder automatisch ausgelöst werden. Das Geld wird in Form einer Sammelposition dem Geschäftskonto des Händlers gutgeschrieben. Von der Kreditkartengesellschaft erhält der Händler eine Abrechnungsliste.

## 4 Merchant Plug-In Schnittstellenbeschreibung

Das Saferpay Merchant Plug-In (MPI) wird über die Standard Saferpay Schnittstellen angesteuert. Es können die Methoden der Saferpay Client Library (Java LIB oder .NET LIB) oder des https Interface verwendet werden.

### 4.1 Abwicklung

Aus Sicht der Web-Applikation sind sechs Schritte für eine Online-Zahlung mit 3-D Secure Authentifizierung des KI möglich.

- Schritt 1 Prüfung, ob der KI am 3-D Secure Verfahren teilnimmt. Die Applikation stellt hierfür den VerifyEnrollmentRequest an das Saferpay MPI.
- Schritt 2 Auswertung der Antwort, des VerifyEnrollmentResponse. Nimmt der KI am Verfahren teil, folgen die Schritte 3 und 4. Andernfalls kann sofort mit der Online- Autorisation, Schritt 5 fortgefahren werden.
- Schritt 3 Weiterleitung des KI an den Issuer zur Authentifizierung. Die Weiterleitung erfolgt durch Aufruf des vom VerifyEnrollmentResponse gelieferten MPI\_PA\_LINK.
- Schritt 4 Ergebnis der Authentifizierung entgegennehmen und überprüfen.
- Schritt 5 Bei erfolgreicher Authentifizierung des KI oder, falls der KI nicht am 3-D Secure Verfahren teilnimmt, folgt die eigentliche Zahlungsanfrage, die Online-Autorisation. Bei dieser muss die MPI\_SESSIONID übergeben werden, sofern sie im VerifyEnrollmentResponse enthalten war, ansonsten ist eine Haftungsumkehr ausgeschlossen.
- Schritt 6 Ergebnis der Autorisation entgegennehmen und auswerten. Anhand des ECI-Wertes in der Autorisationsantwort kann die Haftungsumkehr geprüft werden.

**Hinweis:** Nicht alle Verarbeiter können die Haftungsumkehr während der Autorisation überprüfen und diese gegebenenfalls schon mit der Autorisationsantwort ausschließen (ECI=0). Fragen Sie bei Bedarf direkt bei Ihrem Verarbeiter nach, ob dieser dazu in der Lage ist.

Die Schritte 1 und 2 beziehungsweise 1 bis 4 müssen vor der Online-Autorisation der Kartenzahlung durchgeführt werden!


## 4.2 Schritt 1: VerifyEnrollmentRequest

Zunächst prüft Saferpay anhand der Kreditkartennummer, ob eine Karte am 3-D Secure Verfahren teilnimmt oder nicht. Für den dafür erforderlichen VerifyEnrollmentRequest ist die Angabe der folgenden Parameter notwendig. Wenn nicht anders erwähnt ist ein Parameter obligatorisch.

Parameter	Format	Beschreibung
MSGTYPE	a[..30]	Enthält immer den Wert „VerifyEnrollment“.
ACCOUNTID	ns[..15]	Die Saferpay Kontonummer des Händlers für diese Transaktion. Zum Beispiel „99867-94913159“ für das Saferpay Testkonto.
MPI_PA_BACKLINK	ans[..1024]	Der URL für den Rücksprung des KI zum Shop. Bei erfolgreicher Authentifizierung werden mit dem URL per GET die Details des VerifyEnrollmentResponse übermittelt.
MPI_PA_NOTIFYURL	ans[..1024]	<i>Optional</i> Saferpay sendet die Bestätigungsnachricht (PayConfirm) bei erfolgreicher Authentifizierung des KI direkt an diese Adresse. Im Unterschied zur Benachrichtigung über den MPI_PA_BACKLINK wird die Information hier per POST gesendet. Da der Aufruf von extern und somit außerhalb der Shop Session erfolgt ist es sinnvoll eine Shop SessionID als GET Parameter an die übergebene Adresse anzufügen, um bei Empfang der Antwort im Shop eine Zuordnung zu ermöglichen. Da der Aufruf nicht per Browser Redirect erfolgt, muss die angegebene Adresse voll qualifiziert sein. Der Aufruf erfolgt ausschließlich über die Standardports für http (80) oder https (443). Andere Ports sind nicht zulässig.
PAN	n[..19]	Die „Primary Account Number“, enthält die Kreditkartennummer ohne Leerzeichen, zum Beispiel „9451123100000111“.
CARDREFID	ans[..40]	Bei Verwendung des Dienstes „Saferpay Secure Card Data“ ist der Parameter CARDREFID anstelle von PAN zu verwenden.
EXP	n[4]	Verfalldatum, wie auf der Karte angegeben. Das Format ist MMJJ, zum Beispiel „1215“ für 12/2015.
AMOUNT	n[..8]	Zahlungsbetrag in kleinster Währungseinheit, zum Beispiel „1230“ entspricht dem Betrag 12,30 bei der Währung Euro.
CURRENCY	a [3]	Dreistelliger ISO 4217 Währungs-Code, zum Beispiel „CHF“ oder „EUR“.

