

TECHNICAL SPECIFICATIONS

Web Service



Euronet Merchant Services Payment Institution Single Member S.A.
1 Sachtouri & Poseidonos Ave., 176 74 Kallithea, Athens, Greece
Authorised as a Payment Institution by the Bank of Greece under Law 4537/2018

www.epayworldwide.gr
Tel.: +30 210 38 98 954



History of Changes

Date	Version	Changes
01/07/2009	1.0	Original version
01/12/2009	1.0.1	Addition of test cases in section 7
01/02/2010	1.0.2	Change of Transaction Web Service URL (section 5)
18/10/2011	1.0.3	Acceptance of receipt registration card (section 5), acceptance of American Express cards (section 5) and addition of new test cases (section 7)
24/04/2013	1.0.4	<ul style="list-style-type: none">▪ Support of "MAESTRO" and "UNKNOWN" card type (section 5)▪ Support of various currencies apart from euro
07/08/2013	1.0.5	Addition of new test case for transactions in USD currency (test case 15 in section 7)
28/04/2014	1.0.6	<ul style="list-style-type: none">▪ Support of Discover cards▪ Addition of new test case for transactions with Discover card. (Test case 13 in section 7)
22/01/2016	1.0.7	Addition of new currencies and new Logo
01/06/2017	1.0.8	New Mastercard/Maestro logos
10/07/2019	1.0.9	<ul style="list-style-type: none">▪ Update of Section 4 due to 3D Secure version 2 support.▪ Section 5: The value of the MerchantReference parameter should now be unique/different in each call of the Transaction Web Service▪ Section 5: Addition of new parameters to the Transaction Web Service request message: <u>Request Message:</u><ul style="list-style-type: none">▪ Protocol▪ DsTransID▪ RecurringInd▪ TraceID<u>Response Message:</u><ul style="list-style-type: none">▪ TraceID▪ Update of Section 9 with Visa Secure and Mastercard IdentityCheck logos (3D Secure v2)
08/02/2021	1.1	Section 5: Addition of a note regarding the order the parameters are sent
26/07/2021	1.1.1	Section 7: Update of test cases with new cards
16/03/2022	2.0	Service rebranding to epay e Commerce



Contents

1.	Introduction	2
2.	General Architecture	4
3.	Details for the Creation of a Test Account	5
4.	Strong Customer Authentication ("3D Secure")	6
5.	epay eCommerce Transaction Web Service	8
6.	Merchant Application Action Flow	25
7.	Transaction Web Service Test Cases	29
8.	Security Requirements	46
9.	Use of Icons	47
10.	Tips	49
11.	Implementation Checklist	51
	Annex 1	53
	Annex 2	59
	Glossary	61



1. Introduction

The “**Web Service**” solution of epay eCommerce Service is used for merchant system online communication with epay eCommerce (server-to-server communication) in order to enable card transactions to be executed.

The transaction data are submitted to epay eCommerce using a SOAP Web Service (“**Transaction Web Service**”).

Particularly in the case of online transactions through a website, the “Strong Customer Authentication” process (“**3D Secure**” protocol, “Visa Secure” and “Mastercard Identity Check” services offered by Visa and Mastercard respectively) described in a later section is executed first.

The cards supported by epay eCommerce are the following:

- Visa and Mastercard credit cards issued by any Bank
- Visa and Mastercard debit cards issued by any Bank
- Maestro debit cards (only if the “3D Secure process” is applied)
- Visa and Mastercard prepaid cards issued by any Bank

Besides, if Diners/Discover or American Express cards are included in the collaboration with a merchant, then they are also eligible.



Attention!

To support Diners/Discover or American Express cards, the merchant should first contact Euronet Merchant Services in order to be informed about the necessary business process.

In the sections below, detailed information is provided on the following:

- **Section 2 → General Architecture:**
Outline of the «Web Service» solution overall structure.
- **Section 3 → Details on the creation of a Test Account:**
The details required to be submitted to Euronet Merchant Services so as to create a *test account* to perform test transactions.
- **Section 4 → Strong Customer Authentication (“3D Secure”):**
Reference to the Strong Customer Authentication to be performed as part of each online transaction through a website carried out by the card holder.
- **Section 5 → epay eCommerce Transaction Web Service:**
Description of the “Transaction Web Service” parameters used to submit a transaction’s data to epay eCommerce.

- **Section 6 → Merchant Application Action Flow:**
Chart illustration of the algorithm that should be implemented by the merchant application so that a transaction may be executed.
- **Section 7 → Transaction Web service Test Cases:**
Description of the test cases to be performed in the framework of test transactions using the "Transaction Web Service".
- **Section 8 → Use of icons:**
It concerns systems submitting transactions via a site. Included here is the material about the mandatory and optional icons to be posted on the site.
- **Section 9 → Tips:**
Tips and remarks about key points to consider.
- **Section 10 → Implementation Checklist:**
A list of actions to be performed by the Technical Manager, to conclude the collaboration with the merchant.

2. General Architecture

The chart below illustrates the general architecture of the “Web Service” solution for online transactions performed by merchant sites.

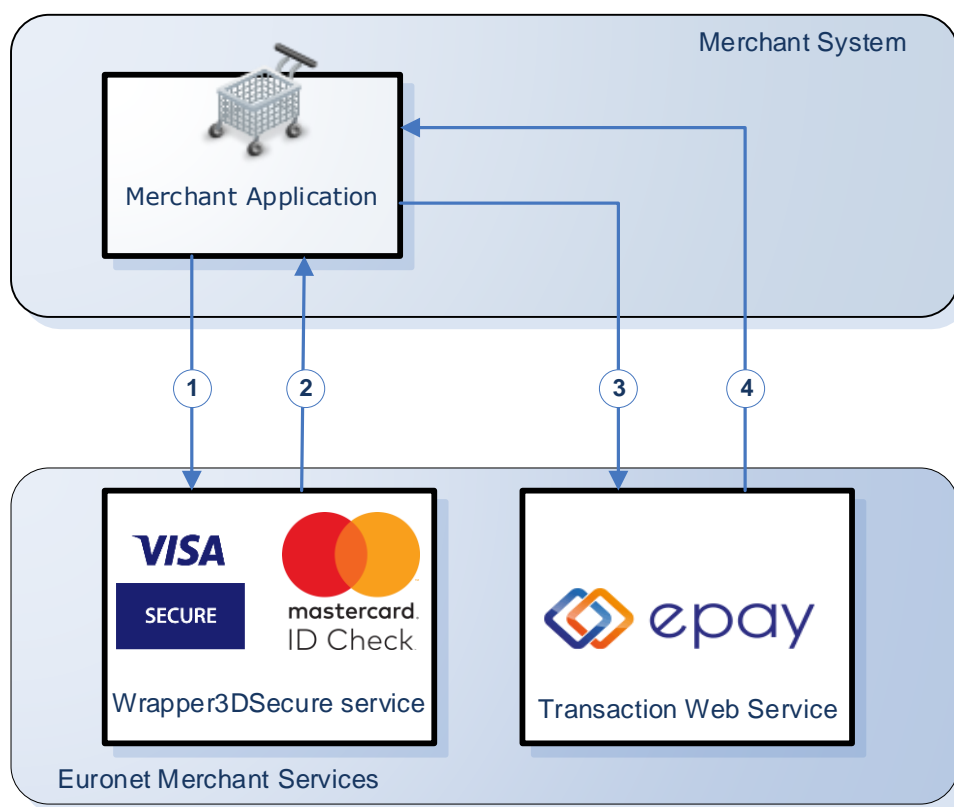


Diagram1: General Architecture

In order for a Visa, Mastercard or Maestro card transaction to be carried out, the merchant’s system initially performs the “**strong customer authentication**” process (“**3D Secure**” protocol, “Visa Secure” and “Mastercard Identity Check” services by Visa and Mastercard respectively). Technical information on this process is included in a separate documentation by Euronet Merchant Services (see also section 4). Where the card holder authentication outcome allows the transaction to be carried out, the Euronet Merchant Services “**Transaction Web Service**” is subsequently used (steps 3, 4) in order to send the transaction details to epay eCommerce, process the transaction and send the response to the merchant (see section 5).

In the case of transactions from systems where card details are provided by the card holder to a third party (e.g. to a Call Center agent – MOTO transactions), the 3D Secure process (steps 1 and 2) is not carried out in advance and transaction details are directly sent to epay eCommerce (steps 3, 4 – see section 5).



3. Details for the Creation of a Test Account

The information to be sent to Euronet Merchant Services in order for the required technical information to be provided (*test account*) for test transactions is as follows (all is required):

- **Details of the technical manager**
 - Name of the technical manager
 - Telephone of the technical manager
 - Email address of the technical manager
 - Company where the technical manager is employed
- **Details of the merchant owning the system:**
 - Distinctive title of the merchant owning the system
 - Tax Registration Number of the merchant owning the system
 - Domain name of the merchant live site (for transactions via a site)
- **Technical data:**
 - **IP address**: The IP address of the server from which the Euronet Merchant Services "Transaction Web Service" will be called.
 - **Installment support**: Reference to whether installments are to be used in test transactions or not.
 - **Receipt card support**: Reference to whether a receipt card is to be used in test transactions.

The *test account* details provided by Euronet Merchant Services after the information is sent, include the following, which are used both in the 3D Secure process (for eCommerce transactions where the "Wrapper3DSecure service" is called) and in the transaction to be sent ("Transaction Web Service" call):

- AcquirerID
- MerchantID
- PosID
- User
- Password
- ChannelType

Information on the usefulness of the details is provided in the following sections.



4. Strong Customer Authentication ("3D Secure")

Sale or preauthorization eCommerce transactions (see transaction types in section 5) initiated by the card holder using a Visa, Mastercard or Maestro card have to be preceded by strong customer authentication ("3D Secure" protocol, "Visa Secure" and "Mastercard Identity Check" by Visa and Mastercard respectively). The technical specifications of this process are included in a separate document.



Attention!

