

Saferpay 3-D Secure MPI Integration Guide

Date: **21.12.2006**
Version: **1.4.3**
Status: **preliminary**
Classification: **public**

TABLE OF CONTENTS

1	<u>INTRODUCTION</u>	3
1.1	SUMMARY	3
1.2	REQUIREMENTS	3
1.3	AUTHENTICATION RESULT	4
1.4	LIABILITY SHIFT AND MERCHANT RISK	4
2	<u>SAFERPAY VIRTUAL TERMINAL</u>	5
2.1	OVERVIEW	5
2.2	PROCESS DESCRIPTION	6
2.3	INTERFACE	6
3	<u>SAFERPAY CARD AUTHORIZATION INTERFACE</u>	7
3.1	OVERVIEW	7
3.2	PROCESS DESCRIPTION	8
4	<u>MERCHANT PLUG-IN INTERFACE DESCRIPTION</u>	8
4.1	INTERACTION WITH THE COMPONENT	8
4.2	STEP 1: VERIFY ENROLLMENT REQUEST	9
4.3	STEP 2: VERIFY ENROLLMENT RESPONSE	9
4.4	STEP 3: CARDHOLDER AUTHENTICATION	10
4.5	STEP 4: VERIFY AUTHENTICATION RESULT	10
4.6	STEP 5 AND 6: AUTHORIZATION REQUEST AND RESULT	10
5	<u>PROGRAMMING EXAMPLES</u>	11
5.1	COMMAND LINE	11
5.2	VISUAL BASIC SCRIPT	12
5.3	OPENING AND CLOSING THE MPI POPUP	13
6	<u>REFERENCE</u>	14

1 INTRODUCTION

This document describes the Saferpay Merchant Plug-In add-on to process 3-D Secure transactions by either the Saferpay Virtual Terminal or the Saferpay Card Authorization Interface.

3-D Secure enrolled cardholders have to authenticate themselves before processing the online payments. Purchases based on 3-D Secure are more secure and the merchant benefits from the payment guarantee (liability shift).

Today 3-D Secure supports cardholder authentication for Visa ("Verified by Visa") and MasterCard ("SecureCode").

1.1 SUMMARY

When ever a cardholder is 3-D Secure enrolled he must perform an online authentication before the payment takes place. The cardholder has to authenticat himself by presenting a password or pin to it's card issuing bank.

If a cardholder is not 3-D Secure enrolled then no authentication is needed. But the payment request has to be flagged as "cardholder not enrolled".

The Saferpay MPI supports this interactions and the secure data exchange between the 3-D Secure components. 3-D Secure is possible for online internet payments only. All 3-D Secure interactions for the customer are internet browser based.

1. The merchant passes the cardholder's credit card data together with the main purchase information to saferpay.
2. Saferpay checks whether the cardholder is 3-D Secure enrolled or not. If enrolled the 3-D Secure authentication will start. Otherwise the payment continues without authentication.
3. The cardholder's internet browser forwards the 3-D Secure request to the card issuing bank. The customer has to authenticate himself by a password or a certificate or any other secure identification method.
4. The result of the authentication is returned by the customers browser to saferpay.
5. Saferpay checks the result and it's digital signature. If the authentication was successfully the payment continues. Otherwise the online payment stops or the customer has to choose another payment method.
6. The Saferpay MPI returns the 3-D Secure result fields to be sent together with the card authorization data to the acquirer to perform the online authorization.

1.2 REQUIREMENTS

The Saferpay Application Component (SAC) is required at the webserver.

The Saferpay Merchant Plug-In Service must be activated for the merchant.

Select on type of 3-D Secure integration:

- Saferpay Virtual Terminal Window or
- Saferpay Card Authorization Interface

Contractual requirements with the acquirer:

- Valid contracts for 3-D Secure with the acquirer is required for “Verified by Visa” and/or “MasterCard SecureCode” to benefit from the liability shift.
- The placement of the 3-D Secure logos or trademarks on the merchant website is one part of this contract.

