Rabobank

Integration Guide

Rabo OmniKassa

Contents

1. INTRODUCTION

This document describes how to integrate the Rabo OmniKassa with the merchant's site (webshop). Installation requires knowledge of at least one programming language, such as PHP or .NET.

Chapters 2, 3 and 4 of this guide tell you what you need to know before getting started with integrating the Rabo OmniKassa with your webshop. Chapter 2 explains the security the Rabo OmniKassa uses, the secret key and access to the Downloadsite. Chapter 3 describes the steps for making a payment in the Rabo OmniKassa, and chapter 4 describes the standard protocol for the messages between the webshop and the Rabo OmniKassa server.

Chapters 5, 6, 7 and 8 provide the information you need to write program codes for the payment request (chapter 5) and the response message (chapter 6).
As soon as your codes are complete, you can test them in the Rabo OmniKassa test environment for various different payment methods (chapter 7). An explanation of the error messages you may see during the testing process is provided in chapter 8.

After the requester has signed the Rabo OmniKassa contract, Rabobank will send you the login data for the Rabo OmniKassa Downloadsite and dashboard. On the Downloadsite, you will find your Rabo OmniKassa secret key. With your merchant ID and your secret key, you can take the Rabo OmniKassa into the production environment and allow your customers to make payments in the Rabo OmniKassa. More information about the production environment is provided in chapter 9. The appendices (chapter 10) provide a list of all variable fields and settings.

Together, the Rabo OmniKassa integration guide and the user guide for the Downloadsite should provide all the information you need to integrate the Rabo OmniKassa with your webshop.
If you have questions about integrating the Rabo OmniKassa, please contact the Support Team Rabo OmniKassa. The Support Team is available by phone on +31 30 7122117 (Mondays through Fridays from 08.00 am to 07.30 pm) or by e-mail at: contact@omnikassa.rabobank.nl.

2. WHAT YOU NEED TO KNOW ABOUT THE RABO OMNIKASSA

2.1 Integrating Rabo OmniKassa and the webshop

In order to allow customers to pay in the Rabo OmniKassa, the webshop must be able to send payment requests to the Rabo OmniKassa server. The Rabo OmniKassa server sends the result of the payment request as a response message back to the webshop. The payment status received in the response message allows the webshop to further process the order.
This guide explains how to program a payment request and response message. Along with the information in this guide, Rabobank provides a number of sample codes (PHP and .NET) that may help you with this programming.
The code examples can be found on the Rabobank website: www.rabobank.nl/omnikassa-support under '+ Hoe integreer ik de Rabo OmniKassa in mijn webwinkel?'.

2.2 Security

The Rabo OmniKassa is PCI DSS-compliant (Payment Card Industry Data Security Standard).
This means that the response message contains no customer information such as name[1], bank account or credit card number, PAN number or other customer information. Instead, a unique transaction reference number (transactionReference) is used to match the response message to the order in the webshop and the appropriate customer. We also recommend using an order number as an extra identification field in the payment request (orderID). See also the footnote at the bottom of this page.

[1] To be able to find (for instance) the name of your customer in a transaction in your own (order) records, it is adVISAble to use the optional field 'orderId'. This field allows you to assign a reference code to the transaction. This reference code will then be included in the response message. Manual or automated reconciliation with the details in your own (order) records will be possible on the basis of the details in that response message*, enabling you (for instance) to find the name of your customer. For this to be possible, your customers must (at some time in the past) have registered with their name in your webshop and every order/purchase must be linked to that registration. See also section 5.1 and chapter 6.

*
The reference code 'orderId' can also be found in the Rabo OmniKassa dashboard (Order Number) and is stated in the Excel attachment in the e-mail message 'Rabo OmniKassa payment details'. See also section 10.7.

2.3 Secret key

The payment request and the response message between the webshop and the Rabo OmniKassa server are exchanged securely, thanks to the use of a secret key. You can find the Rabo OmniKassa secret key on the Downloadsite: https://download.omnikassa.rabobank.nl/.
After the signed Rabo OmniKassa contract is received by Rabobank, the technical contact person will receive the username for the Downloadsite via e-mail. The password will be sent by mail to the contract requester. For more information, see chapter 9 of this guide and the user guide for the Rabo OmniKassa Downloadsite.
You do not need your own secret key to install the Rabo OmniKassa in the test environment. For the test environment, you can use the general test merchant ID and its corresponding secret key. See chapter 7 for more information.

2.4 Rabo OmniKassa dashboard

After Rabobank activates the Rabo OmniKassa the requester will receive two e-mails providing them with the log-in information they need to use the Dashboard: one with the username and one with a link enabling them to set their own password. In the Dashboard the user can find information about the transactions and payments as soon as the Rabo OmniKassa is live. The dashboard can be accessed at: https://dashboard.omnikassa.rabobank.nl/. See the dashboard user guide for more information.

2.5 Rabo OmniKassa payment details

The transactions (details) of the Rabo OmniKassa payment can not only be found in the Rabo OmniKassa Dashboard, but are also reported in the Excel attachment of the e-mail message ‘Rabo OmniKassa payment details’. This e-mail message is sent by Rabobank to the contact person of the webshop on the day a payment is made to the webshop for one or more successful transactions. You will find an explanation of the most important fields of the Excel attachment referred to above in section 10.7.

2.6 What you need to know before installing

- The Rabo OmniKassa supports the payment methods iDEAL, MasterCard, VISA, Maestro, V PAY and Bancontact.
- The Rabo OmniKassa can also support the register services acceptgiro (giro collection form), incasso (direct debit) and rembours (cash on delivery). If a customer selects a register service on the Rabo OmniKassa payment page, the webshop will receive a message. The webshop must ensure that it obtains the customer's name and address information and bank account number. The webshop will immediately start the procedure for processing this payment. Payment using these register services does not go through the Rabo OmniKassa, and these payments are not displayed in the Rabo OmniKassa dashboard. Consult your Rabobank contact person before using the register services.

- The Rabo OmniKassa supports two languages, Dutch (default) and English (option).
- The payment page in Rabo OmniKassa is available for your customers in eight languages. This page will be displayed by default in Dutch, unless in the payment request one of the seven other supported languages is mentioned.
- The Rabo OmniKassa supports payment in a number of different currency types, but payout must always be in euros. iDEAL en Bancontact support euros only.
- The iDEAL system displays the list of banks within the Rabo OmniKassa. This list cannot be displayed in your own webshop.

3. PAYMENT STEPS IN THE RABO OMNIKASSA

Integrating the Rabo OmniKassa with the webshop ensures that for every payment, the webshop sends a payment request to the Rabo OmniKassa server, and that the webshop can then receive and process the response messages.

A payment with the Rabo OmniKassa is a three-step process.