### 4.3 Schritt 2: Verify EnrollmentResponse

Die Webserver-Applikation wertet die Antwort auf den VerifyEnrollmentRequest aus.

Parameter	Format	Beschreibung
MSGTYPE	a[..30]	Enthält immer den Wert „VerifyEnrollmentResponse“
RESULT	n[..3]	Enthält den Antwort-Code auf den VerifyEnrollmentRequest.  0 = Anfrage erfolgreich ausgeführt.  301 = Es besteht keine Haftungsumkehr. Die Händleranwendung kann die Zahlung beenden oder auf eigenes Risiko fortsetzen. Diese Fehlermeldung erscheint, wenn <ul style="list-style-type: none"> <li>• die Kartengesellschaft die Haftungsumkehr aus vertraglichen Gründen ausschließt. Das kann zum Beispiel bei einer Business-Kreditkarte der Fall sein.</li> <li>• der Issuer ein technisches Problem hat, das eine Authentifizierung des KI nicht zulässt.</li> <li>• der Händler nicht für die 3-DS Verarbeitung bei der Kartengesellschaft angemeldet wurde.</li> </ul> ≠0 =  <b>Achtung!</b> Bei einem RESULT ungleich "0" ist die Haftungsumkehr generell ausgeschlossen. Die Weiterführung des Bezahlvorgangs erfolgt auf eigenes Risiko.
ECI	n[1]	Electronic Commerce Indicator Wird zur Kennzeichnung von 3-D Secure Transaktionen benötigt („Verified by Visa“, „MasterCard SecureCode“): 0 = Internet Zahlung ohne Haftungsumkehr. 1 = 3-D Secure Zahlung mit Authentisierung. 2 = 3-D Secure Zahlung, Karte nimmt am Verfahren nicht teil.
MPI_SESSIONID	an[28]	Die Session des VerifyEnrollment-Vorgangs wird für die Autorisationsanfrage benötigt. So wird die Zahlung als 3-D Secure gekennzeichnet.
MPI_PA_LINK	ans[..19]	Enthält den signierten Link zu Saferpay, über den der KI zum Access Control Server (ACS) mit der Authentifizierungsseite seines Issuers geführt wird.
MPI_PA_REQUIRED	a[..3]	Mögliche Werte „yes“ oder „no“. Zeigt an, ob eine Authentifizierung erforderlich ist oder gleich mit der Autorisationsanfrage fortgefahren werden kann.
XID	ans[28]	3-D Secure Transaction Identifier Diese Base64-Zeichenfolge wird vom MPI vergeben und referenziert auf den VerifyEnrollment-Vorgang.

#### 4.4 Schritt 3: Authentifizierung des Karteninhabers

Am 3-D Secure Verfahren teilnehmende KI (ECI=1) müssen von der Web-Applikation des Shops zwecks Authentifizierung zur kartenausgebenden Bank geleitet werden. Dieses geschieht durch Aufruf des im MPI\_PA\_LINK enthaltenen URL. Der KI wird so über seinen Internet Browser zum ACS-Server des Issuers weitergeleitet, wo die Authentifizierung durchgeführt wird, etwa durch Abfrage eines Passworts oder einer PIN.

#### 4.5 Schritt 4: Prüfung der Authentifizierungsantwort

Nach erfolgreicher Authentifizierung des KI prüft das Saferpay MPI die Rückgabedaten und leitet ihn anschließend über den MPI\_PA\_BACKLINK zum Shop zurück. Die Shop-Applikation überprüft daraufhin mit der Saferpay Funktion VerifyPayConfirm die digitale Signatur des Links mittels der Rückgabedaten DATA und SIGNATURE, um Manipulation auszuschließen.

