Virtual POS

Operating and Installation Manual

Sabadell

Chosen by the best in business. And by people like you.

Index

1. INTRODUCTION 4
2. WHAT DO I NEED? 8
    2.1 How is it installed? 9
    2.2 What should my website have? 9
    2.3 What payment regulations must I follow? 10
3. SECURITY MEASURES 12
    3.1 Velocity checks 13
    3.2 Verification of the CVV2 13
    3.3 3D Secure Protocol 13
    3.4 Additional security measures 14
4. OPERATIONAL ASPECTS 16
    4.1 Types of transactions 17
    4.2 Request for payment documentation on the part of the purchaser 20
    4.3 IUPAY 21
5. VIRTUAL POS ADMINISTRATION MODULE 23
    5.1 Access 24
    5.2 Users 25
    5.3 Operations: queries and administration 25
    5.4 Refund of operations 25
    5.5 Checking totals 26
6. INSTALLATION 27
    6.1 Payment form of the merchant's website. 28
    6.2 Locating errors 32
    6.3 Design of the hash algorithm in the internet server 35
    6.4 Online response 36
    6.5 Continuity of the browser session 45
    6.6 Sending transactions to the Virtual POS via XML protocol 45
    6.7 Test environment 48
    6.8 Payment of subscriptions and payments express 50
    6.9 Technical support service for installation 53
ANNEX 54
    Annex I. – ISO country codes 55
    Annex II. – ISO currency codes 57

1.

Introduction

Banco Sabadell is the bank chosen by the best in merchant and as such, is the leader in merchant collection solutions, always anticipating and conducting ongoing research into the most advanced technological media.

eCommerce is no longer exclusive to a certain type of company: small merchants, professionals, SMEs, major corporates, etc., an increasingly large number of companies are adopting eCommerce and require **secure solutions which adapt** to thee reality of their merchant.

In our opinion, this requires a technology capable of delivering multiple requirements. In short, **virtual POSs** which meet the needs of any company or merchant operating online.

For this reason, Banco Sabadell has strengthened its eCommerce service and has a specific unit of agents specialised in virtual payment gateways and a back-office team to offer our customers different secure solutions together with a broad range of services in online sales.

Two types of needs, two POS solutions

Banco Sabadell offers two payment gateways in line with the characteristics of the customer:

- **Virtual POS**. The most widely used solution which effectively covers the requirements of merchants and SMEs. This gateway is easy to install yet offers a broad range of services and specific benefits for eCommerce.

This manual covers the descriptions and installation instructions of the Virtual POS solution services.

- **Virtual Plus POS**. This is a more sophisticated solution which is designed for companies with a high volume of online sales. It offers an advanced set of technical and operating services in addition to ongoing support by agents specialised in eCommerce payments. This solution is defined in a specific manual in addition to this document. If your merchant payments require the Virtual Plus POS services, request the manual from your Banco Sabadell branch or agent.

Security elements

Maximum security is one of Banco Sabadell's top priorities. Our integral **3D Secure Gateway** which operates under international protocols verified by Visa and MasterCard SecureCode (both based on Secure 3D technology), offers high security and payment protection.

These protocols obtain the authentication of the holder when making the purchase, i.e. the **customer is identified** as the legitimate holder of the card being used.

However, there are establishments which prefer to deactivate the 3D Secure protocols and replace them with alternative **fraud control** systems. In this case, they can simply request their bank agent to analyse the merchant and implement the modification if they consider it appropriate.

Likewise, and especially for merchants and SMEs, the Virtual POS of Banco Sabadell is configured with security limits – velocity checks – which validate repeated attempts to purchase with the same card and/or from the same IP, significantly reducing the risk of fraud.

The security requirements are even more rigorous in the case of the Virtual Plus POS, in accordance with the high billing volumes. Specifically, it includes additional security elements such as: **Advanced fraud management rules, daily reports** on doubtful transactions (claimed, disputed or declared illicit by the purchasers) and collaboration and technical integration agreements with major gateways, processers and international fraud-scrubbing companies.

IUPAY, the digital wallet of Banco Sabadell

Banco Sabadell platform allows you to receive funds from your sales directly by IUPAY, the new digital wallet that allows your customers to store very easily all the cards from different banks. So they can shop online in a much more convenient and faster way, but keeping all security guarantees. View IUPAY operational aspects in section 4.3 of this manual.

Payments of subscriptions and Express Payments: Enhancing the user experience

The Banco Sabadell Virtual POSs accept the usual operations: Authorisations, pre-authorisations, authentications, returns management and recurring purchases.

But the true innovation lines in the system via which the card details are stored on the gateway itself.

The advantage is clear: with this functionality the merchant customer enters his card details just once on making the first purchase and does not need to repeat this step in future payments in the same establishment. Thus, the merchant increases its website usability (express payment) and also has a tool for processing subscriptions or other regular payments.

Solutions for internationalisation

In eCommerce the limit is the world. Banco Sabadell has taken special care of this feature, integrating solutions which facilitate cross-border sales:

- The **Multicurrency service** allows customers to purchase in a **wide range of local currencies**, avoiding the obstacles usually associated with currency conversion.
- **DCC transactions** (Dynamic Currency Conversion) offers **online conversion of the local currency into the Euro**. This operation is launched as soon as the Virtual POS detects that the card has been issued outside the Eurozone.
- The gateway is also **multi-language**, both for the merchant and the purchaser. Currently the Virtual POS accepts operations in Spanish, Catalan, Basque, English, French, German, Portuguese, Dutch, Polish, Italian and Swedish.

There are also specific tools for the Virtual Plus POS which have been developed to maximise sales and simplify transactions via international affiliates:

- Many countries have **local payment systems** which are different to financial cards, which are widely accepted. These sales cannot be lost and for this reason, Banco Sabadell has international agreements to access a large number of these payment systems.
- If the company has affiliates in other European countries, thanks to the **Banco Sabadell Cross-Border license** it is possible to process Visa or MasterCard payments at Spanish merchants and affiliates. A single integration with the Virtual Plus POS enables all sales to be managed.

Back Office Tools

We believe the merchant management should be simply and user-friendly, but also a complete solution. The Virtual POS includes a website-based administration module designed to offer simple use and offer all the functionalities.

- **Real time control** of all operations.
- **Access to the account closes**, with permanent availability of those for the last year.
- Maximum **simplicity** in refunds management.
- **List of transactions**, which can be downloaded to the computer and which includes all the important information.
- For large companies, **integration with the corporate intranet or proprietary applications** and availability of files via FTP.

2.
What do I need?

2.1 How is it installed?

The first step in installing the Banco Sabadell Virtual POS is to process apply for a merchant contract and registration of the Virtual POS at your branch.

To contract this service you need to provide us with some basic details of the merchant and your virtual store.

Once the application has been accepted, you will be sent an email with the unique security codes for your merchant to enable you to install the Virtual POS. In order to expedite the integration of the Virtual POS with your web server and synchronise the purchasing mechanisms, before implementing the Virtual POS in real time, we recommend using the codes in a test environment included in this manual.

In the event of any doubt or enquiry, the Banco Sabadell Virtual POS Telephone Support Service will be available to help you via email or over the telephone.

2.2. What should my website have?

Although the installation of the Virtual POS does not affect the basic design and characteristics of your merchant's webpage and the virtual store, there is a set of requirements and recommendations to be taken into consideration to enhance the purchase experience of your customers.

— On the homepage of your website...

The home page of your website can include a section with information on the accepted forms of payment, the obligations and warranties on the part of the purchaser and the obligations and warranties on the part of the establishment.

— In your product catalogue….

In the product catalogue of your webpage we recommend that all the products shown include easily visible information about product availability, delivery times and prices.

It is important this information be included next to each product on the catalogue list before the user selects it by clicking on it.

— In your virtual store…

In addition to the product catalogue, the virtual store of your webpage must also include a “Shopping Basket” where the purchaser stores the products they wish to purchase while browsing the catalogue.

At the end of the process, this space will specify the product or products selected with their prices and any additional amounts included in the final purchase price, provided they are necessary (taxes, delivery costs …).

— The request for details …

When the customer has the list of all the products to be bought in the “Shopping Basket” and the additional expenses, they must accept the order. Your webpage must then provide a detailed form requesting all the necessary details to finalise the sales process. As this is remote selling, the customer must give their personal data, the delivery details for the articles and the desired form of payment.

When the purchaser chooses to pay using a credit card, the Banco Sabadell Virtual POS is activated.

2.3. What payment regulations must I follow?

The Virtual POS, given its nature, is subject to rules arising from its participation in international payment systems and its management by Banco Sabadell.

These regulations are included in the contract signed by Banco Sabadell and the merchant. Please take note of the following rules:

- The merchant may only process transactions originating from the Webpages duly verified by Banco Sabadell.

- The merchant shall immediately cancel card operations when an undue charge occurs or when the sales process and goods delivery has not been completed.

- The merchant will not, under any circumstance, store the card details onsite, except those necessary for operation, in which case it will be subject to the Security program PCI/DSS of VISA and MASTERCARD. Even in this case, it is strictly forbidden to store the CVV2 code (three security digits stamped on the back of the cards) under any circumstance.

3.

Security measures

The Virtual POS associated with your merchant has been configured with a series of security measures to reduce the risk of sales paid for with fraudulent cards (stolen, copied or used without the authorisation of the legitimate holder).

3.1 Velocity checks

These are security restrictions which block unusual operations or purchasing behaviour.

As an additional security and fraud prevention measure, Banco Sabadell will apply a series of security limits on the merchant's operations in keeping with its activity and types of operation. They are limits on the amount and number of operations, which must conform to certain values which do not affect the sales expectations of the merchant but avoid exaggerated deviations from the usual turnover (in most cases they mean that an attack is in progress using stolen and/or fraudulent cards).

There are limits on the basis of the following parameters:

- Maximum number of operations (accepted and denied) per card
- Maximum number of operations (accepted and denied) per user (IP address)
- Maximum amount accumulated per card
- Maximum amount accumulated per user (IP address)

If you consider that these parameters do not conform to your usual merchant operations, please request a modification via your branch or your Banco Sabadell agent

In addition, other rules can be configured in line with the amounts, number of operations, country where the card was issued, country where the IP location of the purchaser, period of use, etc.

If you consider that these parameters do not conform to your usual merchant operations, please request a modification via your branch or your Banco Sabadell agent.

3.2 Verification of the CVV2

The CVV2 is a three-figure code stamped on the back of all financial cards. Validation of this code has proven to be an excellent tool for fraud limitation.

The Banco Sabadell Virtual POS will always request the CVV2 code during the payment process and will validate it online with the financial entity which issued the card.

3.3 3D Secure Protocol

In order to protect the merchant from fraudulent payments or chargebacks of purchasers arguing that they did not make the purchases, all the virtual POSs of Banco Sabadell are certified under the Secure Electronic Commerce protocols (3D Secure) of the Visa (VerifiedbyVisa) and Mastercard (MasterCard-SecureCode) card systems.

In 3D Secure, within the payment process, Banco Sabadell requires the cardholder to authenticate themselves online with their financial entity. The authentication system is first agreed on with the holder and their bank (password, PIN, verification SMS, etc.)

To be taken into account:

- Although the 3D Secure offers security and protection, **if a virtual merchant has alternative fraud control systems and wishes to deactivate the 3D Secure purchase of their Virtual POS, they can request**

this from their branch or Banco Sabadell agent to analyse the case and implement the modification if appropriate

- Card systems do not usually allow company cards (Business, Corporate, etc.) to carry out the holder authentication process. For this reason, this type of card is not accepted by the virtual POS. In the exceptional cases of a merchant considering it necessary to accept company cards, it must request this from its Banco Sabadell branch, previously and expressly accepting the charge-backs arising from these operations
- The authentication of the cardholder does not release the merchant from accepting the charge-back of operations occurring due to other causes in which the customer argues that they carried out the transaction but, for example, claims that they did not receive the service or items paid for. To defend itself from such chargebacks, the merchant must furnish Banco Sabadell with documentation demonstrating indisputably that the cardholder received the product or service in question.