- Card holder authentication refers to Visa, Mastercard and Maestro card transactions.
- The amount, currency and MerchantReference used in the 3D Secure process (PurchAmount, Exponent, Currency, MerchantReference parameters of the "Wrapper3DSecure service") should match those to be used in the Transaction Web Service (Amount, CurrencyCode, MerchantReference parameters).
- The **MerchantReference** (reference code of the transaction originating in the merchant's system) should have a **unique/different value for each transaction**. This means that if a transaction fails and a new 3D Secure process is initiated for a new attempt, the MerchantReference (both in the Wrapper3DSecure service and in the Transaction Web Service) should have a different value (compared to the previous attempt).
- Only **sale** or **preauthorization** transactions are preceded by the authentication process. It is not applied in any other transactions (e.g. refunds, settlements, etc.) (For transaction types, see section 5.)
- In transactions carried out through systems where the holder provides their card details to a third person (e.g. a Call Center agent) no card holder authentication is required.

Upon completion of the 3D Secure process, values are returned to the parameters below which should be transferred to the corresponding fields in the Transaction Web Service call:

Parameter from Wrapper3DSecure	Parameter to Transaction Web Service
Eci (*)	Eci
Cavv	Cavv
Xid	Xid
Protocol	Protocol
DsTransID	DsTransID

(*) If the Wrapper3DSecure service call does not return a value to ECI (e.g. in the case of a technical issue) and the merchant decides to send the transaction, the Transaction Web Service call should include the following default values in ECI:

- **In the case of a Visa card: ECI=07**
- **In the case of a Mastercard or a Maestro card: ECI=00**



5. epay eCommerce Transaction Web Service

epay eCommerce Transaction Web service" is a SOAP Web Service used in order for the details of a transaction to be sent to the epay eCommerce .The URL is:




<https://paycenter.piraeusbank.gr/services/paymentgateway.asmx>







Attention!




- The response timeout is 60 sec.
- The Web Service call should be made through the Server. **No scrip-based cross-origi HTTP requests are allowed.**


Below is a list of the information required to call the "Transaction Web Service" call:




REQUEST PARAMETERS		
Parameter name	Description	Type
AcquirerID	The acquirer id. Provided by Euronet Merchant Services.	String (max. 5 characters)
MerchantID	The merchant ID. Provided by Euronet Merchant Services.	Integer
PosID	<div>The POS ID. Provided by Euronet Merchant Services.</div> <div> Note: A NULL value may be assigned to the PosID. In such a case, the epay eCommerce shall execute the transaction with one of the available PosIDs. This logic applies where a high number of simultaneous transactions is to be sent and Euronet Merchant Services has to be informed in order to generate multiple PosIDs.</div>	Integer
User	User name. Provided by Euronet Merchant Services.	String (max. 50 characters)
Password	User password <u>encrypted using the MD5 hashing algorithm</u> . Provided by Euronet Merchant Services (in non-encrypted form).	String (max. 50 characters)
ChannelType	Terminal channel type. Provided by Euronet Merchant Services.	String (max. 11 characters)

RequestType	<p>The transaction type to be executed. Possible values:</p> <ul style="list-style-type: none"> ▪ SALE: <u>Sale</u> → A transaction to be directly cleared in the current package. ▪ AUTHORIZE: <u>Preauthorization</u> → The amount will be simply committed and later, the preauthorisation will have to be completed (through either the AdminTool or the transaction with RequestType = "SETTLE") so as to be settled. <div style="background-color: #ffffcc; padding: 10px; margin: 10px 0;"> <p> Attention! Preauthorization is available subject to conditions. Communication with and approval by the Bank is required if the merchant intends to use this transaction type.</p> </div> <ul style="list-style-type: none"> ▪ SETTLE: <u>Preauthorization settlement</u> → It concerns the completion of a preauthorization in order to settle the transaction in the current package. ▪ VOIDREQUEST: <u>Preauthorization voiding</u> → Voiding of a preauthorization which is not settled. ▪ REFUND: <u>Sale cancellation/refund</u> → Refund of a sale or preauthorization that has been settled. ▪ FOLLOW_UP: <u>Transaction follow-up</u> → The data of an executed transaction with a specific "MerchantReference" value, are returned (provided that a cancellation/refund has not been carried out for that transaction). ▪ ISAVAILABLE: It is returned if the epay eCommerce is available to receive transactions. <div style="background-color: #ffffcc; padding: 10px; margin: 10px 0;"> <p> Note: At the end of the section there is a chart showing the order in which transactions can be used.</p> </div>	String (max. 20 characters)
RequestMethod	The value "SYNCHRONOUS" should always be submitted.	String (max. 12 characters)
MerchantReference	Transaction reference code. It is generated by the merchant system and identifies uniquely each successful transaction (e.g. order number, contract number, etc.).	String (max. 50 characters)

	<ul style="list-style-type: none"> ▪ "MerchantReference" accepts max. 50 Greek and Latin uppercase and lowercase alphanumeric characters, space and the following special characters: /:_().,+ - ▪ It should have a different value in each transaction. <div>  Attention! <ul style="list-style-type: none"> ▪ If the card holder authentication process is used ("3D Secure"), the value of the "MerchantReference" parameter in sale/preauthorization transactions should be identical to the value of the corresponding parameter when the Wrapper3DSecure service is called. ▪ If an online sale/preauthorization transaction is unsuccessful and needs to be resent, the 3D Secure process should be repeated with a "MerchantReference value which should be different" from that in the previous transaction. ▪ Where a sale or preauthorization transaction has been approved, even if it has been cancelled/refunded, its "MerchantReference" cannot be used in a subsequent transaction. </div>	
TransactionReferenceID	<p>Used only in the following transactions:</p> <ul style="list-style-type: none"> ▪ Preauthorization settlement (RequestType = "SETTLE") ▪ Preauthorization voiding (RequestType = "VOIDREQUEST") ▪ Sale refund (RequestType = "REFUND") <p>It is the transaction id ("TransactionID" parameter in response message) of the transaction requested to be settled / refunded.</p> <div>  Note: <p>If refund is requested for a preauthorisation that has been settled, the "TransactionID" of the settlement (not preauthorization) is submitted to this parameter.</p> </div>	Integer


EntryType	<p>The way the card details were entered. Possible values:</p> <ul style="list-style-type: none"> ▪ KeyEntry: The card details were typed by the card holder. ▪ CardOnFile: The card details were stored and did not have to be entered by the card holder. <p>If no value is sent, KeyEntry is considered the default value.</p>	String
CurrencyCode	<p>The code of the transaction currency. It is 978 for debits in Euros.</p> <div>  Attention! <ul style="list-style-type: none"> ▪ For each different currency, Euronet Merchant Services shall provide a different MerchantID and PosID. ▪ If the card holder authentication process is used ("3D Secure"), the value of the "CurrencyCode" parameter in sale/pre-authorisation transactions should be identical to the value of the corresponding parameter (Currency) when the Wrapper3DSecure service is called. </div> <div>  Note: Supported currency codes are listed in Annex 2. </div>	Integer
Amount	<p>The transaction amount with 2 decimal digits. The following apply to the various transaction types:</p> <ul style="list-style-type: none"> ▪ Preauthorization settlement (RequestType = "SETTLE") The amount can be lower than or equal to the initial transaction amount. ▪ Preauthorization voiding (RequestType = "VOIDREQUEST"): The amount must be equal to the initial transaction amount. ▪ Sale cancellation/refund (RequestType = "REFUND") The amount can be lower than/equal to the initial transaction amount. <div>  Attention! <ul style="list-style-type: none"> ▪ If the card holder authentication process is used ("3D Secure"), the value of the "Amount" parameter in sale/preauthorization transactions should correspond to </div>	Decimal with decimal digits 2

	<p>the same amount expressed by the PurchAmount and Exponent parameters when the Wrapper3DSecure service is called.</p> <ul style="list-style-type: none"> Partial refund in installment transactions will be carried out as one-off (without installments). 	
Installments	<p>The number of transaction installments.</p> <ul style="list-style-type: none"> To support installments, the merchant must state it to Euronet Merchant Services. For non-installment transactions, the value should be 0, 1 or NULL. <p> Note: Euronet Merchant Services provides the “BIN Web Service” which can check whether or not a card supports installments without executing the transaction. In case of interest, the technical specifications should be requested from Euronet Merchant Services.</p>	Integer
ExpirePreauth	<p>Only refers to preauthorization transactions (RequestType = “AUTHORIZE”). It is the number of days within which the preauthorization may be settled.</p> <p>Maximum value: 30 days</p>	Short Integer
TipAmount	For future use. NULL or zero should be sent.	Decimal with 2 decimal digits
Bnpl	For future use. NULL should be sent.	Unsigned Byte
SessionKey	For future use. NULL should be sent.	String (max. 50 characters)
CardType	<p>The card type.</p> <p>There are two alternatives:</p> <p>1) The user is not asked to enter the type of his card. In this case, the «CardType» parameter should have the value «UNKNOWN» and epay eCommerce will decide about the card type.</p>	String (max. 20 characters)

	<p>2) The user is asked to enter the type of his card. In this case, the possible values are as follows:</p> <ul style="list-style-type: none"> ▪ VISA ▪ MasterCard ▪ Maestro: Can be used <u>only if the 3D-Secure process is applied</u> ▪ DinersClub: DinersClub or Discover card ▪ AMEX: American Express <p> Note:</p> <ul style="list-style-type: none"> ▪ To support Diners/Discover or American Express cards, the merchant should first contact Euronet Merchant Services in order to be informed about the necessary business process. ▪ Diners/Discover or American Express card transactions are sent with a <u>different MerchantID and PosID</u> compared to Visa/Mastercard/Maestro transactions and with a <u>"null" value in the "AuthInfo" element</u> (parameters Cavv, Eci, Xid, etc. are included – see below) 	
CardNumber	The transaction's card number. The maximum number of card digits is 19.	String (max. 19 numeric digits)
ExpirationMonth	The card's expiration month.	Short Integer
ExpirationYear	The card's expiration year.	Short Integer
Cvv2	<p>The card verification code (CVV2 or CVC) usually found on the back of the card.</p> <p> Note: In the case of website transactions, characters should not be visible in the CVV2 field as they are typed by the user (e.g. replaced by asterisks).</p>	String (max. 4 numeric digits)
CardHolderName	<p>The card holder's full name as printed on the card.</p> <p> Attention! The full name should be sent using uppercase Latin characters.</p>	String (max. 100 characters)
Aid	Not used, NULL should be sent.	String