Webshop and trademarks:

- If the Virtual Safepay Terminal will be used, there is no need for the merchant to display the 3-D Secure logos and word mark(s). The word mark(s) will be displayed in the Virtual Safepay Terminal once the Merchant Plug-In is activated.
- If the Safepay Card Authorization Interface will be used, the merchant is responsible to display the correct word mark(s) on his website. Please refer to your acquirer for further details and logos.

1.3 ENROLLMENT AND AUTHENTICATION RESULT

A payment is executed in two different ways: either as a 3-D Secure transaction or as a non 3-D Secure transaction.

If an online 3-D Secure authentication has been processed successfully, the following informations must be passed together with the payment data to the acquirer:

- ECI (Electronic Commerce Indicator)
- Optional: XID (Transaction Identifier)
- Optional: CAVV (Visa: Cardholder Authentication Verification Value) or UCAF (MasterCard: Universal Cardholder Authentication Field)

Visa and MasterCard have different names for the same kind of authentication information. Whenever you find the name or attribute “CAVV” within this document, then both values UCAF and CAVV are meant.

1.4 LIABILITY SHIFT AND MERCHANT RISK

As an electronic commerce merchant please take care to be compliant with the rules and regulations by your credit card acquirer. The framework and definitions of “guarantee of payment” or “promise to pay” are given by your acquirer.

It is very important to send the ECI value and the optional fields XID and CAVV together with the authorization request to your acquirer. Otherwise the liability shift will not take place.

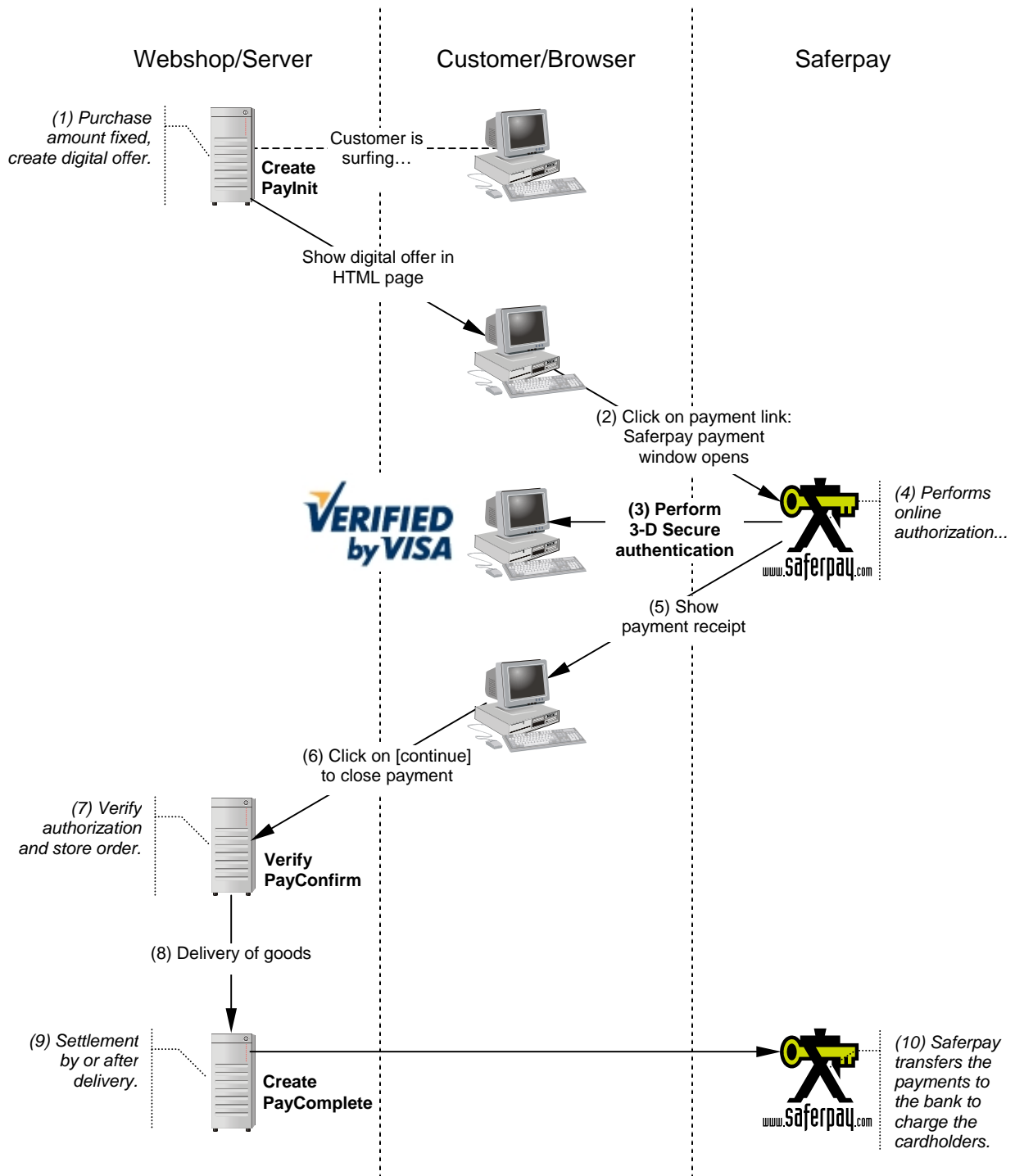
If you are not sure about the liability shift and procedures please contact your credit card acquirer or bank for further information.

