Reference manual for MERCHANT SYSTEM redirect integration

Release n. 2.0.1
December 2019

The information contained in this document is CONFIDENTIAL. Use, transfer or reproduction of this information, in whole or in part, is subject to the prior written consent of SIA.

1. Summary

1.1 Summary

1. SUMMARY 3

1.1 SUMMARY 3
1.2 TABLE OF SCHEMES 4
1.3 TABLE OF PICTURES 4
1.4 REVISIONS 4
1.5 GLOSSARY 5

2 INTRODUCTION 6

3 BACK OFFICE SIA VPOS 7

3.1 E-MAIL MESSAGES 7

4 REDIRECT SIA VPOS INTEGRATION 8

4.1 INTRODUCTION AND SETUP 8
4.1.1 Sending the logo 8
4.1.2 E-Mail messages 8
4.2 HTTP MESSAGES 10
4.2.1 Redirecting SIA VPOS payment initiation 10
4.2.2 The OPTIONS Field 14
4.2.3 Confirmation/outcome of message of effected payment 17

5 SIA VPOS APPENDICES 21

5.1 REFERENCES 21
5.2 GENERATING MAC REDIRECT 22
5.2.1 Generating the MAC for REDIRECT messages 22
5.2.2 Generating the MAC for outcome messages 24
5.3 PARAMETERS AUTHORMODE, ACCOUNTINGMODE AND POSSIBLE SCENARIOS 26
5.3.1 AUTHORMODE 26
5.3.2 ACCOUNTINGMODE 26
5.3.3 Possible scenarios 27
5.4 3DSDATA (REDIRECT) 28

1.2 Table of schemes

1.3 Table of pictures

1.4 Revisions

Date	Changes	Version
2014-05-27	First draft of the English version.	1.2.4
2015-07-09	Second draft of the English version.	1.3.5
2017-07-12	Update to version 1.6.4 and integrations	1.6.5
2018-03-23	Restyling. Missing Scheme added. RBA Messages. Minor fixes.	1.7.0
2018-05-10	Restyling. Added option and exponent on every message. Added name, surname, antifraud and product reference on authorization messages. Added description for some optional fields in the responses.	1.7.1
2018-06-01	API: added cardtype in the auth element; added taxid in auth msgs; fixed description for result code 38. Redirect: added taxid and antifraud. In response added acquirerbin and merchantid (like api; with option) and cardtype (with service). General: added iban network and token pan alias.	1.8.0
2018-06-15	API: fixed description for SENDMAIL on CREATELINK message.	1.8.1
2018-12-17	API: request of order status – Added pan alias section in response if the shop is enabled	1.8.2
2019-02-08	API: new 3DS 2.x API messages	1.9.0
2019-05-27	5.2.1 Redirect: added 3DSDATA field 6.2.1 MAC: added 3DSDATA field 6.5 3DSData: - added inclusion column for Redirect messages. - added threeDSRequestorChallengeInd field	1.9.1
2019-05-31	Rebranding	1.9.2
2019-06-07	- IBANAuthorization and IbanCode - Renaming of 3DS elements in ThreeDS and further modifications in 3DS2.x operations. - URLMERCHANT to MERCHANTURL	1.9.3
2019-09-30	Guide separation in redirect and api. Removed following fields: COMMIS, EXPONENT, BP_POSTEPAY, BP_CARDS from request/response. Updated descriptions for some request field. Various reformatting.	2.0.0
2019-12-11	4.2.2 Added option U 5.2.2 MAC: added CHINFO field	2.0.1

1.5 Glossary

Back office	Used for making reference to the management functions of a store: statements, lists, queries, instructions, etc.
CC	Credit Card
Booking	Transaction creating the accounting effects of a previously authorized transaction
Credit	Accounting transaction for the repayment of a monetary sum to a customer
GET	HTTP protocol communication transaction
Hash	All the N bits (i.e. 128, 160) obtained from a string through a mathematical process in a way that a different result is invariably obtained from a different string
HTTP	Application protocol used for transmitting web pages. Standard RFC 2068
MAC	Message authentication code
MD5	Algorithm for generating a unique 16 byte message identifier. Defined in RFC 1321
Merchant system	Virtual store management software system. Virtual store
SIA	FrontEnd Processor: SIA Spa
POST	HTTP protocol communication transaction
SHA-1	Secure Hash Algorithm. Algorithm for generating hashes. Standard NIST FIPS 180-1
Split	Transaction for subdividing/reducing a payment already effected.
SSL	Secure Socket Layer standard transport protocol created by Netscape Communication
Reversal	Transaction for the cancellation of a granted authorization with repayment of the sum and/or limit of expenditure to the card holder
URL	Universal resource locator
VBV	Verified By Visa, Visa security system for authenticating credit card holders during their purchases online
SecureCode	Security system for authenticating Mastercard and Maestro credit card holders during their purchases online (equivalent to VBV)
SafeKey	Security system for authenticating AMEX credit card holders during their purchases online (equivalent to VBV)

2 Introduction

This document contains important technical information for virtual store designers who wish to integrate their website with the SIA VPOS service. This manual, therefore, is addressed strictly to technical personnel. It does not contain an actual description of the SIA VPOS service, which, on the other hand, is provided by the appropriate documents.

This document provides a description of the **Redirect option** of the SIA VPOS system and of the related integration with the order management systems on the merchant side. For the **API Internet interface** see the related guide.

SIA VPOS is an Internet virtual POS provided directly by SIA to sellers. It enables merchants to carry out transactions online with their credit card using a PC and an Internet connection. The system can be used both to substitute the physical "box" of the traditional POS and as a customizable gateway for credit card transactions. For a general description of its functionalities, see the related document.
The SIA VPOS service is complemented by the functionalities of a back office graphic interface.

As regards the security of the Internet communication route, the degree of reliability offered is equivalent to that of the TLS 1.2 protocol with 256-bit encryption.

For API integration see "Merchant Integration VPOS API".

3 Back office SIA VPOS

The graphic interface of back office can be used by store operators, via browser, in order to manually perform authorization requests, reversals, statements, bookings, etc.

3.1 E-Mail messages

During the payment transactions carried out by store operators through the backoffice graphic interface, the SIA server may generate and send a number of e-mails to the customer and to the merchant.
The e-mail messages cannot be customized. No e-mails are sent when the requests are made using the API. For sending emails from Redirect, see the appropriate paragraph in the Redirect chapter.
The email to the holder is sent only if, at the time of request of authorization, this field has been entered in the authorization request screen.
The email to the operator is sent each and every time. The address used is the compulsory address entered in the authorization request screen.

The contents of the e-mails, if any, will be as follows:

- Amount
- Store sign
- Order number
- Authorization number
- Card type
- Date and time of transaction

4 Redirect SIA VPOS Integration

4.1 *Introduction and setup*

The interface between virtual store and the SIA VPOS system occurs by means of simple HTTP messages. Once the end-user has completed the acquisition phase, the virtual store will redirect the browser to the SIA VPOS system. The browser can be redirected through a form, link or an authentic HTTP redirect (response 30x). When the browser is redirected, a series of parameters are entered, permitting the SIA VPOS system to recognize the origin of the request and to prepare whatever is necessary to enable the customer to complete the payment transaction. At that stage, the acquirer will be requested to fill in a simple form containing the credit card data, the type of card (among those accepted by the store), his e-mail address etc. The user may in any case cancel the transaction and return to the store.
After completing the operation the card holder will be "sent back" to the original website with the data necessary to verify the effected payment and, at the same time, the SIA VPOS system will notify the store via HTTP.