		(max. 50 characters)
Emv	Not used, NULL should be sent.	String (max. 512 characters)
PinBlock	Not used, NULL should be sent.	String (max. 50 characters)
Track1	Not used, NULL should be sent.	String (max. 100 characters)
Track2	Not used, NULL should be sent.	String (37 characters)
Cavv	This refers only to online transactions through a website where a Visa, Mastercard or a Maestro card is used. It contains the value of the " Cavv " parameter returned in the 3D Secure process (see section 4).	String (max. 48 characters)
Eci	This refers only to online transactions through a website where a Visa, Mastercard or a Maestro card is used. It contains the value of the " Eci " parameter returned in the 3D Secure process (see section 4).	String (2 numeric digits)
Xid	This refers only to online transactions through a website where a Visa, Mastercard or a Maestro card is used. It contains the value of the " Xid " field returned in the 3D Secure process (see section 4).	String (max. 40 characters)
Enrolled	No value needs to be sent	String
PAResStatus	No value needs to be sent	String
SignatureVerification	No value needs to be sent	String
Protocol	This refers only to online transactions through a website where a Visa, Mastercard or a Maestro card is used and expresses the version of the 3D Secure protocol used for authentication. It contains the value of the " Protocol " field returned in the 3D Secure process (see section 4). Potential values: <ul style="list-style-type: none"> 1 (for 3D Secure version 1) 2 (for 3D Secure version 2 or EMV 3D Secure) 	String
DsTransID	This refers only to online transactions through a website where a Visa, Mastercard or a Maestro card is used. It contains the value of the " DsTransID "	String



	parameter returned in the 3D Secure process (see section 4).	
RecurringInd	<p>This is used in case the transaction involves a recurring payment, i.e. when there is an agreement between the card holder and the merchant on recurring debits (e.g. standing order). Potential values:</p> <ul style="list-style-type: none"> ▪ R: In the case of a recurring transaction executed at regular intervals ▪ C: In the case of a recurring transaction not executed at regular intervals. 	String
TraceID	In the case of recurring payments and following the second recurrence, it includes the value of the Trace ID of the first transaction, that was returned to the merchant upon the Transaction Web Service call for that first transaction.	String
TaxCardNumber	No value needs to be sent	String






Note:

- With the exception of the "CardHolderName" parameter, spaces may not be used in any of the string-type parameters.
- It is recommended to send the parameters in the order they appear in WSDL.

The parameters sent with the response are the following:

RESPONSE PARAMETERS		
Parameter name	Description	Type
RequestType	<p>The transaction type sent with the request. Possible values:</p> <ul style="list-style-type: none"> ▪ SALE: Sale ▪ AUTHORIZE: Preauthorization ▪ SETTLE: Preauthorization settlement ▪ VOIDREQUEST: Preauthorization voiding ▪ REFUND: Refund of a sale or preauthorization that has been settled ▪ FOLLOW_UP: Data of a transaction already executed with a specific "MerchantReference" (provided that a cancellation/refund has not been carried out for that transaction) ▪ ISAVAILABLE: ePay eCommerce availability check 	String (max. 20 characters)
MerchantID	Merchant id sent with the request.	Integer
PosID	POS id sent with the request.	Integer
User	User name sent with the request.	String

		(max. 50 characters)
ChannelType	Terminal channel type sent with the request.	String (max. 11 characters)
ResultCode	<p>The request result code indicating whether there was any technical problem in the transaction processing. Specifically :</p> <ul style="list-style-type: none"> ▪ Value = 0: There was no problem; the transaction was executed. <u>Then, the «StatusFlag» parameter must be checked to verify that the transaction was approved.</u> ▪ Value ≠ 0: There was a transaction data problem or a technical problem at epay eCommerce, so no transaction was executed. The «ResultDescription» parameter contains the problem description. <p>The following applies specifically to transactions where RequestType= «ISAVAILABLE»:</p> <ul style="list-style-type: none"> ▪ Value = 0: epay eCommerce may accept transactions. ▪ Value ≠ 0: epay eCommerce may not accept transactions. <p> Note: The most frequent «ResultCode» values are shown in Annex 1.</p>	Integer
ResultDescription	<p>The description corresponding to the "ResultCode" parameter value.</p> <p> Note:</p> <ul style="list-style-type: none"> ▪ This information is not recommended to be displayed to the user. ▪ If the request is rejected due to anti-fraud checks (ResultCode= 7001, see Annex 1), the «ResultDescription» parameter contains the code of the rule that was fired-up. <u>The zero value (0) means that the card number is included in a black list.</u> If special anti-fraud rules have been agreed with the merchant, Euronet Merchant Services will provide the 	String (max. 1024 characters)

	relevant rule codes that may be returned.	
SupportReferenceID	<p>Reference id of the submitted request. There is a different value per request (even if the transaction failed to be executed).</p> <p> Note: It is necessary to store the value, so as to be used as a reference in the communication with Euronet Merchant Services, as required.</p>	Long integer
StatusFlag	<p>The parameter value indicating whether the transaction was approved. Possible values:</p> <ul style="list-style-type: none"> ▪ Success: Transaction approved. ▪ Failure: Transaction not approved 	String (max. 12 characters)
ResponseCode	<p>When a transaction has been executed, it contains a response code. The response codes for approved transaction are: 00, 08, 10, 16.</p> <p> Note: The most frequent "ResponseCode" values are shown in Annex 1.</p>	String (2 characters)
ResponseDescription	<p>The description corresponding to the "ResponseCode" parameter value.</p> <p> Note: This information should not be displayed to the user.</p>	String (max. 120 characters)
TransactionID	<p>If the transaction has been executed, it contains a unique transaction id generated by the epay eCommerce.</p> <p> Note: This value is required in the "TransactionReferenceID", if the following transactions are to be used:</p> <ul style="list-style-type: none"> ▪ Preauthorisation settlement (RequestType = "SETTLE") ▪ Preauthorization voiding (RequestType = "VOIDREQUEST") ▪ Sale cancellation/refund (RequestType = "REFUND"), <p>Therefore, if the above transactions are to be used, the parameter value of the initial transaction must be stored (i.e. the preauthorization, settlement or sale "TransactionID").</p>	Integer
MerchantReference	The transaction reference submitted with the request.	String (max. 50 characters)

ApprovalCode	If a successful transaction has been executed (i.e. when ResultCode=0 and StatusFlag=Success), it takes the transaction approval code.	String (max. 6 characters)
PackageNo	If a transaction has been executed (i.e. when ResultCode=0), it takes the number of the package that includes this transaction.	Integer
RetrievalRef	If a transaction has been executed (i.e. when ResultCode=0), it takes the Retrieval Reference Number generated by the acquiring system.	String (max. 12 characters)
TransactionDateTime	If a transaction has been executed (i.e. when ResultCode = 0), the transaction execution date and time are included.	DateTime
SessionKey	For future use. NULL is sent.	String (max. 50 characters)
TransactionTraceNum	If a transaction has been executed (i.e. when ResultCode = 0), the transaction serial number is included in the package it belongs to.	Integer
TraceID	<p>Transaction reference code generated by Visa/Mastercard; it is recommended that this code be stored by the merchant's system.</p> <p><u>Usefulness in recurring transactions:</u> If the transaction is the first in a series of recurring payments preceded by the 3D Secure process, the value of this parameter should be stored so as to be included in the request (TraceID) in each subsequent recurrence (where 3D Secure is not used).</p> <p>(For transaction types SALE, AUTHORIZE, FOLLOW_UP)</p>	String (max. 50 characters)
Token	<p>Tokenized transaction card (with format 888888*****)</p> <p>(For transaction types SALE, AUTHORIZE, FOLLOW_UP)</p>	String
Masked Card	<p>The card number corresponding to the token in masked format, e.g. 411111*****1111 (namely, it includes only the first 6 and the last 4 digits, and the rest are replaced by asterisks).</p> <p>Masked Card data returned when the transaction is successful.</p> <p>(For transaction types SALE, AUTHORIZE, FOLLOW_UP)</p>	String

Card Expiration Date	<p>The expiration date of the card used in the transaction in "MM-YYYY" format, e.g. 10-2025.</p> <p>(For transaction types SALE, AUTHORIZE, FOLLOW_UP)</p>	String
-----------------------------	--	--------



Note:

- The "**SupportReferenceID**" and "**MerchantReference**" parameter values of all transactions must be stored in the merchant system and be available to the merchant responsible person(s).
- It is recommended that the "**TraceID**" parameter be returned with the response be also stored. For now, this value is useful to merchants supporting recurring transactions.
- If some of the preauthorization settlement, preauthorization voiding and/or refund transactions are used, then the "**TransactionID**" should also be stored.
- Of the remaining parameters, it is recommended to also store the "**ResultCode**", "**ResultDescription**", "**StatusFlag**", "**ResponseCode**", "**ResponseDescription**", "**ApprovalCode**", "**PackageNo**" parameter values.
- The transaction decline or technical error message ("**ResultDescription**" or "**ResponseDescription**") should not appear as such on the user page.

The following table shows the "Transaction Web Service" parameters that should be used in the request of any transaction type. In sale ("SALE") and preauthorization ("AUTHORIZE") transactions, the parameters used depend on the "ChannelType" ("3DSecure", "eCommerce", "MOTO") assigned by Euronet Merchant Services.

