Santander

Product Guide

Virtual POS SIS

Redsys (*Owner area: e-commerce*)

Version 2.2

December 2019

Version Control

Version	Date	Affects	Short description of the change
1.0	01/06/2018	All	First Version
1.1	10/01/2019	Point 4.4, Point 4.5 and Point 12.	Validity period of the Pre-authorisation, amount 0 in Authentication and inclusion of point 12 (Reference guides).
1.2	29/01/2019	Point 4.1.1	Includes the Authorisation Cancellation operation.
1.3	06/02/2019	Point 4.5.1	Changes the amount to be confirmed in authentication confirmation operations.
2.0	27/03/2019	Various points	>Information added about EMV 3DS and PSD2 >Reference to REST integration guide deleted. >Reference to PUCE guide deleted.
2.1	04/10/2019	Point 9	Comment about Delegated Authentication added.
2.2	05/12/2019	Point 10	

Interactive index

1. Introduction 4

2. Main Characteristics of the Virtual POS 5

3. Virtual POS Models 6

3.1 Models with business integration 6

3.1.1 Standard Model........ 7

3.1.2 Integration using Payment module 7

3.1.3 In-app integration........ 7

3.1.4 Puce integration 7

3.2 Models with no virtual store 8

3.2.1 Payment via e-mail/sms (Paygold)........ 8

3.2.2 Manual Payment (Moto Payment)........ 9

4. Types of Operations 9

4.1 Authorisation 9

4.1.1 Authorisation Cancellation 9

4.2 Return (Patrial or total) 9

4.3 Return withouth the original 10

4.4 Pre-authorisation 10

4.4.1 Confirmation of Pre-authorisation........ 10

4.4.2 Cancellation of Pre-authorisation 10

4.5 Authentication 10

4.5.1 Confirmation of Authentication 11

4.6 Payment of betting Prize 11

5. Types of Notifications/Responses........ 11

5.1. Models with business integration 11

5.1.1 Standard - Redirection 11

5.1.2 Standard - Host to Host 12

5.1.3 Integration using Payment model........ 12

5.1.4 In-app integration........ 12

5.1.5 Puce integration 12

5.2. Models without business integration 12

Interactive index

6. Payment Methods 13
6.1 Card payment 13
6.2 Wallet 13
6.2.1 Paypal 13
6.2.2 ApplePay 13
6.2.3 Masterpass 13
6.3 Account Payments 13
6.3.1 Bizum 13
6.3.2 Transfer 13
7. Added Value Services 14
7.1 1-Click/Tokenisation payment 14
7.2 DCC 14
8. Virtual POS Administration Module 14
9. Implications of the PSD2 (Advance) 14
10. FAQs 16
11. Annexes 17
11.1 Lenguages 17
11.2 Currencies 17
12. Glossary 17
12.1 PCI-DSS 17
12.2 Puc Protocol 17
12.3 3D Secure 18
12.4 SCA 18
12.5 PSD2 18
12.6 Acquiring Bank 18
13. Reference Guides 19
13.1 Integration of the Virtual POS 19
13.2 Payment Methods 19
13.3 Added ValueServices 19
13.4 Administration Module of the SIS 19

1 | Introduction

The Virtual POS is a system that allows a business with an online store to receive payments for the purchases made by its customers. Redsys' Virtual POS offers businesses an e-commerce platform that is reliable, powerful and easy-to-integrate into their website. It offers different types of connection that adapt to the needs of any type of business. It also has free connection modules for the main online stores (Prestashop, Woocommerce, Magento, Oscommerce, Opencart, Virtuemart, Zencart).

Different payment methods can be integrated on the business' website; payment with both debit and credit cards and different schemes (Visa, Master, Amex, Diners, JCB, UnionPay), Wallets and transfers. It has different types of payments: 1-click-payment and tokenisation, recurring payments, subscriptions, telephone payment, and sending collection requests by e-mail/SMS.
It is a Secure Virtual POS, which has 3D Secure Authentication, Fraud Services and Risk Control. Enables businesses to comply with PCI-DSS.

It is a multi-currency and multi-language platform that can be customised to adapt to the image of the business. It has a management tool that makes it possible to see and control sales, generating reports and statistics.

All these functionalities can be combined, offering a personalised solution for the needs of each business. There is also a 24x7 support service to resolve any queries/incidents.

To contract the Virtual POS, the business must contact its bank, which will establish the contracting conditions. In order to formalise said contracting, the bank will ask the store for some basic information about its business, and may ask to see the website design in advance.