Safepay or Telekurs Card Solutions does never guarantee payments or cover the payment of financial transactions.

2 SAFERPAY VIRTUAL TERMINAL

2.1 OVERVIEW

The following diagram illustrates the process of an online purchase with 3-D Secure authentication by using the virtual SafERPAY terminal window.



2.2 PROCESS DESCRIPTION

Phase 1 – digital offer and checkout

1. When the purchase amount is fixed the webshop server creates the digital offer (Create PayInit). E.g. the order confirmation page shows the payment link as „checkout“ button.
2. The customers clicks the „checkout“ button or link. The virtual Saferpay terminal window opens automatically.

Phase 2 – authentication card owner

3. **The customer selects on of the offered payment methods. If 3-D Secure is enabled the cardholder has to authenticate himself at his card issuing bank by password or by any other identification method.**

Phase 3 – authorization (no financial transfers)

4. After successful authentication of the cardholder, saferpay performs an online payment authorization.
5. Saferpay shows the payment receipt.
6. The customers clicks on [continue] to close the purchase and redirect to the webshop.
7. The merchant verifies the authorization result (PayConfirm) and stores them together with the order information.

Phase 4 – capture (financial transfer)

8. The delivery of goods (or content) will be done.
9. The transaction must be captured to charge the payment amount from the customer (PayComplete).
10. After the balance (daily cutover) each captured payment transaction will be transferred to the credit card companies or payment providers to get the money. The balance will be done automatically or manually.

The money flows directly to the merchants banking account. The payment providers will create and send transaction control lists.

2.3 INTERFACE

In addition to the common PayConfirm attributes the following optional attributes are returned:

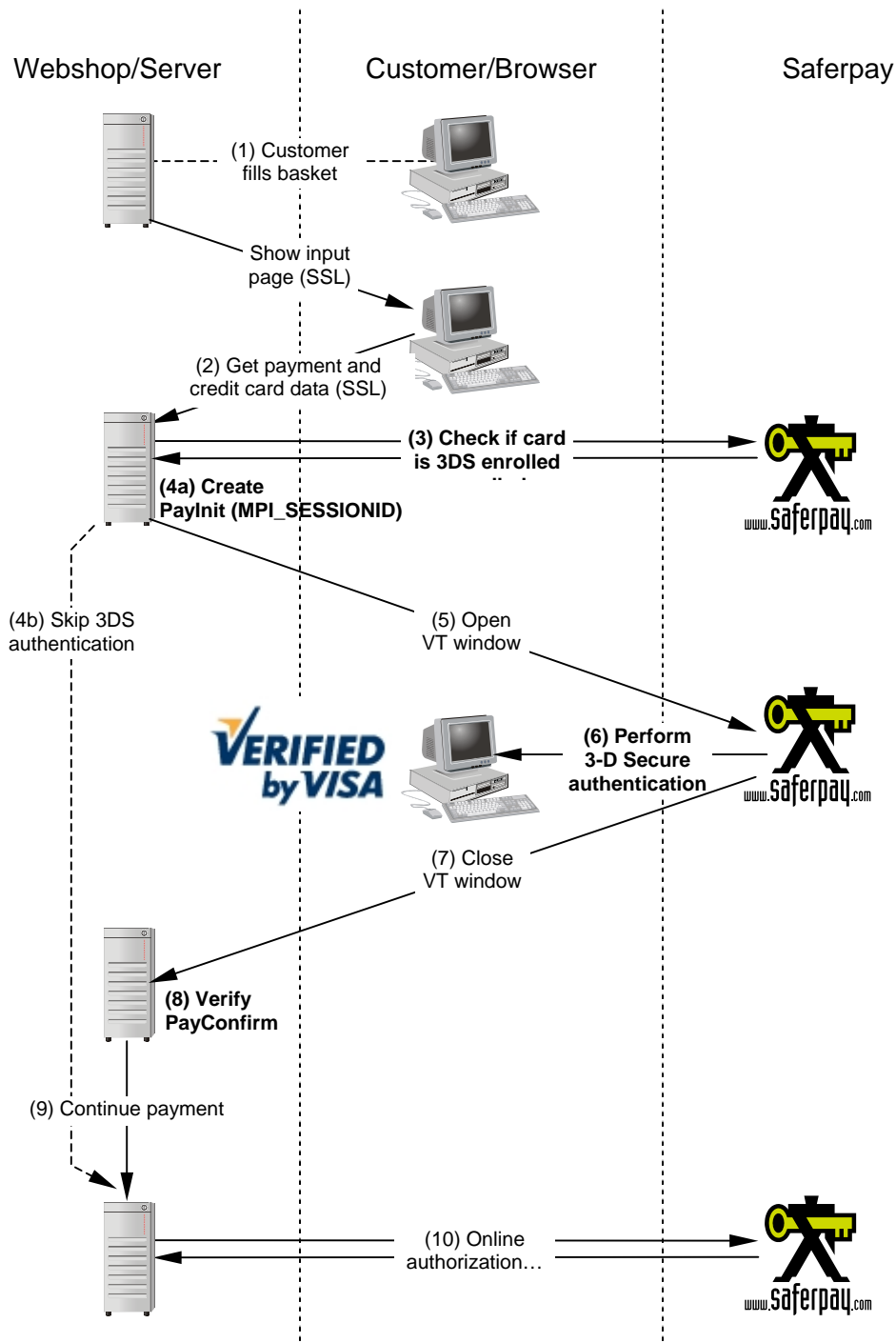
Attribute	Description
ECI	Electronic Commerce Indicator 0 = Payment has been flagged as SSL secured transaction 1 = Payment has been flagged as SSL 3-D Secure authentication transaction (cardholder enrolled) 2 = Payment has been flagged as SSL 3-D Secure authentication transaction (cardholder not enrolled or partial authenticated)
CAVV	Optional: 3-D Secure Cardholder Authentication Verification Value (MasterCard's UCAF value)
XID	Optional: 3-D Secure Transaction Identifier

More information about 3-D Secure control with the virtual terminal window and attributes please refer to the latest documentation of the “Saferpay Implementation Guide” at www.saferpay.com/help.