REQUEST PARAMETERS	SALE (SALE)		AUTHORIZE (Preauthorization)		SETTLE (Preauthorization settlement)	VOIDREQUEST (Preauthorization voiding)	REFUND (Sale cancelation/refund)	FOLLOW_UP (TRANSACTION FOLLOW UP)	ISAVAILABLE (epay eCommerce AVAILABILITY CHECK)
	3D Secure	MOTO or eCommerce	3D Secure	MOTO or eCommerce	For all ChannelType values	For all ChannelType values	For all ChannelType values	For all ChannelType values	For all ChannelType values
AcquirerID	✓	✓	✓	✓	✓	✓	✓	✓	✓
MerchantID	✓	✓	✓	✓	✓	✓	✓	✓	✓
PosID	✓	✓	✓	✓	✓	✓	✓	✓	✓
User	✓	✓	✓	✓	✓	✓	✓	✓	✓
Password	✓	✓	✓	✓	✓	✓	✓	✓	✓
ChannelType	✓	✓	✓	✓	✓	✓	✓	✓	✓
RequestType	✓	✓	✓	✓	✓	✓	✓	✓	✓
RequestMethod	✓	✓	✓	✓	✓	✓	✓	✓	✓
MerchantReference	✓	✓	✓	✓	✗	✗	✗	✓	✗
TransactionReferenceID	✗	✗	✗	✗	✓	✓	✓	✗	✗
EntryType	✓	✓	✓	✓	✗	✗	✗	✗	✗
CurrencyCode	✓	✓	✓	✓	✓	✓	✓	✗	✗
Amount	✓	✓	✓	✓	✓	✓	✓	✗	✗
Installments	(1)	(1)	(1)	(1)	✗	✗	✗	✗	✗
ExpirePreauth	✗	✗	✓	✓	✗	✗	✗	✗	✗
TipAmount	✗	✗	✗	✗	✗	✗	✗	✗	✗

Bnpl	✗	✗	✗	✗	✗	✗	✗	✗	✗
SessionKey	✗	✗	✗	✗	✗	✗	✗	✗	✗
CardType	✓	✓	✓	✓	✗	✗	✗	✗	✗
CardNumber	✓	✓	✓	✓	✗	✗	✗	✗	✗
ExpirationMonth	✓	✓	✓	✓	✗	✗	✗	✗	✗
ExpirationYear	✓	✓	✓	✓	✗	✗	✗	✗	✗
Cvv2	✓	✓	✓	✓	✗	✗	✗	✗	✗
CardHolderName	(2)	(2)	(2)	(2)	✗	✗	✗	✗	✗
Aid	✗	✗	✗	✗	✗	✗	✗	✗	✗
Emv	✗	✗	✗	✗	✗	✗	✗	✗	✗
PinBlock	✗	✗	✗	✗	✗	✗	✗	✗	✗
Track1	✗	✗	✗	✗	✗	✗	✗	✗	✗
Track2	✗	✗	✗	✗	✗	✗	✗	✗	✗
Cavv	(3)	✗	(3)	✗	✗	✗	✗	✗	✗
Eci	✓	✗	✓	✗	✗	✗	✗	✗	✗
Xid	(3)	✗	(3)	✗	✗	✗	✗	✗	✗
Enrolled	✗	✗	✗	✗	✗	✗	✗	✗	✗
PAResStatus	✗	✗	✗	✗	✗	✗	✗	✗	✗
SignatureVerification	✗	✗	✗	✗	✗	✗	✗	✗	✗
Protocol	(3)	✗	(3)	✗	✗	✗	✗	✗	✗
DsTransID	(3)	✗	(3)	✗	✗	✗	✗	✗	✗
RecurringInd	(4)	(4)	(4)	(4)	✗	✗	✗	✗	✗
TraceID	(5)	(5)	(5)	(5)	✗	✗	✗	✗	✗

TaxCardNumber	(6)	(6)	(6)	(6)	×	×	×	×	×
----------------------	-----	-----	-----	-----	---	---	---	---	---

SYMBOL EXPLANATIONS	
Symbol	Explanation
✓	A value must be submitted
×	No value must be submitted
(1)	A value is submitted in the case of a transaction involving installments
(2)	Optional information
(3)	A value is submitted depending on the outcome of the card holder authentication process ("3D Secure") – see section 4.
(4)	A value is submitted in the case of a recurring transaction.
(5)	A value is submitted after the second recurrence of a recurring transaction.
(6)	A value is submitted only if the card holder enters a receipt card number.

The following diagram shows the order in which the various transaction types may be used. The following apply, as shown in the diagram:

- A preauthorization (RequestType="AUTHORIZE"), may either be settled (RequestType="SETTLE") for an amount lower than or equal to the preauthorization amount, or voided (RequestType="VOIDREQUEST") for an amount equal to the preauthorization amount.
- A preauthorization that has been settled, may be refunded (RequestType="REFUND") for an amount lower than or equal to the preauthorization settlement amount. **Attention!** Partial refund in installment transactions will be carried out as one-off (without installments).
- A sale transaction may be refunded (RequestType="REFUND") for an amount lower than or equal to the sale amount. **Attention!** Partial refund in installment transactions will be carried out as one-off (without installments).
- A "RequestType="FOLLOW_UP" transaction may be used at any time and returns the details of a request already sent, provided no cancellation/refund has been performed.



Note:

In the following transactions, a value must be filled in the "**TransactionReferenceID**" parameter:

- Preauthorization settlement (RequestType = "SETTLE")
- Preauthorization voiding (RequestType = "VOIDREQUEST")
- Sale or settlement cancellation/refund (RequestType = "REFUND")

In any case the transaction id ("TransactionID" parameter in response message) of the preceding transaction is submitted. For example, for the preauthorization settlement, the preauthorization "TransactionID" is used, while for the settlement refund, the settlement "TransactionID" is used.

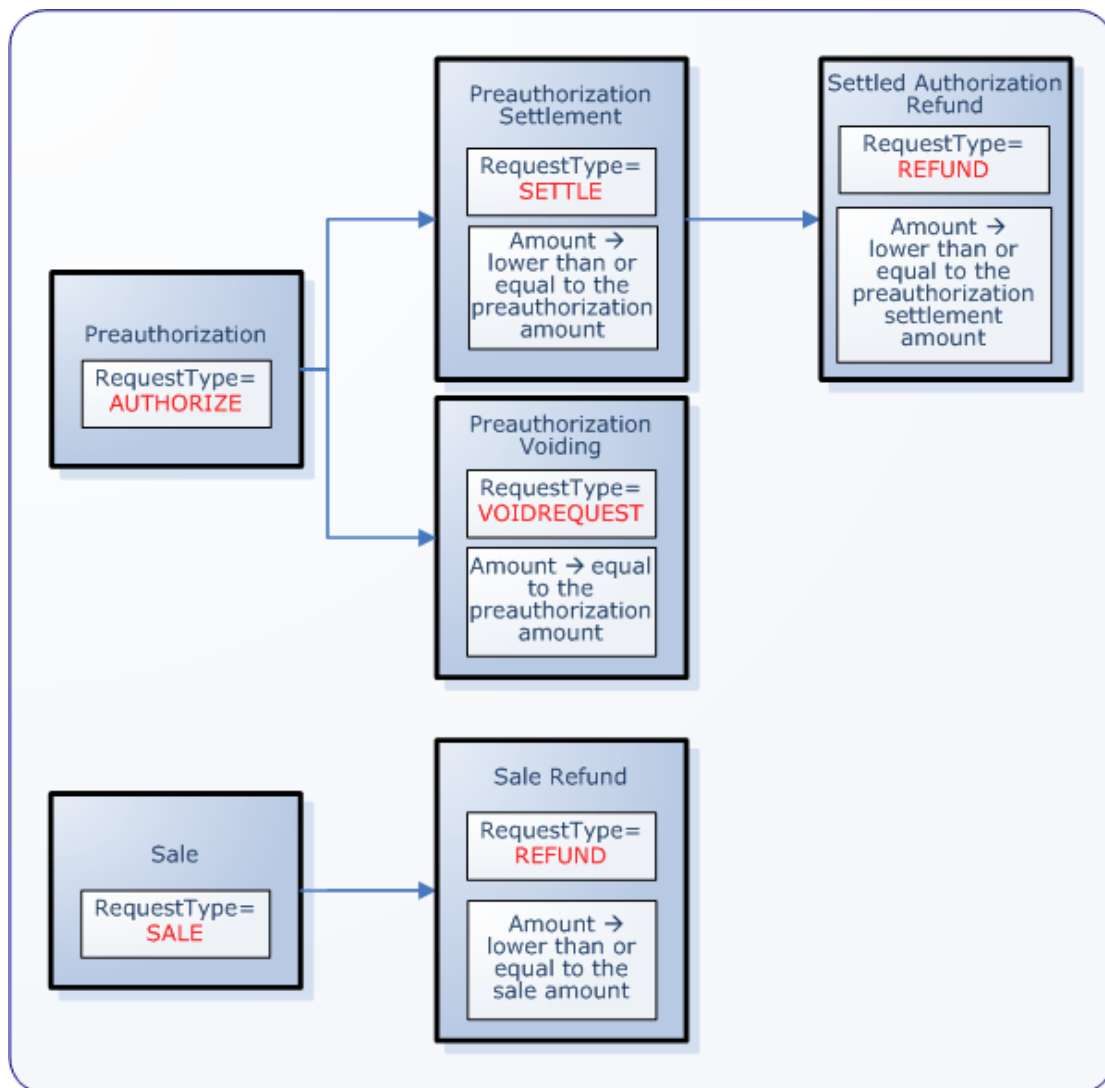


Chart 2: Transaction sequence



6. Merchant Application Action Flow

Following an analysis of all individual process modules to be implemented (strong customer authentication and dispatch of transaction to the epay eCommerce), the diagram shows the flow of actions to be performed by the merchant's application in collaboration with epay eCommerce as required for a transaction execution.

It is important to use the proposed algorithm, so that all cases are taken into account and no problems occur during the application productive operation.