Important Note:

As a result of the entry into force of the European Payments Directive PSD2 during 2020, this guide includes some new features and technical specifications that will be available in the future (in 2020) to facilitate the preparation of the work for businesses that wish to incorporate certain possibilities into their payment transactions, especially in relation to authentication management and authentication exemption covered by the PSD2. If applicable, these headings are marked as "ADVANCE".

2 | Main characteristics of the Virtual POS

Below is a list of the main characteristics of the Virtual POS:

- › **Easy to integrate:** The Virtual POS offers a series of opportunities that allow the business to create their online store according to its needs.
  - › **Own integration:** The business can do its own integration. This option requires more technical knowledge, but offers greater possibilities for configuration and customisation when making payments at its online store. Redsys also provides businesses with a series of **APIs that help businesses** to integrate the Virtual POS into its online store.
  - › **Integration with payment module:** Redsys provides a series of free modules for any business that has its online store at: Prestashop, Woocommerce, Magento, Oscommerce, Opencart, Virtuemart or Zencart. To carry out the integration, the business simply needs to install the chosen module and do a quick configuration with the main identifying values of **the business.**

- › **Adapted to mobile devices:** Our Virtual-POS has a design fully adapted to mobile devices. To this end, Redsys offers two options:
  - › Based on the **responsive design** of our virtual payment gateway. This method allows customers who make payments on their mobile device to have a fully adapted page.
  - › It has **SDKs** for both iOS and for Android. These SDKs have the option of integrating the payment gateway in the business' application with a wide range of personalisation options.

- › **Management and control of the online store:** Redsys provides businesses with management tools that give them full control over their commercial activity using the Virtual POS.
  - › **Administration module:** The administration module gives businesses full control over the transactions made using the Virtual POS with the option to view the transactions using different filters and export them to a spreadsheet to create their own reports, in addition to the operational and transaction conversion reports included within the tool.
  - › Management of the business' **customer portfolio:** This tool is optional and must be activated expressly by the Acquiring Bank.
  - › **Risk Control Tool:** Risk control tool that enables the business to manage a series of configurable rules through the Virtual POS administration module that allows it to control exposure to fraud.
  - › **Fraud control service:** Redsys' Virtual POS has a transaction control service to prevent fraudulent activities in its online store. These control parameters must be defined through the Acquiring Bank.

- › **Insurance:** The Virtual POS has different security measures that guarantee that transactions are made securely.
  - › **3D Secure:** Process that enables secure purchases to be made online, authenticating the purchaser as the legitimate holder of the card being used.
  - › **PCI-DSS compliance:** Using this method, Redsys has express authorisation to store the confidential card information.
  - › **Security standards:** The Virtual POS implements SSL certificates. More specifically, it implements **TLS 1.2** in incoming communications and TLS 1.1 and TLS 1.2 in outgoing communications. The security in the transport layers stops information from being intercepted by third-parties, ensuring the confidentiality of all communications that are sent during the transaction.

› **Personalisation of the payment page:** Businesses will have a tool to personalise the payment page, allowing them to adapt it to their own image, improving browsing and making it more fluid for their customers.

Note: *Details on how to use the personalisation tool can be found in the "Virtual POS- Personalisation Tool_Business Manual" guide.*

› **Evolving and Adaptive:** The Virtual POS is an evolving system that aims to provide businesses with a service that adapts to their commercial activity without causing any impact. It is also adapted to different Wallets and account payments such as Bizum and PayPal.

› **Multi-language.** Likewise, and since the buyer could be in any part of the world, the Virtual POS can independently display the payment page for each transaction in any of the available languages. The business will decide which language to display in each transaction (see Annex 10.1).

› **Multi-currency and DCC.** The Virtual POS permits all international currencies admitted in e-commerce by the card companies (see Annex 10.2) and can therefore be used by businesses that have their prices in currencies other than Euros. There is also the dynamic currency conversion (DCC) service for businesses with prices in Euros that will be explained in more detail in the Added value services section of this document.

› **High availability:** Redsys guarantees businesses a high level of availability in the service with a 24x7 support service. This service can be used to resolve any questions, queries or requests that the business may have, whatever the **time.**

3 | Virtual-POS models

The bank always be aware of the business' operation in order to configure the Virtual POS in one way or another. These Virtual POS configurations or models do not box the business into a specific way of making sales, as they are perfectly combinable.

These terminal models are classified based on whether or not integration is required by the business, which involves developments of a certain technical level. According to this aspect, there are 2 large groups of terminal models: Models with and without business integration.