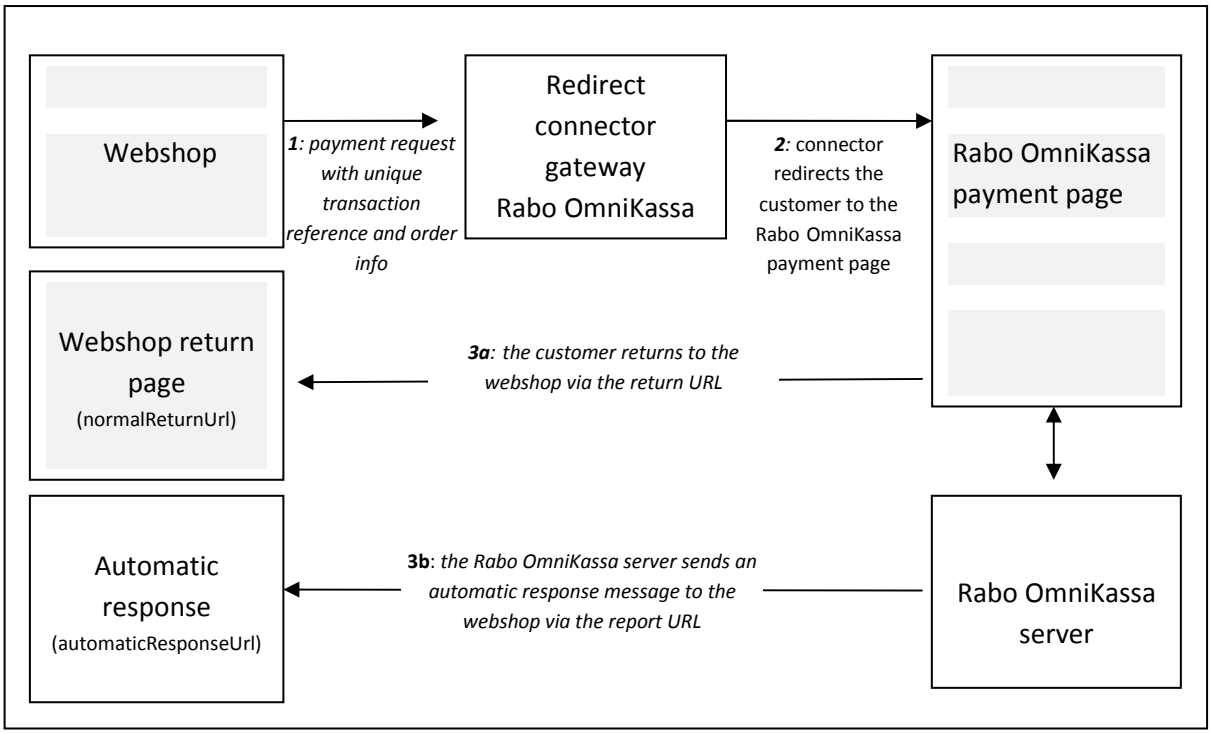

Figure 1: Diagram of a payment in the Rabo OmniKassa. The pages visible to the customer are marked in grey.

Payment step 1: Payment request sent from webshop

After the webshop customer has selected 'pay', the webshop sends a payment request to the Rabo OmniKassa server. This payment request contains unique information about the payment of the order. This flow uses the Rabo OmniKassa redirect connector gateway, the URL: https://payment-webinit.omnikassa.rabobank.nl/paymentServlet.
Payment requests can be sent as an HTML form or as an HTTP-POST message.

Payment step 2: Payment on the Rabo OmniKassa payment page

The customer is redirected to the Rabo OmniKassa server payment page. Depending on how you have installed the Rabo OmniKassa, the client will be able to choose a payment method here from the payment methods the requester has activated in the Rabo OmniKassa. If the customer has already selected a payment method in the webshop, he or she is sent directly to the payment screen for that payment method.
(For more information about the options here, consult the optional field 'paymentMeanBrandList' described in chapter 5, 'Payment request'.)

Payment step 3: Receipt and processing of response message

As soon as the payment is made, the Rabo OmniKassa server sends a response message with the current status of the payment. By default, the Rabo OmniKassa will send a single response message (return-URL) to the return page defined for the customer (field: normalReturnUrl). The webshop receives this message only when the customer has clicked the 'Continue' button on the payment page.
If the customer closes the payment in another way, the webshop will not receive the manual response message.
The Rabo OmniKassa always sends a response message to the report URL, as long as this field is included in the payment request: automaticResponseUrl. If the customer closes the payment screen without returning to the webshop, however, this does generate a response that is sent to the automaticResponseUrl. To be sure that the webshop always receives a response message, we recommend including both response URLs in the payment request.

Read more about coding and implementing the payment requests in chapter 5. Read more about receiving and implementing the response messages in chapter 6.

Note

After an unsuccessful payment action, the customer is redirected to an error page on which he/she can click the 'Continue' button to return to the webshop. At that moment, the payment transaction is stopped. The customer returns to the webshop, and there can select 'pay' again to potentially choose an alternative payment method.

4. MESSAGE PROTOCOL

All messages between the webshop and the Rabo OmniKassa server (payment requests and response messages) are mandatorily composed of three POST fields. When coding the payment request and the response message, always use the following three fields.

POST field	Description
1. Data	Contains all the transaction information collected in a single string.
2. InterfaceVersion	The version of the Rabo OmniKassa connector interface.
3. Seal	Used to validate the integrity of the data. Computed from the Data field and secret key.

4.1. Data field syntax

The Data field value is composed in a single string according to the following system:

<field name>=<value name>|<field name>=<value name>|<field name>=<value name>…

All the fields needed for the transaction must be put in the string. The order of the fields does not matter. Every 'field/value' pair must be separated by | (pipe character).
Read more about what transaction information you can include in the Data field in chapter 5, 'Payment request'.

Example of the Data field in a payment request:

amount=55|currencyCode=978|merchantId=011223744550001|normalReturnUrl=http://www.normalreturnurl.nl|automaticResponseUrl=http://www.automaticresponseurl.nl|transactionReference=534654|orderId=201208345|keyVersion=1

4.2. InterfaceVersion field syntax

This field defines the version of the connection with the Rabo OmniKassa connector.
The current version of the Rabo OmniKassa redirect connector gateway is: **HP_1.0**

The value of the InterfaceVersion field is:
value="HP_1.0"

4.3. Seal field syntax

To prevent messages exchanged between the webshop and the Rabo OmniKassa server from being altered, all messages are securely encoded using the Seal field. The Seal field enables authentication of sender and receiver, because both share the same secret key. This prevents messages from being surreptitiously altered.

The value of the Seal field is built by appending the secret key to the value of the Data field. The bytes of the result are then retrieved as UTF-8 and encrypted with algorithm SHA256. The encryption algorithm (SHA256) produces a result that cannot be unencrypted. The result must be defined in the Seal POST field in hexadecimal.

The value of the Seal field is:
value=SHA256(UTF-8(Data+secretKey))

The value of the Seal field can only be derived with the Rabo OmniKassa secret key. The secret key can be found on the Rabo OmniKassa Downloadsite:
https://download.omnikassa.rabobank.nl

Numeric example to calculate the Seal field value with content of the Data field and the secret key:
SHA256(amount=55|currencyCode=978|merchantId=011223744550001|normalReturnUrl=http://www.normalreturnurl.nl|automaticResponseUrl=http://www.automaticresponseurl.nl|transactionReference=534654|orderId=201208345|keyVersion=1MijnGeheimeSleutel)

Deze voorberekening resulteert in Seal (sha256):
3662d30a179a1186066a109370054a0d3a4ad4e8983b32136c7070fd6a805ad3

You receive the logon information for the Downloadsite after signing the Rabo OmniKassa contract. For more information about the Downloadsite and using the secret keys, consult chapter 9 of this guide and the Downloadsite user guide.
Until you have access to your secret key, you can use the test webshop secret key. Read more about integrating your webshop with the Rabo OmniKassa test environment in chapter 7.

If you know or suspect that the security of your secret key has been compromised, contact the Support Team Rabo OmniKassa immediately. The team is available by phone on +31 30 7122117 (Mondays through Fridays from 08.00 am to 07.30 pm).

