

TECHNICAL SPECIFICATIONS

Rest 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



Change History

Date	Version	Modifications
22/04/2013	1.0	Original version
09/08/2013	1.0.1	Addition of new test case for transactions in USD currency (test case 15 in section 7)
28/04/2014	1.0.2	<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	1.0.3	Addition of new currencies and new Logo
28/04/2014	1.0.2	New Mastercard/Maestro logos
01/02/2022	1.0.4	<ul style="list-style-type: none">▪ Section 4: Update in order to support 3D Secure version 2.▪ Section 7: Update of the test cases for the Rest Web Service with new test cards▪ Section 9: Update with Visa Secure and Mastercard IdentityCheck logos (3D Secure v2)▪ Section 11: Update Implementation Checklist
16/03/2022	2.0	Service rebranding to epay eCommerce
13/10/2022	2.1	Update of manual links
20/09/2022	2.2	"Apple Pay" & "Google Pay" transaction support
12/02/2024	2.3	Support of new transaction type FUNDSTRANSFER



Contents

1. Introduction	2
2. General Architecture	4
3. Details for the Creation of a Test Account	5
4. Cardholder Authentication Process («3D-Secure»)	6
5. Rest Web Service	8
6. Merchant Application Action Flow	25
7. Rest Web Service Test Cases	29
8. Security Requirements	46
9. Use of Icons	47
10. Tips	48
11. Implementation Checklist	50
Annex 1	52
Annex 2	53
Annex 3	61
Glossary	63



1. Introduction

The «**Rest Web Service**» solution of Euronet Merchant Services' epay eCommerce is a Web Service that uses Rest technology and enables card transactions to be executed. The transaction data are submitted to Euronet Merchant Services' e-payment system (epay eCommerce) using messages in JSON format. It is strongly recommended for applications in mobile devices.

Before calling the «Rest Web Service», 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 as follows:

- 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 first)
- 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 for 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 → Rest Web Service:**
Description of the «Rest 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 → Rest Web Service Test Cases:**
Description of the test cases to be performed in the framework of test transactions using the «Rest Web Service».
- **Section 8 → Use of Icons:**
Included here is the material about the mandatory and optional icons to be posted on the application.
- **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 «Rest Web Service» solution including the use of the cardholder authentication process.

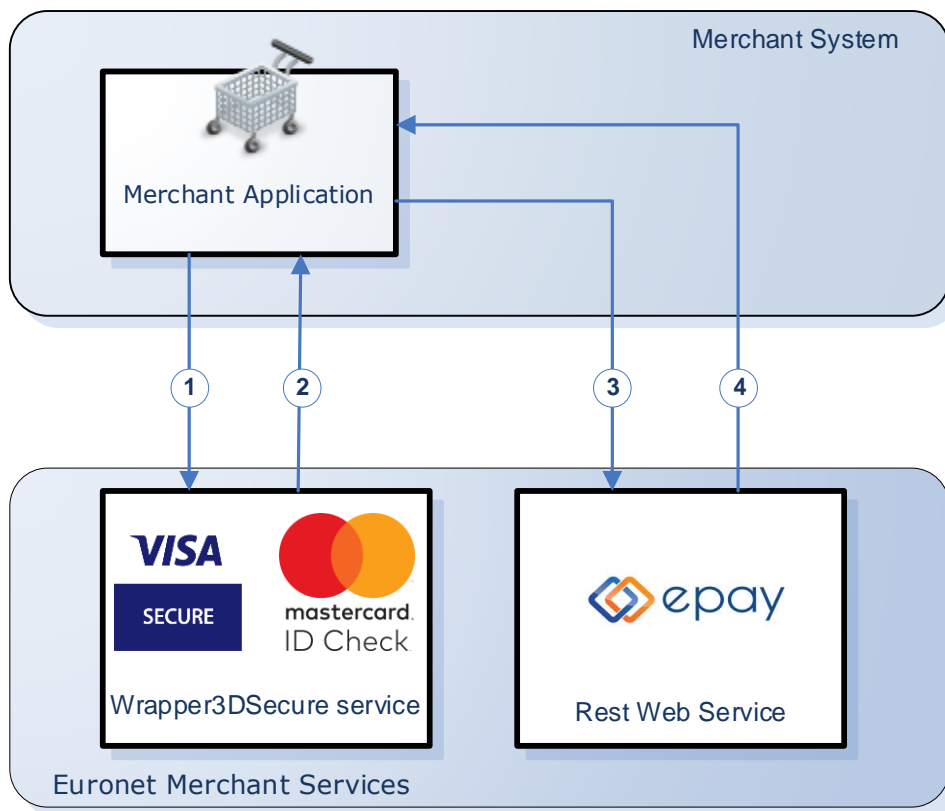


Chart 1: General Architecture

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). For transactions with other cards (e.g. Diners/Discover or American Express), the cardholder authentication process is not applied. If the result of the cardholder authentication process allows the execution of the transaction, then Euronet Merchant Services' «**Rest Web Service**» is used (steps 3, 4) to submit the transaction data to Euronet Merchant Services' e-payment system (epay eCommerce) and receive a response (see section 5).



3. Details for the Creation of a Test Account

The data to be submitted to Euronet Merchant Services in order to provide the necessary technical info (*test account*) for test transactions are as follows (all mandatory):

- **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 (if it's about a web application)
- **Technical data:**
 - **IP address:** The IP address of server calling Euronet Merchant Services «Rest Web Service»
 - **Installments support (YES/NO):** Declare if you are going to use installments in test transactions

The *test account* details provided by Euronet Merchant Services, once the above information is submitted, are 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 ("Rest Web Service" call):

- AcquirerID
- MerchantID
- User
- Password

Information about the use of these details is provided in the following sections.