3.1. Models with business integration

This category requires the business to perform developments with a certain level of technicality. The following are models with business integration:

3.1.1 Standard Model

› **Connection by redirection to the payment page.** This is the most common type for businesses since it is not necessary to have a valid PCI-DSS questionnaire. In this type of store, when the buyer clicks on the "Pay" button on the business' website they will be redirected to the Virtual POS payment gateway where they must fill in their card information. The POS will manage the full transaction cycle, informing both the business and the card holder of the outcome.

This type of connection will authenticate the card holder, for which the suitable payment methods must be set up. As a general rule, since the card holder has been authenticated, these businesses are guaranteed the amount of the transaction in the event of a rejection.

Allows for the tokenisation of cards (1-click-payment), the use of Wallets integrated with the Virtual POS (MasterPass, PayPal, etc.) and the use of account payments (Bizum and transfer).

Note: *The payment methods for authenticating the card holder (Wallets and account payments) will be explained in more detail in the Payment methods section of this document.*

Note 2: *The technical information for carrying out this type of integration is shown in the "Virtual POS Integration Manual - Redirecting.pdf" guide.*

› **Host to Host connection (WebService SOAP or REST).** This type of connection will be useful for businesses that want their buyers' browsing experience to be continuous without leaving the website at any time, not even at the time of making the payment.

Businesses that need to use this type of connection must be authorised by their Acquiring Bank and have a validated PCI-DSS questionnaire, as it will the business that requests the card information from the holder.
With Host to Host connections, the business will capture all the information necessary to make the transaction in its system, including the holder's card information, and will send it to the Virtual POS, which will process the transaction and notify the business of the result, which will be responsible for informing the card holder.

Note: *It must be noted that with this type of connection, transactions cannot be made with Wallet type payments or account payments.*

Note 2: *The technical information for carrying out this type of integration via REST is shown in the "Virtual POS Integration Manual - REST.pdf" guide.*

Note 3: *The technical information for carrying out this type of integration via SOAP is shown in the "Virtual POS Integration Manual - Webservice.pdf" guide.*

› **Redirection + Host to Host connection.** The merchant can use the type of connection that best adapts to its needs at any given time, provided that the Acquiring Bank has correctly configured the Virtual POS and without needing a validated PCI-DSS. questionnaire.

This type of connection is common with merchants that make transactions that need card information with card holder authentication via redirection, and the transactions that do not need card information via Host to Host (returns, confirmations, cancellations, etc.) instead of through the Administration Module.

It is also common to use this type of connection to tokenise cards (1-click-payment), since the first transaction is made through a redirection connection, allowing the Virtual POS to capture the card information (and optionally authenticate), and the following transactions will be made using a Host to Host connection in which the token is sent instead of the card.

Note: *The card tokenisation operation (1-click-payment) will be explained in further detail in the Added value services section of this document.*

› **InSite connection.** This connection model allows a merchant to use the Virtual POS with the advantages of the redirection connection and the Host to Host connection, without needing a validated PCI-DSS. questionnaire.

The buyers' browsing experience is continuous and they do not leave the website at any time, not even at the time of making the payment. It also allows for card holder authentication, so the amount of the transaction is guaranteed in the event of possible rejections.

Note: *The technical information for carrying out this type of integration is shown in the "TPV-Virtual Integración inSite.pdf" guide.*

3.1.2 Integration using Payment module:

Merchants that have virtual stores designed with Prestashop, Woocommerce, Magento, Oscommerce, Opencart, Virtuemart or Zencart have free modules that allow for the activation of card payments in their store.

The payment module is installed quickly and easily, with minimum technical knowledge.

Note: *The details of the installation and configuration of the payment modules are shown in the following link of the Redsys public website "http://www.redsys.es/#descargas".*

3.1.3 In-App integration

This connection model allows merchants that have mobile applications in Android or iOS to integrate card payments.

SDKs are provided to carry out this integration, which the merchant must integrate in its application.

Note: *The technical information for carrying out this type of integration is shown in the following guides: "TPV-Virtual Documentacion - Integracion TPVInLibrary iOS.pdf" and "TPV-Virtual Documentacion - integración TPVvirtualAndroid.pdf".*

3.1.4 PUCE integration

This connection model allows merchants to authenticate card holders through the Virtual POS and then manage the authorisation using the PUC Protocol.