5. PAYMENT REQUEST

In order to initiate a payment in the Rabo OmniKassa, a payment request is sent as an HTTP-POST message to the Rabo OmniKassa redirect connector gateway. This can be sent either as an HTML form or using the POST protocol. The payment request is composed in the field Data, InterfaceVersion and Seal. This chapter provides more information about the content of these fields.

For an example of how to code your payment requests, consult the example code 'PHP' or '.NET' on the Rabobank website: www.rabobank.nl/omnikassa-support under '+ Hoe integreer ik de Rabo OmniKassa in mijn webwinkel?'.
Rabo OmniKassa is not suitable for using 'i-frames' (these are web windows).
Therefore your customer must always be rerouted to the (external) payment page of Rabo OmniKassa and will not remain in your webshop environment. Following completion of the transaction, your customer will return to your webshop via the URL in the normalReturnUrl field.

5.1 Transaction details in the Data field of the payment request

The Data field in the payment request contains the transaction information in a number of subfields in the 'field/value pair' format, in any order. The most important fields are listed in the table below.
Note: field names are case sensitive and must be written exactly as indicated here.

Field name		Description	Format
currencyCode	R	Defines the currency of the transaction. See table 10.3 for the currency codes and amounts for this field.	Numeric, 3 characters.
amount	R	Total amount that the customer must pay, in cents, without decimal separator. Example: €106.55 is coded as: 10655 with currencyCode: 978. See table 10.3 for the currency codes and amounts for this field.	Numeric, max. 12 characters.
merchantId	R	Identity of the merchant/webshop. This code is provided to each webshop after the Rabo OmniKassa contract is signed. For testing purposes, use the ID of the test webshop.	Numeric, 15 characters.
orderId	A	This is an optional field that may be used to give the transaction a unique reference code.	Alphanumeric, max. 32 characters.
normalReturnUrl	R	The URL to which the customer is redirected after payment. POST data is sent to this URL to verify the transaction status (return-URL).	Alphanumeric and special characters, max. 512 characters.
automaticResponseUrl	A	The Rabo OmniKassa server calls this URL with a cronjob to notify status changes.	Alphanumeric and special characters, max. 512 characters.

transactionReference	R	Unique transaction ID used for subsequently updating the status of the order. The webshop must be able to generate a unique code for every payment request. The code is visible to the customer on the Rabo OmniKassa payment page, the account statement of the consumer and would be referenced with a refund, etc.	Alphanumeric, max. 32 characters.
keyVersion	R	Version number of the secret key. Can be found on the Rabo OmniKassa Downloadsite.	Numeric, 10 characters.

R = Required

A = Recommended to be included in the payment request for optimal reconciliation

5.2 Optional fields in the Data field of the payment request

Field name		Description	Format
customerLanguage	O	Language in which the Rabo OmniKassa payment page should be displayed. If this field is not included in the payment request, then the payment page will be displayed by default in Dutch . See table 10.4 for the language codes for this field.	CS = Czech CY = Welsh DE = German EN = English ES = Spanish FR = French NL = Dutch SK = Slovak
paymentMeanBrandList	O	List of payment methods from which the customer can choose on the Rabo OmniKassa payment page. See also table 10.5 with all payment methods. If this field is not supplied in the payment request, then by default the customer will be redirected to the Rabo OmniKassa payment page. On the payment page, the customer can choose from the payment methods offered by the Rabo OmniKassa. These are the payment methods: IDEAL, VISA, MASTERCARD, MAESTRO, V PAY and BCMC. **Exception:** the register services INCASSO (direct debit), ACCEPTGIRO (giro collection form) and REMBOURS (cash on delivery) are not displayed on the Rabo OmniKassa payment page by default. If you wish to offer these register services to the customer on the payment page, then you need to always populate the paymentMeanBrandList field with all the payment methods you wish to offer (provided these have been requested and activated): IDEAL, VISA, MASTERCARD, MAESTRO, VPAY, BCMC, INCASSO,	Brand names of payment methods must be in all caps, with names separated by commas. IDEAL, VISA, MASTERCARD, MAESTRO, V PAY, BCMC, INCASSO, ACCEPTGIRO, REMBOURS The order of names in this field determines the order the methods are presented to your customer!

		ACCEPTGIRO, REMBOURS. If you let the customer choose the payment method while still in your webshop, then you must populate this field of the payment request with only the selected payment method. Populating this field with only one payment method will instruct the Rabo OmniKassa to redirect the customer directly to the payment page for this payment method.	
expirationDate	O	Expiration date of the payment request.	Alphanumeric, 25 characters (ISO8601 format).
captureDay	O	The number of days after authorisation of a credit card transaction after which automatic validation of the transaction follows. [Before use read the note '**Important**' after this.]	Numeric, 2 characters.
captureMode	O	This can be used to indicate that the user of the Rabo OmniKassa dashboard must manually validate credit card transactions after the automatic authorisation of this transaction. (This is in contrast to the standard credit card transaction processing procedure, in which validation is automatic after authorisation.) [Before use read the note '**Important**' after this.]	Use VALIDATION to activate captureMode. Format is alphanumeric, 20 characters (ISO8601 format).

O = Optional

Important:
If you use either one of the two options 'captureDay' and 'captureMode', be sure you are not validating a credit card transaction more than 6 days after authorisation. After that time, the authorisation is no longer valid and you run the risk that the card issuer may reject the transaction.

5.3 Example payment request

A payment request to the Rabo OmniKassa server might look like this:

```
<form method="post" action="[test/live url]">
      <input type="hidden" name="Data" value="[key=value|key=value|key=value]">
      <input type="hidden" name="InterfaceVersion" value="HP_1.0">
      <input type="hidden" name="Seal" value="[SHA256(Data + Secret Key)]">
</form>
```

Explanation of fields

Action URL	To start a payment request in the test environment, the POST data is sent to: https://payment-webinit.simu.omnikassa.rabobank.nl/paymentServlet For a payment request in the production environment, the POST data is sent to: https://payment-webinit.omnikassa.rabobank.nl/paymentServlet
Data	This field contains information about the transaction.
InterfaceVersion	The version of the Rabo OmniKassa protocol. Current version is: HP_1.0
Seal	Contains the result of SHA256(UTF8([Data] + [Secret Key])) You can find your Rabo OmniKassa secret key on the Rabo OmniKassa Downloadsite:

Example of the Data field in a payment request:

amount=55|currencyCode=978|merchantId=002020000000001|normalReturnUrl=http://www.normalreturnurl.nl|
automaticResponseUrl=http://www.autoresponse.nl|transactionReference=534654|orderId=201208345|keyVersion=1

Example of the Seal field in a payment request:

$sSecretKey = '002020000000001_KEY1';

$sData =
'amount=55|currencyCode=978|merchantId=002020000000001|normalReturnUrl=http://www.normalreturnurl.nl|
automaticResponseUrl=http://www.autoresponse.nl|transactionReference=534654|orderId=201208345|keyVersion=1' ;

$sSeal = hash('sha256', utf8_encode($sData . $sSecretKey));

// $sSeal now contains: eb9c2f480e2beaa4c4c81a8293256897b6bc0de4af3947d656e4ffa51b24e117

6. RESPONSE MESSAGE

The Rabo OmniKassa server sends response messages to the URLs defined in the payment request. The response message contains information on the status of the payment. The webshop can then further process the transaction based on this message. The response message is sent as an HTTP-POST message. By default, the Rabo OmniKassa sends a response message to the URL specified in the normalReturnUrl field (return-URL). As an option, a second response message can be sent automatically to the URL in the field automaticResponseUrl (report-URL). If the customer's browser closes during the payment process, the return-URL is not called. Likewise, a status change of a transaction (for example, a change in status from 'open' to 'successful' will not be forwarded to the return- URL. To ensure that a response message with the latest status is always received, you are advised to include both the return-URL and the report-URL in the payment request. The webshop must be able to process the status of the response message through either URL independently, without the response message being processed twice.