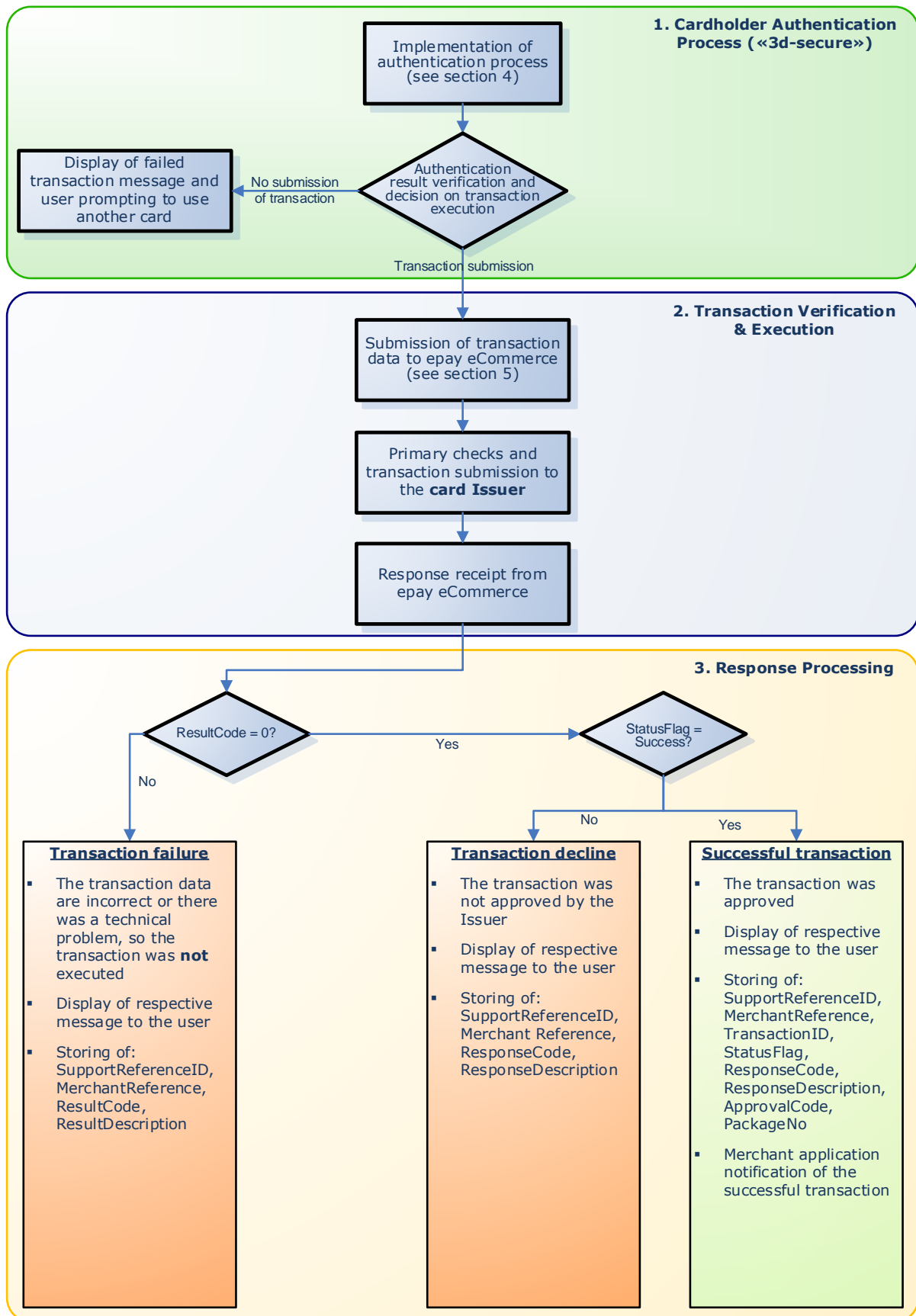


Chart2: **Merchant application actions**

As shown in the chart, the overall process consists of 3 phases:

1. Strong Customer Authentication ("3D Secure") process

In the case of sale or preauthorization transaction executed via a website (online transactions) using a Visa, Mastercard or Maestro card, the strong customer authentication process is carried out (see section 4). Depending on the authentication outcome, the merchant's application determines whether to submit the transaction to epay eCommerce or not.



Attention!

The authentication process is only used for online **sale** or **preauthorization** transactions with Visa, Mastercard or Maestro cards.

2. Transaction Verification & Execution

The merchant system uses the «Transaction Web Service» to submit the transaction data to epay eCommerce (see section 5). The epay eCommerce runs primary checks to the submitted data and, if correct, the transaction data are submitted to the card Issuer. Then, a response is sent to the merchant system.

3. Response Processing

The merchant system must check the response parameters, to verify whether the transaction is successful. Specifically:

- **If ResultCode ≠ «0»**, then there was either a problem with transaction data, or some **technical problem**, thus the transaction was not executed. A problem description is contained in the «ResultDescription» parameter (not to be displayed on the user page). If necessary, the details of the technical problem (SupportReferenceID, MerchantReference, ResultCode, ResultDescription) are stored in the merchant system.
- **If ResultCode = «0»:**
 - If StatusFlag ≠ «Success», then the transaction was executed but not **approved by the card Issuer**. If necessary, the details of the unsuccessful transaction (SupportReferenceID, MerchantReference, ResponseCode, ResponseDescription) are stored in the merchant system.

- If `StatusFlag = «Success»`, then **the transaction was successful**, thus the transaction information, such as `SupportReferenceID`, `MerchantReference`, `TransactionID`, `StatusFlag`, `ResponseCode`, `ResponseDescription`, `ApprovalCode`, `PackageNo` should be stored and the merchant system notified of the successful transaction.

**Attention!**

The «`SupportReferenceID`» value should always be stored so that it may be used as reference in the communication between the merchant and Euronet Merchant Services.

**Note:**

- It is suggested that the transaction approval code («`ApprovalCode`») be indicated and/or sent on a transaction confirmation email from the merchant to the user.
- It is recommended that the transaction decline or technical error messages (`ResultDescription`, `ResponseDescription`) should not appear as such on the user page.



7. Transaction Web Service Test Cases

Below there is a list and description of the test cases that may be executed in the epay eCommerce test environment (call of Transaction Web Service). Test transactions must be performed for all the test cases that are marked as «MANDATORY». Optional test cases may be run to the extent that they are applicable to the system under implementation.

In online transaction systems only, the 3d-secure process must be applied first using any of the Cardinal test cases in section 4.

All in all, the following tests are the most common scenarios occurring in a production system.

Below there is a test cases concise list:

No	TITLE	MANDATORY
Test case 1	APPROVED TRANSACTION (VISA)	YES
Test case 2	DECLINED TRANSACTION	YES
Test case 3	RECHARGE ATTEMPT	YES
Test case 4	COMMUNICATION ERROR	YES
Test case 5	INVALID CARD NUMBER	YES
Test case 6	UNDER-PROCESS TRANSACTION WAS RE-SENT	YES
Test case 7	BATCH IS CLOSING	YES
Test case 8	GENERAL ERROR	YES
Test case 9	APPROVED TRANSACTION WITH INSTALLMENTS	NO
Test case 10	APPROVED TRANSACTION (MASTERCARD)	NO
Test case 11	APPROVED TRANSACTION (DINERS)	NO
Test case 12	APPROVED TRANSACTION (DISCOVER)	NO
Test case 13	APPROVED TRANSACTION (AMERICAN EXPRESS)	NO
Test case 14	APPROVED TRANSACTION (GBP)	NO
Test case 15	APPROVED TRANSACTION (USD)	NO

The following applies to all test cases:

- The «AcquirerID», «MerchantID», «PosID», «User» and «Password» parameter values are provided by Euronet Merchant Services.
- The «RequestType» parameter is entered depending on the transaction type (see section 5).
- The «Amount» parameter may take any valid value (see section 5).
- The «Installments», «CurrencyCode», «ExpirePreauth», «CardType», «CardNumber», «ExpirationMonth», «ExpirationYear» and «CVV2»

parameter values are entered according to the values provided in the test cases.



Note:

- It is reminded that preauthorization is a transaction by means of which the amount is simply committed. The preauthorization must be completed by the merchant (either via the epay eCommerce AdminTool or by calling the Transaction Web Service) within the days defined via the «ExpirePreauth» parameter for the transaction to be settled.
- In preauthorization test transactions, the «ExpirePreauth» parameter must always be given the value 30, but in the live environment its value may vary from 2 to 30 (in case preauthorizations are used).



Test Case 1: APPROVED TRANSACTION (VISA)

MANDATORY

Scenario: Approval of transaction (without installments) with Visa card



It is applicable:

When ResultCode=0 and StatusFlag=Success



Input parameters:

Parameter	Value
ExpirePreauth for sale	0
ExpirePreauth for preauthorization	30
Currency	978
Installments	0
CardType	VISA or UNKNOWN
CardNumber for sale	490845555555557
CardNumber for preauthorization	4020680000000098
ExpirationMonth	01
ExpirationYear	Any future year
CVV2	123



Response parameters:

Parameter	Value
ResultCode	0
ResponseCode	00



Merchant application actions:

- Display of transaction approval message on the user page
- Storing of SupportReferenceID, MerchantReference, TransactionID, StatusFlag, ResponseCode, ResponseDescription, ApprovalCode and PackageNo parameter values
- Merchant application update for the successful transaction



Test Case 2: DECLINED TRANSACTION

MANDATORY

Scenario: Decline of a transaction



It is applicable:

When ResultCode=0 and StatusFlag= Failure



Input parameters:

Parameter	Value
ExpirePreauth for sale	0
ExpirePreauth for preauthorization	30
Currency	978
Installments	0
CardType	VISA or UNKNOWN
CardNumber for sale	4908455555555557
CardNumber for preauthorization	4020680000000098
ExpirationMonth	02
ExpirationYear	<i>Any future year</i>
CVV2	123



Response parameters:

Parameter	Value
ResultCode	0
ResponseCode	12



Merchant application actions:

- Display of transaction decline message received from Issuer on the user page
- Storing of SupportReferenceID, MerchantReference, ResponseCode and ResponseDescription parameter values
- Merchant application update for the declined transaction



Test Case 3: RECHARGE ATTEMPT

MANDATORY

Scenario: Attempt to recharge a transaction (the request sent had a «MerchantReference» value already used for an approved transaction)



It is applicable:

When StatusFlag= Failure & ResultCode=1048



Input parameters:

Parameter	Value
ExpirePreauth for sale	0
ExpirePreauth for preauthorization	30
Currency	978
Installments	0
CardType	VISA or UNKNOWN
CardNumber for sale	490845555555557
CardNumber for preauthorization	4020680000000098
ExpirationMonth	03
ExpirationYear	Any future year
CVV2	123



Response parameters:

Parameter	Value
StatusFlag	Failure
ResultCode	1048



Merchant application actions:

- Display of transaction approval message on the user page
- Storing of SupportReferenceID, MerchantReference, ResultCode, ResultDescription parameter values
- Merchant application update for the recharge attempt (if necessary, to make a thorough check)



Test Case 4: COMMUNICATION ERROR

MANDATORY

Scenario: Failure to execute a transaction due to (technical) communication problem with the transaction processing system



It is applicable:

When ResultCode = 50x (i.e. 500, 501 etc.)