3.4 Additional security measures

To protect the interests of your merchant and reduce the number of incidents, we recommend monitoring the activity of your webpage to detect any of the following suspicious signs of fraud:

- In the VIRTUAL POS ADMINISTRATION MODULE the IP address of the purchaser appears together with the card number (duly masked by asterisks). It is suspicious if:
    - – The same user (IP address) has paid (or attempted to pay) with more than two different cards.
    - – The same user (IP) or the same card have carried out multiple operations over a short period of time.
    - – When making different purchases, the same user (IP) or the same card have been registered on the website with different details.
    - – If the POS has rejected the first card operation, it is suspicious if further operations have been processed with the same IP or with the same card for lower amounts.
    - – Consecutive operations with similar card numbers
- In the response message (“DS_Response” field) or the VIRTUAL POS ADMINISTRATION MODULE it appears if the operation has been accepted (000 to 099 codes) or rejected (other codes). 2xx type rejection codes indicate that the card is blocked due to loss, theft, forgery or fraudulent use of the card number. In these cases the merchant must block the user (identifiable via the IP address and registration details) and not allow any option of re-attempting payment.
- In the response message is the “Ds_Card_Country” field which states the ISO code of the country where the card was issued. By comparing the IP address of the buyer it is possible to filter behaviour suspicious of being fraudulent (e.g. A card issued in one country but operating via an IP of a different country).
- In the purchaser’s registration information:
    - – Check the telephone numbers by using public telephone directories.
    - – Check whether the telephone code and/or prefix match the geographic area of the delivery address.
    - – Check the match between the post code and city of delivery.
    - – Check the email address by sending a

  confirmation order.
  - Check in public details of social networks the purchaser's registration details.

- Also check:
  - Orders with the same delivery address but made with multiple cards.
  - Orders for multiple numbers of the same product.
  - Orders for an amount above usual.
  - Orders for which delivery is urgent or even "for the next day". Criminals wish to fraudulently obtain these products as soon as possible for probable re-sale and are unconcerned about the surcharge on delivery.
  - For websites not translated to international languages payments made with foreign cards and/or from international IPs and/or order to be sent to international addresses.

In addition to monitoring the parameters above, your merchant can significantly reduce its exposure to the risk of fraud by applying its own controls over operations to identify high risk operations. These controls can be automatic (velocity checks) and prior to sending the requests for authorisation to Banco Sabadell; or subsequent manual checks to processing the transaction with Banco Sabadell.

The anti-fraud protocols implemented must be based on the user's registration details (User ID., Name, Telephone no, Address, email, etc.) and, also on the registration details of the recipient of the service/product (name of the travellers if it is a travel agency or similar, product delivery address, contact telephone, etc.).

Should the operation not pass all the above controls, the merchant must reject the card as the means of payment and cancel the operation if already carried out via the Virtual POS.

To minimise the risk of fraud it is therefore necessary for the merchant supervisors to know these security measures, prepare training activities for all the employees handling card payments and periodically check compliance with these measures. Otherwise, there exists the risk that fraudulent operations can be charged back to the merchant and if the number of fraudulent or charged back operations is significant, the terminal is blocked and the contract with Banco Sabadell terminated.

4.

Operational aspects

4.1 Types of transactions

In accordance with the needs of each merchant, the Virtual POS offers a wide range of authorisation requisitions which the merchant can combine as required.

Standard payment or authorisation
(Ds_Merchant_TransactionType = "0")

This is the most widespread case in which the transaction is initiated by the holder who is connected via the Internet to the webpage of the merchant during the payment process. Once the purchase requisition has been received by the merchant, the Virtual POS requests the details to perform the authorisation transaction.

If the merchant is configured as 3D Secure (Secure eCommerce) and the bank of the cardholder has an authentication system, the bank will request the cardholder proof of identification.

The request for Authorisation is carried out in real time, entailing an immediate charge to the account of the holder associated with the card (credit or debit).

Partial or Total Refund
(Ds_Merchant_TransactionType = "3")

These are book transactions initiated by the merchant, which can also use the Virtual POS administration module to perform them manually.

The Virtual POS checks for existence of the original authorisation to be refunded, and that the sum of the amounts refunded does not exceed the original authorised amount under any circumstance.

They produce a book effect on the holder's account (some issuing entities take several days to pay the holder) and are therefore captured automatically and sent to the settlement process of Banco Sabadell which will make the relevant charge in the merchant's account.

Pre-authorisation
(Ds_Merchant_TransactionType = "1")

NOTE: In accordance with the regulations of the international cards, this operation is restricted to those merchants whose activity is one of the following: hotels, travel agencies and vehicle rental.

It can be used when at the time of the purchase the exact amount of same cannot be determined or if, for some reason, the merchant does not want the amount to be charged to the customer account immediately.

The transaction is transparent for the holder who at all times acts exactly the same as in the previous case, i.e. furnishes his details and is authenticated if necessary.

The request for pre-authorisation is carried out in real time, producing a withholding for the amount of the sale in the holder's account.

The transaction is not captured and therefore produces no book effect in the holder's account nor payment to the merchant **(in the case of debit cards certain issuing entities do make a book entry for the holder which is automatically cancelled after several days)**.

Any Pre-authorisation must have Confirmation of Pre-authorisation within a maximum of 7 calendar days. Otherwise, it loses its validity as guarantee of payment.

To activate the Pre-authorisation service, the merchant must expressly request same from its Banco Sabadell branch.

Confirmation of Pre-authorisation
(Ds_Merchant_TransactionType = "2")

This is an inseparable supplement to the above operation.

In this transaction the holder is not connected to the merchant's website and it is always initiated by the merchant.

It must be carried out within the 7 days following the original pre-authorisation and the amount must be less than or equal to the original amount.

This transaction is posted, automatically regularising the entry in the holder's account and sending it to the settlement process of Banco Sabadell for payment to the merchant.

Confirmation of pre-authorisation guarantees payment and conserves the conditions with regard to the secure transaction of its original Pre-authorisation.

The Virtual POS will check for the existence of the original operation and the amount to be confirmed, rejecting the operation if any error exists.

Cancellation of Pre-authorisation

(Ds_Merchant_TransactionType = "9")

The holder is not connected to the merchant's website and therefore this transaction is always initiated by the merchant. It must be carried out within 7 days following the original pre-authorisation.

The Virtual POS will check the existence of the original operation, rejecting the operation if any error exists.

Deferred Pre-

(Ds_Merchant_TransactionType = "O")

They are similar operations to pre-authorisations but are available to all sectors of merchant. Authorisation is obtained from the issuing bank in real time which requires confirming within the 72 hours following if the operation is to be definitive.

If 72 hours elapse from the day/time of the pre-authorisation without confirmation being sent, the authorisation is automatically cancelled and cannot therefore be confirmed.

Unlike traditional pre-authorisations, the amount of the Confirmation of Deferred Pre-authorisation must be exactly the same as the respective re-authorisation.

The request for pre-authorisation is carried out in real time, producing a withholding for the amount of the sale in the holder's account.

The transaction is not captured and therefore produces no book effect in the holder's account nor payment to the merchant **(in the case of debit cards certain issuing entities do make a book entry for the holder which is automatically cancelled after several days).**

To activate the Deferred Pre-authorisation service, the merchant must expressly request same from its Banco Sabadell branch.

Confirmation of Deferred Pre-authorisation

(Ds_Merchant_TransactionType = "P")

This is an inseparable supplement to the above operation.

The holder is not connected to the merchant's website and therefore this transaction is always initiated by the merchant. It must be carried out within the 72 days following the original pre-authorisation and the amount must be THE SAME AS the original amount.

This transaction is posted, automatically regularising the entry in the holder's account and sending it to the daily settlement process of Banco Sabadell for payment to the merchant. Confirmation of pre-authorisation guarantees payment and conserves the conditions with regard to the secure transaction of its original Pre-authorisation.

The Virtual POS will check for the existence of the original operation and the amount to be confirmed, rejecting the operation if any error exists.

Cancellation of Deferred Pre-authorisation

(Ds_Merchant_TransactionType = “Q”)

The holder is not connected to the merchant’s website and therefore this transaction is always initiated by the merchant. It must be carried out within 72 days following the original pre-authorisation.

The Virtual POS will check the existence of the original operation, rejecting the operation if any error exists.

Authentication

(Ds_Merchant_TransactionType = “7”)

This type of operation can be used by the merchant when the sale amount cannot be precisely determined at the time of the sale.

The operation is similar to the Pre-authorisation, although in this case only the first part of the operation is performed, i.e. the authentication of the holder. Request for authorisation does not occur, so the transaction is not posted and causes no withholding in the cardholder’s account.

Subsequently, and within the following 45 calendar days, the merchant will send a confirmation of authentication which will complete the original operation.

Confirmation of Authentication

(Ds_Merchant_TransactionType = “8”)

This is an inseparable supplement to the above operation.

The cardholder is not connected to the merchant’s website and it is always initiated by the merchant.

The amount may vary from the original operation (even greater), and must be carried out within the 45 days following the original authentication.

This transaction is posted, causing an entry in the cardholder’s account and sending it to the daily settlement process of Banco Sabadell for payment to the merchant.

Confirmations of authentication are stored under the same security conditions as the original authentication.

The Virtual POS will check the existence of the operation, rejecting it if any error exists.

Payment of Subscriptions and Express Payments

(Ds_Merchant_Identifier)
(Ds_Merchant_Group)
(Ds_Merchant_DirectPayment)

In order to increase the conversion rate and facilitate as far as possible the process of purchase, Banco Sabadell Virtual POS incorporates an innovative feature that allows payment of subscriptions and express payments using an identifier equivalent to the number of card.

This method allows more easily manage purchases by regular customers, because they do not need to enter the card data in each transaction. The buyer only has to fill the card details in the first purchase. The merchant will receive, together with the payment response, an identifier for use in subsequent purchases.

In addition, the merchant will be informed of the expiry date of the card and optionally the number of the card, properly masked, ie with certain digits replaced by asterisks.

The card details are stored on the servers of Banco Sabadell and thus avoid the merchant having to fulfill the PCI-DSS security requirements.

To activate the Payment of Subscriptions or Express Payments, the merchant must expressly request same from its Banco Sabadell branch or agent.

If you wish to have further information, and full details of the operational aspects of this type of operation, please contact the Technical Support Service. (See section 6.9 of this manual)

4.2 Request for payment documentation on the part of the purchaser

In online shopping, the time when the purchase is made does not usually coincide with the time the purchaser receives the details from their bank about operations made with the credit card. If, in addition, the name of the merchant on the bank statement does not match or cannot be associated with the webpage where the purchase was made, this may cause the purchaser to doubt if it was really they who performed the transaction.

Therefore the purchaser is entitled to request the merchant the relevant documentation proving that it was they who made the purchase. The maximum period for this request is 12 months as from the operation date.

It should be taken into account that when a cardholder requests documentation, in many cases this is a prior step to sending a charge-back for the amount charged. To minimise the percentage of charge-backs received (and which may incur penalties if they exceed the ratios deemed acceptable by the control programs of the Card Brands), it is advisable for a merchant supervisor to analyse the requests for documentation and return those operations which, according to hid findings, may be fraudulent.

In these cases, the card issuing entity may request the merchant send proof of the operation. The request is made by sending a physical letter to the merchant with the details of the transaction. **The merchant is under the obligation to respond within a maximum of 7 merchant days**. The response may be sent by fax to 93 368 72 91 or to the following email: peticionfotocopias@bancsabadell.com

If delivery of goods takes place, the certificate of delivery of the delivery company must be attached. As a general rule this certificate must be signed by the cardholder, not by a third person.

As an exception, and for those cases in which it is not possible to delivery the goods to the cardholder (either due to inability to be in the place and time agreed for receipt or because it is a gift) delivery to a third person is allowed. In this case, this circumstance must be recorded on the order form which the customer completed for the merchant, with the following information:

- Authorised person, identified by name and identity document (DNI, Passport, etc.). The order must only be delivered to this person and the delivery note must include the signature of the recipient and the entry confirming that the identity document provided was checked.

- For receipt at hotels or similar; it will be necessary to identify the name and address of the hotel, and also the name and document of the guest who is to receive it. The receipt must be signed by a properly identified employee of the hotel and stamped by the latter. In addition, the proof of receipt must record verification that the recipient of the goods is staying at the hotel.

It is advisable not to specify a concrete delivery date for the goods, unless essential, but rather an interval of days, as any breach is sufficient cause for return.