In order to allow the user's browser to be redirected to the appropriate pages of the virtual store, the virtual store will enter three special fields in the first message sent to the SIA VPOS system containing three URLs:

- The URL to which the user is to be sent in case the payment process is cancelled and return to the change cart page (URLBACK)
- The URL to which the user is to be sent in case the transaction is successfully completed (URLDONE)
- The URL to be used by the SIA VPOS system in order to notify the store of the outcome of the completed transaction (URLMS)

The URLs for access to the service are the following:

- TEST environment: https://atpostest.ssb.it/atpos/pagamenti/main?PAGE=LAND
- PRODUCTION environment: https://atpos.ssb.it/atpos/pagamenti/main?PAGE=LAND

4.1.1 Sending the logo

The operator may customize the graphic payment interface by requesting the entry of its logo or brand in the space dedicated to the summary information on the order. The image must be sent via email to the address serviziopos@sia.eu. The image can be provided in GIF, JPG or PNG format and cannot be larger than 140x140 pixels and weigh more than 100Kb.

4.1.2 E-Mail messages

When a consumer carries out a payment transaction, the SIA server may generate and send a number of e-mails to the customer and to the merchant.
The transmission of e-mails to the merchant can be configured at the time the store subscribes to the service, choosing one of the following options:

1. Never
2. Always
3. Only in case of positive outcome
4. Always (data in XML format)
5. Only in case of positive outcome (data in XML format)

In case of change of e-mail address, the merchant shall communicate its new address to SIA.

The e-mails to the consumer, on the other hand, are sent always according to the two following cases:

1. Online authorization granted →Successful online transaction E-mail

2. Online authorization denied → Denied online transaction E-mail (giving reasons for the denial)

The information contained in the e-mail message can be in standard or XML format.

In case of standard format, the contents, if any, will be the following:

- Date of transaction
- Order number
- Amount
- Authorization number
- Store sign

The XML format, on the other hand, is required strictly for sending e-mails to the merchant and corresponds to the element Authorization of the SIA VPOS APIs. The subject of the e-mails in such format will be the following: "Authorization: order number <OrderID>"

The messages sent by SIA cannot be customized.

4.2 *HTTP messages*

4.2.1 Redirecting SIA VPOS payment initiation

The first step that the merchant must take is to have the customer's browser generate a payment process initiation message to SIA. This can be done either through a redirect or a link (using the HTTP GET method) or by sending a form with hidden fields (which can use the HTTP POST method).

The payment transaction initiation message sent to SIA by the user's browser must contain the following fields:

Name	Compulsory	Description
AMOUNT	Y	Amount expressed in the smallest currency unit (EUR cents). Minimum length 2 maximum length 8.
CURRENCY	Y	Currency: ISO code (EUR = 978)
ORDERID	Y	Order unique identifier: this must be an alphanumerical code with a maximum length of 50 characters. **Its unique nature must be guaranteed for at least 5 years.** Admitted characters include letters, numbers, "-" and "_". The regular expression [a-zA-Z0-9\-_] is applied.
SHOPID	Y	Identifier of the merchant's shop assigned by SIA.
URLBACK	Y	Complete URL to which the user is to be redirected to go to the store (it may include all the necessary parameters) in case the payment process is cancelled. Maximum length 254 characters.
URLDONE	Y	Complete URL to which the customer's browser is to be redirected once the transaction has been successfully completed (it may include all the necessary parameters). The outcome parameters are appended to the selected URL. Maximum length 254 characters.
URLMS	Y	URL of the merchant system to which SIA performs the GET or POST confirming the effected payment (it may contain any parameters set by the store). The outcome parameters are appended to the selected URL. Maximum length 400 characters.
ACCOUNTINGMODE	Y	Type of booking to be used for this order: • D deferred • I immediate See appendix 5.3.2.
AUTHORMODE	Y	Type of authorization to be used for this order: • I immediate See appendix 5.3.1.
MAC	Y	Message Authentication Code: it prevents the end user from changing the order data. For the related calculation see appendix 5.2.1.

LANG	N	The language in which the messages for interacting with the end user are to be displayed. This field is optional; the default language is English. The following are currently available: ITA Italian EN English
SHOPEMAIL	N	It contains the e-mail address to which the transaction results are to be sent. If it is not present, the one present in the store configuration data will be used. Minimum length 7 alphanumerical characters maximum length 50.
OPTIONS	N	It contains the indicators of the additional options to be activated for the payment. The order through which the options appear is irrelevant. The contents of the field are not case sensitive. See the corresponding paragraphs for further details
LOCKCARD	N	It contains the circuit code corresponding to the type of payment instrument by which the merchant has chosen to make the payment. The possible values for this parameter are the following: **01** – Visa **02** – Mastercard **04** – Maestro **06** – American Express **07** – Diners **08** – JCB **49** – Paypass / Masterpass **80** – IBAN **81** – AmazonPay **82** – EnelX **89** – ApplePay **91** – Jiffy / BancomatPay **92** – Paga con Postepay **94** – Postepay **96** – MyBank **97** – Paypal **A1** – GooglePay **CC** – Credit cards **NC** – Other payment instruments If the indicated lockcard is a credit card code (**01**, **02**, **04**, **06**, **07** or **08**), the user will be redirected to the payment page with the network field preselected and unchangeable. For lockcard **49** – Masterpass and **97** – Paypal the user will be automatically redirected to the login page of the related payment instrument, without displaying the instrument selection page. For lockcards **80** – IBAN, **81** – AmazonPay, **82** – EnelX, **89** – ApplePay, **96** – MyBank and **A1** – GooglePay the payment page will be activated only for the chosen payment instrument.

		For lockcard **92** – Paga con Postepay the user will be automatically redirected to the Postepay payment system. For lockcard **91** – BancomatPay a BPay transaction will be started automatically only if the field PHONENUMBER has been assigned a value. Otherwise, the user will land on the payment page in order to enter the telephone number. While indicating the **CC** circuit, the payment instrument selection page will contain only the credit cards to be selected. While indicating the **NC** circuit, the payment instrument selection page will contain only the circuits other than the credit cards to be selected. If the field is filled in with **NC** and an error occurs during the payment process, the user will be redirected to the URLBACK page.
EMAIL	N	Customer's e-mail address. If the field is not present, it will be requested to the user together with the credit card data. Minimum length 7 alphanumerical characters maximum length 50 .
ORDDESCR	N	Order description (see OPTIONS O or OPTIONS V). Maximum length 140.
VSID	N	Validation service identifier for MyBank transactions. If present, the MyBank bank selection page is skipped and the user is redirected to the home banking associated with the received ID. Maximum length 35.
OPDESCR	N	Additional description of the accounting operation, at merchant's discretion (only in case of immediate booking). Maximum length 100.
REMAININGDURATION	N	Minimum duration of validity in months of a credit card (for OPTIONS D).
USERID	N	User identifier. Alphanumerical with max length 255 characters.
PHONENUMBER	N	Telephone number for payments on BancomatPay circuit
CAUSATION	N	Reason for payments on BancomatPay circuit
USER	N	User for payments on BancomatPay circuit
NAME	N	Buyer's first name (only with OPTIONS B)
SURNAME	N	Buyer's surname (only with OPTIONS B)
TAXID	N	Buyer's tax id
PRODUCTREF	N	Sale identifier

ANTIFRAUD	N	Antifraud data payload containing additional information used for antifraud checks. Field is mandatory if SV69 is active.
3DSDATA	N	3DS data payload containing additional information used for the 3D secure 2.0.