6.1 Manual response messages (return-URL)

After the customer has completed the payment, he/she can click the 'Continue' button on the payment page to return to the webshop The Rabo OmniKassa server then redirects the customer to the webshop (the URL specified in the normalReturnUrl field in the payment request).
The webshop receives the response message from the Rabo OmniKassa at this URL at the same time. If the customer closes his/her browser immediately without returning to the webshop, the Rabo OmniKassa cannot send back a response message to the webshop. This is why the manual response message alone cannot be relied on as a signal of completion of the payment request.

6.2 Automatic response messages (report-URL).

As an option, the Rabo OmniKassa can be configured to send a response message directly to the webshop. This allows the webshop to receive the current status, to allow the order to be processed automatically. In order to receive an automatic response message, the field automaticResponseUrl must be supplied with the payment request. Due to the uncertainty on the receipt of a manual response message, we recommend that the automatic response message be configured as standard. This gives the webshop the required information about the payment. Keep in mind that some transactions may initially be assigned a status of 'open'. If this status is later updated to 'successful' or 'stopped', the Rabo OmniKassa server calls the report-URL again with the new status. This call runs as follows: every five minutes in the first hour after the transaction moment, every hour for the rest of the transaction day, once a day for the next four days. The manual and automatic response messages sent from the Rabo OmniKassa server are identical in structure. The content may vary depending on the status of the payment request.

6.3 Transaction data in the Data field of the response message

Field name		Description	Format
amount		As provided in the payment request field.	
currencyCode		As provided in the payment request field.	
merchantId		As provided in the payment request field.	
transactionReference	R	As provided in the payment request field. This unique ID allows the order to be retrieved by a search in the webshop.	
keyVersion		As provided in the payment request field.	
orderId		As provided in the payment request field.	
responseCode	R	The status of the transaction. A numerical code is returned. For example: 00 'successful' 17 'cancelled' 60 'awaiting status report' 97 'expired' There are a number of additional codes that indicate a negative result.	Numeric, 2 characters. See lists with response codes in the following paragraphs: 10.6.1 MasterCard/Maestro, 10.6.2 VISA/V PAY, 10.6.3 Bancontact/MisterCash, 10.6.4 iDEAL.
transactionDateTime		Time at which the payment is sent to the acquirer or the moment at which the response code is created on the Rabo OmniKassa server.	Alphanumeric string, ISO8601 format.
authorisationId*		Identifier of the authorisation provided by the acquirer. Configured by the merchant/webshop for manual authorisation.	Alphanumeric, 16 characters.
paymentMeanBrand*		Brand name of payment method the customer has selected.	See list in paragraph: 10.5.
captureDay		The number of days after authorisation of a credit card transaction after which automatic validation of the transaction follows.	Numeric, 2 characters.
captureMode		This can be used to indicate that the user of the Rabo OmniKassa dashboard must manually validate credit card transactions after the automatic authorisation of this transaction. (This is in contrast to the standard credit card transaction processing procedure, in which validation is automatic after authorisation.)	AUTHOR_CAPTURE is displayed. Format is alphanumeric, 20 characters (ISO8601 format).

Field name		Description	Format
maskedPan*		Hidden Primary Account Number.	nnnnnn.nnnn (n is a number between 0 and 9).

R = the webshop must be capable of processing at least these fields in a response message

* these fields are supplied if available, depending on the status of the transaction and the payment method selected.

6.4 Example of a response message

The Rabo OmniKassa server response message might look like this:

```
<form method="post" action="[test/live url]">
      <input type="hidden" name="Data" value="[key=value|key=value|key=value]">
      <input type="hidden" name="InterfaceVersion" value="HP_1.0">
      <input type="hidden" name="Seal" value="[SHA256(Data + Secret Key)]">
</form>
```

Always check and make sure that the value in the response message in the Data field has not been manipulated.
Do this by checking the value of the Seal field against your own calculation of the value.

Sample verification of Seal field value

```
$sSecretKey = '002020000000001_KEY1';

$sHash = hash('sha256', utf8_encode($_POST['Data'] . $sSecretKey));

if(strcmp($sHash, $_POST['Seal']) === 0) // Valid seal

{

    // Data has NOT been manipulated!

}

else // Invalid seal

{

    // Data HAS been manipulated!

}
```

For an example of how to code your response messages, consult the ‘return’ and ‘report’ example code on the Rabobank website. These example codes are provided in the example codes 'PHP’ or ‘.NET’ on the Rabobank website: www.rabobank.nl/omnikassa-support under ‘+Rabo OmniKassa integreren’.

7. TESTING IN THE RABO OMNIKASSA TEST ENVIRONMENT

Before you take the Rabo OmniKassa into production, we recommend that you first integrate the Rabo OmniKassa with the test environment. This allows you to test payment requests from your webshop in the Rabo OmniKassa while you wait for your login data for the Rabo OmniKassa Downloadsite. You can test with the payment methods iDEAL, VISA, MasterCard and Maestro, and with the register services Acceptgiro (giro collection form), Incasso (direct debit) and rembours (cash on delivery). It is not possible and necessary to test with Bancontact/Mister Cash and V PAY. A succesfull test with the payment methods iDEAL and Maestro will lead to the same result.

To integrate with the test environment, use the simulation URL, the test merchant ID and the general secret key for the test webshop. If you try to use your own merchant ID in the test environment, you will receive an error message.
To integrate the webshop with the Rabo OmniKassa test environment, use the following data for the test webshop:

Simulation URL connector	https://payment-webinit.simu.omnikassa.rabobank.nl/paymentServlet
merchantId	002020000000001
secretKey	002020000000001_KEY1
keyVersion	1

Note: a payment request in the test environment requires a unique transaction reference code

A payment request must always have a unique transaction reference in the transactionReference field. As soon as you have received the log-in details from the Downloadsite, your own webshop ID will be available and you should be able to create a unique transaction reference code by default. In a test environment, however, an invoice number in combination with the test merchant ID may not be unique for the Rabo OmniKassa server.
For the test transactions, you must incorporate a unique transaction reference code in the payment requests. Until you have your own merchant ID, you need to use another number for this purpose, such as your Chamber of Commerce number, followed by a code for your webshop that you pick (if you have more than one webshop) and any reference of your choice.
*Example: your Chamber of Commerce number is **12345678**, the webshop code is **01** and the invoice number in your webshop package is **1**. This results in the transaction reference number **12345678011**.*
You can also use the 'settings' example code on the Rabobank site for configuring your Rabo OmniKassa. This example code is provided in the example codes 'PHP' or '.NET' on the Rabobank website: www.rabobank.nl/omnikassa-support under '+Rabo OmniKassa integreren'.

7.1 Testing iDEAL transactions

When you select iDEAL, you are redirected to the iDEAL test server, which simulates an iDEAL transaction with the amount of the test transaction. For the purposes of this test transaction, it does not matter which bank you select in the iDEAL payment screen. You are then redirected back to the Rabo OmniKassa server, which displays a message showing the results of the transaction.

iDEAL simulation lines:

Transaction amount	iDEAL response
2€	Transaction cancelled
3€	Transaction expired
4€	Transaction opened
5€	Transaction failure
Other cases	Transaction success

7.2 Testing card transactions MasterCard, VISA and Maestro,

When you select MasterCard, VISA or Maestro as payment method, you are redirected to the Rabo OmniKassa server for simulating credit card transactions.