In the case of a merchant offering services and not products, i.e. there is no goods delivery, the merchant will enter the following details on the response form:

- Name of merchant
- Tax ID/Code of the merchant
- Merchant Code (FUC)
- Authorisation number
- Operation date
- Card number
- Webpage address (URL)
- Transaction amount
- Currency
- Name of the Purchaser
- Description of product purchased
- Define the policy on returns or indicate the URL where users may obtain the relevant information

4.3 IUPAY – Operational aspects

IUPAY is a bank digital wallet (wallet) that allows any user to store all their cards to make purchases online. Banco Sabadell offers IUPAY to all its merchants.

Due that IUPAY needs to operate under buyer's browser, in gateways 'WebService' and 'operaciones', both Host to Host, IUPAY is not allowed.

Those online merchants that accept IUPAY facilitate its customers to pay with any card that have been included in the wallet. In this way, customers will feel safer not having to re-enter card details in their online purchases.

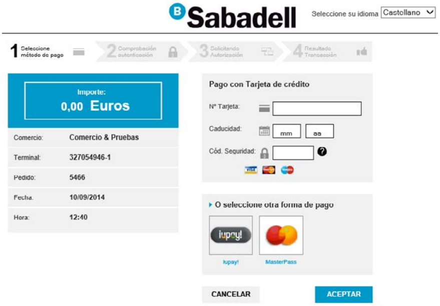
Merchants can offer IUPAY to its customers in a couple of methods:

1) Using the payment page of Banco Sabadell Virtual POS

2) Inserting the IUPAY button on merchant's website

1) Using the payment page of Banco Sabadell Virtual POS

The payment page of Banco Sabadell Virtual POS and already includes IUPAY as an alternative method of payment. Thus, the merchant do not need to perform any technical adaptation or modification in its website parameters, and is not necessary send any other parameter than the usual parameters already defined in this manual.


Sabadell
Seleccione su idioma
1 Seleccione método de pago
2 Comprobación autenticación
3 Solicitando Autorización
4 Resultado Transacción
Pago con Tarjeta de crédito
Nº Tarjeta:
Caducidad:
mm
aa
Cód. Seguridad:
O seleccione otra forma de pago
iupay!
Iupay!
MasterPass
CANCELAR
ACEPTAR

Seleccione su idioma: Castellano

Importe: 0,00 Euros

Comercio: Comercio & Pruebas
Terminal: 327054946-1
Pedido: 5466
Fecha: 10/09/2014
Hora: 12:40

2) Inserting the IUPAY button on merchant's website

If merchant prefers to insert directly the IUPAY button in his website, should perform some minor modifications in the website in order to add IUPAY as an optional payment method in the checkout process. Specifically the IUPAY button should be included along with the other usual methods of payment of the web.

To include the IUPAY payment button the merchant can choose one of the following images (white or dark grey background):

These buttons are available in:

https://sis.redsys.es/sis/graficos/logotipos/comunes/iupayBtnWhite.png

https://sis.redsys.es/sis/graficos/logotipos/comunes/iupayBtnBlack.png

At the moment that the customer clicks the IUPAY payment button, the payment form that merchant sends through the Virtual POS must include the information for the new Ds_Merchant_PayMethod field.

Possible new field values are:

- **Ds_Merchant_PayMethod = “O”** In this case the payment with IUPAY will be activated by using one of the cards that have been stored in the digital wallet of the customer.
- **Ds_Merchant_PayMethod = “C”.** In this case payment with IUPAY will not be activated and payment will be effected in the traditional way.

The POS Technical Support Service of Banco Sabadell will attend any questions concerning the IUPAY service. See contact details in section 6.9 of this manual.

5.

Virtual POS administration module

5.1 Access

The Banco Sabadell Virtual POS includes access to an administration module of operations performed. Access to the intranet is effected via a webpage and offers endless advantages for your merchant management.

The administration module offers **real time control of all sales**.

In addition to viewing the operations performed, you can always process the refund of incorrect payments and display the transactions which have not been correctly finalised obtaining information on the error or reason for rejection.

You can access the merchant's administration module at the following web addresses:

- Test environment:
  https://sis-t.REDSYS.es:25443/canales
- Real environment
  https://sis.REDSYS.es/canales

A page will appear for you to enter the user code and administrator password provided earlier by Banco Sabadell, together with the language in which you wish to operate with the administration module.

5.2 Users

Procedures related to registration of new users and modification of access profiles can be carried out in the "Users" section of the Virtual POS administration module. You can also change your password for another which is easy to remember or which you consider more secure.

Two different profiles can be assigned to new users upon registration:

1. **Informative profile**: only transactions and totals can be consulted.
2. **Administrator profile**: in addition to transaction and totals queries it is possible to perform returns, in whole or in part, of sales operations.

The "Users" section of the administration module includes the following options:

1. **Password**: the user access password can be modified.
2. **Users**: all queries, registration, de-registration and modification of merchant users can be carried out.
3. **Generate Users**: this enables you to automatically generate, using a merchant code and terminal node, a user to access the administration module with certain default characteristics or permits and to send data to this user to the email address of the specified merchant.

In addition, in accordance with the type of queries allowed for users, the administrator can register two types of users:

1. **Terminal**: to manage the operations performed with a given merchant and terminal.
2. **Merchant**: to manage the operations performed by all the terminals of a merchant.

5.3 Operations: queries and administration

The ‘Queries” section of the administration module allows you to check the details of operations authorised or rejected by your merchant over the past 365 calendar days. To do so, enter a start and end date for the period to be queried to locate an operation.

Queries concerning operations in the administration module are restricted to 1-month periods. If you need to check longer periods, you must perform consecutive queries of 30-day periods.

For greater search speed, is you know the reference number of the operation you can enter it and access the details immediately.

When you have entered the search parameters and pressed the ACCEPT button a screen appears with a list of the operations matching the search criteria.

The search result, in addition to being displayed on the screen, can be PRINTED or EXPORTED to a text file with separator delimited fields “;”.

The response codes shown in the “Result Authorisation No or response code” field, both for operations approved and rejected, match those defined in the table of section 6.4– Online Response of this manual.

5.4. Refund of operations

The Virtual POS administration module allows the merchant to check and generate total or partial refunds of operations which have been processed.

Only those users accessing the administration module with an administrator profile password are authorised to carry out refunds.

To perform a total or partial refund of the selected operation, press the red button in the “Generate return” column which corresponds to the desired operation and a page will appear to enter the refund amount. The refund amount must never exceed the amount of the original operation.

In the case of DCC operations (Dynamic Currency Conversion) or Multicurrency operations, the amount must be entered in the currency of the terminal.

When the refund is accepted, a ticket refund page will be shown which can be printed or filed if desired.

Those merchants which carry out pre-authorisation, pre-authentication or deferred pre-authorisation operations can generate confirmations and cancellations of same from the Virtual POS administration module.

5.5 Checking totals

The Virtual POS administration module enables the merchant to check the totals processed.

By pressing the ‘Totals’ button on the left of the homepage a list of the last 45 sessions appears. Select the desired sessions and pres ’Accept.

A screen appears with the total amounts and number of operations.

There exists the option of checking the totals with Breakdown (by card brand) or without Breakdown (360 last sessions).

6.

Installation

This Virtual POS manual provides the necessary information for you or your IT department to install the Virtual POS on your virtual store's website. The installation is simple and basically consists of entering computer instructions in the website which remotely run the Virtual POS software resident on the secure server of Banco Sabadell.

The message has an additional security field where the chief purchase details are transmitted securely via the Hash Sha-1 algorithm.

6.1 Payment form of the merchant's website.

The payment page of the merchant's webpage must include a button for the purchaser to identify it with the type of card payment.

The button must be associated with the hidden payment form described below. When the consumer selects this button, the merchant must send the operation payment form to the Banco Sabadell server at the following address:

- Test environment:
  https://sis-t.redsys.es:25443/sis/realizarPago
- Real environment:
  https://sis.redsys.es/sis/realizarPago

For 3D Secure merchants, **the window or frame where the Virtual POS opens must have vertical and horizontal scroll bars** to adapt to the different authentication pages the holder is shown during subsequent processes.

Below are the data to be included in the payment form:

DATUM	NAME OF FIELD	LENGTH	COMMENTS
Amount	Ds_Merchant_Amount	12 N	**Required.** The last two positions are considered decimals, except in Yen.
Currency	Ds_Merchant_Currency	4 N	**Required.** 978 - Euro 840 – Dollar 826 - Pound Sterling 392 – Yen 32 – Argentine Peso 124 - Canadian Dollar 152 - Chilean Peso 170 - Columbian Peso 356 - Indian Rupee 484 – New Mexican Peso 604 – New Soles 756 - Swiss Franc 986 - Brazilian Real 937 –Venezuelan Bolivar 949 - Turkish Lira
Order code	Ds_Merchant_Order	Mín. 4N Máx. 12 AN For “Card on File” in field must be max. 10 positions The Virtual POS will add two more positions indicating the payment order number.	**Required.** The first 4 digits must be numerical; the remaining digits can only use the following ASCII characters From 30 = 0 to 39 = 9 From 65 = a to 90 = Z From 97 = a to 122 = z The code must be different from previous transactions.
Product Description	Ds_Merchant_ ProductDescription	Máx.125 AN	This field is shown to the holder on the purchase confirmation screen.
Name and surnames of holder	Ds_Merchant_Titular	Max. 60 AN	This field is shown to the holder on the purchase confirmation screen.
Merchant number Fuc code	Ds_Merchant_ MerchantCode	9 N	**Required.** Fixed code assigned by Banco Sabadell.
URL	Ds_Merchant_ MerchantURL	250 AN	Required if merchant has online notification. URL of merchant which will receive a post with the transaction data.

DATUM	NAME OF FIELD	LENGTH	COMMENTS
URLOK	Ds_Merchant_UrlOK	250 AN	**Optional.** If sent it will be used as URLOK, ignoring that configured in the administration module if any.
URLKO	Ds_Merchant_UrlKO	250 AN	**Optional.** If sent it will be used as URLKO, ignoring that configured in the administration module if any.
Name of merchant	Ds_Merchant_ MerchantName	25 AN	**Optional.** Name of merchant appearing on customer payment page, if any.
Holder's language	Ds_Merchant_ ConsumerLanguage	3 N	**Optional.** 0 – Customer 6 – Dutch 12 – Galician 1 – Spanish 7 – Italian 13 – Basque 2 – English 8 – Swedish 3 – Catalan 9 – Portuguese 4 – French 10– Valencian 5 – German 11 – Polish
Signature of merchant	Ds_Merchant_ MerchantSignature	40 AN	**Required.** See section 6.3. Design of the hash algorithm in the internet server
Terminal number	Ds_Merchant_ Terminal	3 N	**Required.** Standard: 1 – Operations in euros (Ds_Merchant_Currency = 978) If more terminals are necessary, contact the Banco Sabadell technical service
Merchant data	Ds_Merchant_ MerchantData	1024 AN	**Optional.** Free information of merchant to be received in online response (via URL or e-mail).
Type of transaction	Ds_Merchant_ TransactionType	1 N	**Optional (default equal to "0").** 0 – Standard payment 1 – Pre-authorisation 2 – Confirmation of pre-authorisation 3 – Partial or full refund 7 – Authentication 8 – Confirmation of authentication 9 – Cancellation of pre-authorisation L – Card in Initial File (Subscriptions/Express payments) M – Successive Card on File (Subscriptions/Express P.) O – Deferred pre-authorisation P – Confirmation of Deferred Pre-authorisation P – Cancellation of Deferred Pre-authorisation
Authorisation code	Ds_Merchant_ AuthorisationCode	6 N	**Optional.**

DATUM	NAME OF FIELD	LENGTH	COMMENTS
Identifier	Ds_Merchant_ Identifier	Max. 40 AN	Value of the field is Required for first payment transaction. For subsequent payments, the value will be the identifier that the Bank has sent in the first payment response message.
Group of merchants	Ds_Merchant_Group	Max. 9 N	Optional. Allows to associate an identifier to a set of merchants.
Additional screens	Ds_Merchant_ DirectPayment	'True' or 'false'	Optional. This parameter acts as a flag to indicate if additional screens must be shown.
Payment method	Ds_Merchant_ PayMethod	1 AN	Only applicable to merchants that allows payments via IUPAY and that have added the IUPAY button in the web. C - Traditional card payment O - IUPAY payment

6.2 Locating errors

During the installation of the Virtual POS, when sending the payment form, some of the parameters of the form field may be erroneous.