Note: *The technical details of this Virtual POS are shown in the "TPV- Virtual Manual Integración - REST".*

3.2. Models with no virtual store integration

This category allows the merchant to use the advantages of the Virtual POS without the need for any type of development to integrate a virtual store. The following Virtual POS models do not have merchant integration:

3.2.1 Payment by e-mail/SMS (Paygold)

Payment by e-mail/SMS (Paygold) consists in sending a link to the card holder vis e-mail or SMS with a payment request from the merchant. The holder must use the link to complete the payment. This type of payment does not require integration by the merchant since payment request is sent through the administration module.

Card holders will receive a link in their inbox or via SMS with the transaction information. The customer must click on the link to complete the purchase. This way, the merchant does not handle card information during any stages of the payment.

This type of operation can be useful, for example, with donation merchants, merchants with specific promotions that require a mass sending, and a company that sends its customers emails every time it wants to request payment for its services (or similar) instead of setting up direct debits.

The merchant can also automate the sending of the payment request using a Host to Host connection, for which it will need to carry out an integration.

Note: *The technical details of this Virtual POS are shown in the "TPV- Virtual Pago por e-mail_SMS.pdf guide.".*

3.2.2 Manual Payment (MOTO Payment)

With the manual payment or MOTO payment, the card holder is not present at the time of the payment. They give the card information to the merchant, either by telephone or via e-mail, and the merchant makes the payment through the Administration Module of the Virtual POS, so no integration with the merchant's website is required. This type of payment is normally used in call centres.

Note: *The technical details of this Virtual POS are shown in the "TPV- Virtual Pago MOTO.pdf" guide.*

4| Types of Transactions

The Virtual POS has a large variety of transaction types. The merchant can use several types according to its needs and according to the configuration that its Acquiring Bank allows. Below is a description of the types admitted by the platform:

4.1. Authorisation

This is the common sale transaction. The transaction is initiated by the card holder, who is connected to the merchant's website during the purchase process, so authentication may be required if the merchant is configured as such.

The transaction is automatically captured by the Virtual POS and sent to the issuing bank, producing an immediate charge in the holder's account that is associated with the card (credit or debit). Once the card holder has been authorised or rejected, the merchant will be informed of the result thereof.

4.1.1 Cancellation of the Authorisation

This must be sent by the merchant, since the holder is not present, and the amount charged to the holder during the transaction is refunded as soon as possible. Authorisation and cancellation transactions may or may not be shown in the holder's account, at the issuer's discretion.

This transaction must be made by a backoffice developed by the merchant itself.

4.2. Return (partial or total)

These are accounting transactions initiated by the merchant, in which the Virtual POS will check that there is an original authorisation to be returned, as well making sure that the sum of the returned amounts do not exceed the amount originally authorised under any circumstance.

This can be done by the administration module offered with the POS and from a backoffice that has been developed by the merchant itself. The moment at which the card holder is refunded depends on the commercial policy of each issuing bank.

4.3. Return without the original

These are accounting transactions initiated by the merchant, in which the merchant does not have information about the original authorisation to be returned, so the Virtual POS will NOT check that there is an original authorisation or the returned amounts.

This type of transaction can only be performed by the backoffice that has been developed by the merchant itself. The moment at which the card holder is refunded depends on the commercial policy of each issuing bank.

Note: *These types of transactions require an extra configuration that must be provided by the Acquiring Bank.*

4.4. Pre-authorisation

The pre-authorisation withholds the amount in the holder's account and does not result in a charge, although exceptions can be made depending on the policy of the card issuer. This can be used when it is not possible to determine the exact amount to be charged to the holder at the time of the purchase.

The transaction is transparent for the holder, and is exactly the same as an authorisation transaction at all times, i.e., they provide their information and authenticates if necessary.
The validity period of a pre-authorisation is 7 days. This period may be greater is the Acquiring Bank of the Virtual POS so decides.

The pre-authorisation transaction is only allowed with Visa and Master cards.

4.4.1 Pre-authorisation confirmation

This must be sent by the merchant, since the holder is not present, and it completes the pre-authorisation transaction. This transaction already has an accounting charge, and the amount may be less than, the same as or up to 15% more than the original amount. This can be done by the administration module of the Virtual-POS and also by a backoffice developed by the merchant itself.

4.4.2 Cancellation of the pre-authorisation

This must be sent by the merchant since the card holder is not present, releasing the amount withheld from the holder in the pre-authorisation transaction. This can be done by the administration module of the Virtual-POS and also by a backoffice developed by the merchant itself.