Compulsory: Y, = yes, N = no

Please note: 3DSDATA field, if present, could become very large. Due to this it will not be possible any more to use the http GET method to pass the parameters in the URL to the SIA VPOS system. The redirect from the merchant site to the SIA VPOS payment gateway should be performed using the POST http method submitting an hidden form.

Note: the names of the fields contained in the tables above are all in capital letters and are case sensitive.

The order in which the fields appear in the initiation message is irrelevant.

In the communication process between the merchant and SIA there is the risk that a foreign party, after having intercepted the message, may attempt to alter its content, and later forward the altered message to the final addressee. This incident can only be prevented through the use of an authentication process, which assigns a MAC (Message Authentication Code) to each message.

The method adopted for generating MACs is the following: a hash HMAC256 or MD5 or SHA-1 is calculated for the string resulting from the sequence of parameters to be transmitted. For MD5 and SHA-1 the secret key is queued to the string; for HMAC256 the secret key is used directly in the calculation. The secret key consists of 50 or 100 characters and is provided by SIA to the operators. The addressee of the message in possession of the same secret string is able to verify the MAC and, hence, whether or not the parameters received are original.

The merchant has two secret strings:

- **Start key**: this is the string for calculating the MAC in the payment initiation messages referred to above
- **API-Result key**: this is the string for verifying the MAC of the outcome messages sent by SIA and for using the SIA VPOS APIs

The methods for calculating the MAC for payment requests and for the results (communicated by SIA) are set out, respectively, in appendices 5.2.1 and 5.2.2 of this document. The secret strings are safely communicated by SIA to the store upon initiation of the service.

The contents of the fields URLDONE, URLBACK and URLMS are at the store's full discretion. As regards URLDONE and URLMS, it should be noted that the order identification data are in any case affixed by SIA at the bottom of these two strings, as documented in the following paragraph. The maximum length of URLDONE and URLBACK is 254 characters, whilst that of URLMS is 400 characters.

If the original strings representing the merchant system's URL include special parameters or characters, they will need to be entered in the MIME application/x-www-form-urlencoded format (Special characters are transformed into %XX). If the form submit is used, the conversion will be performed automatically by the browser; if, on the other hand, a redirect is used, the conversion must be performed by the virtual store.

The user is redirected by the browser to the URLs URLDONE and URLBACK using the HTTP GET method.

The URLs URLDONE and URLBACK must start with "http://" or "https://" (or any other HTTP form which is valid and can be interpreted by the browsers).
The URL URLMS must start with "http://" or "https://", **only the standard ports can be used: 80 for http, 443 for https**.
The values set out above must in any case comply with the first instruction, that is, they must be transmitted in the MIME application/x-www-form-urlencoded format.

4.2.2 The OPTIONS Field

The field OPTIONS permits to activate various additional behaviors for the payment underway. Said options are indicated with a letter of the alphabet. The options currently available are the following:

- **B** – The system accepts two additional fields in the incoming message: NAME and SURNAME. The value of these fields, if any, is stored and associated to the order being processed. The fields cannot be changed by the customer and they are not displayed. In order to ensure that the values cannot be changed, the fields become part of the string for calculating the MAC. The fields NAME and SURNAME, however, are not compulsory.

- **D** – The system accepts the parameter RESIDUALDURATION to set a minimum credit card validity period.

- **G** – If authorization is granted, the system will not show the outcome of the transaction to the consumer, but rather, it will immediately redirect the latter to the URLDONE so as to enable the virtual store to show its own customized “receipt”. If authorization is denied to the user, the “enter your card” screen will be displayed again.

- **H** – In case of card payment, the fields ACQUIRERBIN and MERCHANTID are returned in URLMS and URLDONE.

- **I** – If authorization is granted, the system will add the field ISSUERCOUNTRY, containing information on the issuer’s country of origin, to the information already contained in the URLMS and URLDONE.

- **L** – In case of duplicated order, the system will send an URLMS with outcome code 07.

- **M** – OPTION M is used when the user is PAN ALIAS service enabled (at the adhering bank’s discretion).
  If authorization is granted, a Pan Alias will be generated and will be returned in the URLMS and URLDONE in the field PANALIAS. For further details on said additional functionality see the specific integration manual.

- **N** – If authorization is denied, the system will not show the transaction results to the consumer, but rather, it will immediately redirect the latter to URLDONE.

- **O** – In case of MyBank transaction, this option requires to enter the DESCRORD (order description) field value in field D13 (*remittance information*), instead of ORDERID (order number), as per normal procedure.

- **P** – The field AUTHCODE, representing the response code returned by the authorization backend, is returned in URLMS and URLDONE.

- **Q –** In case of Paypal payment, the system adds to URLMS and URLDONE the following information: PAYERID, PAYER and PAYERSTATUS. In case of Amazon Pay payment, the system adds to URLMS and URLDONE the following information: PAYER (cardholder email address).

- **R –** The MAC is calculated and sent to URLMS and URLDONE even if the result is negative. Rules for MAC attribution are the same used for the positive case.

- **U –** If option G or N is set, the system adds to URLMS, URLDONE and URLBACK the optional parameter named CHINFO which contains the URL encoded value of cardholder info field (optionally) returned by ACS during 3DS 2.x authentication.

- **V –** The content of the field ORDDESCR is shown in the payment page and in the receipt, for the skin SIA mobile.

- **W** – The system is preset to work inside a modal window.

- **X** – Add the EXPONENT field in the response also for the Euro currency.

The order in which the options appear is irrelevant.
The options may be indicated in both capital and lowercase letters: *OPTIONS=b* is the same as *OPTIONS=B*.

Example

The example set out below is not operational: it only gives an indication of how to initiate the payment process using a form.

```
<html>
<body>
<br><center>
SIA VPOS

<form action="http://atpostest.ssb.it/atpos/pagamenti/main" method="POST">

       <input type="hidden" name="PAGE" value="LAND">
       <input type="hidden" name="AMOUNT"  value="5000">
       <input type="hidden" name="CURRENCY"  value="978">
       <input type="hidden" name="LANG"  value="ENG">
       <input type="hidden" name="SHOPID"  value="129280000000211">
       <input type="hidden" name="ORDERID"  value="7893133444445">
       <input type="hidden" name="URLDONE"
              value="http://demo.demo.net/mimesys/urlok.html?oper=900">
       <input type="hidden" name="URLBACK"
              value="http://demo.demo.net/demoshop/backfromtl.html?IdShop=00000000000">
       <input type="hidden" name="URLMS"
              value="http://demo.ssb.net/index.html?EMAILCLI=tryme@demo.net&CART=02">
       <input type="hidden" name="ACCOUNTINGMODE" value="D">
       <input type="hidden" name="AUTHORMODE" value="I">
       <input type="hidden" name="OPTIONS" value="G">
       <input type="hidden" name="EMAIL" value="tryme@demo.net">
       <input type="hidden" name="SHOPEMAIL" value="tryme2@demo.net">
       <input type="hidden" name="MAC" value="376b61c1189ca70ef88e49c5d3631be7">

       <input type=submit value="Go...">
</form>
</body>
</html>
```

The URLs in the hidden fields must be set out normally as the browsers automatically perform the necessary coding when the user performs the submit.