3 SAFERPAY CARD AUTHORIZATION INTERFACE

3.1 OVERVIEW

The following diagram illustrates the process of an online purchase with 3-D Secure authentication by using the Saferpay Card Authorization Interface together with the virtual Saferpay terminal window.



3.2 PROCESS DESCRIPTION

Phase 1 – digital offer and checkout

1. The customer has to pay to collected items. The webserver shows an checkout formular with input fields.
2. The customers fills the formular with his personal data and credit card information. This data should be received SSL secured by the webserver.

Phase 2 – authentication card owner

3. **The webserver asks saferpay whether the cardholder is 3-D Secure enrolled or not (AuthenticationRequest).**
4. **a) If the cardholder is 3DS enrolled the webserver creates a Paylnit URL for 3DS authentication (attribute MPI_SESSIONID) and continues with step 5.**
b) Otherwise the webserver continues the payment without 3-D Secure authentication.
5. The Saferpay terminal window opens automatically (JavaScript).
6. **The cardholder has to authenticate himself at his card issuing bank by password or by any other identification method.**
7. The Saferpay terminal window closes automatically (JavaScript) and redirects to the webserver's success URL.
8. **The webserver verifies the authentication result (PayConfirm) and stores the 3-D Secure information (ECI, XID and CAVV).**
9. If everything is okay the webserver continues with the payment process.

Phase 3 – authorization (no financial transfers)

10. The webserver performs an online authorization. **If present, the webserver adds the 3-D Secure information to the authorization request.**

Phase 4 – capture (financial transfer)

To perform the financial transfer the steps 8 – 10 must be executed as described in "Virtual Saferpay Terminal".

4 MERCHANT PLUG-IN INTERFACE DESCRIPTION

The usage of the Saferpay Merchant Plug-In (MPI) is similar to the usage of the Saferpay Application Component (SAC) where the component is accessed through a C, COM or Java interface. This chapters describes the Saferpay MPI interface.

4.1 INTERACTION WITH THE COMPONENT

From the applications point of view there are two actions necessary to perform an online authentication of the cardholder: The first two steps are called "Verify Enrollment" request and response, the secondary two steps – if the cardholder is 3-D Secure enabled – is the authentication of the cardholder by opening the Saferpay popup browser window and performing the online authentication.

Once a cardholder is detected as "enrolled" (step 1 and 2), Saferpay will return an MPI session identifier (MPI_SESSIONID), which is used to start the online authentication of the cardholder (step 3 and 4). After successful authentication the payment process should continue by adding the authentication result data to the authorization request.

4.2 STEP 1: VERIFY ENROLLMENT REQUEST

This step must be executed before the online authorization of the payment happens. Saferpay checks if the given card number is enrolled for 3-D Secure or not.

To prepare the authentication request the following set of attributes is passed to the SAC. After the request has been executed *successfully* the application will receive another set of attributes used for further processing of the transaction.

Attribute	Description
ACCOUNTID	The saferpay account identifier to use for the transaction. e.g. 99867-94913159 = Saferpay test account id
PAN	Credit card: Primary Account Number as printed on the credit card, e.g. 9451123100000004
EXP	Credit card: Expiration date as printed on the card. The format is MMY, e.g. 1206 for 12/2006
AMOUNT	Payment amount in minor currency unit e.g. 1230 in EUR means EUR 12,30.
CURRENCY	ISO 4217 three-letter currency code e.g. CHF, USD, EUR

4.3 STEP 2: VERIFY ENROLLMENT RESPONSE

A successful authentication request-response operation *does not* imply the successful authentication. The Merchant Application *must* evaluate the RESULT attribute of the response to retrieve the authentication status.

A run-time error is returned from the SAC if the received response is wrong or missing.