Note: *These types of transactions require a specific configuration of the merchant which must be done by the Acquiring Bank.*

4.5. Authentication

This type of operation is similar to the pre-authorisation operation (see point 4.4). It does not produce a withholding in the holder's account since the amount finally sent to the issuer is 0. The card information is validated, checking the CVV2/CVC2, the expiry date and whether the card is active.

The transaction is transparent for the holder, and is exactly the same as an authorisation transaction at all times, i.e., they provide their information and authenticates if necessary. The merchant has 45 calendar days to confirm it or to simply let it expire.

4.5.1 Authentication Confirmation

This must be sent by the merchant, since the holder is not present, and it completes the authentication operation. This transaction already has an accounting charge, and the amount may be less than, the same as or up to 15% more than the original amount. This can be done by the administration module of the Virtual POS and also by a backoffice developed by the merchant itself.

4.6. Payment of betting prizes

This is a type of operation for betting payment websites that use the Virtual POS to pay prizes. These are accounting transactions initiated by the merchant, which sends a payment order to the customer's bank which will make the payment in the holder's account associated with the card with which the bet was placed.

This type of operation requires a specific configuration by the Acquiring Bank.

Note: *The technical details of this model for this type of operation are shown in the "TPV- Virtual Pago de premios de apuestas en TPV Virtual.pdf" guide.*

5 | Types of notifications/responses

The Virtual POS has several ways of informing the merchant of the result of a transaction, which will depend on the Virtual POS model used:

5.1. Models with merchant integration

All the terminal models with integration by the merchant can see the result of their transactions by consulting the administration module of the Virtual POS or through an e-mail notification. Furthermore, the Virtual POS has functionalities to inform of the result of the transactions in real time, without having to access the administration module of the Virtual POS. These functionalities are individual to each Virtual POS with integration that is used:

5.1.1 Standard - Redirection

For these types of Virtual POS models, the "online notification" will be used, which is an optional function that allows the online store to receive the result of a transaction online and in real time once the customer has completed the Virtual POS process.

The merchant must capture and validate all the parameters together with the signature of the online notification before any execution on its server.

The Virtual POS has different types of notifications, as follows:

› **Synchronous:** Implies that the result of the first purchase is sent to the merchant and then to the customer with the value. The transaction cannot be cancelled, even if the notification is incorrect.

› **Asynchronous:** Implies that the result of the authorisation is communicated to the merchant and the customer at the same time. The transaction cannot be cancelled, even if the notification is incorrect. In this case the notification is added to a queue, which guarantees that it is always sent, even if there are occasional delays. Its use is recommended.

Note: *The technical information about the "online notification" and its different versions is shown in the "TPV-Virtual Manual Integración - Redirección.pdf" guide.*

5.1.2 Standard – Host to Host

With these types of Virtual POS models, the response from the Host to Host request sent by the merchant will be used, informing of the result of a transaction in real time once the process has been completed in the Virtual POS.

Note: *The technical information of the Host to Host response via REST is shown in the "TPV-Virtual Manual Integración - REST.pdf" guide.*

Note 2: *The technical information of the Host to Host response via SOAP is shown in the "TPV-Virtual Manual Integración - Webservice.pdf" guide.*

5.1.3 Integration using the payment module

For these types of Virtual POS models, the "online notification" will be used but with the exception that the merchant will not have to capture or validate the parameters together with the signature of the online notification, since the model will run all the necessary validations.

5.1.4 In-App integration

A different type of notification or response will be received according to the type of In-App integration used by the merchant:

› **Webview:** The "online notification" will be used for these types of In-App integration models, which is an optional function that allows the online store to receive the result of a transaction online and in real time once the customer has completed the process in the Virtual POS.

› **Direct Payment:** For these types of In-App integration models, the response from the direct request (Host to Host) sent by the merchant will be used, informing of the result of a transaction in real time once the process has been completed in the Virtual POS.

Note: *The technical information for carrying out this type of integration is shown in the following guides: "TPV-Virtual Documentacion - Integracion TPVInLibrary iOS.pdf" and "TPV-Virtual Documentacion - integración TPVvirtualAndroid.pdf".*

5.1.5 PUCE Integration

In the Virtual POS model with PUCE integration, the response from the request sent by the merchant will be used, informing of the result of the transaction in real time once the process has been completed in the Virtual POS.

Note: *The technical details of this Virtual POS are shown in the "TPV- Virtual Manual Integración - REST".*

5.2. Models without merchant integration

All the terminal models without integration by the merchant can see the result of their transactions by consulting the administration module of the Virtual POS or through an e-mail notification.