To locate the erroneous field, see the source code of the error page and search in the HTML text for the chain “**–SIS**”. The xxxx numeric value next to the instruction “**<!–SISxxxx:–>**” will indicate the type of error according to the table included.

The table below lists the possible error values which may be received in the response from the Virtual POS together with the field affected (if any) and the meaning of each one. It also specifies the error message the customer (purchaser) will see in each of these errors.

SISxxxx	FIELD AFFECTED	REASON	MESSAGE
SIS0007		Error disassembling input XML	MSG0008
SIS0008	Ds_Merchant_MerchantCode	Field missing	MSG0008
SIS0009	Ds_Merchant_MerchantCode	Format error	MSG0008
SIS0010	Ds_Merchant_Terminal	Field missing	MSG0008
SIS0011	Ds_Merchant_Terminal	Format error	MSG0008
SIS0014	Ds_Merchant_Order	Format error	MSG0008
SIS0015	Ds_Merchant_Currency	Field missing	MSG0008
SIS0016	Ds_Merchant_Currency	Format error	MSG0008
SIS0018	Ds_Merchant_Amount	Field missing	MSG0008
SIS0019	Ds_Merchant_Amount	Format error	MSG0008
SIS0020	Ds_Merchant_Signature	Field missing	MSG0008
SIS0021	Ds_Merchant_Signature	Field empty	MSG0008
SIS0022	Ds_TransactionType	Format error	MSG0008
SIS0023	Ds_TransactionType	Unknown value	MSG0008
SIS0024	Ds_ConsumerLanguage	Value exceeds 3 positions	MSG0008
SIS0025	Ds_ConsumerLanguage	Format error	MSG0008
SIS0026	Ds_Merchant_MerchantCode	Error Merchant inexistent / Terminal sent	MSG0008
SIS0027	Ds_Merchant_Currency	Error currency does not match that assigned for that Terminal.	MSG0008
SIS0028	Ds_Merchant_MerchantCode	Error Merchant/Terminal is de-registered	MSG0008
SIS0030	Ds_TransactionType	In card payment a type of operation has arrived which is not payment nor pre-authorisation	MSG0000
SIS0031	Ds_Merchant_TransactionType	Method of payment not defined	MSG0000
SIS0034		Error accessing database	MSG0000
SIS0038		Error in JAVA	MSG0000
SIS0040		The merchant / Terminal has not assigned method of payment	MSG0008
SIS0041 SIS0042	Ds_Merchant_Signature	Error calculating HASH algorithm	MSG0008
SIS0043		Error making online notification	MSG0008
SIS0046		Card BIN (the first four digits of the card number) not registered	MSG0002
SIS0051	Ds_Merchant_Order	Repeated order number	MSG0001
SIS0054	Ds_Merchant_Order	No operation to make refund	MSG0008
SIS0055	Ds_Merchant_Order	Operation to be refunded is not valid	MSG0008
SIS0056	Ds_Merchant_Order	Operation to be refunded is not authorised	MSG0008
SIS0057	Ds_Merchant_Amount	Amount to be refunded exceeds limit	MSG0008
SIS0058		Inconsistent data in validation of confirmation	MSG0008
SIS0059	Ds_Merchant_Order	Error, operation for confirmation does not exist	MSG0008
SIS0060	Ds_Merchant_Order	Confirmation for this pre-authorisation already exists	MSG0008

SIS0061	Ds_Merchant_Order	The pre-authorisation to be confirmed is not authorised	MSG0008
SIS0062	Ds_Merchant_Amount	Amount to be confirmed exceeds limit	MSG0008
SIS0063 SIS0064 SIS0065		Error in card number	MSG0008
SIS0066 SIS0067 SIS0068 SIS0069 SIS0070		Error in card expiry date	MSG0008
SIS0071		Expired CARD	MSG0000
SIS0072	Ds_Merchant_Order	Operation cannot be cancelled	MSG0000
SIS0074	Ds_Merchant_Order	Field missing	MSG0008
SIS0075	Ds_Merchant_Order	Value has fewer than 4 positions or more than 12	MSG0008
SIS0076	Ds_Merchant_Order	Value is not numerical	MSG0008
SIS0078	Ds_TransactionType	Unknown value	MSG0005
SIS0093		Card not found within table of ranges	MSG0006
SIS0094		Card not authenticated as 3D Secure	MSG0004
SIS0112	Ds_TransactionType	Value not allowed	MSG0008
SIS0114		A GET has been called instead of a POST	MSG0000
SIS0115	Ds_Merchant_Order	No operation to make instalment payment	MSG0008
SIS0116	Ds_Merchant_Order	Operation for instalment payment is not valid.	MSG0008
SIS0117	Ds_Merchant_Order	Operation for instalment payment is not authorised.	MSG0008
SIS0132		The Confirmation of Authorisation date cannot exceed pre-authorisation date by more than 7 days	MSG0008
SIS0133		The confirmation of Authentication date cannot exceed prior authentication by more than 45 days	MSG0008
SIS0139		Initial recurrent payment is duplicated	MSG0008
SIS0142		Time exceeded for payment	MSG0000
SIS0198		Amount exceeds limit allowed for merchant	MSG0008
SIS0199		The number of operations exceeds limit allowed for merchant	MSG0008
SIS0200		Amount accumulated exceeds limit allowed for merchant	MSG0008
SIS0214		Merchant does not accept refunds	MSG0008
SIS0216		The CVV2 has more than three positions	MSG0008
SIS0217		Format error in CVV2	MSG0008
SIS0218		"Operations" input does not allow secure payments	MSG0008

SIS0219		The number of card operations exceeds limit allowed for merchant	MSG0008
SIS0220		Accumulated amount of card exceeds limit allowed for merchant	MSG0008
SIS0221		Error. The CVV2 is required:	MSG0008
SIS0222		Cancellation for this pre-authorisation already exists	MSG0008
SIS0223		The pre-authorisation to be cancelled is not authorised	MSG0008
SIS0224		Merchant does not allow cancellations due to lack of extended signature	MSG0008
SIS0225		No operation to make cancellation	MSG0008
SIS0226		Inconsistent data in validation of a cancellation	MSG0008
SIS0227	Ds_Merchant_TransactionDate	Invalid value	MSG0008
SIS0229		No deferred payment code requested	MSG0008
SIS0252		Merchant does not allow card to be sent	MSG0008
SIS0253		Card does not comply with check-digit	MSG0008
SIS0254		The number of operations per IP exceeds limit allowed for merchant	MSG0008
SIS0255		Amount accumulated per IP exceeds limit allowed for merchant	MSG0008
SIS0256		Merchant cannot perform pre-authorisations.	MSG0008
SIS0257		Card does not allow pre-authorisations	MSG0008
SIS0258		Inconsistent confirmation data	MSG0008
SIS0261		Operation exceeds an operating limit defined by Banco Sabadell	MSG0008
SIS0270	Ds_Merchant_TransactionType	Type of operation not activated for this merchant	MSG0008
SIS0274	Ds_Merchant_TransactionType	Type of operation unknown or not allowed for this input to the SIS.	MSG0008
SIS0281		Operation exceeds an operating limit defined by Banco Sabadell	MSG0008
SIS0296		Error validating initial operation data “Card on File (Subscriptions P./Express P)”.	MSG0008
SIS0297		Maximum number of operations exceeded (99 oper. or 1 year) for successive transactions in “Card on File (Subscriptions P. /Express P.)”. A new “Initial File Card” operation is necessary to start the cycle.	MSG0008
SIS0298		Merchant not configured to make “Card on File (Subscriptions/Express P.)”	MSG0008

The table below lists the messages the payment page may show the cardholder for the various errors which may occur.

CODE	MESSAGE
MSG0000	System occupied, try later
MSG0001	Repeated order number
MSG0002	Card Pin not registered on FINANET
MSG0003	System launching, try again in a few moments
MSG0004	Authentication Error
MSG0005	No valid payment method exists for your card
MSG0006	Non-SERVICE CARD
MSG0007	Data missing, please check your browser accepts cookies
MSG0008	Error in data sent. Contact your merchant.

6.3 Design of the hash algorithm in the internet server

The merchant will be provided with a code to be used to sign the data furnished by it, so as to verify not only the identification of the merchant but also that the data have not been altered at any time. The public algorithm Hash SHA-1 will be used as the security protocol, which guarantees the minimum security requisites as regards authentication of origin. The code is provided to be included in the merchant website.

The same algorithm will be used to assure the merchant of the authenticity of the response data if the notification URL is supplied by the merchant.

The type of SHA1 code is not available in php versions lower than version 4.3.0. If your server uses any previous version contact the technical service of Banco Sabadell to find an alternative solution.

The electronic signature of the merchant must be calculated as follows:

Digest=SHA-1(Ds_Merchant_Amount+Ds_Merchant_Order +Ds_Merchant_MerchantCode + DS_Merchant_Currency +Ds_Merchant_TransactionType + Ds_Merchant_MerchantURL + SECRET CODE)

If the merchant does not have an online notification URL, the Ds_Merchant_MerchantURL field should be left blank.

Example:

AMOUNT (Ds_Merchant_Amount) = 1235 (multiplied by 100 to be equal to Ds_Merchant_Amount).
ORDER NUMBER (Ds_Merchant_Order) = 29292929
MERCHANT CODE (Ds_Merchant_MerchantCode) = 201920191
CURRENCY (Ds_Merchant_Currency) = 978

SECRET CODE= h2u282kMks01923kmqpo

Result chain:
123529292929201920191978h2u282kMks01923kmqpo

Result SHA-1:
c8392b7874e2994c74fa8bea3e2dff38f3913c46

IMPORTANT NOTE:

– The secret code must never be disclosed to third parties, nor appear in the source code of the merchant's website nor be accessible within the website's file structure.

– The calculation of the Hash SHA-1 algorithm must be implemented on the private section of the merchant's Internet server.

– If the merchant resides on an unrelated server under a hosting arrangement or similar, contact the provider to ascertain how to implement the cryptographic algorithm.

If you wish, Banco Sabadell can provide you with examples of connection to the Virtual POS of your merchant in different programming languages.

Referencias SHA-1

- Secure Hash Standard, FIPS PUB 180-1.

  http://www.itl.nist.gov/fipspubs/fip180-1.htm

  http://csrc.nist.gov/publications/fips/fips180-1/fips180-1.pdf

- List of Validated Implementations of SHA-1

  http://csrc.nist.gov/cryptval/dss/dsaval.htm

- The specifications of the Secure Hash Standard (Algorithm SHA-1):

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

- What are SHA and SHA-1?

  http://www.rsasecurity.com/rsalabs/faq/3-6-5.html

6.4 Online response

There are four response systems for merchants who wish to have the result of payments immediately after being made. The four systems, which can coexist simultaneously are:

1. Query via the Internet of the **Virtual POS administration module.**
2. Implementation of an **Online response solution**.

   At the same time the cardholder receives the response to the card payment requisition, the merchant website receives a message with the same information.

3. Reception of **file with list of operations**.

   The file will be periodically generated (generally a daily file) and sent to BS Online so the merchant can download it.

4. **Query via SOAP.**

   This enables the merchant to query an operation using SOAP-XML technology

The **Online response** is the most widely used system. If you wish to use a file with the list of operations or SOAP query it is necessary to contact the Banco Sabadell technical service, which will supply the necessary instructions.

There are two online response reception modes which can be combined, using both at the same time or one of them as a backup if the other fails:

- **Vía e-mail**:

  The response to the payment authorisation will be received at the email address the merchant indicated when requesting registration of the Virtual POS.

- **Vía URL**:

  The response to the payment authorisation will be received at the URL address indicated on the payment form. This option requires some simple computer developments on the merchant website, both to enable reception of the response and to integrate it in the merchant database. This option is only valid for merchants installed with the active verification field. It is the recommended option.

To implement the online response via URL the payment requisition form must provide an URL for reception of the responses (Ds_Merchant_MerchantURL field). This URL will be a CGI, Servlet or similar, developed in the language considered suitable for the merchant server to interpret the response sent by the Virtual POS. The URL will not be loaded in the browser and will therefore not be visible to the user. It can receive and collect data of the online response and enter them in the merchant's database.