Attribute	Description
RESULT	The result code of the authentication request: 0 Request successfully processed, continue with authentication or payment. Note, the value of the ECI attribute must be checked for further processing! 301 Application Error: The merchant application could choose to stop payment or to continue payment without authentication and without liability shift (ECI = 0) . xx The RESULT attribute could contain any other value as they are defined by the Saferpay Card Authorization Interface. In this case the payment should be stopped.
ECI	Electronic Commerce Indicator 0 = Continue payment as SSL secured transaction (default) 1 = Continue with 3-D Secure authentication (cardholder enrolled) 2 = Continue payment as 3-D Secure transaction (cardholder not enrolled)
MPI_SESSIONID	Returned only if RESULT = 0 and ECI = 1. In this case the merchant application has to continue with the 3-D Secure authentication via the Saferpay MPI (step 3). The customer has to authenticate himself online via the Saferpay MPI.
AUTHMESSAGE	Contains a description of the response message result.

4.4 STEP 3: CARDHOLDER AUTHENTICATION

If the card holder is 3-D Secure enrolled (RESULT=0), the merchant application has to open the saferpay merchant plug-in as a popup window. To create the saferpay MPI url, the merchant application has to set the following attributes at the SAC. The saferpay MPI url will be created by performing CreatePayInit step.

The customers browser will be forwarded to the card issuing bank. The card holder has to authenticate himself by password or pin.

Attribute	Description
ACCOUNTID	The saferpay account identifier to use for the transaction. e.g. 99867-94913159 = test account id
AMOUNT	Payment amount in minor currency unit e.g. 1230 in EUR means EUR 12,30.
CURRENCY	ISO 4217 three-letter currency code e.g. CHF, USD, EUR
MPI_SESSIONID	Must contain the same value as returned by the Authentication Response.
SUCCESSLINK	An URL identifying the web page where saferpay has to send the result of the authentication process.
FAILLINK	The saferpay MPI opens this URL if the authentication failes.
BACKLINK	The saferpay MPI opens this URL if the authentication aborts.
LANGID	<i>Optional:</i> Specifies the language of the virtual terminal / merchant plug-in session: en English de German fr French it Italian

4.5 STEP 4: VERIFY AUTHENTICATION RESULT

After the customer has authenticated himself at his card issuing bank, saferpay verifies the authentication and passes the authentication data to the merchant application (SUCCESSLINK with appended parameters DATA and SIGNATURE). The popup window closes automatically if JavaScript is enabled at the client browser.

The merchant application receives DATA and SIGNATURE and has to verify its contents by performing VerifyPayConfirm. The returned values must be passed to the following authorization request.

Attribute	Description
ECI	Electronic Commerce Indicator 1 = 3-D Secure transaction, cardholder authenticated 2 = 3-D Secure transaction, cardholder partial authenticated
CAVV	Cardholder Authentication Verification Value or UCAF field
XID	3-D Secure Transaction Identifier

4.6 STEP 5 AND 6: AUTHORIZATION REQUEST AND RESULT

Now the authorization of the payment amount could be executed.

Attention – mandatory!

Make sure to add the ECI attribute always and the optional XID and CAVV values to the authorization request if available. This is important to get the correct 3-D Secure flagging of the payment transaction and the liability shift.

5 PROGRAMMING EXAMPLES

You may use the following card numbers for testing purposes at the saferpay test account 99867-94913159:

Not 3-D Secure enrolled: 9451 1231 0000 0004 (12/06)
 3-D Secure enrolled: 9451 1231 0000 0111 (12/06)

5.1 COMMAND LINE

Step 1: Verify Enrollment Request

```
saferpay -exec -p . -m VerifyEnrollment -a ACCOUNTID "99867-94913159" -a PAN
"9451123100000111" -a EXP "1208" -a AMOUNT "1295" -a CURRENCY "EUR"
```

Step 2: Verify Enrollment Response

```
<IDP RESULT="0" ECI="1" ACCOUNTID="99867-94913159"
MPI_SESSIONID="19U082ApYUGtvA5WIYEzb3nlt65b"
AUTHMESSAGE="Card enrolled, continue authentication" />
```