Note: *The details of how to see the transactions in the administration module of the Virtual POS is shown in the "TPV-Virtual Módulo de Administración.pdf" guide.*

6| Payment methods

The Redsys virtual POS makes it possible to offer the customer different payment methods that can be divided into: methods associated with Card Payments, the use of Wallet or Account Payments.

6.1. Card payment

Makes it possible to integrate the payment with both domestic and international cards from the main companies: Visa, Master, Amex, JCB, Diners, etc. It also makes it possible to authenticate the customer using the card holder authentication system by means of the 3D Secure process.

6.2. Wallet

6.2.1 Paypal

For a merchant to be able to work with PayPal through the Vitual POS, it will have to follow the steps below:

› The Acquiring Bank must authorise the adhesion to this payment method.

› The merchant must register with PayPal.

› The Acquiring Bank must be given the connection information provided by PayPal.

Note: *The technical information of this Wallet is shown in the "TPV-Virtual Manual Integración PayPal.pdf" guide.".*

6.2.2 ApplePay

For a merchant to be able to work with ApplePay through the Virtual POS.

Note: *The technical information of this Wallet is shown in the "TPV-Virtual ApplePay - Guía de Integración de los Comercios.pdf" guide.*

6.2.3 Masterpass

For a merchant to be able to work with MasterPass through the Virtual POS.

Note: *The technical information of this Wallet is shown in the "TPV-Virtual Masterpass.pdf" guide.*

6.3. Account Payments

6.3.1 Bizum

For a merchant to be able to work with Bizum through the Virtual POS.

Note: *The technical information of this Wallet is shown in the "TPV-Virtual Guia de Integracion BIZUM comercios SIS.pdf" guide.*

6.3.2 Transfer

For a merchant to be able to offer payments via bank transfer.

Note: *The technical information of this payment method is shown in the "TPV-Virtual Transferencia.pdf" guide.*

7 | Added value services

The Virtual POS offers a wide range of added service that are shown below:

7.1. 1-Click Payment / Tokenisation

The 1-click-payment allows card holders to make regular purchases on a website with just one click and without entering their card information. They will just need to enter their card information for the first purchase.

The technical implementation of this payment method in Redsys is done in such a way that the merchant does not need to be certified as complying with the PCI-DSS protocol, as it will not need to store card holder's information to process the payments.

Note: *The technical information of this added value service is shown in the "TPV-Virtual Pago-1-click.pdf" guide.*

7.2. DCC

The DCC operation allows card holders whose currency is different to the one configured in the Virtual POS to be able to pay in their own currency.

Once the transaction has been processed, the customer will be shown the outcome. If the customer chooses their card currency, the outcome will always be displayed in English.

Note: *This type of transaction requires an extra configuration that must be provided by the Acquiring Bank with which the merchant has contracted the Virtual POS.*

Note 2: *The technical information of this added value service is shown in the "TPV-Virtual Integración DCC.pdf" guide.*

8 | Administration Module of the Virtual POS

The Virtual POS has an administration module in which transactions that do not require card information (i.e. they do not require the card holder to be present) can be viewed and managed. The appearance of the administration module may change according to the Acquiring Bank.

Note: *The details of how to see the transactions in the administration module of the Virtual POS are shown in the "TPV-Virtual Módulo de Administración.pdf" guide.*

9 | Implications of the PSD2 (Advance)

PSD2 is the acronym of Payment Services Directive 2 and that alludes to the second EU Payment Services Directive. By means of its transposition to the Member States, this directive incorporates measures that have an important impact on all electronic payments, in particular remote payments such as internet purchases.

According to the regulations that enter into force on 14 September 2019 (when the technical regulation or RTS enter into force), in general, all e-commerce transactions within the EEA (European Economic Area) must use enhanced authentication (SCA - Strong Customer Authentication), although it does include some exceptions (exemptions).

For a merchant that accepts payments remotely, complying with this regulation will depend on the payment method used, the main solution being the implementation of 3D Secure as an authentication protocol for card payments. Other payment methods such as X-pays (Apple Pay, Google pay, etc.) may include other authentication systems delegated by the card issuer or may already have these SCA mechanisms incorporated (e.g. Bizum) and do not require 3D Secure.

Cases of remote payment that do not require the use of SCA are those included in the exemptions of the directive, or that are outside the scope of the directive:

- **Out of the scope of PSD2:**
  - **Payments initiated by the merchant without customer participation** (MIT - Merchant Initiated Transactions), and recurring payments for a subscription.
  - **Telephone or e-mail payments.**
  - **Non-payment transactions, such as card validations** with an amount of zero.