Input parameters:

Parameter	Value
ExpirePreauth for sale	0
ExpirePreauth for preauthorization	30
Currency	978
Installments	0
CardType	VISA or UNKNOWN
CardNumber for sale	4908455555555557
CardNumber for preauthorization	4020680000000098
ExpirationMonth	04
ExpirationYear	<i>Any future year</i>
CVV2	123



Response parameters:

Parameter	Value
ResultCode	500
ResponseCode	



Merchant application actions:

- Display of a transaction failure message on the user page (with a prompt to try again later)
- Storing of SupportReferenceID, MerchantReference, ResultCode and ResultDescription parameter values
- Merchant application update for the failure to execute the transaction



Test Case 5: INVALID CARD NUMBER

MANDATORY

Scenario: Failure to execute a transaction due to incorrect card details or a card not supported by the system



It is applicable:

When ResultCode = 981



Input parameters:

Parameter	Value
ExpirePreauth for sale	0
ExpirePreauth for preauthorization	30
Currency	978
Installments	0
CardType	VISA or UNKNOWN
CardNumber for sale	490845555555557
CardNumber for preauthorization	4020680000000098
ExpirationMonth	05
ExpirationYear	<i>Any future year</i>
CVV2	123



Response parameters:

Parameter	Value
ResultCode	981
ResponseCode	



Merchant application actions:

- Display of a transaction failure message on the user page (with a prompt to try again and check the card details or enter a different card)
- Storing of SupportReferenceID, MerchantReference, ResultCode and ResultDescription parameter values
- Merchant application update for the failure to execute the transaction



Test Case 6: UNDER-PROCESS TRANSACTION WAS RE-SENT

MANDATORY

Scenario: Attempt to send a transaction with the same «MerchantReference» as that of the transaction currently processed by epay eCommerce (it is possible that a response has not been received from the Issuer or a problem has occurred in the transaction processing system; as a result the transaction is «stalled»)



It is applicable:

When ResultCode = 1045



Input parameters:

Parameter	Value
ExpirePreauth for sale	0
ExpirePreauth for preauthorization	30
Currency	978
Installments	0
CardType	VISA or UNKNOWN
CardNumber for sale	490845555555557
CardNumber for preauthorization	4020680000000098
ExpirationMonth	06
ExpirationYear	Any future year
CVV2	123



Response parameters:

Parameter	Value
ResultCode	1045
ResponseCode	



Merchant application actions:

- Display of a transaction failure message on the user page (with a prompt to try again later)
- Storing of SupportReferenceID, MerchantReference, ResultCode and ResultDescription parameter values
- Merchant application update for the failure to execute the transaction prompting the merchant to investigate the transaction status via the epay eCommerce AdminTool



Note:

A user prompt to try again later is recommended, because if the transaction is finally executed successfully, then a subsequent attempt will reproduce Test case 3.



Test Case 7: BATCH IS CLOSING

MANDATORY

Scenario: Failure to execute a transaction because the current transaction batch is being settled (batch closing)



It is applicable:

When ResultCode = 1072



Input parameters:

Parameter	Value
ExpirePreauth for sale	0
ExpirePreauth for preauthorization	30
Currency	978
Installments	0
CardType	VISA or UNKNOWN
CardNumber for sale	4908455555555557
CardNumber for preauthorization	4020680000000098
ExpirationMonth	07
ExpirationYear	<i>Any future year</i>
CVV2	123



Response parameters:

Parameter	Value
ResultCode	1072
ResponseCode	



Merchant application actions:

- Display of a transaction failure message on the user page (with a prompt to try again later)
- Storing of SupportReferenceID, MerchantReference, ResultCode and ResultDescription parameter values
- Merchant application update for the failure to execute the transaction (if necessary)



Test Case 8: GENERAL ERROR

MANDATORY

Scenario: Failure to execute a transaction due to a temporary technical problem



It is applicable:

When ResultCode = 1



Input parameters:

Parameter	Value
ExpirePreauth for sale	0
ExpirePreauth for preauthorization	30
Currency	978
Installments	0
CardType	VISA or UNKNOWN
CardNumber for sale	4908455555555557
CardNumber for preauthorization	4020680000000098
ExpirationMonth	08
ExpirationYear	<i>Any future year</i>
CVV2	123



Response parameters:

Parameter	Value
ResultCode	1
ResponseCode	



Merchant application actions:

- Display of a transaction failure message on the user page (with a prompt to try again later)
- Storing of SupportReferenceID, MerchantReference, ResultCode and ResultDescription parameter values
- Merchant application update for the failure to execute the transaction (if necessary)



Test Case 9: APPROVED TRANSACTION WITH INSTALLMENTS

OPTIONAL

Scenario: Approval of installment transaction



It is applicable:

When ResultCode=0 and StatusFlag=Success



Input parameters:

Parameter	Value
ExpirePreauth for sale	0
ExpirePreauth for preauthorization	30
Currency	978
Installments	3
CardType	VISA or UNKNOWN
CardNumber for sale	490845555555557
CardNumber for preauthorization	4020680000000098
ExpirationMonth	09
ExpirationYear	Any future year
CVV2	123
Amount	Greater than 90



Response parameters:

Parameter	Value
ResultCode	0
ResponseCode	00



Merchant application actions:

- Display of transaction approval message on the user page in «x» installments (where «x», the number of installments entered)
- Storing of SupportReferenceID, MerchantReference, TransactionID, StatusFlag, ResponseCode, ResponseDescription, ApprovalCode and PackageNo parameter values
- Merchant application update for the successful transaction



Test Case 10: APPROVED TRANSACTION (MASTERCARD)

OPTIONAL

Scenario: Approval of transaction (without installments) with Mastercard



It is applicable:

When ResultCode=0 and StatusFlag=Success



Input parameters:

Parameter	Value
ExpirePreauth for sale	0
ExpirePreauth for preauthorization	30
Currency	978
Installments	0
CardType	MasterCard or UNKNOWN
CardNumber for sale and for preauthorization	5194993333333335
ExpirationMonth for sale	01
ExpirationMonth for preauthorization	02
ExpirationYear	<i>Any future year</i>
CVV2	123

On the screen displayed, please enter "Yes" for the transaction to be completed.



Response parameters:

Parameter	Value
ResultCode	0
ResponseCode	00



Merchant application actions:

- Display of transaction approval message on the user page
- Storing of SupportReferenceID, MerchantReference, TransactionID, StatusFlag, ResponseCode, ResponseDescription, ApprovalCode and PackageNo parameter values
- Merchant application update for the successful transaction



Test Case 11: APPROVED TRANSACTION (DINERS)

OPTIONAL

Scenario: Approval of transaction (without installments) with Diners card



It is applicable:

When ResultCode=0 and StatusFlag=Success



Input parameters:

Parameter	Value
ExpirePreauth for sale	0
ExpirePreauth for preauthorization	30
Currency	978
Installments	0
CardType	DinersClub or UNKNOWN
CardNumber for sale	36131111111119
CardNumber for preauthorization	36131100000000
ExpirationMonth	01
ExpirationYear	Any future year
CVV2	123



Note:

Transactions with Diners/Discover card should have «null» value in «AuthInfo» element (it contains the Cavv, Eci, Xid, Enrolled, PAResStatus, SignatureVerification elements – see section 5).



Response parameters:

Parameter	Value
ResultCode	0
ResponseCode	00



Merchant application actions:

- Display of transaction approval message on the user page
- Storing of SupportReferenceID, MerchantReference, TransactionID, StatusFlag, ResponseCode, ResponseDescription, ApprovalCode and PackageNo parameter values
- Merchant application update for the successful transaction



Test Case 12: APPROVED TRANSACTION (DISCOVER)

OPTIONAL

Scenario: Approval of transaction (without installments) with Discover card



It is applicable:

When ResultCode=0 and StatusFlag=Success



Input parameters:

Parameter	Value
ExpirePreauth for sale	0
ExpirePreauth for preauthorization	30
Currency	978
Installments	0
CardType	DinersClub or UNKNOWN
CardNumber for sale	6011111111111117
CardNumber for preauthorization	6011000000000004
ExpirationMonth	01
ExpirationYear	Any future year
CVV2	123



Note:

Transactions with Diners/Discover card should have «null» value in «AuthInfo» element (it contains the Cavv, Eci, Xid, Enrolled, PAResStatus, SignatureVerification elements – see section 5).