Simulation lines for MasterCard, VISA and Maestro

Card type	Card prefix

VISA	410000
MASTERCARD	510000
MAESTRO	500000

- The card payment method is defined by the first six characters (card prefix). The length of the PAN (Primary Account Number) must be between 16 and 19 characters.
- Choose for expiry date a month/year in the future.
- You can simulate all supported response codes for card transactions by changing the last two characters of each. The length of the security code to be used must be 3 or 4 characters. The last three figures of the Card prefix (000) will do.

  Example: by using card number 4100000000000005, you will simulate a VISA card payment; this payment will be refused with the response code '05 – authorization refused'.

7.3 Testing Bancontact- and V PAY transactions

It is not possible and necessary to test with Bancontact/Mister Cash and V PAY. A succesfull test with the payment methods iDEAL (in stead of Bancontact) and Maestro (in place of V PAY) will lead to the same result. This is because the responscodes are equal.

7.4 Testing ACCEPTGIRO/INCASSO/REMBOURS transactions

When you select any of these register services, you are redirected to the appropriate payment page. The only button available on this payment page will be 'Continue'.
As soon as you click this button, you will be sent to the URL in the normalReturnUrl (return-URL) field.

The Rabo OmniKassa cannot give a status report, because these payments are processed outside the Rabo OmniKassa. This is why the response message for a register service will be 60 (awaiting status report) or 97 (expired).

Based on the response message received, the webshop can take the appropriate further action, whether that action is to send a giro collection form, perform a direct debit of the customer's bank account or send the order cash on delivery.

8. ERROR MESSAGES

8.1 Payment request error messages

When the payment request is received by the Rabo OmniKassa server, the values of the fields supplied are checked. This may result in an error message. This chapter presents a list of the error messages, with an explanation of the potential cause of the error and how to resolve it.

Important:
The error message is only displayed in the test environment. In the production environment, the customer only sees a simple error page with a generic response:
'An error has occurred. Please contact your merchant.'.

Error message	Cause	Solution
Invalid POST field: <field name>	The POST request contains an unknown field.	Check the available POST fields in the integration guide.
Missing mandatory POST field: <field name>	The mandatory POST field <field name> is missing in the POST request.	Check the mandatory POST fields in the integration guide.
Unknown interface version: <version>	The value <version> of the POST field InterfaceVersion is unknown.	Check available interface versions.
Invalid keyword: <param name>=<param value>	The request contains an unexpected parameter.	Check the payment request parameters.
Invalid parameter size: <param name>=<param value>	Value of parameter <param name> does not have the correct size.	Check the size of the parameter in the payment request.
Invalid parameter value: <param name>=<param value>	Value of parameter <param name> is not in correct format.	Check the format of the parameter.
Missing mandatory parameter: <param name>	The mandatory parameter <param name> is missing in the payment request.	Check the mandatory payment request parameters.
Unknown key version: <version>	The value <version> of the parameter keyVersion is unknown.	Check the key version in the Rabo OmniKassa dashboard.
Unknown merchant ID: <ID>	The value for merchantId is not found in the database.	Check the merchantId.
Invalid seal	The payment request seal check failed due to a miscomputed value in the payment request or a modification of one or more parameters.	Check the rules for computing the seal.

Transaction already processed: <transaction reference>	The Rabo OmniKassa server has already received and processed a payment request with the same value for transactionReference.	Ensure that the transaction reference is always unique. This also applies for test transactions.
Other messages		Contact the Support Team Rabo OmniKassa.

8.2 Response message error messages

If you have problems receiving response messages or processing the messages in your webshop, you can check the following:

- Check whether the right URLs are being supplied with the payment request in the fields <<normalReturnUrl>> and <<automaticResponseUrl>>.
- Check in the payment request whether the format of the URLs is valid.
- Check whether the response URLs are accessible from an external internet connection. Any access control (login/password or IP filter) or firewall may be blocking access to your server.
- Hits to URLs for response messages should be appearing in your server's access log (hit history).
- If you are using a nonstandard port, it must be within the range 80 to 9999.
- You cannot add context parameters to the response URLs. Instead, use the unique transaction reference in the payment request field transactionReference.
  You can also use the orderID field, which is likewise supplied with the parameters of the response message.
- If you receive the error 'unknown merchantID', the Rabo OmniKassa server cannot seal the response message because the secret key used for the webshop cannot be retrieved. In this case, the Rabo OmniKassa server will send a response message without the Seal field. To resolve this, check the merchant ID in the payment request.

8.3 Support Team Rabo OmniKassa

You can also contact the Support Team Rabo OmniKassa with any questions or issues by phone on +31 30 7122117. (Mondays through Fridays from 08.00 am to 07.30 pm). The team can also be contacted by e-mail at: contact@omnikassa.rabobank.nl.

9. GOING LIVE WITH THE RABO OMNIKASSA (PRODUCTION ENVIRONMENT)

When you are ready to go live with the Rabo OmniKassa and allow your customers to make payments through it, you must take the Rabo OmniKassa into the production environment. This requires your own merchant ID and your own secret key with corresponding version number. You can find this information on the Rabo OmniKassa Downloadsite:
https://download.omnikassa.rabobank.nl

To access the Downloadsite you need a username and password.
After the Rabo OmniKassa contract is signed and approved, the technical contact person will receive the username for the Downloadsite via e-mail. The password for the Downloadsite will be sent separately by mail to the requester of the contract, to the attention of the technical contact person. For more information about the Downloadsite, see the Rabo OmniKassa Downloadsite User Guide. This guide can be found on the Rabobank website: www.rabobank.nl/omnikassa-support under '+Downloadsite Rabo OmniKassa '.

At the same time, the requester will receive two e-mails providing him with the log-in information he needs to use the Dashboard: https://dashboard.omnikassa.rabobank.nl/. One with the username and one with a link enabling him to set his own password. The dashboard lets you access the Rabo OmniKassa transactions. For more information, see the user guide for the Rabo OmniKassa dashboard on the Rabobank web site: www.rabobank.nl/omnikassa-support under '+Downloadsite Rabo OmniKassa '.

9.1 From test environment to production environment

To integrate the webshop with the Rabo OmniKassa, change the URL of the test environment to the URL of the production environment: https://payment-webinit.omnikassa.rabobank.nl/paymentServlet

You must also change the test webshop details to your own identification details:

1. your merchant ID (merchantId)
2. your own secret key (secretKey)*
3. the version number of your secret key (keyVersion)

URL redirect connector	https://payment-webinit.omnikassa.rabobank.nl/paymentServlet
merchantId	<<enter your merchant ID here>>
secretKey	<<enter your secret key here>>
keyVersion	<<enter your secret key's version number here>>

After you have made the changes above, your Rabo OmniKassa is in production.
Your customers can now pay for their purchases in your webshop using the Rabo OmniKassa.

*Please note: the secret key (secretKey) is only available on the Downloadsite for a period of 30 days after activation. After expiry of this period, you must request a new secret key via the Downloadsite.

10. APPENDICES: LIST OF FIELDS AND CODES

10.1 Key to abbreviations

The appendices contain a number of tables. The table below provides a description of the abbreviations used in the 'Format' column.