Die in DATA zusätzlich enthaltenen Parameter der Authentifizierung:

Parameter	Format	Beschreibung
MSGTYPE	a[..30]	Enthält immer den Wert „AuthenticationConfirm“.
RESULT	n[..3]	Antwort-Code auf den „VerifyEnrollmentRequest“. 0 = Anfrage erfolgreich ausgeführt. 311 = Die Authentifizierung ist aufgrund eines technischen Problems auf dem ACS-Server gescheitert. Ein Fortfahren mit der Autorisationsanfrage sollte vom ECI-Wert abhängig gemacht werden.
ECI		Electronic Commerce Indicator 0 = SSL gesicherte Internet-Zahlung, keine Haftungsumkehr. 1 = SSL gesicherte Internet-Zahlung mit 3-DS und Haftungsumkehr, KI nimmt am Verfahren teil. 2 = SSL gesicherte Internet-Zahlung mit 3-DS und Haftungsumkehr, KI nimmt nicht am Verfahren teil oder Authentifizierung nicht möglich.
MPI_SESSIONID	an[28]	Die Session des VerifyEnrollment-Vorgangs wird für die Autorisationsanfrage benötigt. So wird die Zahlung als 3-D Secure gekennzeichnet.
MPI_TX_ECI	an [28]	Original “Electronic Commerce Indicator” des Issuers. Im Gegensatz zum Saferpay ECI, der die Werte für Visa und MasterCard zur Vereinfachung zusammenfasst, sind hier die originalen, aber je nach Kartentyp unterschiedlichen Werte enthalten.
MPI_TX_STATUS	a [1]	Gibt den Status der Authentifizierung an. Y = Authentifizierung erfolgreich U = Authentifizierungsantwort nicht verfügbar
XID	ans[28]	Diese Base64-Zeichenfolge wird vom MPI vergeben und referenziert auf den Vorgang im 3-D Secure Protokoll.
CAVV	ans[28]	Cardholder Authentication Verification Value Bei einer MasterCard ist hier der UCAF-Wert enthalten. Saferpay benutzt unabhängig vom Kreditkartentyp den Wert CAVV.

#### 4.6 Schritt 5: Autorisationsanfrage

Im Anschluss an die 3-D Secure Verarbeitung findet die eigentliche Zahlungsanfrage, die Autorisation der Kreditkartenzahlung statt. Eine detaillierte Beschreibung dieses Ablaufs findet sich in der Spezifikation des „Saferpay Authorization Interface“.



Bei der Autorisationsanfrage muss das Attribut MPI\_SESSIONID zwingend gesetzt sein. Nur dann können Zahlungen als „3-D Secure“ gekennzeichnet werden und die Haftungsumkehr kann greifen.

#### 4.7 Schritt 6: Autorisationantwort



Der Verarbeiter kann aus verschiedenen Gründen die Haftungsumkehr ablehnen, sodass der Händler das volle Risiko für die Zahlung trägt. Einige Verarbeiter sind technisch in der Lage die Haftungsumkehr bereits während der Autorisation zu überprüfen und diese gegebenenfalls schon mit der Autorisationsantwort auszuschließen. Dem Shop wird dies dann mit einem veränderten Wert im ECI bekannt gegeben (ECI=0). Deshalb sollte die Autorisationsantwort stets auf Haftungsumkehr geprüft werden.

**Hinweis:** Nicht alle Verarbeiter können die Haftungsumkehr während der Autorisation überprüfen. Bei Bedarf fragen Sie bitte direkt bei Ihrem Verarbeiter nach, ob dieser dazu in der Lage ist.

## 5 Saferpay Testkonto

Während der Integrationsphase des MPI in den Webshop empfiehlt sich die Verwendung des Saferpay Testkontos.

**ACCOUNTID** 99867-94913159

**spPassword** XAjc3Kna (Der Parameter wird nur für das https Interface benötigt)

Kartenummer	Beschreibung
9451123100000202	Saferpay Testkarte „unable to enroll“, liefert ECI=0 im VerifyEnrollmentResponse.
9451123100000004	Saferpay Testkarte „not enrolled“, liefert ECI=2 im VerifyEnrollmentResponse.
9451123100000111	Saferpay Testkarte „enrolled“, liefert ECI=1 im VerifyEnrollmentResponse und mit der Authentifizierungsantwort.
9451123100000228	Saferpay Testkarte „enrolled“, liefert ECI=1 im VerifyEnrollmentResponse und mit der Authentifizierungsantwort ECI=2.
9451123100000210	Saferpay Testkarte „enrolled“, liefert ECI=1 im VerifyEnrollmentResponse und mit der Authentifizierungsantwort ECI=0.

Das Testkonto wird von mehreren Entwicklern genutzt. Daher kommt es vor, dass auf dem Testkonto Vorgänge und Buchungen erscheinen, die von anderen stammen.