4.2.3 Confirmation/outcome of message of effected payment

If authorization is granted, the outcome of the transaction will be communicated to the merchant system according to two different procedures. The first one goes through the user's browser, the second one occurs directly from the SIA server to the store.

In particular, said outcome will be communicated to the merchant using the addresses set out in the parameters URLDONE and URLMS; the first one will be contacted, at the acquirer's discretion, only at the end of the transaction; the second one, on the other hand, will be contacted by the SIA server, regardless of the customer's actions, as soon as the authorization circuit responds to the request submitted by the SIA VPOS system. The use of the second address provides a reasonable guarantee that the outcome of the transaction will be communicated to the merchant system regardless of the customer's actions.

At the time of subscription the user may choose whether or not to use URLMS to obtain notification through this mechanism only for transactions with a positive outcome or for all transactions, that is, with either a positive or negative outcome. The first option is recommended: notification of transactions with positive outcome only.

If the second option is selected, account should be taken of the fact that the customer, in the case of failure of the first transaction, may make various consecutive payment attempts for the same order. In that case, the merchant system will be notified N negative outcomes for N failures, and in the end a positive outcome.

The transaction confirmation message contains the following data:

Name	Description
ORDERID	order number: value copied from the field of the start message ORDERID
SHOPID	Shop identification code: value copied from the homonymous field of the start message
AUTHNUMBER	Authorization number: identifier of authorization assigned by the card issuer (only in case of positive outcome). If authorization is not granted, the field will be filled in with "NULL". This is a string with a maximum length of 6 characters for all circuits excluding MyBank; the latter, on the other hand, has a fixed length of 35 characters and contains the identifier of the transaction assigned by the Validation Service. It is irrelevant if the transaction is carried out through the Paypal circuit.
AMOUNT	Amount: value copied from the homonymous field of the start message
CURRENCY	Currency: value copied from the homonymous field of the start message
TRANSACTIONID	Identifier of transaction assigned by the SIA VPOS system. This is a 25-character string
MAC	Value for authenticating the confirmation message. For the related calculation see appendix 5.2.2. This is a 32, 40 or 64-character string.
RESULT	Outcome of the transaction. See the following page.
AUTHORMODE	Type of authorization: I immediate D deferred. Value copied from the homonymous field of the initiation message.
ACCOUNTINGMODE	Type of booking: I immediate D deferred. Value copied from the homonymous field of the initiation message.
NETWORK	Type of card used by the customer for the payment. See following page.
TRANSACTIONTYPE	This field indicates the type of transaction carried out (see table of values for the field TRANSACTIONTYPE).
ISSUERCOUNTRY	This field is present in the URLMS and URLDONE only if requested through option (I) and only upon granted authorization; it indicates the country of origin of the card issuer.

PAYERID	For “Q” OPTION and Paypal payments. Additional information about the acquirer. Max 13 characters alphanumerical string.
PAYER	For “Q” OPTION and Paypal payments. Additional information about the acquirer. Max 127 characters alphanumerical string.
PAYERSTATUS	For “Q” OPTION and Paypal payments. Additional information about the acquirer. Max 10 characters alphanumerical string.
HASHPAN	MD5 hash of the card or the payerid (for Paypal transactions), if the shop is enabled for the service.
IBAN	For MyBank payments, only if the store is enabled for the appropriate return service (SV58) or for IBAN payments.
ACCOUNTHOLDER	For MyBank payments, only if the store is enabled for the appropriate return service (SV58)
ALIASSTR	For payments with Postepay Button circuit, only if the store is enabled for the appropriate return service (SV62)
PANTAIL	Only for payments with a card and only if the store is enabled for the appropriate return service (SV64)
PANEXPIRYDATE	Only for payments with a card and only if the store is enabled for the appropriate return service (SV64)
PANALIAS	Only in the presence of option M and if the store is enabled to one of the Alias Pan services. It contains the alias pan associated with the card used by the client. Numerical with a length of 19
PANALIASREV	Only in the presence of option M and if the store is enabled to one of the services of Alias Pan. It contains the revoked alias pan. Numerical with a length of 19
PANALIASEXPDATE	Only in the presence of option M and if the store is enabled to one of the services of Alias Pan. It contains the expiry date of the alias pan in YYMM format.
PANALIASTAIL	Only in the presence of option M and if the store is enabled to one of the services of Alias Pan. Alphanumerical for requests with Paypal, otherwise it is numerical and corresponds to the last 4 figures of the pan.
MASKEDPAN	Only in the presence of option M and if the store is enabled to the masked return service (SV61). It contains the masked pan (first six and last four characters).
ACQUIRERBIN	Only in the presence of option H and if the customer payed with card. It contains the international code of the acquirer for the transaction.
MERCHANTID	Only in the presence of option H and if the customer payed with card. It contains the acquirer code of the merchant.
CARDTYPE	C for Credit; D for Debit; P for prepaid. Only for payments with a card, if the shop is SV82 enabled and the information is available.

The merchant system will receive a message at the URL URLMS and URLDONE consisting of the following:

URLMS:
URLMS&<confirmation>&MAC=<mac>

URLDONE:
URLDONE&<confirmation>&MAC=<mac>

Where:

<confirmation>=ORDERID=<orderId>&SHOPID=<shopId>&AUTHNUMBER=<authNumber>&AMOUNT=<amount>&TRANSACTIONID=<transactionId>&CURRENCY=<currency>&AUTHORMODE=<type of authorization>&RESULT=<outcome>& TRANSACTIONTYPE=<type of transaction>& ISSUERCOUNTRY=<country of issuer (if present)>&NETWORK=<type of card>&ACCOUNTINGMODE=<type of booking>

The field RESULT can have the following values:

Code	**Description**

00	Success
01	*Denied by system*
02	*Denied due to store configuration issues*
03	*Denied due to communication issues with the authorization circuits*
04	*Denied by card issuer*
05	*Denied due to incorrect card number*
06	*Unforeseen error during processing of request*
07	*Duplicated order*

In case of enablement to the service for the supply of explicit antifraud outcome (SV54) the following outcomes will also be possible:

Code	**Description**
60	Denied due to failed Riskshield antifraud check
61	Denied due to failed antifraud check AmexPan
62	Denied due to failed antifraud check AmexPanIP
63	Denied due to failed antifraud check H3GPan
64	Denied due to failed antifraud check ItaPanCountry
65	Denied due to failed antifraud check PaypalCountry
66	Denied due to failed antifraud check CardEnrolledAuthenticate
67	Denied due to failed antifraud check PanBlackList
68	Denied due to failed antifraud check CountryPan
69	Denied due to failed antifraud check PrepaidPan
70	Denied due to failed antifraud check DebitPan
71	Denied due to failed antifraud check VirtualPan
72	Denied due to failed antifraud check ThresholdAmount
73	Denied due to failed antifraud check H3GPanLit

Note: in the current implementation the only value of OUTCOME in URLDONE is 00

The field NETWORK can have the following values:

Code	**Description**
01	Visa
02	Mastercard
04	Maestro
06	American Express
07	Diners
08	JCB
80	IBAN
81	AmazonPay
82	EnelX
91	BancomatPay (Jiffy)
94	Postepay
96	MyBank
97	Paypal

The field TRANSACTIONTYPE may have the following values:

Code	**Description**
TT01	SSL
TT06	VBV
TT07	Secure Code
TT08	Merchant VBV

TT09	Merchant Secure Code
TT10	Not authenticated owner VBV
TT11	Mail Order Telephone Order
TT13	SafeKey
TT14	Merchant SafeKey
TT15	Not authenticated owner SafeKey
TT16	ProtectBuy
TT17	Merchant ProtectBuy
TT18	Not authenticated owner ProtectBuy

NOTE in case of transactions with cards from the Masterpass wallet, the transaction type code will be in the “TMnn” format, instead of “TTnn”. Numbers and meaning of the transaction type remain unchanged.

A “?” question mark will be affixed on the URLMS and URLDONE, unless already present.

IMPORTANT: The field names are all in capital letters and case sensitive; the order in which the parameters are entered in the GET or POST HTTP is irrelevant.

The MAC field is not calculated in case the transaction result is negative, unless “R” OPTION was requested. Therefore, its normal value is the “NULL” constant string.

If the outcome of the authorization request is not positive or if a problem has occurred during the calculation of the MAC or if the transaction is with PAYPAL without return of BILLINGAGREEMENT, the PANALIAS, PANALIASREV, PANALIASEXPDATE and PANALIASTAIL elements will have the value of “NULL”.

In case of unexpected error in the system due to which the alias pan is not generated and/or stored, the value of the PANALIAS, PANALIASREV, PANALIASEXPDATE and PANALIASTAIL elements will be “ERROR”.

For further information on the calculation and verification of the MACs for outcome messages see appendix C2.

The store is specifically responsible for calculating the MAC using the secret string "API-Result key" in its possession, in order to verify that it matches the one entered in the message received. Failure to make this check may cause the merchant system to consider valid also confirmation messages that have not been sent by SIA, but rather, by third parties.

It should be borne in mind that, over the course of integration, the HTTP messages sent to URLDONE, URLMS and URLBACK may in the future, thanks to the development of the system, present additional parameters which were not originally present. **The applications must therefore ignore any parameters which they do not recognize without the occurrence of failures.**

Should communication to the merchant system via URLMS fail, no message repeat mechanisms are envisaged. The site can query the SIA VPOS system through the API SIA VPOS in order to verify the state of any “pending” orders during the payment process.

5 SIA VPOS Appendices

5.1 References

Here below is a list of useful sources to which reference can be made for merchant system integration purposes.

SIA S.p.A. does not provide any type of warranty or support for the third party products set out below.

To obtain the hash MD5 or hash SHA-1 constituting the MAC, the SIA server makes use of the object Java MessageDigest of JDK Oracle. To calculate the HMAC-256, it makes use of the javax.crypto.Mac class with the HmacSHA256 algorithm, also provided by JDK.

A form for calculating hash MD5 in PERL can be obtained from the following URL:

http://www.perl.com/CPAN-local/modules/by-module/MD5/

A number of (business) forms for calculating the hash MD5 in visual basic can be obtained from the following addresses:

http://www.aspencrypt.com/index.html
http://www.hotscripts.com/ASP/Scripts_and_Components/Security_Systems/
http://www.anei.com/aneimd5.asp
http://www.aspin.com/func/search?qry=md5&cat=all&IMAGE1.x=25&IMAGE1.y=7

Function **md5** for calculating the hash on a string is available in the standard libraries of PHP3.

For a definition of the standard MD5 see:

http://www.columbia.edu/~ariel/ssleay/rfc1321.html

For a definition of the standard SHA-1 see:

http://csrc.nist.gov/cryptval/shs.html

For a definition of the HMAC-256 standard and examples of implementation in various languages, see:

https://en.wikipedia.org/wiki/Hash-based_message_authentication_code

https://www.supermind.org/blog/1102/generating-hmac-md5-sha1-sha256-etc-in-java

https://www.jokecamp.com/blog/examples-of-creating-base64-hashes-using-hmac-sha256-in-different-languages

5.2 Generating MAC Redirect

5.2.1 Generating the MAC for REDIRECT messages

The MAC that must be transmitted enclosed in the messages starting the payment process is obtained with the procedure described below.

The hash function can be selected by the merchant from among three standard algorithms: SHA-1 (also known as SHA), MD5 and HMAC-256 (recommended). Given that the three algorithms produce a different number of bits (160 the first, 128 the second, 256 the third) the system is capable of automatically recognizing the type of function used for generating the MAC. The store site is free to change the algorithm used.

The merchant and SIA share a secret string of 50 or 100 characters. To produce the MAC for the data a hash of the text to be signed is performed, queuing the secret string for SHA-1 and MD5, using the secret string as a key for HMAC-256.

For transaction initiation messages, the text to be signed must contain the following fields, in this order:

• URLMS	
• URLDONE	
• ORDERID	
• SHOPID	
• AMOUNT	
• CURRENCY	
• EXPONENT	(if present)
• ACCOUNTINGMODE	
• AUTHORMODE	
• OPTIONS	(if present)
• NAME	(if present, for OPTIONS B)
• SURNAME	(if present, for OPTIONS B)
• TAXID	(if present)
• LOCKCARD	(if present)
• COMMIS	(if present, for OPTIONS F)
• ORDDESCR	(if present, for OPTIONS O or V)
• VSID	(if present)
• OPDESCR	(if present)
• REMAININGDURATION	(if present, for OPTIONS D)
• USERID	(if present)
• PHONENUMBER	(if present, for Jiffy circuit)
• CAUSATION	(if present, for Jiffy circuit)
• USER	(if present, for Jiffy circuit)
• PRODUCTREF	(if present)
• ANTIFRAUD	(if present)
• 3DSDATA	(if present)

An example of a string for calculating the MAC SHA1 or MD5 is:

```
MAC=Hash(URLMS=<urlms>&URLDONE=<urldone>&ORDERID=<orderid>&SHOPID=<shopid>
&AMOUNT=<Amount>&CURRENCY=<Currency>&ACCOUNTINGMODE=<accountingmode>&A
UTHORMODE=<authormode>&<startsecretstring>)
```

With OPTIONS it can become, for example**:**

MAC=Hash(URLMS=<urlms>&URLDONE=<urldone>&ORDERID=<orderid>&SHOPID=<shopid>&AMOUNT=<Amount>&CURRENCY=<Currency>&ACCOUNTINGMODE=<accountingmode>&AUTHORMODE=<authormode>&OPTIONS=B&NAME=<name>&SURNAME=<surname>&<startsecretstring>)

A similar example of a string for calculating the MAC HMAC-256 is:

```
MAC=Hash(URLMS=<urlms>&URLDONE=<urldone>&ORDERID=<orderid>&SHOPID=<shopid>
&AMOUNT=<Amount>&CURRENCY=<Currency>&ACCOUNTINGMODE=<accountingmode>&A
UTHORMODE=<authormode>, <startsecretstring> )
```

In this case the secret string is not queued to the string to be signed, but it contributes directly as a key in calculating the HMAC-256.