Response parameters:

Parameter	Value
ResultCode	0
ResponseCode	00



Merchant application actions:

- Display of transaction approval message on the user page
- Storing of SupportReferenceID, MerchantReference, TransactionID, StatusFlag, ResponseCode, ResponseDescription, ApprovalCode and PackageNo parameter values
- Merchant application update for the successful transaction



Test Case 13: APPROVED TRANSACTION (AMERICAN EXPRESS)

OPTIONAL

Scenario: Approval of transaction (without installments) with American Express card



It is applicable:

When ResultCode=0 and StatusFlag=Success



Input parameters:

Parameter	Value
ExpirePreauth for sale	0
ExpirePreauth for preauthorization	30
Currency	978
Installments	0
CardType	AMEX or UNKNOWN
CardNumber for sale	375537111111116
CardNumber for preauthorization	375537000000008
ExpirationMonth	01
ExpirationYear	Any future year
CVV2	1234



Note:

Transactions with American Express card should have «null» value in «AuthInfo» element (it contains the Eci, Xid, Enrolled, PAREsStatus, SignatureVerification elements – see section 5).



Response parameters:

Parameter	Value
ResultCode	0
ResponseCode	00



Merchant application actions:

- Display of transaction approval message on the user page
- Storing of SupportReferenceID, MerchantReference, TransactionID, StatusFlag, ResponseCode, ResponseDescription, ApprovalCode and PackageNo parameter values
- Merchant application update for the successful transaction



Test Case 14: APPROVED TRANSACTION (GBP)

OPTIONAL



Attention!

For every different currency, a different test and live account is required

Scenario: Approval of transaction (without installments) in GBP currency



It is applicable:

When ResultCode=0 and StatusFlag=Success



Input parameters:

Parameter	Value
ExpirePreauth for sale	0
ExpirePreauth for preauthorization	30
Currency	826
Installments	0
CardType	VISA or UNKNOWN
CardNumber for sale and for preauthorization	4908456666666663
ExpirationMonth for sale	01
ExpirationMonth for preauthorization	02
ExpirationYear	Any future year
CVV2	123

On the screen displayed, please enter "Yes" for the transaction to be completed.



Response parameters:

Parameter	Value
ResultCode	0
ResponseCode	00



Merchant application actions:

- Display of transaction approval message on the user page
- Storing of SupportReferenceID, MerchantReference, TransactionID, StatusFlag, ResponseCode, ResponseDescription, ApprovalCode and PackageNo parameter values
- Merchant application update for the successful transaction



Test Case 15: APPROVED TRANSACTION (USD)

OPTIONAL



Attention!

For every different currency, a different test and live account is required

Scenario: Approval of transaction (without installments) in USD currency



It is applicable:

When ResultCode=0 and StatusFlag=Success



Input parameters:

Parameter	Value
ExpirePreauth for sale	0
ExpirePreauth for preauthorization	30
Currency	840
Installments	0
CardType	VISA or UNKNOWN
CardNumber for sale and for preauthorization	4908456666666663
ExpirationMonth for sale	03
ExpirationMonth for preauthorization	04
ExpirationYear	Any future year
CVV2	123

On the screen displayed, please enter "Yes" for the transaction to be completed.



Response parameters:

Parameter	Value
ResultCode	0
ResponseCode	00



Merchant application actions:

- Display of transaction approval message on the user page
- Storing of SupportReferenceID, MerchantReference, TransactionID, StatusFlag, ResponseCode, ResponseDescription, ApprovalCode and PackageNo parameter values
- Merchant application update for the successful transaction



8. Security Requirements

With regard to the security requirements that must be met by the merchant system, the following should be considered:

- According to the Visa/Mastercard organizations specifications, no card detail (i.e. card number, expiry date, cvv2) must be stored in the merchant system.
- If transactions are performed via a site, then SSL encryption with min. 128-bit key size should be used on the page where the user enters his/her card details, so that they may be transferred securely.



Note:

In order for the live account details to be sent, SSL should have been used on the live site so that it can be checked by Euronet Merchant Services.

- The use of ssl on the card details entry page of the merchant site must be visible to the user through the relevant icons used by the various browsers. Therefore, the card details entry page may not be in any kind of frame (FrameSet, IFrame) because the secure address of the page with the respective browser symbols indicating its validity and security are suppressed. On the contrary, in this case the Frame parent page address is displayed, which might not be secure thus creating a wrong impression to the user.
- For transactions via a site, characters should not be visible when typed by the user in the cvv2 field (e.g. asterisks should be displayed instead).

9. Use of Icons

If transactions are performed via a site, it is necessary to use some necessary icons according to the specifications of Visa and Mastercard organizations.

All relevant material can be downloaded from the following link :
<https://paycenter.piraeusbank.gr/services/Manuals/Icons/Icons.zip>

Specifically:

Supported card icons

The icons of the supported cards are included in the folder (Icons/CardsIcons) and they are as follows:

Visa (<i>Visa.png</i>)
Mastercard (<i>Mastercard.png</i>)
Maestro (<i>Maestro.png</i>)

If the merchant supports Diners/Discover and/or American Express cards, then the relevant cards icons must be also included:

Diners (<i>Diners.jpg</i>)
Discover (<i>Discover.jpg</i>)
American Express (<i>Amex.jpg</i>)

The above icons should be displayed on the website homepage.

3D Secure icons

In the case of online transactions through a website, the following 3D Secure icons should be displayed on the website homepage, on the page where card details are entered and on the security information page:

- **Visa Secure service:**
One of the icons included in (Icons/Visa Secure) should be displayed.
- **Mastercard Identity Check:**
One of the icons included in (Icons/MasterCard Identity Check) should be displayed.

epay logo

Logo of epay may optionally be displayed on the merchant site. The relevant icons are included in the (Icons/epay) folder.

10. Tips

A list of remarks-tips which must be taken into account is given below:


- 💡 A preauthorization transaction can be completed by the merchant (either via the epay eCommerce AdminTool or by calling the Transaction Web Service) within the days defined via the "ExpirePreauth" parameter (maximum 30 days). After that period of time, the preauthorization cannot be settled.
- 💡 Refund transactions can be carried out through either the epay eCommerce AdminTool (web application provided to all merchants) or a Web Service call.
- 💡 According to the Visa/Mastercard organizations specifications, no card detail (i.e. card number, expiry date, cvv2) must be stored in the merchant system.
- 💡 The "Password" parameter in the "Transaction Web Service" (see section 5) must be sent encrypted with the MD5 hashing algorithm.
- 💡 The "**MerchantReference**" parameter in the "Transaction Web Service" should have a unique/different value in each new sale or pre-authorisation transaction. Even if the transaction fails and a new attempt is made (i.e. a new transaction), the 3D Secure process should be repeated (if supported) and the Transaction Web Service call should contain a new "Merchant Reference" value.
- 💡 It is important that the "**MerchantReference**" parameter has a value that has a special meaning and is known to the merchant (e.g. order number, contract number, etc.). This value, uniquely designating every successful transaction, appears in the "AdminTool" provided by Euronet Merchant Services to merchants to monitor their transactions. Using the "AdminTool" merchants can find transactions using the "**MerchantReference**" value as search criterion.
- 💡 For better merchant support by Euronet Merchant Services, the "**SupportReferenceID**" parameter should be stored with every attempt and be available to the merchant managers, so that it may be used in the communication with PiraeuEuronet Merchant Services Bank to solve potential problems. The same parameter must be sent by technicians to Euronet Merchant Services in the event of issues during test transactions.
- 💡 Interest-free installments are only supported by certain cards issued by Greek banks (depending on BIN, i.e. the first 6 digits of the card number). Euronet Merchant Services provides the "**BIN Web Service**" API which can be used in order to check if a card supports installments without sending a charge transaction. In case of interest, the technical specifications should be requested from Euronet Merchant Services.
- 💡 If communication with ePOS epay eCommerce is interrupted and no response is received by the merchant system, a refund request may be submitted (RequestType = "REFUND") sending a value in the

"MerchantReference" parameter instead of the **"TransactionReferenceID"** parameter. This functionality is only provided for transaction cancellations (i.e. cancellation of transactions included in an open package).



11. Implementation Checklist

No.	TASK
1.	⇒ CONTRACT SIGNING Signing of acquiring contract for the "Web Service" solution between the company and Euronet Merchant Services.
2.	⇒ TECHNICAL IMPLEMENTATION Implementation of: <ul style="list-style-type: none">■ Strong customer authentication process for online card transactions (Visa, Mastercard and Maestro through a website ("3D Secure" - see section 4)■ Software calling the "Transaction Web Service"
3.	⇒ TEST ACCOUNT INFORMATION SUBMISSION Submit the required information to Euronet Merchant Services to create a test account (see section 3)
4.	⇒ CONDUCT OF TEST TRANSACTIONS <ul style="list-style-type: none">■ Euronet Merchant Services forwards the following test account details:<ul style="list-style-type: none">■ AcquirerID■ MerchantID■ PosID■ User■ Password■ ChannelType■ <u>Only for systems supporting online transactions through a website:</u> Execution of all test cases of the 3D Secure process (see relevant documentation).■ Perform test transactions using the "Transaction Web Service" (see section 7).
5.	⇒ USE OF ICONS <u>For systems sending transactions through a website:</u> Posting of the necessary icons on the merchant website (see section 9)


6.	<div data-bbox="411 199 1046 230" data-label="Section-Header"> <h4>➡ COMPLETION OF TEST TRANSACTIONS</h4> </div> <ul style="list-style-type: none"> ■ Inform Pireaus Bank about the successful completion of test transactions, the use of icons and SSL and dispatch of test transaction details to the Bank for review. The following should be sent: <ul style="list-style-type: none"> ▪ the "MerchantReference" value for each test case of the 3D Secure process (see relevant documentation). ▪ The "SupportReferenceID" value of each test case where the Transaction Web Service is called (see section 7). ■ Euronet Merchant Services checks the test transactions and notifies the technical manager of the result within one week. ■ Send the IP address of the server submitting the live transactions (merchant system) to Euronet Merchant Services. ■ Dispatch to Euronet Merchant Services of a merchant email to be used for updates regarding epay eCommerce.
7.	<div data-bbox="411 844 826 875" data-label="Section-Header"> <h4>➡ LIVE ACCOUNT RECEIPT</h4> </div> <ul style="list-style-type: none"> ■ Euronet Merchant Services forwards live account details: <ul style="list-style-type: none"> ▪ AcquirerID ▪ MerchantID ▪ PosID ▪ User ▪ Password ▪ ChannelType ■ Replace the test account details with the live account details. <div data-bbox="373 1256 1362 1435" data-label="Complex-Block"> <div data-bbox="373 1256 427 1317"></div> <div data-bbox="443 1256 528 1288" data-label="Section-Header"> <p>Note:</p> </div> <div data-bbox="443 1301 1350 1368" data-label="Text"> <p>The Transaction Web Service URL is the same both for test and actual transactions:</p> </div> <div data-bbox="443 1382 1342 1417" data-label="Text"> <p>https://paycenter.piraeusbank.gr/services/paymentgateway.asmx</p> </div> </div>


> Annex 1

The table below shows the most frequent values of the "ResultCode" (i.e. eventual technical problems) and "ResponseCode" (i.e. most common responses sent by Issuers) parameters.