- **Cases with a possible application of exemptions (optional).** These are low-risk cases that, in conjunction with a risk analysis system, allow for the optional non-application of SCA.
  - **Low value exemption:** payments of < €30 and when no more than €100 or 5 transactions in a row are accumulated without SCA. The card issuer bank is responsible for **controlling these counters.**
  - **Low risk exemption - Transaction Risk Analysis (TRA).** Its application requires additional conditions on the accumulated fraud history that must be assessed by the Acquiring Bank.
  - **Secure Corporate Payment Protocol Exemption**. Use restricted to special cases of payments between companies where the channel used is not available to the general public and incorporates other security mechanisms at the same level as an SCA.

In order for a merchant to apply the exemptions, it must have authorisation from its Acquiring Bank.

To send a transaction without reinforced authentication without it being denied, the case that applies from the previous list must be reported. This means that to avoid rejections by the acquirer or the issuer for not using 3DSecure, transactions must be properly marked to justify the non-use of 3DSecure (more information in the technical integration manuals):

Reason for not applying SCA	Method for reporting in the Virtual POS
Transaction initiated by the merchant	Exemption indicator (DS_MERCHANT_EXCEP_SCA): MIT value
Low amount transaction	Exemption indicator (DS_MERCHANT_EXCEP_SCA): LWP value
Mail order/ telephone order	Input ID field MO/TO (DS_MERCHANT_DIRECTPAYMENT) mail order/telephone order
Card validation transactions (zero amount)	According to the requested transaction (DS_MERCHANT_TRANSACTIONTYPE)
Low risk exemption/TRA	Exemption indicator (DS_MERCHANT_EXCEP_SCA): TRA value
Secure Corporate Payment Protocol Exemption.	Exemption indicator (DS_MERCHANT_EXCEP_SCA): COR value
Transaction completed with delegated SCA authentication	Exemption indicator (DS_MERCHANT_EXCEP_SCA): ATD value

10 | FAQs

› Can I have two e-mail addresses for sending confirmations registered on the Virtual POS?

Redsys will only send one notification per transaction to an e-mail address: the one configured in the Email-Channels Merchant section. However, the merchant can send this notification to as many addresses as it considers necessary.

› I want to change my merchant's payment methods.

All requests to change the payment methods that the merchant has activated in the SIS Virtual POS must be processed by the Acquiring Bank with which the merchant works.

› I want to customise the Virtual POS screens with my merchant's image. What steps must I follow?

Redsys has a customisation tool for merchants included in the administration tool to which you are currently connected, and through which you can change the visual aspect of the payment gateway. Once the changes have been made, the bank that owns the POS must approve the changes to make them effective.

› What types of cards does the Virtual POS accept?

As a general rule, the POS accepts all cards that work with e-commerce.

› I am a merchant and I want to have access to the customer's payment information (card number, expiry, etc.).

Due to their confidential nature, all requests to access payment information (card number, expiry, etc.) must be managed directly with the Acquiring Bank.

› Can I make instalments/deferred payments with the Virtual POS?

The Virtual POS has different functionalities depending on the bank with which the merchant works. The bank will inform about the particularities of its operation.

› Can I make instalments/deferred payments with the Virtual POS?

The Virtual POS has different functionalities depending on the bank with which the merchant works. The bank will inform about the particularities of its operation.

› I have two online businesses. Is it possible to manage two business through the same username?

Yes it is, provided that the address set up for both users is the same. If it is different, you must contact your financial institution.

11 Annexes

Below are the different annexes that are cited in the document:

11.1. Languages

The languages available for the payment page are those listed below:

- Spanish
- Catalan
- Valencian
- Galician
- Czech
- Danish
- German
- Estonian
- Greek
- English
- French
- Croatian
- Japanese
- Latvian
- Lithuanian
- Hungarian
- Maltese
- Dutch
- Italian
- Romanian
- Swedish
- Polish
- Portuguese
- Russian
- Bulgarian
- Slovenian
- Slovak
- Finnish
- Turkish
- Indian

11.2. Currencies

The available international currencies permitted in e-commerce by the card companies are:

- Euros
- Dollars
- Pounds
- Pesos Yen
- Swiss Francs
- Autralian Dollars
- Canadian Dollars
- Swedish Krona
- Norwegian Krone
- Costa Rican Colones
- Uruguayan Pesos
- Zlotys
- Argentine Australes
- Peruvian Nuevo Soles
- Chinese Yuan
- Turkish Liras
- Etc.