The protocol used in response via URL can be http or https, the format of this message is an HTML form, sent via POST, and whose fields are as follows:

DATUM	NAME OF DATUM	LENGTH	COMMENTS
Date	Ds_Date	10 A	Transaction date (DD-MM-YYYY).
Time	Ds_Hour	5 A	Transaction time (HH:MM).
Amount	Ds_Amount	12 N	Same value as in requisition.
Currency	Ds_Currency	4 N	Same value as in requisition.
Order code	Ds_Order	12 N	Same value as in requisition.
Merchant Code/ FUC Code	Ds_MerchantCode	9 N	Same value as in requisition.
Terminal number	Ds_Terminal	3 N	Same value as in requisition.
Signature for merchant	Ds_Signature	40 AN	See instructions at bottom of table.
Response code	Ds_Response	4 N	See list at bottom of table.
Type of transaction	Ds_TransactionType	1 AN	Same value as in requisition.
Secure payment	Ds_SecurePayment	1 N	0 – Payment NOT secure 1 - Secure payment
Merchant data	Ds_MerchantData	1024 AN	Optional information sent by merchant in payment requisition form.

DATO	NOMBRE DEL DATO	LONG.	COMENTARIOS
Holder’s country	Ds_Card_Country	3 N	Country of card issuance See ANNEX 1 with list of countries
Authorisation code	Ds_ AuthorisationCode	6 AN	Alphanumerical code of authorisation assigned to approval by authorising institution.
Holder’s language	Ds_ ConsumerLanguage	3 N	The value 0 will indicate that customer language has not been determined. (Optional)
Card type	Ds_Card_Type	1 AN	C - Credit Card D - Debit card

(In the Ds_Currency, Ds_Terminal and Ds_ConsumerLanguage fields the length is considered the maximum so it is unnecessary to fill in with zeros to the left. The signature will be generated with the fields exactly as sent.)

In the same way as in the payment requisition of a purchase, the online response includes an electronic signature which guarantees the integrity of the responses.

The algorithm will be the same and the formula to be taken into account for the calculation will be:

Digest=SHA-1(Ds_ Amount + Ds_ Order + Ds_MerchantCode + Ds_ Currency + Ds _Response + CLAVE SECRETA)

The connection used to communicate the online confirmation between the Virtual POS and the merchant can be TLS.

The default Virtual POS can communicate with ports 80, 443, 8080 and 8081 of the merchant. Other ports must be checked with the Banco Sabadell technical service.

Once the merchant receives the form, the values of the Response code field (Ds_Response) indicate whether the operation is approved or rejected and if so, the reason for rejection.

Below is a full list of the available codes:

A) CODES FOR APPROVED TRANSACTIONS

CODE	TITLE	DESCRIPTION
000	TRANSACCION APROBADA	Transaction authorised by card issuing bank
001	TRANSACCION APROBADA PREVIA IDENTIFICACION DE TITULAR	Exclusive code for transactions Verified by Visa or MasterCard SecureCode. The transaction has been authorised and the issuing bank informs us that it has correctly authenticated the identity of the cardholder.
002 - 099	TRANSACCION APROBADA	Transaction authorised by issuing bank

B) CODES FOR REJECTED TRANSACTIONS

b.1.) Transactions rejected due to generical reasons

CODE	TITLE	DESCRIPTION
101	EXPIRED CARD	Transaction rejected because card expiry date entered during payment is prior to that currently valid.
102	CARD TEMPORARILY BLOCKED OR UNDER SUSPICION OF FRAUD	Card temporarily blocked by issuing bank or under suspicion of fraud
104	OPERATION NOT ALLOWED	Operation not allowed for this type of card.
106	NO. ATTEMPTS EXCEEDED	Number of attempts with erroneous PIN exceeded.
107	CONTACT ISSUER	Issuing bank does not allow automatic authorisation. It is necessary to call your authorisation centre to obtain manual approval.
109	IDENTIFICATION OF MERCHANT OR TERMINAL INVALID	Rejected because merchant is not correctly registered in international card systems.
110	AMOUNT INVALID	Transaction amount unusual for this type of merchant requesting payment authorisation.
114	CARD DOES NOT SUPPORT TYPE OF OPERATION REQUESTED	Operation not allowed for this type of card.

116	INSUFFICIENT BALANCE	The cardholder has insufficient credit to meet payment.
118	CARD NOT REGISTERED	Card inexistent or not registered by issuing bank.
125	CARD NOT EFFECTIVE	Card inexistent or not registered by issuing bank.
129	CVV2/CVC2 ERROR.	The CVV2/CVC2 code (three digits on back of card) entered by consumer is erroneous.
167	CONTACT ISSUER SUSPECTED FRAUD	Due to suspicion that transaction is fraudulent the issuing bank does not allow automatic authorisation. It is necessary to call your authorisation centre to obtain manual approval.
180	NON-SERVICE CARD	Operation not allowed for this type of card.
181-182	CARD WITH DEBIT OR CREDIT RESTRICTIONS	Card temporarily blocked by issuing bank
184	AUTHENTICATION ERROR	Exclusive code for transactions Verified by Visa or MasterCard SecureCode. Transaction rejected because issuing bank cannot authenticate the cardholder.
190	REJECTION WITHOUT SPECIFYING MOTIVE	Transaction rejected by issuing bank but without reporting the reason.
191	ERRONEOUS EXPIRY DATE	Transaction rejected because card expiry date entered during payment does not match that currently valid.

b.2.) Transactions rejected due to motives in which the card issuing bank considers there are signs of fraud.

CODE	TITLE	DESCRIPTION
201	EXPIRED CARD	Transaction rejected because card expiry date entered during payment is prior to that currently valid. In addition, the issuing bank considers that the card is subject to possible fraud.
202	CARD TEMPORARILY BLOCKED OR UNDER SUSPICION OF FRAUD	Card temporarily blocked by issuing bank or under suspicion of fraud In addition, the issuing bank considers that the card is subject to possible fraud.
204	OPERATION NOT ALLOWED	Operation not allowed for this type of card. In addition, the issuing bank considers that the card is subject to possible fraud.

207	CONTACT ISSUER	Issuing bank does not allow automatic authorisation. It is necessary to call your authorisation centre to obtain manual approval. In addition, the issuing bank considers that the card is subject to possible fraud.
208 - 209	CARD LOST OR STOLEN	Card blocked by issuing bank as holder has reported it is stolen or lost. In addition, the issuing bank considers that the card is subject to possible fraud.
280	CVV2/CVC2 ERROR.	Exclusive code for transactions in which 3-figit CVV2 code is requested (Visa card) or CVC2 (MasterCard) on back of card. The CVV2/CVC2 code entered by purchaser is erroneous. In addition, the issuing bank considers that the card is subject to possible fraud.
290	REJECTION WITHOUT SPECIFYING MOTIVE	Transaction rejected by issuing bank but without reporting the reason. In addition, the issuing bank considers that the card is subject to possible fraud.

C) CODES REFERRING TO CANCELLATIONS OR REFUNDS (Ds_Merchant_TransactionType = 3) REQUESTED BY MERCHANT

CODE	TITLE	DESCRIPTION
400	CANCELLATION ACCEPTED	Cancellation or partial chargeback transaction accepted by issuing bank.
480	ORIGINAL OPERATION NOT FOUND OR TIME-OUT EXCEEDED	The cancellation or partial chargeback not accepted because original operation not located or because issuing bank has not responded within predefined time-out limit.
481	CANCELLATION ACCEPTED	Cancellation or partial chargeback transaction accepted by issuing bank. However, issuing bank response received late, outside predefined time-out limit.

D) CODES REFERRING TO RECONCILIATIONS OF PRE-AUTHORISATIONS OR PRE-AUTHENTICATIONS (Ds_Merchant_TransactionType = 2, 8, O o R)

CÓDIGO	TÍTULO	DESCRIPCIÓN
500	RECONCILIATION ACCEPTED	Reconciliation transaction accepted by issuing bank.

501 - 503	ORIGINAL OPERATION NOT FOUND OR TIME-OUT EXCEEDED	The reconciliation was not accepted because original operation not located or because issuing bank has not responded within predefined time-out limit.
9928	CANCELLATION OF PRE—AUTHORISATION PERFORMED BY SYSTEM	System has cancelled deferred pre-authorisation as over 72 hours have passed.
9929	CANCELLATION OF PRE-AUTHORISATION PERFORMED BY MERCHANT	The cancellation of the pre-authorisation was accepted

E) ERROR CODES SENT BY PAYMENT GATEWAY OF BANCO SABADELL

CÓDIGO	TÍTULO	DESCRIPCIÓN
904	MERCHANT NOT REGISTERED IN FUC	There is a problem in configuration of merchant code. Contact Banco Sabadell to solve it.
909	SYSTEM ERROR	Error in stability of Banco Sabadell payment gateway or exchange systems of Visa or MasterCard.
912	ISSUER NOT AVAILABLE	Authorising centre of issuing bank not operational at this time.
913	DUPLICATED TRANSMISSION	A transaction with the same order number was recently processed (Ds_Merchant_Order).
916	AMOUNT TOO SMALL	Not possible to operate with this amount.
928	TIME-OUT EXCEEDED	Issuing bank does not respond to authorisation request within predefined time-out.
940	TRANSACTION CANCELLED EARLIER	Cancellation or partial chargeback of a transaction requested which was already cancelled.
941	AUTHORISATION TRANSACTION ALREADY CANCELLED BY PREVIOUS CANCELLATION	Confirmation of a transaction is being requested with an order number (Ds_Merchant_Order) which matches an operation already cancelled.
942	ORIGINAL AUTHORISATION TRANSACTION REJECTED	Confirmation of a transaction is being requested with an order number (Ds_Merchant_Order) which matches an operation already rejected.
943	DIFFERENT ORIGINAL TRANSACTION DATA	An erroneous confirmation is being requested.
944	ERRONEOUS SESSION	A third session is being requested. In the payment process only two sessions may be open (the current one and previous pending closure).
945	DUPLICATED TRANSMISSION	A transaction with the same order number was recently processed (Ds_Merchant_Order).

946	OPERATION TO BE CANCELLED IN PROGRESS	Cancellation or partial chargeback of an original transaction is requested which is still in progress and pending response.
947	DUPLICATED TRANSMISSION IN PROGRESS	A transaction with the same order number is being attempted (Ds_Merchant_Order) of another still pending response.
949	TERMINAL NON-OPERATIONAL	The merchant number (Ds_Merchant_MerchantCode) or terminal (Ds_Merchant_Terminal) are not registered or not operational.
950	REFUND NOT ALLOWED	Refund not allowed by regulation.
965	COMPLIANCE INFRINGEMENT	Infringement of Visa or Mastercard compliance
9064	CARD LENGTH INCORRECT	No. positions of card incorrect
9078	NO PAYMENT METHOD EXISTS	The types of payment defined for the terminal (Ds_Merchant_Terminal) by the transaction processor do not allow payment with the type of card entered.
9093	CARD DOES NOT EXIST:	Inexistent card
9094	REJECTION OF ISSUERS	Operation rejected by international issuers
9104	SECURE OPER. NOT POSSIBLE	Merchant with obligatory authentication and holder without secure purchase code
9142	PAYMENT TIME LIMIT EXCEEDED	The cardholder not authenticated during maximum time allowed.
9218	SECURE OPERATIONS CANNOT BE PERFORMED	The Operations input does not allow Secure operations
9253	CHECK-DIGIT ERRONEOUS	Card does not comply with check-digit (position 16 of card number calculated using Luhn algorithm).
9256	PRE-AUTHORISATIONS NOT ENABLED	Card cannot perform Pre-authorisations
9261	OPERATING LIMIT EXCEEDED	Transaction exceeds operating limit set by Banco Sabadell
9283	EXCEEDS BLOCKING ALERTS	The operation exceeds the blocking alerts; cannot be processed
9281	EXCEEDS BLOCKING ALERTS	The operation exceeds the blocking alerts; cannot be processed
9912	ISSUER NOT AVAILABLE	Authorising centre of issuing bank not operational at this time.
9913	ERROR IN CONFIRMATION	Error in the confirmation sent by merchant to Virtual POS (only applicable in SOAP synchronisation option)
9914	CONFIRM "KO"	Confirmation "KO" of merchant (only applicable in SOAP synchronisation option)
9915	PAYMENT CANCELLED	User has cancelled payment

9928	DEFERRED AUTHORISATION CANCELLED	Cancellation of deferred authorisation made by SIS (batch process)
9929	DEFERRED AUTHORISATION CANCELLED	Cancellation of deferred authorisation made by merchant
9997	SIMULTANEOUS TRANSACTION	The Virtual POS is simultaneously processing another operation with the same card.
9998	OPERATION STATUS REQUESTED	Temporary status while operation is processed. When the operation ends this code will change.
9999	OPERATION STATUS AUTHENTICATING	Temporary status while POS authenticates holder. Once this process has finalised, the POS will assign a new code to the operation.