Step 3: Authentication by MPI (Create PayInit URL)

```
saferpay -payinit -p . -a ACCOUNTID "99867-94913159"
-a AMOUNT "1295" -a CURRENCY "EUR"
-a MPI_SESSIONID "19U082ApYUGtvA5WIYEzb3nlt65b"
-a SUCCESSLINK "http://www.myshop.com/pay.asp?status=continue"
-a BACKLINK "http://www.myshop.com/pay.asp?status=aborted"
-a FAILLINK "http://www.myshop.com/pay.asp?status=failed"
```

Created URL:

```
https://www.saferpay.com/vt/Pay.asp?DATA=%3cIDP%20MSGTYPE%3d%22PayInit%22%20KEY
ID%3d%22%2d99867%2d568c6924a52546c48aaf643b257cf9f1%22%20TOKEN%3d%22fd3c1aad2
4d4e198c554e34c6c26121%22%20ALLOWCOLLECT%3d%22no%22%20DELIVERY%3d%22yes%22%20EX
PIRATION%3d%2220031217%2017%3a04%3a55%22%20ACCOUNTID%3d%2299867%2d94913159%22%2
0AMOUNT%3d%221295%22%20CURRENCY%3d%22EUR%22%20MPI%5fSESSIONID%3d%2219U082ApYUGt
vA5WIYEzb3nlt65b%22%20SUCCESSLINK%3d%22http%3a%2f%2fwww%2emyshop%2ecom%2fpay%2e
asp%3fstatus%3dcontinue%22%20BACKLINK%3d%22http%3a%2f%2fwww%2emyshop%2ecom%2fpa
y%2easp%3fstatus%3daborted%22%20FAILLINK%3d%22http%3a%2f%2fwww%2emyshop%2ecom%2
fpay%2easp%3fstatus%3dfailed%22%2f%3e&SIGNATURE=5a38021836db7c31a6f614d22d3f220
29238762ed86833ebd83c7d11e136acaf79ef6e44e079f6ad19302477074ead7b56f98a19bc0208
2fb66d9aa83e2d9d54
```

Step 4: Verify Authentication Data from MPI (SUCCESSLINK with DATA parameter)

```
saferpay -payconfirm -p . -d '<IDP MSGTYPE="PayConfirm" KEYID="1-0"
ACCOUNTID="99867-94913159" ECI="1" XID="t3Q1E3AffSxCtAMtQQ2jAGtGGodA"
CAVV="AAABAHgRWEcSJyYMRFYAAAAAAA=" />' -s 6984e3ec1905f0d3ff72342b214e
61228be6d77c1769012a48c3594f77a2e0b855b2e9e9649f7d8eaab0b9e8f1ce1466
8009a625ddae4f817859a0f0be2637
```

Step 5: Authorization Request Important! Please read chapter 4.6

```
saferpay -exec -p . -m Authorization -a ACCOUNTID "99867-94913159"
-a PAN "9451123100000111" -a EXP "1208" -a AMOUNT "1295"
-a CURRENCY "EUR" -a ECI "1" -a XID "t3Q1E3AffSxCtAMtQQ2jAGtGGodA"
-a CAVV "AAABAHgRWEcSJyYMRFYAAAAAAA="
```

5.2 VISUAL BASIC SCRIPT

Step 1: Verify Enrollment

```
Set mf = CreateObject("Saferpay.MessageFactory")
Set req = mf.CreateRequest("VerifyEnrollment")
req.SetAttribute "ACCOUNTID", "99867-94913159"
req.SetAttribute "PAN", "9451123100000111"
req.SetAttribute "EXP", "1208"
req.SetAttribute "AMOUNT", "12050" ' 120.50 EUR
req.SetAttribute "CURRENCY", "EUR"
Set res = req.Execute
```