The order in which the fields appear is clearly essential. The secret string to be used is that called "start key".

In calculating the MAC the fields URLMS and URLDONE must be used in their not "encoded" form, even if they contain parameters.

An example of such a string could be the following:

URLMS=http://www.dominio.it/ok.asp?par=45&nord=23684&URLDONE=http://www.dominio.it/negozio.asp?par=45&nord=23684&ORDERID=A4845b2&SHOPID=123456789012345&AMOUNT=100&CURRENCY=978&ACCOUNTINGMODE=I&AUTHORMODE=D&Absd830923fk32..

The MAC, which is the result of a hash, must be coded appropriately for it to be transmitted in HTTP. To that end, an hexadecimal conversion must be performed.
The result of said conversion is a 32-character string, if the hash function used is MD5. If, on the other hand, SHA-1 is used, the result will be a 40-character string. If HMAC-256 is used, the result will be a 64-character string.

The MAC is not case sensitive. Capital and lowercase letters can be used without distinction.

5.2.2 Generating the MAC for outcome messages

The MAC which SIA VPOS encloses in the outcome messages shipped to the merchant system is obtained with the procedure described herein. The merchant and SIA share a secret string of 50 or 100 characters. To produce the MAC of the data, a hash of the connection between text to be signed and secret string is performed. Otherwise, an HMAC-256 is calculated using the secret string as key for the text to be signed. Note that SIA uses a secret string other than the start key for calculating the MAC of the outcome messages; this string is called "API-result" key because it is used also for access to the API SIA VPOS.

The hash function used by the system for generating the MAC is the same as that adopted by the operator for generating the MAC of the start message. Given that the SHA1, MD5 and HMAC256 algorithms produce a varying number of bits (160 the first, 128 the second, 256 the third) the system is capable of automatically recognizing the type of function used for generating the MAC of the start message, and using in turn the same algorithm to reply.
In brief, if the MAC of the start message is calculated with MD5, also the MAC of the outcome will be calculated with MD5, if the MAC of the start message is calculated with SHA1, also the MAC of the outcome will be calculated with SHA-1. If the start message is in HMAC256, so will be the outcome message.

For confirmation messages, the signed text will contain the following fields:

- ORDERID
- SHOPID
- AUTHNUMBER (if the authorization is not present, the field will have the value of "NULL")
- AMOUNT
- CURRENCY
- TRANSACTIONID
- ACCOUNTINGMODE
- AUTHORMODE
- RESULT
- TRANSACTIONTYPE
- ISSUERCOUNTRY (if requested via OPTIONS I)
- AUTHCODE (if requested via OPTIONS P)
- PAYERID, PAYER, PAYERSTATUS (for Paypal payments, if requested via OPTIONS Q)
- HASHPAN (if the store is enabled to the service)
- PANALIASREV, PANALIAS, PANALIASEXPDATE, PANALIASTAIL (if OPTION M and authorized transaction)
- MASKEDPAN (if OPTION M, authorized transaction and service SV61)
- PANTAIL, PANEXPIRYDATE (if the store is enabled to the SV64 service)
- ACCOUNTHOLDER (for MyBank payments, if the store is enabled to the SV58 service)
- IBAN (for MyBank payments, if the store is enabled to the SV58 service, or for IBAN payments)
- ALIASSTR (for payments with the Postepay Button circuit, if the store is enabled to the SV62 service)
- ACQUIRERBIN, MERCHANTID (for card payment, if requested via OPTIONS H)
- CARDTYPE (for card payment, if the store is enabled to the SV82 service)
- CHINFO (optional and only if requested via OPTIONS U and OPTIONS G or N)

An example of a string for calculating the MAC SHA1 or MD5 is:

```
MAC=Hash(ORDERID=<orderId>&SHOPID=<shopId>&AUTHNUMBER=<authNumber>&AMOUN
T=<Amount>&CURRENCY=<Currency>&TRANSACTIONID=<transactionId>&ACCOUNTINGMO
DE=<accountingMode>&AUTHORMODE=<authorMode>&RESULT=<Result>&TRANSACTIONTY
PE=<transactionType>&ISSUERCOUNTRY=<issuerCountry>&CHINFO=<chinfo>&<API-Result key
>)
```

A similar example of a string for calculating the MAC HMAC-256 is:

```
MAC=Hash(ORDERID=<orderId>&SHOPID=<shopId>&AUTHNUMBER=<authNumber>&AMOU
NT=<Amount>&CURRENCY=<Currency>&TRANSACTIONID=<transactionId>&ACCOUNTING
MODE=<accountingMode>&AUTHORMODE=<authorMode>&RESULT=<Result>&TRANSACTI
ONTYPE=<transactionType>&ISSUERCOUNTRY=< issuerCountry>, <API-Result key >)
```

The order in which the fields appear is clearly essential. The secret string to be used is that called “API-result key”.

An example of such a string could be the following:

ORDERID=A4845b2&SHOPID=123456789012345&AUTHNUMBER=HJ89KR&AMOUNT=100&CURRENCY=978&TRANSACTIONID=HK84HL2G&ACCOUNTINGMODE=I&AUTHORMODE=I&RESULT=00&TRANSACTIONTYPE=TT01&Absd830923fk32&ISSUERCOUNTRY=ITA

The MAC, which is the result of a hash, must be coded appropriately for it to be transmitted in HTTP. To that end, an hexadecimal conversion must be performed. The result of said conversion is a 32-character string, if the hash function used is MD5. If, on the other hand, SHA-1 is used, the result will be a 40-character string. If HMAC-256 is used, the result will be a 64-character string.

The MAC must not be treated as case sensitive. The SIA server uses capital letters.

Note: If the outcome of the transaction is negative, unless OPTION "R" has been requested, the MAC will not be calculated and it will have the value of “NULL”.

5.3 Parameters AUTHORMODE, ACCOUNTINGMODE and possible scenarios

Here follows a brief description of the meaning of the parameters TAUTOR and TCONTAB in connection with the various possible uses of the SIA VPOS system.

5.3.1 AUTHORMODE

Immediate authorization I

The immediate authorization procedure provides that during the online payment phase the authorization request is sent immediately to the international circuits. Once the transaction has been successfully completed, the merchant is certain that what is owed by the customer has been "booked" from his ceiling.

5.3.2 ACCOUNTINGMODE

Immediate booking I

The immediate booking procedure permits the merchant to make any authorized transactions automatically bookable. Without merchant's intervention, the same evening of the day on which the transaction took place, the front end processor automatically performs a clearing of the transactions for the full authorized amount.
This procedure can be adopted, for example, in the case where the goods/services sold can be used immediately by the acquirer (software, music, online services, etc.).