Das Testkonto unterstützt nur Saferpay Testkarten. Andere Kartentypen sind nicht verfügbar. Die Testkarten besitzen keine fest zugehörige Kartenprüfnummer (CVC2 / CVV2) und Verfalldatum. Beides kann frei gewählt werden, mit der Einschränkung, dass die Kartenprüfnummer dreistellig numerisch sein und das Verfalldatum in der Zukunft liegen muss. Ansonsten gleicht der Bezahlvorgang mit den Saferpay Testkarten dem mit Kreditkarten in einer produktiven Umgebung.



## 6 Beispiele

### 6.1 Wichtiger Hinweis



Bitte beachten Sie, dass eigene Werte HTML-kodiert werden sollten, entweder als HTML-Entity oder Unicode. So stellen Sie sicher, dass alle Sonderzeichen korrekt an Saferpay übergeben werden.

### 6.2 C# mit der .NET LIB

#### Schritt 1: Verify Enrollment Anfrage

```
MessageFactory mf = new MessageFactory();
mf.Open(""); // Saferpay configuration path, e.g. "c:\\Programme\\Saferpay\\Client"
MessageObject response = null;
MessageObject request = null;
request = mf.CreateRequest("VerifyEnrollment");

request.SetAttribute("ACCOUNTID", "99867-94913159");
request.SetAttribute("AMOUNT", "12500");
request.SetAttribute("CURRENCY", "EUR");
request.SetAttribute("PAN", "9451123100000111");
request.SetAttribute("EXP", "1214");
request.SetAttribute("MPI_PA_BACKLINK", "http://www.testshop.de/success.aspx");
request.SetAttribute("MPI_PA_NOTIFYURL", "http://www.testshop.de/verifyenrollment_log.aspx");

response = request.Execute();
```

### Schritt 2: VerifyEnrollmentResponse

```
int result = Convert.ToInt32(response.GetAttribute("RESULT"));
string mpi_session = null;
string mpi_link = null;

switch(result)
{
    case 0:
        string eci = response.GetAttribute("ECI");
        switch (eci)
        {
            case "1":
                mpi_session = response.GetAttribute("MPI_SESSIONID");
                mpi_link = response.GetAttribute("MPI_PA_LINK");
                //...call mpi_link for cardholder's authentication
                break;
            case "2":
                mpi_session = response.GetAttribute("MPI_SESSIONID");
                //...continue 3DS payment without authentication
                break;
            case "0":
                //...continue payment depending on chosen cardtype
                break;
        }
        break;

    case 301:
        //...if RESULT = 301 then "ECI=0" (stop here or continue payment without
        liability shift at own risk)
        break;
}
```

### Schritt 3: Authentifizierung des Karteninhabers

Aufruf des MPI\_PA\_LINK leitet den KI zur Authentifizierung zum ACS-URL.

### Schritt 4: Prüfung der Authentifizierungsantwort

```
string data = Request.QueryString.Get("DATA");
string signature = Request.QueryString.Get("SIGNATURE");

MessageFactory mf = new MessageFactory();
mf.Open("");
MessageObject payconfirm = mf.VerifyPayConfirm(data, signature);
string eci = payconfirm.GetAttribute("ECI");
string mpi_session = payconfirm.GetAttribute("MPI_SESSIONID");
//...continue 3DS payment with MPI_SESSIONID
```

### Schritt 5: Autorisationsanfrage

```
MessageFactory mf = new MessageFactory();
mf.Open("");
MessageObject request = mf.CreateRequest("Authorization");
request.SetAttribute("ACCOUNTID", "99867-94913159");
request.SetAttribute("AMOUNT", "12500");
request.SetAttribute("CURRENCY", "EUR");
request.SetAttribute("PAN", "9451123100000111");
request.SetAttribute("EXP", "1214");
request.SetAttribute("CVC", "123");
request.SetAttribute("MPI_SESSIONID", mpi_session);
request.SetAttribute("ORDERID", "123456789"; // merchant reference number

MessageObject response = request.Execute();
```

### Schritt 6: Autorisationsantwort

Das Ergebnis auswerten und den erhaltenen ECI Wert auf Haftungsumkehr prüfen.