Value	Description
N	Indicates that a numerical value [0-9] is accepted.
A	Indicates that an alphabetical value [aA-zZ] is accepted.
S	Indicates that special characters are accepted.
ISO8601	Standard format for establishing 'date-time': YYYY-MM-DDThh:mm:sszzzzzz YYYY-MM-DD: year, month, day with '-' as separator T : static value indicating that a time description follows. hh:mm:ss: hours, minutes, seconds with ':' as separator zzzzzz: TimeZone in comparison to UTC, using one of the following formats: « Z » or « +hh:mm » or « -hh:mm »
url	Indicates that a URL is accepted.
listString	ANS with the following accepted special characters [_@.-+,] and [space]

10.2 Full list of fields

The table below describes all possible fields with a specification of the format.

Field name	Format	Description
amount	N12	Final amount of a transaction (debit or credit) or amount of an operation (refund, cancellation, etc.).
authorisationId	AN10	Identification of the authorisation provided by the acquirer. Sent by the merchant for manual authorisation.
automaticResponseUrl	ANS512 url	This is the address the Rabo OmniKassa server will automatically notify with the current status after a payment or process.
captureDay	N2	The number of days after authorisation of a credit card transaction after which automatic validation of the transaction follows. [Before use read the note '**Important**' after this.]
captureMode	ANS20	This can be used to indicate that the user of the Rabo OmniKassa dashboard must manually validate credit card transactions after the automatic authorisation of this transaction. (This is in contrast to the standard credit card transaction processing procedure, in which validation is automatic after authorisation.) [Before use read the note '**Important**' after this.]
currencyCode	N3	Currency of the amount. See table 10.3 for the currency codes and amounts for this field.
customerLanguage	A2	Language of the customer; used for presentation to customers on the Rabo OmniKassa payment page and other pages. See table 10.4 for the language codes for this field.
expirationdate	ANS25 ISO8601	Expiration date of the payment request (UTC timezone).
keyVersion	N10	Identifier of the merchant secret key.
maskedPan	NS11	Masked Primary Account Number. Format is nnnnnn.nnnn (n is a number between 0 and 9).
merchantId	N15	Identifier of the merchant/webshop.
normalReturnUrl	ANS512 url	The page to which the customer is redirected after payment and where the Rabo OmniKassa server sends the manual response message.

orderId	AN32	Open field that can be used to link the identification of the order in the webshop to the payment in the Rabo OmniKassa.
paymentMeanBrand	ANS20	Brand name of the payment method. See table 10.5 with all payment methods.
paymentMeanBrandList	ANS128 listString	List of payment methods from which the customer can choose, separated by a comma. If using the register services INCASSO (direct debit), ACCEPTGIRO (giro collection form) and REMBOURS (cash on delivery), these payment methods must always be included in the list. Brand names of payment methods must be entered in all caps. The order of names in this field determines the order the methods are presented to your customer. See table 10.5 with the codes and types of all payment methods.
responseCode	N2	Rabo OmniKassa response code for a payment request. See lists with all the response codes in the following paragraphs: 10.6.1 MasterCard/Maestro, 10.6.2 VISA/V PAY, 10.6.3 Bancontact/MisterCash, 10.6.4 iDEAL.
transactionDateTime	ANS25 ISO8601	If the payment is sent to the acquirer for authorisation: date/time in the Rabo OmniKassa server at which the payment is sent to the acquirer, in the merchant/webshop's time zone. Otherwise: date and time at which the Rabo OmniKassa response code is generated on the Rabo OmniKassa server.
transactionReference	AN35	Identifier of the transaction.

Important:
If you use either one of the two options ‘captureDay’ and ‘captureMode’, be sure you are not validating a credit card transaction more than 6 days after authorisation. After that time, the authorisation is no longer valid and you run the risk that the card issuer may reject the transaction.

10.3 List of currency codes and amounts

The Rabo OmniKassa supports payment in different currencies.
Note that the payment methods iDEAL and Bancontact only allow payments in euros.
The currency codes are given in ISO 4217 numeric codification.

Currency name	Currency code value	Fractional unity	Example	
			Amount	Amount field
Euro	978	2	106.55	10655
American dollar	840	2	106.55	10655
Swiss Franc	756	2	106.55	10655
Pound Sterling	826	2	106.55	10655
Canadian Dollar	124	2	106.55	10655
Japanese Yen	392	0	106	106
Australian Dollar	036	2	106.55	10655
Norwegian Crown	578	2	106.55	10655
Swedish Crown	752	2	106.55	10655
Danish Crown	208	2	106.55	10655

10.4 List of language codes

The list of language codes used (ISO 639-1 Alpha2) can be used for the language in which the payment page is displayed to customers. See paragraph 5.4 5.2 Optional fields in the Data field of the payment request (customerLanguage). The payment page will be displayed by default in the language (setting) of the browser your customer is using at that time.

Code	Language
CS	Czech
CY	Welsh
DE	German
EN	English
ES	Spanish
FR	French
NL	Dutch
SK	Slovak

10.5 List of payment methods

paymentMeanBrand
IDEAL
VISA MASTERCARD MAESTRO VPAY BCMC
INCASSO (direct debit)
ACCEPTGIRO (giro collection form)
REMBOURS (cash on delivery)

10.6 About acquiring and server response codes

The acquirer and server response codes are shown in the subwindow 'Technical details' of the Rabo OmniKassa dashboard. See for more information paragraph 3.2.2 until 3.2.4 of the User Guide Rabo OmniKassa Dashboard.
The Rabo OmniKassa server sends response messages (HTTP POST) to the URLs defined in the payment request. It will send them to the URL specified in the normalReturnUrl field (return-URL) by default. As an option, a second response message can be sent automatically to the URL in the field automaticResponseUrl (report-URL). The response message contains information on the status of the payment (one of the server response codes listed below) on the basis of which the webshop can further process the transaction. More information about response messages is provided in chapter 6 of this guide.
You will find all acquirer and server response codes for all payment means below (10.6.1-10.6.5).

10.6.1 List of acquirer and server response codes for MasterCard and Maestro

MasterCard/Maestro		Rabo OmniKassa Dashboard		
Acquirer response code	**Description**	**Server response code**	**Description**	**Status**
00	Successful approval/completion	00	Captured	Successful
00	Successful approval/completion	00	To validate	To authorize[1]
		00	Successful	To be settled[2]
01	Contact card issuer	05	Refused	Niet succesvol
02	Refer to card issuer	02	Referral	Not successful
03	Invalid merchant	03	Refused	Not successful
04	Capture card	05	Refused	Not successful
04	Lost card	05	Refused	Not successful
04	Stolen card	05	Refused	Not successful

[1] This status appears if one of the optional fields 'captureDay' and 'captureMode' is used in the Data field of the payment request in case of a MasterCard transaction and capturing/authorization is not yet done.
[2] This status indicates that a refund of a MasterCard or Maestro transaction has been initiated succesfully.

MasterCard/Maestro		Rabo OmniKassa Dashboard		
Acquirer response code	**Description**	**Server response code**	**Description**	**Status**
05	Do not honour	05	Refused	Not successful
05	Invalid/nonexistent "To Account" specified	05	Refused	Not successful
05	Invalid/nonexistent "From Account" specified	05	Refused	Not successful
05	Invalid/nonexistent specified (general)	05	Refused	Not successful
12	Invalid transaction	12	Refused	Not successful
12	Invalid Authorization Lifecycle	12	Refused	Not successful
13	Invalid amount	30	Refused	Not successful
14	Invalid card number (no such number)	14 => 75[3]	Refused	Not successful
15	Invalid Issuer	05	Refused	Not successful
25	Unable to route transaction	25	Refused	Not successful
31	Authorization System or issuer system inoperative	90	Cancelled	Not successful
51	Insufficient funds/over credit limit	05	Refused	Not successful
54	Expired card	05	Refused	Not successful

[3] After three attempts the first mentioned code changes into the last mentioned code.