Deferred booking D

The deferred booking procedure provides that authorized transactions are explicitly made bookable by the merchant. The merchant has a preset number of days from the time authorization is granted to book a transaction.

This procedure makes available to the merchant the following transactions:

- Overall booking: a transaction is made bookable for the full amount of the authorized sum.
- Partial booking: a transaction is made bookable for an amount which is lower than the authorized sum; a partial booking transaction may refer to an authorization for which a partial booking (split shipment) has already been requested, provided that the final booking term has not expired.
- Cancellation: a booking transaction carried out during the day is cancelled, the transaction can be booked again.

5.3.3 Possible scenarios

Here below is a list of possible scenarios of the system operation

Functionality	**Mechanism that can be used**
Payment of immaterial goods (download or services)	Payment initiation with immediate authorization AUTHORMODE=I, immediate or deferred booking
Payment of inseparable material goods always available	Initiation of payment with immediate authorization AUTHORMODE=I, immediate or deferred booking
Payment of material goods to be procured	Initiation of payment with deferred authorization (AUTHORMODE=D) and subsequent authorization request with immediate booking
Split shipment (division and/or reduction): delivery of goods at different stages Assumption: • The store knows beforehand that it will deliver in pieces • The total amount is known in advance	Initiation of payment with deferred authorization (AUTHORMODE=D) and N subsequent authorization requests with immediate booking
Split shipment (division and/or reduction): delivery of goods at different stages Assumption: • The store did not know in advance that it was to deliver by instalments • An online authorization has been sent for the full amount	In this circumstance, a split (division and/or reduction) of the authorization must be performed: this transaction will transform an online order into a deferred order. After the split (division and/or reduction) transaction, N authorization requests can be sent as in the case of a normal deferred authorization

5.4 3DSData (Redirect)

3DSDATA field must be obtained through AES encryption of the JSON representation of all the fields the merchant wants to send to the networks. The following table contains all the fields that can be include within 3DSDATA.
Encryption algorithm must be AES/CBC/PKCS5Padding and must use as encrypting key the first 16 bytes of the API secret key. The initialization vector to be used for data encryption must be 16 bytes length equal to 0. Encrypted byte array must encoded to base64.

The following table lists all the fields that can be used in the JSON object for the 3DSDATA. The JSON object is a simple unordered set of name/value pairs. All strings are UTF-8 encoded.
To be more precise the fields descriptions reported in the table are directly extracted from the EMVco standard defining 3DS 2.

Field Name	Short Description	Description	Values	Inclusion
threeDSRequestorChallengeInd	3DS Requestor Challenge Indicator	Indicates whether a challenge is requested for this transaction. For example: For 01-PA, a 3DS Requestor may have concerns about the transaction, and request a challenge. For 02-NPA, a challenge may be necessary when adding a new card to a wallet. For local/regional mandates or other variables.	Length: 2 characters JSON Data Type: String Values accepted: • 01 = No preference • 02 = No challenge requested • 03 = Challenge requested: 3DS Requestor Preference • 04 = Challenge requested: Mandate • 05–79 = Reserved for EMVCo future use (values invalid until defined by EMVCo) • 80-99 = Reserved for DS use Note: If the element is not provided, the expected action is that the ACS would interpret	O
addrMatch	Address Match Indicator	Indicates whether the Cardholder Shipping Address and Cardholder Billing Address are the same.	Y or N	R
chAccAgeInd	Cardholder Account Age Indicator	Length of time that the cardholder has had the account with the 3DS Requestor.	• 01 = No account (guest check-out) • 02 = Created during this transaction • 03 = Less than 30 days • 04 = 30-60 days • 05 = More than 60 days	Or
chAccChange	Cardholder Account Change	Date that the cardholder's account with the 3DS Requestor was last changed, including Billing or Shipping address, new payment account, or new user(s) added.	Date format = YYYYMMDD	Or

chAccChangeInd	Cardholder Account Change Indicator	Length of time since the cardholder's account information with the 3DS Requestor was last changed, including Billing or Shipping address, new payment account, or new user(s) added.	• 01 = Changed during this transaction • 02 = Less than 30 days • 03 = 30-60 days • 04 = More than 60 days	O
chAccDate	Cardholder Account Date	Date that the cardholder opened the account with the 3DS Requestor.	Date format = YYYYMMDD	O
chAccPwChange	Cardholder Account Password Change	Date that cardholder's account with the 3DS Requestor had a password change or account reset.	Date format = YYYYMMDD	O
chAccPwChangeInd	Cardholder Account Password Change Indicator	Indicates the length of time since the cardholder's account with the 3DS Requestor had a password change or account reset.	• 01 = No change • 02 = Changed during this transaction • 03 = Less than 30 days • 04 = 30-60 days • 05 = More than 60 days	O
nbPurchaseAccount	Cardholder Account Purchase Count	Number of purchases with this cardholder account during the previous six months.	String max 4	O
txnActivityDay	Number of Transactions Day	Number of transactions (successful and abandoned) for this cardholder account with the 3DS Requestor across all payment accounts in the previous 24 hours.	String max 3	O
txnActivityYear	Number of Transactions Year	Number of transactions (successful and abandoned) for this cardholder account with the 3DS Requestor across all payment accounts in the previous year.	String max 3	O
shipAddressUsage	Shipping Address Usage	Date when the shipping address used for this transaction was first used with the 3DS Requestor.	Date format = YYYYMMDD	O

shipAddressUsageInd	Shipping Address Usage Indicator	Indicates when the shipping address used for this transaction was first used with the 3DS Requestor.	• 01 = This transaction • 02 = Less than 30 days • 03 = 30-60 days • 04 = More than 60 days	O
shipNameIndicator	Shipping Name Indicator	Indicates if the Cardholder Name on the account is identical to the shipping Name used for this transaction.	• 01 = Account Name identical to shipping Name • 02 = Account Name different than shipping Name	O
acctID	Cardholder Account Identifier		String max 64	O
billAddrCity	Cardholder Billing Address City	The city of the Cardholder billing address associated with the card used for this purchase.	String max 50	R
billAddrCountry	Cardholder Billing Address Country	The country of the Cardholder billing address associated with the card used for this purchase.	ISO 3166-1 numeric three-digit country code, other than exceptions listed in Table A.5.	R
billAddrLine1	Cardholder Billing Address Line 1	First line of the street address or equivalent local portion of the Cardholder billing address associated with the card used for this purchase.	String max 50	R
billAddrLine2	Cardholder Billing Address Line 2	Second line of the street address or equivalent local portion of the Cardholder billing address associated with the card used for this purchase.	String max 50	O
billAddrLine3	Cardholder Billing Address Line 3	Third line of the street address or equivalent local portion of the Cardholder billing address associated with the card used for this purchase.	String max 50	O
billAddrPostCode	Cardholder Billing Address Postal Code	ZIP or other postal code of the Cardholder billing address associated with the card used for this purchase	String max 16	R
billAddrState	Cardholder Billing Address State	The state or province of the Cardholder billing address associated with the	Variable, maximum 3 characters. Should be country subdivision code defined in ISO 3166-2	R