## 6.3 Kommandozeilenaufrufe mit der Java LIB

### Schritt 1: Verify Enrollment Anfrage

```
java -jar saferpay.jar -exec -m VerifyEnrollment -p c:\programme\safepay\client\keys\99867 -a
ACCOUNTID 99867-94913159 -a PAN 9451123100000111 -a EXP 1212 -a AMOUNT 12500 -a CURRENCY EUR -
a MPI_PA_BACKLINK http://support.saferpay.de/scripts/demo/scd.asp?status=success -a
MPI_PA_NOTIFYURL https://support.saferpay.de/scripts/trace.asp
```

### Schritt 2: VerifyEnrollmentResponse

```
<IDP MSGTYPE="VerifyEnrollmentResponse" MESSAGE="request was processed successfully"
ACCOUNTID="99867-94913159" RESULT="0" MPI_PA_REQUIRED="yes" MPI_LIABILITYSHIFT="yes"
MPI_XID="RmxNZQqyZx5CBAVhHzEKrnlgFg4=" AUTHMESSAGE="3D Secure Verification: Card is enrolled -
perform 3D Secure Authentication" ECI="1" XID="RmxNZQqyZx5CBAVhHzEKrnlgFg4="
MPI_PA_LINK="https://www.saferpay.com/VT2/Pay.aspx?DATA=%3cIDP+MSGTYPE%3d%22PayerAuthenticatio
n%22+ACCOUNTID%3d%2299867-
94913159%22+MPI_SESSIONID%3d%22Qx8bv3bj9lKxSA9nd8nEA6UQjfnb%22+KEYID%3d%22%24SCAIve-
99867%22+%2f%3e&SIGNATURE=a46793afe4fca244966ce907ba5ad837c9d70168853865daa0e385822a50c185
738c2df190d2f9e1f6dd429f3d77ddc89141a1863d8a01753bcf0bcbdlc5bada"
MPI_SESSIONID="Qx8bv3bj9lKxSA9nd8nEA6UQjfnb"/>
```

### Schritt 3: Authentifizierung des Karteninhabers

Aufruf des MPI\_PA\_LINK leitet den KI zur Authentifizierung zum ACS-URL:

```
https://www.saferpay.com/VT2/Pay.aspx?DATA=%3cIDP+MSGTYPE%3d%22PayerAuthenticatio%22+ACCOUNTI
D%3d%2299867-
94913159%22+MPI_SESSIONID%3d%22Qx8bv3bj9lKxSA9nd8nEA6UQjfnb%22+KEYID%3d%22%24SCAIve-
99867%22+%2f%3e&SIGNATURE=a46793afe4fca244966ce907ba5ad837c9d70168853865daa0e385822a50c185738c
2df190d2f9e1f6dd429f3d77ddc89141a1863d8a01753bcf0bcbdlc5bada
```



#### Schritt 4: Prüfung der Authentifizierungsantwort

Rücksprung nach der Authentifizierung des KI in den Shop zum MPI\_PA\_BACKLINK:

```
http://support.saferpay.de/scripts/demo/scd.asp?status=success&DATA=%3cIDP+MSGTYPE%3d%22AuthenticationConfirm%22+KEYID%3d%221-0%22+ACCOUNTID%3d%2299867-94913159%22+RESULT%3d%220%22+MESSAGE%3d%223DS+Payer+Authentication+Succeeded%22+MPI_SESSIONID%3d%22Qx8bv3bj9lKxSA9nd8nEA6UQjfnb%22+MPI_LIABILITYSHIFT%3d%22yes%22+MPI_TX_CAVV%3d%22AAABBIIFmAAAAAAAAAAAAAAAAAAAA%3d%22+MPI_TX_ECI%3d%2205%22+MPI_TX_STATUS%3d%22Y%22+MPI_XID%3d%22RmxNZQyZx5CBAVhHzEKrnlgFg4%3d%22+AUTHMESSAGE%3d%22Authentication+succeeded.%22+CAVV%3d%22AAABBIIFmAAAAAAAAAAAAAAAAAAAA%3d%22+ECI%3d%221%22+XID%3d%22RmxNZQyZx5CBAVhHzEKrnlgFg4%3d%22+%2f%3e&SIGNATURE=551fa20e3e12d5771be3ealcbel115d02c0e5c64dc98a0f0c279ce9861863d09df550101d3ce2c466986891494e0eae b83a63fe1ce501bb313f561dce786e3567
```

#### Empfangenes DATA:

```
<IDP MSGTYPE="AuthenticationConfirm" KEYID="1-0" ACCOUNTID="99867-94913159" RESULT="0" MESSAGE="3DS Payer Authentication Succeeded" MPI_SESSIONID="Qx8bv3bj9lKxSA9nd8nEA6UQjfnb" MPI_LIABILITYSHIFT="yes" MPI_TX_CAVV="AAABBIIFmAAAAAAAAAAAAAAAAAAAA" MPI_TX_ECI="05" MPI_TX_STATUS="Y" MPI_XID="RmxNZQyZx5CBAVhHzEKrnlgFg4" AUTHMESSAGE="Authentication succeeded." CAVV="AAABBIIFmAAAAAAAAAAAAAAAAAAAA" ECI="1" XID="RmxNZQyZx5CBAVhHzEKrnlgFg4="/>
```