ResultCode FREQUENT VALUES			
ResultCode	ResultDescription	Explanation	Action
1	An error occurred. Please check your data or else contact epay eCommerce administrator	General error code which is returned when there is a technical problem	Try again later when the problem has been rectified
100	Authentication Error	Wrong value is used in «Username» / «User» parameter and/or «Password» parameter	Use correct values in «Username» / «User» and «Password» parameter
130	Field «x» contains invalid characters	The «x» parameter contains invalid characters.	Use valid value in «x» parameter
151	Check that field «x» contains data	No value is sent in «x» parameter	Send (valid) value in «x» parameter
215	AMEX cards require 4 digit cvv2	An American Express card was used and the cvv2 did not consist of 4 digits as it should	Re-send the transaction using the correct (4-digit) cvv2
216	Wrong cvv2	An invalid value was used in «Cvv2» parameter (e.g. characters)	Re-send the transaction using a valid cvv2
50x (e.g. 500, 501 etc.)	Communication Error	Communication problem with the transaction processing system	Try again later when the problem has been rectified

981	Invalid Card number/Exp Month/Exp Year	No valid values were used in card details (e.g. wrong card number, past expiration date etc) or unsupported card was used	Re-send the transaction using correct card details
1006	Unknown BIN	The user card is not eligible for Euronet Merchant Services's interest-free installments program	Use another card or re-send the transaction without installments
1007	Merchant does not support given bin	It concerns installment transaction. The card bin (i.e. the first 6 digits) may not be used in installment transaction in this merchant	Use another card or re-send the transaction without installments
1010	Wrong original transaction	It concerns settlement transactions (SETTLEMENT), preauthorization cancellations (VOIDREQUEST), refund transactions (REFUND) or follow up requests (FOLLOW_UP). The request is rejected because there is no successful transaction for which the settlement, the preauthorization cancelation, the refund transaction or the follow up is asked.	Check the initial transaction and send correct value in «TransactionReferenceID» parameter
1012	Original transaction already settled, or being settled	It concerns a preauthorization settlement transaction («SETTLEMENT»). A settlement is requested for a preauthorization which has	Check if the preauthorization is finally settled using epay eCommerce AdminTool.

		already been settled or is being settled.	
1014	Refunding amount cannot exceed remaining amount of the original transaction	It concerns refund transactions («REFUND»). The refund amount is greater than the initial charge amount.	Re-send the transaction using correct amount.  Note: A lot of partial refund transactions may be sent provided that the sum of the amounts used in all partial refunds is not greater than the amount of the initial charge transaction.
1017	Preorder date has expired	It concerns a preauthorization settlement transaction («SETTLEMENT»). The settlement cannot be carried out because the preauthorization has expired.	Submit a new preauthorization transaction.
1019	Too many installments asked	The number of installments requested is higher than the maximum allowed for this merchant	Use a lower number of installments
1026	Merchant does not support instalments	Installments were used in the transaction but the merchant does not support installments.	Contact Euronet Merchant Services in order to activate the use of installments
1034	Terminal does not support given card type	Transaction with unsupported card type	Check the «CardType» parameter value and contact Euronet Merchant Services
1040, 1041	«Error validating IP address. Contact sysadmin.» (1040), «Invalid IP address.» (1041)	The IP address validation failed as the request was sent through a server with different IP address than the one that was	Check the server's IP address and if it's necessary, contact Euronet Merchant Services in order to change the IP address

		provided by the technical Manager to Euronet Merchant Services	that corresponds to the specific merchant id.
1042	Refund maximum allowed period exceeded	Attempted refund after the allowed period of 365 days.	Contact Euronet Merchant Services.
1045	Duplicate transaction references are not allowed	The request was sent with the same «MerchantReference» as that of a transaction currently processed by epay eCommerce	Try again later in order for the initial transaction to have been completed. If the initial transaction is finally approved, then the ResultCode 1048 will be returned in the new attempt (see test case 3 in section 7), otherwise a new transaction will be carried out. Alternatively, check if the initial transaction is approved using epay eCommerce AdminTool.
1048	Transaction already processed and completed	The request sent had a «MerchantReference» value already used for an approved transaction	Re-send the transaction using a different «MerchantReference» value.
1072	Pack is still closing	The batch settlement process is in progress (batch closing)	Try again later after the batch has been closed
1802	Wrong amount value	Invalid value used in «Amount» parameter (e.g. zero amount)	Use a valid value in «Amount» parameter
7001	<i><Code of anti-fraud rule that was fired-up></i>	The request was rejected due to anti-fraud checks. The «ResultDescription» parameter contains the code of the rule that was fired-up. <u>The zero value (0) means that the card number is included in a black list.</u> If special anti-fraud rules have been agreed with the	<p>Prompt the user for another form of payment or ask for a different card.</p> <div>  Attention! The end user should not be informed that the transaction was rejected due to anti-fraud checks. </div>

		merchant, Euronet Merchant Services will provide the relevant rule codes that may be returned.	
--	--	--	--

ResponseCode FREQUENT VALUES				
ResponseCode	ResponseDescription	Explanation	Action	Transaction approval
05	Declined	Transaction declined by the Issuer	Cardholder should contact his/her Bank or use another card	No
12	Declined	Transaction declined by the Issuer	Cardholder should contact his/her Bank or use another card	No
51	Declined	Transaction declined by the Issuer	Cardholder should contact his/her Bank or use another card	No
34 43	Lost card Stolen card, pick-up	Transaction declined by the Issuer	Cardholder should contact his/her Bank or use another card	No
54	Expired card	The card has expired and has not been renewed	Use another card	No
62	Restricted Card	Transaction declined by the Issuer	Cardholder should contact his/her Bank or use another card	No
92	Declined	Communication problem with the payment Organisation (Visa, Mastercard etc.)	Try again later	No

I2	Installment amount below allowed minimum	Refers to instalment transaction where the individual installment value is lower than the allowed minimum	Repeat transaction with lower number of installments	No
-----------	--	---	--	----



Note:

More values may be returned in addition to the ones listed in the tables above.



Annex 2

Supported currency codes:

Currency Code	Currency
008	ALBANIAN LEK (ALL)
032	ARGENTINA PESO (ARS)
036	AUSTRALIAN DOLLAR (AUD)
124	CANADIAN DOLLAR (CAD)
152	CHILEAN PESO (CLP)
156	CHINESE YUAN (CNY)
170	COLOMBIAN PESO (COP)
191	CROATIAN KUNA (HRK)
203	CZECH KORUNA (CZK)
208	DANISH KRONE (DKK)
344	HONG KONG DOLLAR (HKD)
348	FIORINT (HUF)
356	INDIAN RUPEE (INR)
360	RUPIAH (IDR)
376	ISRAELI NEW SHEQEL (ILS)
392	YEN (JPY)
398	TENGE (KZT)
410	WON (KRW)
414	KUWAITI DINAR (KWD)
440	LITHUANIAN LITAS (LTL)
446	PATACA (MOP)
458	MALAYSIAN RINGGIT (MYR)
484	MEXICAN PESO (MXN)
504	MORROCAN DIRHAM (MAD)
554	NEW ZEALAND DOLLAR (NZD)
578	NORWEGIAN KRONE (NOK)
604	NUEVO SOL (PEN)
608	PHILIPPINE PESO (PHP)
643	RUSSIAN ROUBLE (RUB)
682	SAUDI RIYAL (SAR)
702	SINGAPORE DOLLAR (SGD)
710	RAND (ZAR)

752	SWEDISH KRONA (SEK)
756	SWISS FRANC (CHF)
764	BAHT (THB)
784	UNITED ARAB EMIRATES DIRHAM (AED)
818	EGYPTIAN POUND (EGP)
826	POUND STERLING (GBP)
840	US DOLLAR (USD)
937	BOLIVAR FUERTE (VEF)
941	SERBIAN DINAR (RSD)
946	ROMANIAN LEU (RON)
949	TURKISH LIRA (TRY)
975	BULGARIAN LEV (BGN)
978	EURO (EUR)
980	UKRAINIAN HRYVNIA (UAH)
985	POLISH ZLOTY (PLN)
986	BRAZILIAN REAL (BRL)
933	BELARUSIAN RUBLE (BYN)



Glossary

3D Secure	The name of the protocol used in the strong customer authentication process ("Visa Secure" and "Mastercard Identity check" by Visa and Mastercard respectively).
Acquirer	An organization enabling merchants to execute card transactions. Euronet Merchant Services in this case.
BIN	The first 6 digits of a card number identifying the Issuer bank.
Live account	The merchant account through which live transactions are executed. It comprises the following: <ul style="list-style-type: none">▪ AcquirerID▪ MerchantID▪ PosID▪ User▪ Password▪ ChannelType
Merchant id	The " <i>merchant identification</i> " assigned to the company.
Pos id	The " <i>pos identification</i> " (P oint O f S ale) of the merchant.
Test account	The test account provided by Euronet Merchant Services through which test transactions are carried out. It comprises the same elements as the "live account" but has different values.
Transaction Web Service	Euronet Merchant Services's SOAP Web Service via which transactions are submitted to epay eCommerce.
epay eCommerce	The Euronet Merchant Services electronic payments system.