6.5 Continuity of the browser session

Once the cardholder finalises the payment process and is shown the screen with the result, this screen must include the “Close” button for the purchaser to return to the merchant’s website session.

The way in which the merchant session with the customer continues will depend on the instructions associated with the ‘Close” button. These instructions, about which the merchant owner will have informed Banco Sabadell in the questionnaire effected to commence the registration process, may be:

– **“CLOSE WINDOW” instruction**: On selecting ‘Close the window or frame with the payment result will close and the session continued on the merchant page which was in the background.

– **“URL_OK and URL_KO” instruction**: On selecting ’Close the browser session will continue in the same payment page window, rerouting to an URL of which the merchant will first inform Banco Sabadell. This URL may be different if the payment has been authorised (URL_OK) or rejected (URL_KO).

Take into account that if the purchaser closes the browser window, the URL_OK/URL_KO will not be operative and the session will continue on the merchant page which was in the background.

– **Option for merchants with ONLINE RESPONSE via URL**: In addition to the two above instructions, for merchants with the ONLINE RESPONSE VIA URL service, session continuity can be performed by the merchant website by closing the payment page upon receiving the online response.

6.6 Sending transactions to the Virtual POS via XML protocol

There is the possibility of sending the transaction via XML protocol, enabling automation of the Host to Host dispatch of transactions.

It is very important to remember that this type of resource is only valid for the following types of transaction (Ds_Merchant_TransactionType), as the absence of the holder prevents authentication:

1 – Pre-authorisation
2 – Confirmation of pre-authorisation
3 – Automatic refund
8 – Confirmation of authentication

9 – Cancellation of pre-authorisations
A – Insecure payment without authentication
O – Deferred pre-authorisation
P – Confirmation of Deferred Pre-authorisation
P – Cancellation of Deferred Pre-authorisation
L - “Initial File Card” transaction (subscriptions and Express Payments)
M - “Successive File Cards” transactions (subscriptions and Express Payments)

Except types 3 and 8, the rest are not default activated. Merchants which consider it necessary must request activation from their Banco Sabadell branch or agent. All operations sent via this system will be considered INSECURE as there is not authentication of the cardholder.

Types 1, A, O and L which are processed via this protocol, require the merchant to directly request the purchaser for the card number and expiry date. Merchants which consider it necessary must request activation from their Banco Sabadell branch or agent. In addition, this option requires that the merchant first have filled in the questionnaires of the PCI-DSS security program in the card data.

Communication is carried out by sending the XML document to the address indicated by the Virtual POS. The system will interpret the XML document and conduct the relevant checks so as to process the operation. Depending on the result of the operation a response XML document will be created with the result.

The XML document will be transmitted by sending it with POST to the following address:

» Test environment: https://sis-t.REDSYS.es:25443/sis/operaciones

» Real environment: https://sis.REDSYS.es/sis/operaciones

This is sent by simulating the requisition carried out by a form with a single input called ‘entry. The “entry” value will be the XML document, which must be in x-www-form urlencoded format.

Below we describe the specifications of the two possible types of messages:

a. DATOSENTRADA: Request message sent.

b. RETORNOXML: Response to the requisition.

a. Specification of the DATOS ENTRADA document.

This message will be sent to request an operation from the Virtual POS gateway:

Version 1.0:

```
<!ELEMENT DATOSENTRADA
(DS_Version,
DS_MERCHANT_AMOUNT,
DS_MERCHANT_CURRENCY,
DS_MERCHANT_ORDER,
DS_MERCHANT_MERCHANTCODE,
DS_MERCHANT_MERCHANTURL,
DS_MERCHANT_MERCHANTNAME ?,
DS_MERCHANT_CONSUMERLANGUAGE ?,
DS_MERCHANT_MERCHANTSIGNATURE,
DS_MERCHANT_TERMINAL,
DS_MERCHANT_TRANSACTIONTYPE,
DS_MERCHANT_MERCHANTDATA ?,
DS_MERCHANT_PAN?,
DS_MERCHANT_EXPIRYDATE ?,
DS_MERCHANT_CVV2 ?)>

<!ELEMENT DS_Version (#PCDATA)>
<!ELEMENT DS_MERCHANT_AMOUNT (#PCDATA)>
<!ELEMENT DS_MERCHANT_CURRENCY (#PCDATA)>
<!ELEMENT DS_MERCHANT_ORDER (#PCDATA)>
<!ELEMENT DS_MERCHANT_MERCHANTCODE (#PCDATA)>
<!ELEMENT DS_MERCHANT_MERCHANTURL (#PCDATA)>
<!ELEMENT DS_MERCHANT_MERCHANTNAME (#PCDATA)>
<!ELEMENT DS_MERCHANT_CONSUMERLANGUAGE (#PCDATA)>
<!ELEMENT DS_MERCHANT_MERCHANTSIGNATURE (#PCDATA)>
<!ELEMENT DS_MERCHANT_TERMINAL (#PCDATA)>
```

Where:

- DS_Version: Dtd version used to validate the XML
- DS_MERCHANT_AMOUNT: see SECTION 6.1.
- DS_MERCHANT_CURRENCY: see SECTION 6.1.
- DS_MERCHANT_ORDER: see SECTION 6.1.
- DS_MERCHANT_MERCHANTCODE: see SECTION 6.1.
- DS_MERCHANT_MERCHANTURL: see SECTION 6.1.
- DS_MERCHANT_MERCHANTNAME: see SECTION 6.1.
- DS_MERCHANT_CONSUMERLANGUAGE : see SECTION 6.1.
- DS_MERCHANT_MERCHANTSIGNATURE:
  SHA1 de los campos Ds_Merchant_Amount + Ds_Merchant_Order +Ds_Merchant_MerchantCode + DS_Merchant_Currency + DS_MERCHANT_PAN + DS_MERCHANT_CVV2 + DS_MERCHANT_TRANSACTIONTYPE + SECRET CODE.

DS_MERCHANT_PAN only included if message is sent.
DS_MERCHANT_CVV2 only included if message is sent.

- DS_MERCHANT_TERMINAL: see SECTION 6.1.
- DS_MERCHANT_TRANSACTIONTYPE: Only following types allowed:
  - 1- Pre-authorisation (valid only if the merchant is authorised and works in non-secure mode).
  - 2- Confirmation of pre-authorisation
  - 3- Automatic refund
  - 8- Confirmation of authentication
  - 9- Cancellation of preauthorisation.
  - A- Insecure payment without authentication
  - O- Deferred pre-authorisation
  - P- Confirmation of Deferred Pre-authorisation
  - P- Cancellation of Deferred Pre-authorisation
  - L- “Initial File Card” transaction (subscriptions and Express Payments)
  - M- “Successive File Cards” transactions (subscriptions and Express Payments

- DS_MERCHANT_MERCHANTDATA: see SECTION 6.1.
- DS_MERCHANT_PAN : Card number
- DS_MERCHANT_EXPIRYDATE : Expiry date (YYMM).
- DS_MERCHANT_AUTHORISATIONCODE : only valid for refunds of successive recurring transactions. See SECTION 5.1.
- DS_MERCHANT_TRANSACTIONDATE : only valid for refunds of successive recurring transactions. See SECTION 5.1.
- DS_MERCHANT_CVV2: Código CVV2/CVC2 de la tarjeta (Dato opcional). code of card (Optional). If included, the signature must be added as follows:
signature = SHA1(data + code_entity)

Where ‘data’ is a chain formed by:
data=amount + order + merchant + currency
- If it is an authorisation or pre-authorisation: data = data + card
- If it is a traditional payment, CVV2 is sent:
data = data + CVV2
Lastly, the type of operation is always added:
data = data + type_operation

Below is an example of the message:

```
<DATOSENTRADA>
<DS_Version>
0.1
</DS_Version>
<DS_MERCHANT_CURRENCY>
978
</DS_MERCHANT_CURRENCY>
<DS_MERCHANT_MERCHANTURL>
https://pruebaCom.jsp
</DS_MERCHANT_MERCHANTURL>
<DS_MERCHANT_TRANSACTIONTYPE>
2
</DS_MERCHANT_TRANSACTIONTYPE>
<DS_MERCHANT_MERCHANTDATA>
Mouse+pad
</DS_MERCHANT_MERCHANTDATA>
<DS_MERCHANT_AMOUNT>
45
</DS_MERCHANT_AMOUNT>
<DS_MERCHANT_MERCHANTNAME>
Test Merchant
</DS_MERCHANT_MERCHANTNAME>
<DS_MERCHANT_MERCHANTSIGNATURE>
a63dfa507e549936f41f4961ccdace126b8ecdea
</DS_MERCHANT_MERCHANTSIGNATURE>
<DS_MERCHANT_TERMINAL>
1
</DS_MERCHANT_TERMINAL>
<DS_MERCHANT_MERCHANTCODE>
999008881
</DS_MERCHANT_MERCHANTCODE>
<DS_MERCHANT_ORDER>
114532
</DS_MERCHANT_ORDER>
</DATOSENTRADA>
```

b. Specification of the RETORNOXML document

This message is the one sent by the gateway as a result of the operation

```
<!ELEMENT RETORNOXML (DS_Version
?,CODIGO,(OPERACION|RECIBIDO ))>
<!ELEMENT DS_Version (#PCDATA)>
<!ELEMENT CODIGO (#PCDATA)>
<!ELEMENT OPERACION (Ds_Amount, Ds_Currency, Ds_Order,
Ds_Signature, Ds_MerchantCode, Ds_Terminal, Ds_Response,
Ds_AuthorisationCode,Ds_TransactionType, Ds_SecurePayment,
Ds_Reference ?, Ds_Language ?, Ds_CardNumber ?, Ds_
ExpiryDate ?, Ds_MerchantData ?, Ds_MerchantDTD)>
<!ELEMENT Ds_Amount (#PCDATA)>
<!ELEMENT Ds_Currency (#PCDATA)>
<!ELEMENT Ds_Order (#PCDATA)>
<!ELEMENT Ds_Signature (#PCDATA)>
<!ELEMENT Ds_MerchantCode (#PCDATA)>
<!ELEMENT Ds_Terminal (#PCDATA)>
<!ELEMENT Ds_Response (#PCDATA)>
<!ELEMENT Ds_AuthorisationCode (#PCDATA)>
<!ELEMENT Ds_TransactionType (#PCDATA)>
<!ELEMENT Ds_SecurePayment (#PCDATA)>
<!ELEMENT Ds_Reference (#PCDATA)>
<!ELEMENT Ds_Language (#PCDATA)>
<!ELEMENT Ds_CardNumber (#PCDATA)>
<!ELEMENT Ds_ExpiryDate (#PCDATA)>
<!ELEMENT Ds_MerchantData (#PCDATA)>
<!ELEMENT RECIBIDO (#PCDATA)>
```

Where:

- DS_Version: version used to validate the XML.
- CODIGO (CODE): indicates whether or not the operation was correct (does not indicate if it was authorised, only if processed). An 0 indicates that the operation was correct. If different from 0, it will have the error code and the operation information will not appear.

CODE is not Ds_Response an operation may have a CODE = 0 and be Rejected (Ds_Response other than 0).

- Ds_Amount: amount of the operation,
- Ds_Currency: currency of the Operation.
- Ds_Order: Order of the operation.
- Ds_Signature: signature of the operation, calculated with the fields.

Ds_Amount + Ds_Order + Ds_MerchantCode + Ds_Currency + Ds_Response + Ds_CardNumber + Ds_TransactionType + Ds_SecurePayment + Code.
The Ds_CardNumber field will only form part of the signature if the card is sent. If the card is sent with an

asterisk, the Ds_CardNumber field will also form part of the signature with the value asterisked.
- Ds_MerchantCode: operation merchant code.
- Ds_Terminal: terminal number of the operation.
- Ds_Response: value indicating the result of the operation. It will indicate whether or not it was authorised. Its possible values are those of PRICE.
- Ds_AuthorisationCode: authorisation code if any.
- Ds_TransactionType: type of operation performed.
- Ds_MerchantData: see SECTION 6.1.
- Ds_SecurePayment: see SECTION 6.4
- Ds_Reference: optional field for payment by reference.
- Ds_Language: indicates language sent by the merchant.
- Ds_CardNumber: credit card number.
- Ds_ExpiryDate: year and month of expiry of the YYMM card.
- RECIBIDO: this is a text chain which contains the XML that the merchant sent us via POST in the input field.