#### Empfangene SIGNATURE:

```
551fa20e3e12d5771be3ealcbel115d02c0e5c64dc98a0f0c279ce9861863d09df550101d3ce2c466986891494e0eae b83a63fe1ce501bb313f561dce786e3567
```

#### VerifyPayConfirm:

```
java -jar saferpay.jar -payconfirm -p C:\Programme\Saferpay\keys\99867 -d %3cIDP+MSGTYPE%3d%22AuthenticationConfirm%22+KEYID%3d%221-0%22+ACCOUNTID%3d%2299867-94913159%22+RESULT%3d%220%22+MESSAGE%3d%223DS+Payer+Authentication+Succeeded%22+MPI_SESSIONID%3d%22Qx8bv3bj9lKxSA9nd8nEA6UQjfnb%22+MPI_LIABILITYSHIFT%3d%22yes%22+MPI_TX_CAVV%3d%22AAABBIIFmAAAAAAAAAAAAAAAAAAAA%3d%22+MPI_TX_ECI%3d%2205%22+MPI_TX_STATUS%3d%22Y%22+MPI_XID%3d%22RmxNZQyZx5CBAVhHzEKrnlgFg4%3d%22+AUTHMESSAGE%3d%22Authentication+succeeded.%22+CAVV%3d%22AAABBIIFmAAAAAAAAAAAAAAAAAAAA%3d%22+ECI%3d%221%22+XID%3d%22RmxNZQyZx5CBAVhHzEKrnlgFg4%3d%22+%2f%3e -s 551fa20e3e12d5771be3ealcbel115d02c0e5c64dc98a0f0c279ce9861863d09df550101d3ce2c466986891494e0eae b83a63fe1ce501bb313f561dce786e3567
```



### Schritt 5: Autorisationsanfrage

```
java -jar saferpay.jar -exec -p "c:/programme/saferpay/client/keys/99867/" -m Authorization -a  
ACCOUNTID 99867-94913159 -a PAN 9451123100000111 -a EXP 1214 -a CVC 123 -a AMOUNT 12500 -a  
CURRENCY EUR -a ORDERID "Testeinkauf saferpay.jar" -a MPI_SESSIONID  
Qx8bv3bj9lKxSA9nd8nEA6UQjfnb
```

### Schritt 6: Autorisationsantwort

```
<IDP MSGTYPE="AuthorizationResponse" RESULT="0" ACCOUNTID="99867-94913159"  
ID="Qx8bv3bj9lKxSA9nd8nEA6UQjfnb" PROVIDERID="90" PROVIDERNAME="Saferpay Test Card"  
CONTRACTNUMBER="123456789" CCCOUNTRY="XX" TOKEN="(unused)" AUTHRESULT="1"  
MPI_TX_CAVV="AAABBIIFmAAAAAAAAAAAAAAAAAAAA=" MPI_LIABILITYSHIFT="yes"  
MPI_XID="RmxNZQQyZx5CBAVhHzEKrnlgFg4=" CAVV="AAABBIIFmAAAAAAAAAAAAAAAAAAAA=" ECI="1"  
XID="RmxNZQQyZx5CBAVhHzEKrnlgFg4=" AUTHDATE="20110121 15:26:22" EXP="1214" AUTHCODE="198657"  
PAN="xxxx xxxx xxxx 0111" PAYMENT_PROTOCOL="CARCDS" REFERRAL="017772357" AUTHMESSAGE="request  
was processed successfully"/>
```

Das Ergebnis auswerten und den erhaltenen ECI Wert auf Haftungsumkehr prüfen.

## 6.4 Verwendung des https Interface

### Schritt 1: Verify Enrollment Anfrage

```
https://www.saferpay.com/hosting/VerifyEnrollment.asp?spPassword=XAjc3Kna&AMOUNT=12500&CURRENC  
Y=EUR&ACCOUNTID=99867-  
94913159&PAN=9451123100000111&EXP=1214&MPI_PA_BACKLINK="http://support.saferpay.de/scripts/dem  
o/scd.asp?status=success"&MPI_PA_NOTIFYURL="https://support.saferpay.de/scripts/trace.asp"
```