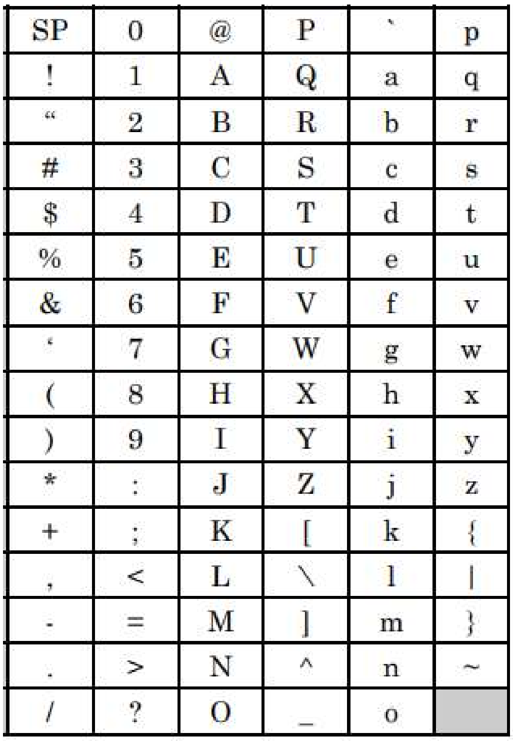
		card used for this purchase.		
homePhone	Cardholder Home Phone Number	The home phone number provided by the Cardholder.	country code(1-3) - number (max 15)	Or
mobilePhone	Cardholder Mobile Phone Number	The mobile phone number provided by the Cardholder.	country code(1-3) - number (max 15)	Or
shipAddrCity	Cardholder Shipping Address City	City portion of the shipping address requested by the Cardholder. Required unless shipping information is the same as billing information (addrMatch = Y).	String max 50	C
shipAddrCountry	Cardholder Shipping Address Country	Country of the shipping address requested by the Cardholder. Required unless shipping information is the same as billing information (addrMatch = Y).	ISO 3166-1 numeric three-digit country code, other than exceptions listed in Table A.5.	C
shipAddrLine1	Cardholder Shipping Address Line 1	First line of the street address or equivalent local portion of the shipping address requested by the Cardholder. Required unless shipping information is the same as billing information (addrMatch = Y).	String max 50	C
shipAddrLine2	Cardholder Shipping Address Line 2	Second line of the street address or equivalent local portion of the shipping address requested by the Cardholder.	String max 50	O
shipAddrLine3	Cardholder Shipping Address Line 3	Third line of the street address or equivalent local portion of the shipping address requested by the Cardholder.	String max 50	O
shipAddrPostCode	Cardholder Shipping Address Postal Code	The ZIP or other postal code of the shipping address requested by the Cardholder. Required	String max 16	C

		unless shipping information is the same as billing information (addrMatch = Y).		
shipAddrState	Cardholder Shipping Address State	The state or province of the shipping address associated with the card being used for this purchase. Required unless shipping information is the same as billing information (addrMatch = Y).	Variable, maximum 3 characters. Should be country subdivision code defined in ISO 3166-2	C
workPhone	Cardholder Work Phone Number	The work phone number provided by the Cardholder.	country code(1-3) - number (max 15)	O
deliveryEmailAddress	Delivery Email Address	For Electronic delivery, the email address to which the merchandise was delivered.	String max 254	Or
deliveryTimeframe	Delivery Timeframe	Indicates the merchandise delivery timeframe.	• 01 = Electronic Delivery • 02 = Same day shipping • 03 = Overnight shipping • 04 = Two-day or more shipping	Or
preOrderDate	Pre-Order Date	For a pre-ordered purchase, the expected date that the merchandise will be available.	Date format = YYYYMMDD	Or
preOrderPurchaseInd	Pre-Order Purchase Indicator	Indicates whether Cardholder is placing an order for merchandise with a future availability or release date.	• 01 = Merchandise available • 02 = Future availability	Or
reorderItemsInd	Reorder Items Indicator	Indicates whether the cardholder is reordering previously purchased merchandise.	Length: 2 characters JSON Data Type: String Values accepted: • 01 = First time ordered • 02 = Reordered	Or

shipIndicator	Shipping Indicator	Indicates shipping method chosen for the transaction. Merchants must choose the Shipping Indicator code that most accurately describes the cardholder’s specific transaction, not their general business. If one or more items are included in the sale, use the Shipping Indicator code for the physical goods, or if all digital goods, use the Shipping Indicator code that describes the most expensive item.	• 01 = Ship to cardholder’s billing address • 02 = Ship to another verified address on file with merchant • 03 = Ship to address that is different than the cardholder’s billing address • 04 = “Ship to Store” / Pick-up at local store (Store address shall be populated in shipping address fields) • 05 = Digital goods (includes online services, electronic gift cards and redemption codes) • 06 = Travel and Event tickets, not shipped • 07 = Other (for example, Gaming, digital services not shipped, emedia subscriptions, etc.)	Or

Please note that:

- According to the EMVCo 3DS standards “3DS Requestor” stands for “Merchant”.
- All strings must use UTF-8-character set.
- **Inclusion** column meaning:
  - “R” required
  - “Or” optional recommended
  - “O” optional
  - “C” conditional



SP	0	@	P	`	p
!	1	A	Q	a	q
“	2	B	R	b	r
#	3	C	S	c	s
$	4	D	T	d	t
%	5	E	U	e	u
&	6	F	V	f	v
‘	7	G	W	g	w
(	8	H	X	h	x
)	9	I	Y	i	y
*	:	J	Z	j	z
+	;	K	[	k	{
,	<	L	\	l	|
-	=	M	]	m	}
.	>	N	^	n	~
/	?	O	_	o	

Code example

The following Java code is provided just as a mean to clarify the encryption process to be applied to produce the 3DSDATA field.

```
import java.security.InvalidAlgorithmParameterException;
import java.io.UnsupportedEncodingException;
import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;

import javax.crypto.BadPaddingException;
import javax.crypto.Cipher;
import javax.crypto.IllegalBlockSizeException;
import javax.crypto.NoSuchPaddingException;
import javax.crypto.spec.IvParameterSpec;
import javax.crypto.spec.SecretKeySpec;
import javax.xml.bind.DatatypeConverter;

public class Utility {

   public static String encode3DSdata(String APISecretMerchant, String
JSONobject) throws Throwable {

        // Initialization vector
        byte[] iv = { 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 };

        // AES Key from the API merchant key
        byte[] key = APISecretMerchant.substring(0, 16).getBytes();
        IvParameterSpec ivParameterSpec = new IvParameterSpec(iv);
        SecretKeySpec secretKeySpec = new SecretKeySpec(key, "AES");

        // What we should encrypt
        byte[] toEncrypt = JSONobject.getBytes("UTF-8");
        // Encrypt
        Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
        cipher.init(Cipher.ENCRYPT_MODE, secretKeySpec, ivParameterSpec);
        byte[] encrypted = cipher.doFinal(toEncrypt);

        // Convert to base64
        return DatatypeConverter.printBase64Binary(encrypted);

    }
}
```