The DS_Version field will only appear if the operation was correct as it is a value sent to us by the merchant; otherwise the data will be in the RECIBIDO field.

Sending OPERACIÓN or RECIBIDO depends also on whether or not the operation was correct.

Below are three examples of the message:

1 - Operation correct and Authorised:

```
<RETORNOXML>
    <DS_Version>1.0</DS_Version>
    <CODIGO>0</CODIGO>
    <OPERACION>
        <Ds_Amount>100</DS_Amount>
    <Ds_Currency>978</DS_Currency>
        <Ds_Order>0001</DS_Order>
        <Ds_Signature>EEFF45687hgth</DS_Signature>
        <Ds_MerchantCode>999008881</DS_MerchantCode>
        <Ds_Terminal>1</DS_Terminal>
        <Ds_Response>0</DS_Response>
        <Ds_AuthorisationCode>222FFF</ Ds_AuthorisationCode>
        <Ds_TransactionType>2</ Ds_TransactionType >
        <Ds_SecurePayment>1</Ds_SecurePayment>
        <Ds_MerchantData>Mis Datos</ Ds_MerchantData>
    </OPERACION>
</RETORNOXML>
```

2 - Operation correct and rejected (190 – Rejected by the entity):

```
<RETORNOXML>
    <DS_Version>1.0</ DS_Version >
    <CODIGO>0</CODIGO>
    <OPERACION>
        <Ds_Amount>100</DS_Amount>
    <Ds_Currency>978</DS_Currency>
        <Ds_Order>0001</DS_Order>
        <Ds_Signature>EEFF45687hgth</DS_Signature>
        <Ds_MerchantCode>999008881</DS_MerchantCode>
        <Ds_Terminal>1</DS_Terminal>
        <Ds_Response>190</DS_Response>
        <Ds_AuthorisationCode>222FFF</ Ds_AuthorisationCode>
        <Ds_TransactionType>2 Ds_TransactionType >
        <Ds_SecurePayment>1</Ds_SecurePayment>
        <Ds_MerchantData>Mis Datos</ Ds_MerchantData>
    </OPERACION>
</RETORNOXML>
```

3 - Operation incorrect (051 – Repeated Order No.). Will never be authorised:

```
<RETORNOXML>
    <CODIGO>SIS0051</CODIGO>
    <RECIBIDO>
        <DATOSENTRADA>
            <DS_MERCHANT_CURRENCY>
            978
            </DS_MERCHANT_CURRENCY>
            <DS_MERCHANT_MERCHANTURL>
            https://pruebaCom.jsp
            </DS_MERCHANT_MERCHANTURL>
            <DS_MERCHANT_TRANSACTIONTYPE>
            2
            </DS_MERCHANT_TRANSACTIONTYPE>
            <DS_MERCHANT_MERCHANTDATA>
            Alfombrilla+para+raton
            </DS_MERCHANT_MERCHANTDATA>
            <DS_MERCHANT_AMOUNT>
            45
            </DS_MERCHANT_AMOUNT>
            <DS_MERCHANT_MERCHANTNAME>
            Comercio de Pruebas
            </DS_MERCHANT_MERCHANTNAME>
            <DS_MERCHANT_MERCHANTSIGNATURE>
            a63dfa507e549936f41f4961ccdace126b8ecdea
            </DS_MERCHANT_MERCHANTSIGNATURE>
            <DS_MERCHANT_TERMINAL>
            1
            </DS_MERCHANT_TERMINAL>
            <DS_MERCHANT_MERCHANTCODE>
            999008881
            </DS_MERCHANT_MERCHANTCODE>
            <DS_MERCHANT_ORDER>
            114532
            </DS_MERCHANT_ORDER>
            <DS_Version>
            1.0
            </ DS_Version >
        </DATOSENTRADA>
    </RECIBIDO>
</RETORNOXML>
```

6.7 Test environment

To conduct tests before implementing the codes in a real environment to be provided by Banco Sabadell, the following environment can be integrated. This environment is identical to the real environment but without the payments having accounting validity.

The test environment codes provided below are common to other customers of Banco Sabadell. If you wish to have test codes exclusively for your merchant, please contact the Technical Support Service to request installation of the Banco Sabadell Virtual POS.

The test environment parameters are:

1. URLs for sending the payment orders:

   Input "realizarpago (HTML)":
   https://sis-t.redsys.es:25443/sis/realizarPago

   Input "operaciones (XML)":
   https://sis-t.redsys.es:25443/sis/operaciones

2. Merchant number (Ds_Merchant_MerchantCode): 327234688

3. Secret code (Ds_Merchant_MerchantSignature): qwertyasdf0123456789

4. Terminals (Ds_Merchant_Terminal):

- 001 - For payments in EUROS (Ds_MerchantCurrency = 978) of merchants under protocol 3D Secure (Secure eCommerce -VERIFIED BY VISA and MASTERCARD SECURECODE-)

- 002 - For payments in EUROS (Ds_MerchantCurrency = 978) of merchants under Non-3D Secure protocol (payments considered INSECURE)

5. Card accepted:

- 4548 8120 4940 0004 with expiry date 12/12 and CVV2 code from back of card: 123

  For 3D Secure payments in which purchaser authentication is required, the Personal Identification Code (PIC) is 123.

6. URL Administration Module:
   https://sis-t.redsys.es:25443/canales/

7. Access to administration module:

» For terminal 001 (3D Secure):

  User: 327234688-001
  Password: 123456a

» For terminal 002 (NON-3D Secure):

  User: 327234688-002
  Password: 123456a

6.8. Payment of subscriptions and payments express

In order to increase the conversion rate and facilitate as far as possible the process of purchase, Banco Sabadell Virtual POS incorporates an innovative feature that allows payment of subscriptions and payments express through an identifier equivalent to the number of card.

This method allows more easily manage purchases by regular customers, because they do not need to enter the card data in each transaction. The buyer only has to fill the card details in the first purchase. The merchant will receive, together with the payment response, an identifier for use in subsequent purchases. In addition, the merchant will be informed of the expiry date of the card and optionally the number of the card, properly masked, ie with certain digits replaced by asterisks.

The card details are stored on the servers of Banco Sabadell and thus avoid the merchant having to fulfill the PCI -DSS security requirements.

- **Operating process for the first payment:**

  The merchant requests Virtual POS for payment. Together with the necessary payment details, a new parameter is sent to request generation of an identifier associated with the card details. This request may be made via any of the current Virtual POS gateways (realizarPago, entradaXMLentidad, operaciones or WebService).

If the merchant has not sent the card, the Virtual POS will request same from the holder together with the expiry date and CVV2.

The Virtual POS processes the payment request and stores the card details (only Card and Expiry Date, never the CVV2) associated with an internally generated ID. The identifier will only be generated if payment is authorised.

The Virtual POS returns the identifier and expiry date together with the payment response so the merchant can use it subsequently. Optionally, the Virtual POS can send together with the payment message, the number of the card properly masked.

Depending on the type of connection used by the merchant, the reference will be returned via the following channels:

- **Operating process for the subsequent payments:**

Once the merchant has an identifier, it can use it in subsequent payments instead of sending the card and expiry date. The operating process would be as follows:

– New payment: The merchant requests payment from Virtual POS and therefore sends the identifier than Banco Sabadell sent in the first payment. This payment method is valid for any transaction type (Ds_Merchant_TransactionType).The merchant may opt to indicate whether or not it wishes to display additional screens (DCC, Splitting and Authentication).

— The merchant can use any gateway to the Virtual POS of those available (realizarPago, entradaXMLEntidad, operations or WebService).

– The Virtual POS validates the identifier associated with the merchant and recovers the card details.

– Once the card details have been located, the Virtual POS proceeds to make payment. If it was chosen not to display screens, payment will be made without showing the DCC or splitting screens and without using a secure payment method. The expiry date will only be included in the reply if the merchant is configured for this.

For those cases in which the merchant, when applying for a payment to Virtual POS, has not requested a creation of an identifier, or were using the previous payment method of Banco Sabadell, called ‘Card on File’, will be possible to create identifier afterwards. To do Banco Sabadell has a batch process called ‘GenerarReferencias’, through which you can filter the transactions for which you want to create identifiers.

Restrictions

Once the merchant has an identifier, it can use it in subse

merchant using this operation must bear in mind the following restrictions:

i. The identifier will also be associated with the number of the merchant making the request. If the merchant wants this identifier to be used by other merchants, they must be previously configured to form a group. In order to form groups, you must ask your Banco Sabadell account manager.

ii. The card details will be stored until expiry of its validity date.

iii. The validity of the identifier will be limited to the expiry date of the card and will always be returned in the response when a new identifier is requested. In other cases it will only be returned in the response to merchants that are configured accordingly.

iv. It is only possible to not display screens when a valid reference is used. When generation of a new identifier is requested and in any other case, the merchant cannot request that screens not be shown.

New Parameters

The new parameters for this functionality are described below. The other parameters necessary for payment do not differ from those of an ordinary payment.

- **Ds_Merchant_Identifier**

  This parameter will be used to handle the reference associated with the card details. It is an alphanumeric field with a maximum of 40 positions whose value is generated by the Virtual POS.

  1st Request: In the first request for the merchant to seek generation of a new identifier the value “REQUIRED” must be sent. The Virtual POS will return the generated identifier associated with the card in a parameter with the same name. The Virtual POS will always return the expiry date which will be in the parameters Ds_ExpiryDate. As we indicated above, both parameters will be return in the online Notification, URL OK or response to WebService depending on the connection used by the merchant.

  The Ds_Merchant_Identifier parameters must be included in the Hash signature calculation chain (see section 7.6.4 of this manual). It **must be concatenated at the end of the data chain** and before the value of the code or Ds_Merchant_Group parameter if any.

  2nd and successive requests: The merchant must send the reference in the Ds_Merchant_Identifier parameter and not provide the card details. The expiry date will only be included in the reply if the merchant is configured for this.

  The Ds_Merchant_Identifier parameters must be included in the Hash signature calculation chain (see section 7.6.4 of this manual). It must be concatenated at the end of the data chain and before the value of the code or Ds_Merchant_Group parameter if any or the Ds_Merchant_DirectPayment parameter if any and the Ds_MerchantGroup parameter does not exist.

- **Ds_Merchant_DirectPayment**

  This parameter acts as a flag to indicate if additional screens must be shown (DCC, Splitting and Authentication). It is an optional parameter that can only have the values “true” or “false”. Itf used with the value “true”, no additional screens will be displayed (DCC, Splitting and Authentication) during payment and it must be used in conjunction with the Ds_Merchant_Identifier parameter containing a valid reference. If it is not used or is used with the value “false”, payment will be made as usual and all the additional screens will be displayed (DCC, Splitting and Authentication) which are required depending on the merchant configuration.

  This parameter must be included in the Hash signature calculation chain (see section 7.6.4 of this manual). It must be concatenated just after the Ds_Merchant_Group parameter (if any) and before the value of the code.

Migration of identifiers

(Only for those merchants that are already using the existing Banco Sabadell payment method called ‘Card on File’)

A merchant can continue to use the existing Card on File operation until that time or start to use Payment of Subscriptions / Payments Express.

In some cases, the merchant will want to use the new operation for previous transactions. To do this a identifier migration process has been developed, from Card on File operations to the new Payment of Subscriptions / Payments Express.

The migration of identifiers will be made by means of an express request to your Banco Sabadell account manager. Once the request has been processed, the merchant will have a file with the following data by transaction:

- Merchant ID
- Terminal No.
- Transaction Date
- Original operation order code
- Identifier generated and recorded for the card of the original transaction

With this file the merchant can update its systems to use identifiers.