MasterCard/Maestro		Rabo OmniKassa Dashboard		
Acquirer response code	**Description**	**Server response code**	**Description**	**Status**
57	Transaction not permitted to issuer/cardholder	05	Refused	Not successful
58	Transaction not permitted to acquirer/terminal	05	Refused	Not successful
61	Exceeds withdrawal amount limit	05	Refused	Not successful
61	Exceeds withdrawal count limit	05	Refused	Not successful
62	Restricted card	05	Refused	Not successful
89	Invalid PIN	89 => 75[3]	Refused	Not successful
89	Allowable number of PIN tries exceeded	89 => 75[3]	Refused	Not successful
89	Unacceptable PIN - Transaction Declined- Retry	89 => 75[3]	Refused	Not successful
94	Duplicate transmission detected	90	Cancelled	Not successful
96	Format error	30	Refused	Not successful
96	PIN validation not possible	90	Cancelled	Not successful
96	Cryptographic failure	90	Cancelled	Not successful
96	System error	90	Cancelled	Not successful

* After 3 attempts the first mentioned code changes into the last mentioned code.

10.6.2 List of acquirer and server response codes for VISA and V PAY

VISA/V PAY		Rabo OmniKassa Dashboard		
Acquirer response code	**Description**	**Server response code**	**Description**	**Status**
00	Successful approval/completion	00	Captured	Successful
00	Successful approval/completion	00	To validate	To authorize[1]
		00	Successful	To be settled[2]
03	Invalid merchant or service provider	03	Refused	Not successful
04	Retain card	05	Refused	Not successful
04	Retain card special condition (other than lost/stolen card)	05	Refused	Not successful
04	Retain card (lost card)	05	Refused	Not successful
04	Retain card (stolen card)	05	Refused	Not successful
05	Do not honour	05	Refused	Not successful
05	Invalid biller information	05	Refused	Not successful
05	PIN Change/Unblock request declined	05	Refused	Not successful
05	Unsafe PIN	05	Refused	Not successful
05	Stop Payment Order	05	Refused	Not successful

[1] This status appears if one of the optional fields 'captureDay' and 'captureMode' is used in the Data field of the payment request in case of a VISA transaction and capturing/authorization is not yet done.

[2] This status indicates that a refund of a VISA or V PAY transaction has been initiated succesfully.

VISA/V PAY		Rabo OmniKassa Dashboard		
Acquirer response code	**Description**	**Server response code**	**Description**	**Status**
05	Revocation of Authorization Order	05	Refused	Not successful
05	Revocation of All Authorization Order	05	Refused	Not successful
12	Invalid transaction	12	Refused	Not successful
12	Security violation	12	Refused	Not successful
12	Unable to locate previous message (no match on retrieval reference number)	12	Refused	Not successful
12	Previous message located for a repeat or reversal	12	Refused	Not successful
12	Transaction cannot be completed; violation of law	12	Refused	Not successful
12	Surcharge amount not permitted on Visa cards	12	Refused	Not successful
12	Cash service not available	12	Refused	Not successful
12	Cash request exceeds issuer limit	12	Refused	Not successful
13	Invalid amount	30	Refused	Not successful
14	Invalid account number (no such number)	14	Refused	Not successful

VISA/V PAY		Rabo OmniKassa Dashboard		
Acquirer response code	**Description**	**Server response code**	**Description**	**Status**
14	No checking account	14	Refused	Not successful
14	No savings account	14	Refused	Not successful
15	No such issuer	05	Refused	Not successful
25	Unable to locate record in file or account number is missing from the inquiry	25	Refused	Not successful
25	Invalid date (For use in private label card transactions and check acceptance transactions)	25	Refused	Not successful
25	Issuer or switch inoperative (STIP not applicable or available for this transaction)	25	Refused	Not successful
25	Destination cannot be found for routing	25	Refused	Not successful
33	Expired card	05	Refused	Not successful
51	Insufficient funds	05	Refused	Not successful
57	Transaction not permitted to cardholder	05	Refused	Not successful
58	Transaction not allowed at terminal	05	Refused	Not successful
61	Exceeds withdrawal amount limit (activity amount limit exceeded)	05	Refused	Not successful

VISA/V PAY		Rabo OmniKassa Dashboard		
Acquirer response code	**Description**	**Server response code**	**Description**	**Status**
61	Activity count limit exceeded	05	Refused	Not successful
62	Restricted card	05	Refused	Not successful
77	Re-enter transaction	05	Refused	Not successful
89	Incorrect PIN	89 => 75[3]	Refused	Not successful
89	Allowable number of PIN-entry tries exceeded	89 => 75[3]	Refused	Not successful
89	Incorrect CVV	89 => 75[3]	Refused	Not successful
89	Decline for CVV2 failure	89 => 75[3]	Refused	Not successful
89	Card authentication failed	89 => 75[3]	Refused	Not successful
96	Error	90	Cancelled	Not successful
96	File is temporarily unavailable	90	Cancelled	Not successful
96	PIN cryptographic error found (error found by VIC security module during PIN decryption)	90	Cancelled	Not successful
96	Unable to verify PIN	90	Cancelled	Not successful
96	System malfunction	90	Cancelled	Not successful
96	Force STIP	90	Cancelled	Not successful

[3] After 3 attempts the first mentioned code changes into the last mentioned code.

10.6.3 List of acquirer and server response codes for Bancontact

Bancontact		Rabo OmniKassa Dashboard		
Acquirer response code	**Description**	**Server response code**	**Description**	**Status**
00	Successful approval/completion	00	Captured	Successful
02	Refer to card issuer	02	Referral	Not successful
03	Invalid merchant	03	Refused	Not successful
04	Retain the Card	05	Refused	Not successful
05	Do not honour	05	Refused	Not successful
13	Invalid amount	30	Refused	Not successful
14	Invalid card number (no such number)	14 => 75[2]	Refused	Not successful
15	Card Issuer unknown	05	Refused	Not successful
25	Unable to locate record in file	25	Refused	Not successful
30	Format error	30	Refused	Not successful
31	Identifier of acquirer entity unknown	90	Refused	Not successful
33	Expiry date of the card has passed	05	Refused	Not successful
41	Card lost	05	Refused	Not successful
51	Insuffient funds or credit limit exceeded	05	Refused	Not successful

[2] After three attempts the first mentioned code changes into the last mentioned code.

Bancontact		Rabo OmniKassa Dashboard		
Acquirer response code	**Description**	**Server response code**	**Description**	**Status**
54	Expiry date of the card has passed	05	Refused	Not successful
57	Transaction not permitted to issuer/cardholder	05	Refused	Not successful
58	Transaction not permitted to acquirer/terminal	05	Refused	Not successful
61	Exceeds withdrawal amount limit	05	Refused	Not successful
62	Restricted card	05	Refused	Not successful
77	Re-enter transaction	05	Refused	Not successful
89	Allowable number of PIN tries exceeded	89 => 75[2]	Refused	Not successful
90	Unexpected responce code	90	Refused	Not successful
94	Duplicate transmission detected	90	Refused	Not successful
95	Reconcile error	90	Refused	Not successful
96	System functioning incorrectly	90	Refused	Not successful
97	Expiry of the global monitoring delay	90	Refused	Not successful
98	Unreachable server	90	Refused	Not successful

[2] After three attempts the first mentioned code changes into the last mentioned code.