12 Glossary

12.1. PCI-DSS

PCI-DSS compliance refers to the fact that the confidential card information is not normally known by the merchant, unless the bank that owns the POS authorises as such if the merchant meets the required conditions. This prevents third parties from being able to steal this information from the merchant for fraudulent purposes. The best way to safeguard sensitive information is by NOT having it. Instead, the information is appropriately stored by Redsys. However, there are other connection variants for merchants that wish to take on PCI-DSS and the handling of payment information to better adapt to their business requirements.

12.2. PUC Protocol

The Unified Commerce Protocol [Protocolo Unificado Comercio] (PUC) is the protocol by which an Establishment/Business/-Service Provider, with all the HW and SW infrastructure adapted to EMV (card interoperability standard with integrated circuit), can connect its Host to the Processing Centre (REDSYS) in order to exchange messages directly or indirectly originated by the use of the card: Request for authorisation, Sending deferrals, Loading/Updating the Black List, etc.

12.3. 3D Secure

3D Secure refers to the authentication standard that, during an online purchase, certifies the consumer's identity as the legitimate owner of the card being used. This process is specially designed to prevent card fraud with remote transactions where there is no actual physical presence of the card.

In addition, the Virtual POS allows authentication with any of the versions of 3D Secure, including the new version, 3D Secure 2 (3DS2). This new version is the principal route to comply with future PSD2 Enhanced Customer Authentication (SCA) regulations, allowing for less problematic authentication and a better user experience.

One of the main improvements of the 3DS2 is the frictionless authentication, an authentication that, according to the information collected about the card holder, the device used, etc. will allow for authentication without requiring any intervention from the card holder.

If you already use 3D Secure by redirecting, you will be moved to version 2 with no changes in the integration, although you can make changes to add further optional information to the payment transaction and thus make better use of the characteristics if this new version of 3D Secure.

12.4. SCA

Strong Customer Authentication refers to the use of several factors (instead of just one) to authenticate the user's identity. The factors must be from different categories (knowledge: something that only the user knows, possession: something you have, and finally something that you are). For example: the combination of a password or PIN (knowledge) and a card chip (something that you have) or the combination of a password (something you know) + a code sent by SMS (something you have, the telephone the code is sent to).

12.5. PSD2

PSD2 is the acronym of Payment Services Directive (2) that alludes to the second EU Payment Services Directive. Incorporates measures that have a important impact on all e-payments, in particular remote payments such as internet purchases. According to the regulations that will come into effect on 14 September, in general, all e-commerce transactions must use stronger authentication (SCA), although it does include certain exceptions (exemptions).

With this regulation a series of exemptions will come into effect to carry out different operations, and as such, authentications will not be requested for considerations that fall under said regulation. There will be exemptions for low amounts, for recurring or scheduled transactions, provided that the first one is SCA authenticated, and exemptions for risk analysis by the merchant.

12.6. Acquiring Bank

The Acquiring Bank refers to the banking institution through which the merchant has contracted their Virtual POS.

13 | Reference Guides

This point shows the list of reference guides for the Virtual POS

13.1. Integration of the Virtual POS

> *TPV-Virtual Manual Integración - Redirección.pdf*
> *TPV-Virtual Manual Integración - REST.pdf*
> *TPV-Virtual Manual Integración - Webservice.pdf*
> *TPV-Virtual Integración inSite.pdf*
> *TPV-Virtual Documentacion - Integracion TPVInLibrary iOS.pdf" and "TPV-Virtual Documentacion - integración TPVvirtualAndroid.pdf*
> *TPV-Virtual Pago por e-mail_SMS .pdf*
> *TPV-Virtual Pago MOTO.pdf*
> *TPV-Virtual Pago de premios de apuestas en TPV Virtual.pdf*

13.2. Payment methods

> *TPV-Virtual Manual Integración PayPal.pdf*
> *TPV-Virtual ApplePay - Guía de Integración de los Comercios.pdf*
> *TPV-Virtual Masterpass.pdf*
> *TPV-Virtual Guia de Integracion BIZUM comercios SIS.pdf*
> *TPV-Virtual Transferencia.pdf*

13.3. Added value services

> *TPV-Virtrual Pago-1-click.pdf*
> *TPV-Virtual Integración DCC.pdf*
> *TPV-Virtual Consulta SOAP.pdf*

13.4. SIS adminitration module

> *TPV-Virtual Módulo de Administración.pdf*
> *TPV-Virtual- Herramienta Personalización_Manual Comercios*