Example of file with identifiers

Merchant;Terminal;Order;Date;Identifier

999008881;1;130211123726;2013-02-11-12.37.27.381; 7490da446dee0a...25b6bd52e086c3181

999008881;1;130211123739;2013-02-11 12.37.40.429;d5ac083cb97d183...548f168c32c7bb5ab7d

6.9 Technical support service for installation

To offer all the necessary support during the registration and installation process of the Banco Sabadell Virtual POS, we place at your disposal a specialised support service:

Service timetable:
Monday to Sunday, from 8 am to 10 pm
Telephone no: 902 365 650 (opc. 2)
Email:
tpvvirtual@bancsabadell.com

Only in cases of **communication-related incidents, system instability and similar, please call 902 198 747 24 hours a day** every day of the year (support service provided by RedSys).

ANNEX.

Annex I. ISO country codes.
Annex II. ISO currency codes.

Annex I. ISO country codes.

004	Afghanistan
008	Albania
012	Algeria
016	American Samoa
020	Andorra
024	Angola
028	Antigua and Barbuda
031	Azerbaijan
032	Argentina
036	Australia
040	Austria
044	Bahamas
048	Bahrain
050	Bangladesh
051	Armenia
052	Barbados
056	Belgium
060	Bermuda
064	Bhutan
068	Bolivia, Plurinational State of
070	Bosnia and Herzegovina
072	Botswana
074	Bouvet Island
076	Brazil
084	Belize
086	British Indian Ocean Territory
090	Solomon Islands
092	Virgin Islands, British
096	Brunei Darussalam
100	Bulgaria
104	Myanmar
108	Burundi
112	Belarus
116	Cambodia
120	Cameroon
124	Canada
132	Cape Verde
136	Cayman Islands
140	Central African Republic
144	Sri Lanka
148	Chad
152	Chile
156	China
158	Taiwan, Province of China
162	Christmas Island
166	Cocos (Keeling) Islands
170	Colombia
174	Comoros
175	Mayotte
178	Congo
180	Congo, the Democratic Republic of the
184	Cook Islands
188	Costa Rica
191	Croatia
192	Cuba
196	Cyprus
203	Czech Republic
204	Benin
208	Denmark
212	Dominica
214	Dominican Republic
218	Ecuador
222	El Salvador
226	Equatorial Guinea
231	Ethiopia
232	Eritrea
233	Estonia
234	Faroe Islands
238	Falkland Islands (Malvinas)
239	South Georgia and the South Sandwich Islands
242	Fiji
246	Finland
248	Aland Islands
250	France
254	French Guiana
258	French Polynesia
260	French Southern Territories
262	Djibouti
266	Gabon
268	Georgia
270	Gambia
275	Palestinian Territory, Occupied
276	Germany
288	Ghana
292	Gibraltar
296	Kiribati
300	Greece
304	Greenland
308	Grenada
312	Guadeloupe
316	Guam
320	Guatemala
324	Guinea
328	Guyana
332	Haiti
334	Heard Island and McDonald Islands
336	Holy See (Vatican City State)
340	Honduras
344	Hong Kong
348	Hungary
352	Iceland
356	India
360	Indonesia
364	Iran, Islamic Republic of
368	Iraq
372	Ireland
376	Israel
380	Italy
384	Cote d'Ivoire !Côte d'Ivoire
388	Jamaica
392	Japan
398	Kazakhstan
400	Jordan
404	Kenya
408	Korea, Democratic People's Rep. of
410	Korea, Republic of
414	Kuwait
417	Kyrgyzstan
418	Lao People's Democratic Republic
422	Lebanon
426	Lesotho
428	Latvia

Annex I. ISO country codes.

430	Liberia
434	Libya
438	Liechtenstein
440	Lithuaniaa
442	Luxembourg
446	Macao
450	Madagascar
454	Malawi
458	Malaysia
462	Maldives
466	Mali
470	Malta
474	Martinique
478	Mauritania
480	Mauritius
484	Mexico
492	Monaco
496	Mongolia
498	Moldova, Republic of
499	Montenegro
500	Montserrat
504	Morocco
508	Mozambique
512	Oman
516	Namibia
520	Nauru
524	Nepal
528	Netherlands
531	Curaçao
533	Aruba
540	New Caledonia
548	Vanuatu
554	New Zealand
558	Nicaragua
562	Niger
566	Nigeria
570	Niue
574	Norfolk Island
578	Norway
580	Northern Mariana Islands
583	Micronesia, Federated States of
584	Marshall Islands
585	Palau
586	Pakistan
591	Panama
598	Papua New Guinea
600	Paraguay
604	Peru
608	Philippines
612	Pitcairn
616	Poland
620	Portugal
624	Guinea-Bissau
626	Timor-Leste
630	Puerto Rico
634	Qatar
638	Reunion
642	Romania
643	Russian Federation
646	Rwanda
652	Saint Barthélemy
654	Saint Helena, Ascension and T. da Cunha
659	Saint Kitts and Nevis
660	Anguilla
662	Saint Lucia
663	Saint Martin (French part)
666	Saint Pierre and Miquelon
670	Saint Vincent and the Grenadines
674	San Marino
678	Sao Tome and Principe
682	Saudi Arabia
686	Senegal
688	Serbia
690	Seychelles
694	Sierra Leone
702	Singapore
703	Slovakia
704	Viet Nam
705	Slovenia
706	Somalia
710	South Africa
716	Zimbabwe
724	Spain
728	South Sudan
729	Sudan
732	Western Sahara
740	Suriname
744	Svalbard and Jan Mayen
748	Swaziland
752	Sweden
756	Switzerland
760	Syrian Arab Republic
762	Tajikistan
764	Thailand
768	Togo
772	Tokelau
776	Tonga
780	Trinidad and Tobago
784	United Arab Emirates
788	Tunisia
792	Turkey
795	Turkmenistan
796	Turks and Caicos Islands
798	Tuvalu
800	Uganda
804	Ukraine
807	Macedonia
818	Egypt
826	United Kingdom
831	Guernsey
832	Jersey
833	Isle of Man
834	Tanzania, United Republic of
840	United States
850	Virgin Islands, U.S.
854	Burkina Faso
858	Uruguay
860	Uzbekistan
862	Venezuela, Bolivarian Republic of
876	Wallis and Futuna
882	Samoa
887	Yemen
894	Zambia

Annex II. ISO currency codes.

Currency	ISO CODE	
Lek	ALL	8
Algerian Dinar	DZD	12
Angola Kwanza	AON	24
Argentine Peso	ARS	32
Australian Dollar	AUD	36
Bahamian Dollar	BSD	44
Bahraini Dinar	BHD	48
Taka	BDT	50
Armenian Dram	AMD	51
Barbados Dollar	BBD	52
Bermudian Dollar	BMD	60
Ngultrum	BTN	64
Boliviano	BOB	68
Dinar	BAM	70
Pula	BWP	72
Cruzeiro	BRC	76
Belize Dollar	BZD	84
Solomon Islands Dollar	SBD	90
Brunei Dollar	BND	96
Kyat	MMK	104
Burundi Franc	BIF	108
Bellarusian Ruble	BYB	112
Riel	KHR	116
Canadian Dollar	CAD	124
Cape Verde Escudo	CVE	132
Cayman Islands Dollar	KYD	136
Sri Lanka Rupee	LKR	144
Chilean Peso	CLP	152
Yuan Renminbi	CNY	156
Chinese Renmimbi	CNH	157
Chinese Renmimbi	CNX	158
Colombian Peso	COP	170
Comoro Franc	KMF	174
Costa Rican Colon	CRC	188
Croatian Kuna	HRK	191
Cuban Peso	CUP	192
Cyprus Pound	CYP	196
Koruna	CSK	200
Czech Koruna	CZK	203
Danish Krone	DKK	208
Dominican Peso	DOP	214
El Salvador Colon	SVC	222
Ethiopian Birr	ETB	230
Nakfa	ERN	232
Kroon	EEK	233
Falkland Islands Pound	FKP	238
Fiji Dollar	FJD	242
Djibouti Franc	DJF	262
Dalasi	GMD	270
Ghana Cedi	GHC	288
Gibraltar Pound	GIP	292
Quetzal	GTQ	320
Guinea Franc	GNF	324
Guyana Dollar	GYD	328
Gourde	HTG	332
Lempira	HNL	340
Hong Kong Dollar	HKD	344
Forint	HUF	348
Iceland Krona	ISK	352
Indian Rupee	INR	356
Rupiah	IDR	360
Iraqi Dinar	IQD	368
New Israeli Sheqel	ILS	376
Jamaican Dollar	JMD	388
Yen	JPY	392
Tenge	KZT	398
Jordanian Dinar	JOD	400
Kenyan Shilling	KES	404
Won	KRW	410
Kuwaiti Dinar	KWD	414
Som	KGS	417
Kip	LAK	418
Lebanese Pound	LBP	422
Loti	LSL	426
Latvian Lats	LVL	428
Liberian Dollar	LRD	430
Libyan Dinar	LYD	434
Lithuanian Litas	LTL	440
Pataca	MOP	446
Malagassy Franc	MGF	450
Kwacha	MWK	454
Malaysian Ringgit	MYR	458
Rufiyaa	MVR	462
Mali	MLF	466
Maltese Lira	MTL	470
Ouguiya	MRO	478
Mauritius Rupee	MUR	480
Mexican Peso	MXN	484
Tugrik	MNT	496
Moldovan Leu	MDL	498
Moroccan Dirham	MAD	504
Rial Omani	OMR	512
Namibia Dollar	NAD	516

Annex II. ISO currency codes.

Nepalese Rupee	NPR	524
Netherlands Antillian Guilder	ANG	532
Aruban Guilder	AWG	533
Yugoslavian New Dian	NTZ	536
Vatu	VUV	548
New Zealand Dollar	NZD	554
Naira	566	556
Cordoba Oro	NIO	558
Naira	NGN	566
Norwegian Krone	NOK	578
Pacific Island	PCI	582
Pakistan Rupee	PKR	586
Balboa	PAB	590
Kina	PGK	598
Guarani	PYG	600
Nuevo Sol	PEN	604
Philippine Peso	PHP	608
Guinea-Bissau Peso	GWP	624
Timor Escudo	TPE	626
Qatari Rial	QAR	634
Russian Ruble	RUB	643
Rowanda Franc	RWF	646
Saint Helena Pound	SHP	654
Dobra	STD	678
Saudi Riyal	SAR	682
Seychelles Rupee	SCR	690
Leone	SLL	694
Singapore Dollar	SGD	702
Dong	VND	704
Slovenian Tolar	SIT	705
Somali Shilling	SOS	706
Rand	ZAR	710
Zimbabwe Dollar	ZWD	716
Yemeni Dinar	YDD	720
Sudanese Pound	SDP	736
Sudan Airlines	SDA	737
Lilangeni	SZL	748
Swedish Krona	SEK	752
Swiss Franc	CHF	756
Syrian Pound	SYP	760
Tajik Ruble	TJR	762
Baht	THB	764
Pa’anga	TOP	776
Trinidad and Tobago Dollar	TTD	780
UAE Dirham	AED	784
Tunisian Dinar	TND	788
Turkish Lira	PTL	793
Manat	TMM	795
Uganda Shilling	UGX	800
Karbovanet	UAK	804
Denar	MKD	807
Egyptian Pound	EGP	818
Pound Sterling	GBP	826
Tanzanian Shilling	TZS	834
US Dollar	USD	840
Peso Uruguayo	UYU	858
Uzbekistan Sum	UZS	860
Tala	WST	882
Yemeni Rial	YER	886
Serbian Dinar	CSD	891
Zambian Kwacha	ZMK	894
New Taiwan Dollar	TWD	901
Manat	TMT	934
Cedi	GHS	936
Bolivar Fuerte	VEF	937
Serbian Dinar	RSD	941
Metical	MZN	943
Azerbaijanian Manat	AZN	944
New Leu	RON	946
Turkish Lira	TRY	949
CFA Franc BEAC	XAF	950
East Caribbean Dollar	XCD	951
CFA Franc BCEAO	XOF	952
CFP Franc	XPF	953
European Currency UN	XEU	954
Kwacha	ZMW	967
Surinam Dollar	SRD	968
Malagasy Ariary	MGA	969
Afghani	AFN	971
Somoni	TJS	972
Kwanza	AOA	973
Belarussian Ruble	BYR	974
Bulgarian Lev	BGN	975
Congolese Franc	CDF	976
Convertible Marks	BAM	977
Euro	EUR	978
Hryvnia	UAH	980
Lari	GEL	981
Zloty	PLN	985
Brazilian Real	BRL	986
Peseta Convertible	ESB	995

IV-2015