### Schritt 2: VerifyEnrollmentResponse

```
OK:<IDP RESULT="0" ECI="1" MSGTYPE="VerifyEnrollmentResponse"  
XID="fVpAFgBnc3RpBDoBcCcJfGVoBwc=" AUTHMESSAGE="3D Secure Verification: Card is enrolled -  
perform 3D Secure Authentication" MPI_XID="fVpAFgBnc3RpBDoBcCcJfGVoBwc="  
MPI_SESSIONID="7d1K3YAAfI29vAf006QYb1bnYW0A" MPI_PA_REQUIRED="yes"  
MPI_PA_LINK="https://www.saferpay.com/VT2/Pay.aspx?DATA=%3cIDP+MSGTYPE%3d%22PayerAuthenticatio  
n%22+ACCOUNTID%3d%2299867-  
94913159%22+MPI_SESSIONID%3d%227d1K3YAAfI29vAf006QYb1bnYW0A%22+KEYID%3d%22%24SCAIve-  
99867%22+%2f%3e&SIGNATURE=2ada5c4f8cdb4d7cc8a23900442b67b38dc9d7a1ab340c9e64667e0642c7525c  
0d8dc8f93f440fa29031b270ed0545ee770aa8608460376c31800b58e0b8baa0" MPI_LIABILITYSHIFT="yes"/>
```

### Schritt 3: Authentifizierung des Karteninhabers

Aufruf des MPI\_PA\_LINK leitet den KI zur Authentifizierung zum ACS-URL:

```
https://www.saferpay.com/VT2/Pay.aspx?DATA=%3cIDP+MSGTYPE%3d%22PayerAuthentication%22+ACCOUNTI  
D%3d%2299867-  
94913159%22+MPI_SESSIONID%3d%227d1K3YAAfI29vAf006QYb1bnYW0A%22+KEYID%3d%22%24SCAIve-  
99867%22+%2f%3e&SIGNATURE=2ada5c4f8cdb4d7cc8a23900442b67b38dc9d7a1ab340c9e64667e0642c7525c0d8d  
c8f93f440fa29031b270ed0545ee770aa8608460376c31800b58e0b8baa0
```



#### Schritt 4: Prüfung der Authentifizierungsantwort

Rücksprung nach der Authentifizierung des KI in den Shop zum MPI\_PA\_BACKLINK:

```
http://support.saferpay.de/scripts/demo/scd.asp?status=success&DATA=%3CIDP+MSGTYPE%3d%22AuthenticationConfirm%22+KEYID%3d%221-0%22+ACCOUNTID%3d%2299867-94913159%22+RESULT%3d%220%22+MESSAGE%3d%223DS+Payer+Authentication+Succeeded%22+MPI_SESSIONID%3d%227d1K3YAAfI29vAf006QYb1bnYW0A%22+MPI_LIABILITYSHIFT%3d%22yes%22+MPI_TX_CAVV%3d%22AAABBIIFmAAAAAAAAAAAAAAAAAAAA%3d%22+MPI_TX_ECI%3d%2205%22+MPI_TX_STATUS%3d%22Y%22+MPI_XID%3d%22fVpAFgBnc3RpBD0BcCcJfGVoBwc%3d%22+AUTHMESSAGE%3d%22Authentication+succeeded.%22+CAVV%3d%22AAABBIIFmAAAAAAAAAAAAAAAAAAAA%3d%22+ECI%3d%221%22+XID%3d%22fVpAFgBnc3RpBD0BcCcJfGVoBwc%3d%22+%2f%3E&SIGNATURE=a477b4d0865e0d041abd708f7dfc25176f9aca8d01e4c2397653e674863a8cd261bdda2653f67de17b6fee09528b331eda557f3e02e1c803e7a566b828038445
```

#### Empfangenes DATA:

```
<IDP MSGTYPE="AuthenticationConfirm" KEYID="1-0" ACCOUNTID="99867-94913159" RESULT="0" MESSAGE="3DS Payer Authentication Succeeded" MPI_SESSIONID="7d1K3YAAfI29vAf006QYb1bnYW0A" MPI_LIABILITYSHIFT="yes" MPI_TX_CAVV="AAABBIIFmAAAAAAAAAAAAAAAAAAAA" MPI_TX_ECI="05" MPI_TX_STATUS="Y" MPI_XID="fVpAFgBnc3RpBD0BcCcJfGVoBwc" AUTHMESSAGE="Authentication succeeded." CAVV="AAABBIIFmAAAAAAAAAAAAAAAAAAAA" ECI="1" XID="fVpAFgBnc3RpBD0BcCcJfGVoBwc" />
```

#### Empfangene SIGNATURE:

```
a477b4d0865e0d041abd708f7dfc25176f9aca8d01e4c2397653e674863a8cd261bdda2653f67de17b6fee09528b331eda557f3e02e1c803e7a566b828038445
```