Step 2: Verify Enrollment Response

```
RESULT = res.GetAttribute("RESULT")
if RESULT = 0 then
    ECI = res.GetAttribute("ECI")
    if ECI = 1 then
        '...card holder is 3-D Secure enrolled
        MPI_SESSIONID = res.GetAttribute("MPI_SESSIONID")
        '...create link to saferpay merchant plug-in
    else
        '...continue payment without authentication
    end if
else
    '...application or other error
    ' if RESULT = 301 then "ECI=0" (continue payment without authent.)
end if
```

Step 3: Authentication by MPI (Create PayInit URL)

```
Set mf = CreateObject("Saferpay.MessageFactory")
Set pi = mf.CreatePayInit()
pi.SetAttribute "ACCOUNTID", "99867-94913159"
pi.SetAttribute "AMOUNT", "12050"
pi.SetAttribute "CURRENCY", "EUR"
pi.SetAttribute "MPI_SESSIONID", MPI_SESSIONID
pi.SetAttribute "SUCCESSLINK", _
    "http://www.myshop.com/pay.asp?status=continue"
pi.SetAttribute "BACKLINK", _
    "http://www.myshop.com/pay.asp?status=aborted"
pi.SetAttribute "FAILLINK", _
    "http://www.myshop.com/pay.asp?status=failed"
url = pi.GetURL() ' open url as popup automatically...
```

Step 4: Authentication Data from MPI (SUCCESSLINK with DATA parameter)

```
DATA = Request.QueryString("DATA")
SIGNATURE = Request.QueryString("SIGNATURE")
Set mf = CreateObject("Saferpay.MessageFactory")
Set pc = mf.VerifyPayConfirm(DATA, SIGNATURE)
ECI = pc.GetAttribute("ECI")
XID = pc.GetAttribute("XID")
CAVV = pc.GetAttribute("CAVV")
' continue payment with 3-D Secure authentication data...
```

Step 5: Authorization Request Important! Please read chapter 4.6

```
Set mf = CreateObject("Saferpay.MessageFactory")
Set rq = mf.CreateRequest("Authorization")
req.SetAttribute "ACCOUNTID", "99867-94913159"
req.SetAttribute "PAN", "9451123100000111"
req.SetAttribute "EXP", "1208"
req.SetAttribute "AMOUNT", "12050" ' 120.50 EUR
req.SetAttribute "CURRENCY", "EUR"
req.SetAttribute "ORDERID", "0815-4711"
req.SetAttribute "ECI", ECI
req.SetAttribute "XID", XID ' if available!
req.SetAttribute "CAVV", CAVV ' if available!
Set res = req.Execute

...parsing the result...
```

5.3 OPENING AND CLOSING THE MPI POPUP

To automatically open the MPI popup window you should add the following code to your HTML document:

```
<script SRC="http://www.saferpay.com/OpenSaferpayScript.js"></script>
```

Use the JavaScript function "OpenSaferpayTerminal()" to open the popup automatically:

```
<a href="https://www.saferpay.com/pay.asp?xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
"
  onClick="OpenSaferpayTerminal(this.href, this, 'LINK')">
  Open MPI Popup...
</a>
```

The popup's name will be "SaferpayTerminal". After successful authentication of the cardholder the popup redirects to the given SUCCESSLINK and closes itself automatically.

6 REFERENCE

The documents listed below are integral part of this specification.

	Description	Version	Date
1	http://www.saferpay.com/help	1.0	
2	Saferpay Implementation Guide	1.2	17.01.2002
3	Saferpay Card Authorization Interface	1.5	07.08.2003

History

Version	Description	Date
1.0.0	Document initiated	07.10.2002
1.1.0	Implementation examples added	15.12.2003
1.2.0	“Summary” and “Requirements” enhanced, “Authentication Result” added	02.02.2004
1.3.0		19.02.2004
1.3.1		
1.4.0		
1.4.1		
1.4.2		