10.6.4 List of acquirer and server response codes for iDEAL

iDEAL		Rabo OmniKassa Dashboard		
Acquirer response code[1]	**Description**	**Server response code**	**Description**	**Status**
01	Open	60[2]	Awaiting status report	In behandeling
03	Success	00	Captured	Successful
		00	Successful	To be settled[3]
04	Cancelled	17	Aborted	Not successful
05	Expired	97	Aborted	Not successful
06	Failure	05[4]	Error	Not successful

[1] The acquirer responsecode is not displayed in the Rabo OmniKassa Dashboard (empty field).
[2] Transaction is not yet completed; Rabo OmniKassa is waiting for final status from iDEAL.
[3] This status indicates that a refund of an iDEAL transaction has been initiated succesfully.
[4] iDEAL does not make a distinction between technical problems and functional refusal.

10.6.5 Response codes for Incasso, Acceptgiro, rembours

Due to the way the Rabo OmniKassa supports the register services Incasso (direct debit), Acceptgiro (giro collection form) and rembours (cash on delivery), there are no specific response codes for the register services.
The response message for a register service will be 60 (awaiting status report) or 97 (expired).

10.7 Explanation of fields in Excel attachment (specification) with e-mail message "Rabo OmniKassa specificatie uitbetaling" (e-Statement)

The transactions (details) of the Rabo OmniKassa payment can not only be found in the Rabo OmniKassa Dashboard, but are also reported in the Excel attachment of the e-mail message 'Rabo OmniKassa payment details'. This e-mail message (e-Statement) is sent by Rabobank to the contact person of the webshop on the day a payment is made to the webshop for one or more successful transactions.

Example of Excel attachment:

SETTLEMENT_ADDRESS	info@xxxx.xx							
SETTLEMENT_HEADER_TITLE	contractNbr	accountNbr	settlementDateTime	paymentReference	paymentSign	paymentAmount	currency	
SETTLEMENT_HEADER	20200000	123456789	2013-11-27T06:21:22+0100	1707599	+	67,66	EUR	
PAYMENT_TITLE	paymentReference	shopId	orderId	operationDateTime	paymentType	paymentMeanBrand	transactionAmount	transactionCurrency
PAYMENT	1707599	1	148	2013-11-25T11:51:38+0100	DEBIT	IDEAL	59,2	EUR
PAYMENT	1707599	1	144	2013-11-25T18:27:21+0100	DEBIT	IDEAL	8,46	EUR
SETTLEMENT_TRAILER	1707599	2						

Explanation of fields:

1. "contractNbr"

   The fixed number of the Rabo OmniKassa contract that is linked to the Rabobank business account of the web retailer concerned ('accountNbr').

   This number is the same as the value in the field 'merchantId' in the payment request for a transaction minus its 1st and 4 last positions.

2. "accountNbr"

   The Rabobank business account number to which the Rabo OmniKassa contract is linked and to which the payment will be credited.

3. "settlementDateTime"

   The date on which the successful Rabo OmniKassa transactions have been credited as a single aggregate amount (gross, without withholding charges) to the Rabobank business account ('accountNbr') of the web retailer by Rabo OmniKassa.

   That payment will be effected 2 working days after the date of the transaction ('settlementDate') for successful transactions in euros, and 4 working days after the date of the transaction for successful transactions in foreign currencies.

   A transaction date can be any calendar day of the year, from 00.00 am to 12.00 pm (i.e. 24 hrs).

The successful transactions carried out via the Rabo OmniKassa will be credited/paid as follows:

TRX-DAG	EUR-TRX	NON-EUR-TRX
MA	WO	VR
DI	DO	MA
WO	VR	DI
DO	MA	WO
VR t/m ZO	DI	DO

4. “paymentReference”

   A unique number for each payment; it has no logical structure from a web retailer’s perspective.

   This number is not the same as the values in the fields ‘transactionReference’ or ‘orderId’ in the payment request for a transaction, as a payment can consist of several transactions. The ‘paymentReference’ is also stated on the (electronic) account statement.

   Note: This reference will be unique for a period of 13 months in each instance, after which the same ‘paymentReference’ can be re-used for payments.

5. “paymentSign”

   A plus (+) or minus sign (-) indicating whether the ‘paymentAmount’ will be or has been credited or debited to the web retailer’s ‘accountNbr’.

6. “paymentAmount”

   The amount that will be or has been credited or debited to the web retailer’s ‘accountNbr’.

   It consists of the sum of the amounts of successful Rabo OmniKassa transactions minus the sum of the amounts of reversals (on the web retailer’s initiative) and of charge backs (on the credit card holder’s initiative). All amounts are gross amounts, i.e. without charges being withheld. Charges are billed separately.

7. “currency”

   The currency in which the ‘paymentAmount’ is credited or debited.

   This is not always the same as the value in the field ‘currencyCode’ in the payment request for a transaction, as a payment/direct debit is always carried out in euros. The conversion of a foreign currency transaction (if possible) is carried out automatically by the payment method, applying the current exchange rate.

8. “shopId”

   The reference (number) of the webshop to which the specification relates.

   This number is the same as the last 4 positions in the field ‘merchantId’ in the payment request for a transaction. A total of 9,999 webshops can be linked to each contract. A web retailer can conclude several contracts, but never more than one for each business account. Minimum value: 0001, maximum value: 9999.

9. “OrderId" [2]

   A variable reference that can be copied from the webshop package in the field ‘orderID’ designated for that purpose in the payment request, in order to achieve comprehensive tracking and tracing for the transaction. See also the Integration Guide Rabo OmniKassa, section 2.2 and following.

10. “operationDateTime”

    The date and time of the successful performance of the transaction by the customer/buyer/payer in Rabo OmniKassa.

    Each date and time originates from one of the transaction-processing servers that processed the transaction concerned for Rabo OmniKassa at the time concerned. All these servers are in the same time zone: CET – Central European Time.
    The designation ‘+0100’ in effect means: GMT – Greenwich Mean Time plus 1 hour (= CET).

11. “paymentType”

    A designation (DEBIT/CREDIT) of the payment method used (‘paymentMeanBrand’).

12. “paymentMeanBrand”

    A brand designation of the payment method used.

    This designation is the same as the value in the field ‘paymentMeanBrandList’ in the payment request for a transaction, unless this optional field has not been used. In that case it will refer to the payment method that the buyer has selected on the standard payment page in Rabo OmniKassa. This page shows all contracted payment methods.

13. “transactionAmount”

    The amount of the successful Rabo OmniKassa transaction concerned, without charges being withheld by Rabo OmniKassa.

    This amount is the same as the value in the field ‘amount’ in the payment request for a transaction.

    The costs vary for each payment method and are billed separately. Rabo OmniKassa credits all amounts of successful transactions in aggregated form as a single gross amount to the web retailer’s Rabobank business account (‘accountNbr’). Accordingly, there is never a discrepancy between the sum of the ‘transactionAmount’ amounts and the ‘paymentAmount’ amount.

14. “transactionCurrency”

    The currency of the transaction amount (‘transactionAmount’).

    This currency is the same as the value in the field ‘currencyCode’ in the payment request for a transaction.

    All foreign currency amounts of Rabo OmniKassa transactions are converted into euro amounts (EUR), as Rabo OmniKassa only pays amounts in euros.