#### https Aufruf VerifyPayConfirm:

```
https://www.saferpay.com/hosting/verifypayconfirm.asp?spPassword=XAjc3Kna&ACCOUNTID=99867-94913159&DATA=%3CIDP+MSGTYPE%3d%22AuthenticationConfirm%22+KEYID%3d%221-0%22+ACCOUNTID%3d%2299867-94913159%22+RESULT%3d%220%22+MESSAGE%3d%223DS+Payer+Authentication+Succeeded%22+MPI_SESSIONID%3d%227d1K3YAAfI29vAf006QYb1bnYW0A%22+MPI_LIABILITYSHIFT%3d%22yes%22+MPI_TX_CAVV%3d%22AAABBIIFmAAAAAAAAAAAAAAAAAAAA%3d%22+MPI_TX_ECI%3d%2205%22+MPI_TX_STATUS%3d%22Y%22+MPI_XID%3d%22fVpAFgBnc3RpBD0BcCcJfGVoBwc%3d%22+AUTHMESSAGE%3d%22Authentication+succeeded.%22+CAVV%3d%22AAABBIIFmAAAAAAAAAAAAAAAAAAAA%3d%22+ECI%3d%221%22+XID%3d%22fVpAFgBnc3RpBD0BcCcJfGVoBwc%3d%22+%2f%3E&SIGNATURE=a477b4d0865e0d041abd708f7dfc25176f9aca8d01e4c2397653e674863a8cd261bdda2653f67de17b6fee09528b331eda557f3e02e1c803e7a566b828038445
```

#### Antwort liefert MPI\_SESSIONID:

```
OK: ID=7d1K3YAAfI29vAf006QYb1bnYW0A
```



### Schritt 5: Autorisationsanfrage

```
https://www.saferpay.com/hosting/Execute.asp?spPassword=XAjc3Kna&AMOUNT=12500&CURRENCY=EUR&ORDERID="Testkauf https Interface"&ACCOUNTID=99867-94913159&PAN=945112310000111&EXP=1214&CVC=123&MPI_SESSIONID=7d1K3YAAfI29vAf006QYb1bnYW0A
```

### Schritt 6: Autorisationsantwort

```
OK:<IDP RESULT="0" MSGTYPE="AuthorizationResponse" ID="7d1K3YAAfI29vAf006QYb1bnYW0A"
TOKEN="(unused)" AUTHRESULT="1" AUTHMESSAGE="request was processed successfully"
AUTHCODE="483624" PROVIDERID="90" PROVIDERNAME="Saferpay Test Card" ECI="1"
CAVV="AAABBIIFmAAAAAAAAAAAAAAAAAAAA=" CCCOUNTRY="XX" XID="fVpAFgBnc3RpBDoBcCcJfGVobwc="
CONTRACTNUMBER="123456789" MPI_TX_CAVV="AAABBIIFmAAAAAAAAAAAAAAAAAAAA="
MPI_XID="fVpAFgBnc3RpBDoBcCcJfGVobwc=" AUTHDATE="20110121 16:34:18" EXP="1214" PAN="xxxx xxxx
xxxx 0111"/>
```

Das Ergebnis auswerten und den erhaltenen ECI Wert auf Haftungsumkehr prüfen.





## 7 Kontakt

### 7.1 Saferpay Integration Team

Haben Sie Fragen zu diesem Dokument oder Probleme bei der Saferpay Integration oder benötigen Unterstützung? Dann wenden Sie sich gern an das Integration Team:

Saferpay Schweiz

**SIX Payment Services AG**

Hardturmstrasse 201

8021 Zürich

+41 848 66 44 44

[www.saferpay.com](http://www.saferpay.com)

[integration@saferpay.com](mailto:integration@saferpay.com)

Saferpay Europa

**SIX Payment Services (Germany) GmbH**

Langenhorner Chaussee 92-94

22415 Hamburg

+49 40 325 967- 280

[www.saferpay.com](http://www.saferpay.com)

[integration@saferpay.com](mailto:integration@saferpay.com)

### 7.2 Saferpay Support Team

Haben Sie Fragen zu Fehlermeldungen oder gibt es Probleme im laufenden Betrieb? Dann steht Ihnen unser Support Team zur Verfügung:

Saferpay Schweiz

**SIX Payment Services AG**

Hardturmstrasse 201

8021 Zürich

+41 848 66 44 44

[www.saferpay.com](http://www.saferpay.com)

[support@saferpay.com](mailto:support@saferpay.com)

Saferpay Europa

**SIX Payment Services (Germany) GmbH**

Langenhorner Chaussee 92-94

22415 Hamburg

+49 40 325 967- 250

[www.saferpay.com](http://www.saferpay.com)

[support@saferpay.com](mailto:support@saferpay.com)

*Das Saferpay Team wünscht Ihnen viel Erfolg mit Ihrer Saferpay E-Payment Lösung!*