4. Cardholder Authentication Process («3D-Secure»)

Sale, preauthorization or digital wallet top up eCommerce transactions (see transaction types in section 5) initiated by the card holder using a Visa, Mastercard or Maestro card must 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 Rest 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, preauthorization** or **digital wallet top up** 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 Rest Web Service call:

Parameter from Wrapper3DSecure	Parameter to Rest 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 Rest 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. Rest Web Service

The «Rest Web Service» submits request messages to Euronet Merchant Services using HTTP protocol and JSON format. In particular, a request message should be submitted using HTTP protocol and the following characteristics:

Method	POST
Accept	application/json
Content-Type	application/json

Samples of all available JSON messages are shown in [Annex 1](#).



Attention!

The response timeout should be set to 60 sec.

The available transaction types are as follows:

■ SALE

Transaction to be immediately settled in the current package.

■ PREAUTHORIZATION

The amount will be simply committed and later, the preauthorisation will have to be completed (through either the AdminTool or a Rest Web Service call [«SETTLEMENT»]) so as to be settled



Attention!

A preauthorization transaction can be completed within **30 days**. After that period of time, the preauthorization cannot be either completed or cancelled.

■ PREAUTHORIZATION SETTLEMENT

It concerns the completion of a preauthorization in order to settle the transaction in the current package

■ PREAUTHORIZATION CANCELLATION [VOIDREQUEST]

Voiding of a preauthorization which is **not settled**.

■ REFUND

Refund of a sale or preauthorization that has been settled or cancellation of digital wallet top up that has not been settled.

■ FOLLOW-UP

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).

■ FUNDSTRANSFER


Transfer to own digital wallet account. Transaction that concerns digital wallet top up with funds using own VISA or MasterCard **EU debit** cards.




The URLs that the transaction's data should be posted depend on the transaction type and are as follows:



SALE: https://paycenter.piraeusbank.gr/Services/PaymentGatewayrest.svc/Sale
PREAUTHORIZATION: https://paycenter.piraeusbank.gr/Services/PaymentGatewayrest.svc/Authorize
PREAUTHORIZATION SETTLEMENT: https://paycenter.piraeusbank.gr/Services/PaymentGatewayrest.svc/Settle
PREAUTHORIZATION CANCELLATION [VOIDREQUEST]: https://paycenter.piraeusbank.gr/Services/PaymentGatewayrest.svc/Voidrequest
REFUND: https://paycenter.piraeusbank.gr/Services/PaymentGatewayrest.svc/Refund
FOLLOW-UP: https://paycenter.piraeusbank.gr/Services/PaymentGatewayrest.svc/Followup
FUNDSTRANSFER: https://paycenter.piraeusbank.gr/Services/PaymentGatewayrest.svc/FundsTransfer



Below there is a list of the information required to call the «Rest Web service»:

REQUEST PARAMETERS		
Parameter name	Description	Type
HEADER DATA		
AcquirerID	The acquirer identification. Value will be provided by Euronet Merchant Services.	String
MerchantID	The merchant identification number. Value will be provided by Euronet Merchant Services.	Integer

User	The user name. Value will be provided by Euronet Merchant Services.	String
Password	The user password <u>encrypted with the MD5 hashing algorithm</u> . Value will be provided by Euronet Merchant Services (in non-encrypted form).	String
BODY DATA		
MerchantReference	<p>Transaction reference. It is generated by the merchant system and identifies uniquely each successful transaction (e.g. order number, contract number, etc.).</p> <ul style="list-style-type: none"> «MerchantReference» can be up to 50 characters long, containing only Greek or Latin lowercase & uppercase alphanumeric characters, space, or the following special characters /:_().,+ - It has to be unique to each successful 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/ digital wallet top up transactions should be identical to the value of the corresponding parameter when the Wrapper3DSecure service is called. If an online sale/preauthorization/ digital wallet top up transaction is unsuccessful and needs to be resent, the 3D Secure process should be repeated with a <u>"MerchantReference value which should be different"</u> from that in the previous transaction. When a sale/preauthorisation/ digital wallet top up has been approved, even if it is refunded, it is impossible to re-use the «MerchantReference» of that transaction in any future transaction (see section 6). </div>	String
TransactionReferenceID	<p>Used only in the following transactions:</p> <ul style="list-style-type: none"> Preauthorization settlement 	Integer

	<ul style="list-style-type: none"> ▪ Preauthorisation voiding ▪ Refund <p>It is the transaction id («TransactionID» parameter in response message) of the transaction requested to be settled / refunded.</p> <p> Note: If refund is requested for a preauthorisation that has been settled, the «TransactionID» of the settlement (not preauthorization) is submitted to this parameter.</p>	
CurrencyCode	<p>The code of the transaction currency. It is 978 for debits in euro.</p> <p> Attention!</p> <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/ digital wallet top up transactions should be identical to the value of the corresponding parameter (Currency) when the Wrapper3DSecure service is called. <p> Note: The supported currency codes are shown in Annex 3.</p>	Integer
Amount	<p>The transaction amount with 2 decimal digits. The following applies to various transaction types:</p> <ul style="list-style-type: none"> ▪ Preauthorization settlement: The amount can be lower than or equal to the initial transaction amount. ▪ Preauthorization voiding: The amount must be equal to the initial transaction amount. ▪ Sale refund: The amount can be lower than or equal to the initial transaction amount. ▪ Cancellation of digital wallet top up: 	Decimal (with 2 decimal digits)

	<p>The amount can only be equal (not lower) to the initial transaction amount.</p> <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/ digital wallet top up transactions should correspond to the same amount expressed by the PurchAmount and Exponent parameters when the Wrapper3DSecure service is called. <u>Partial refund in installment transactions</u> will be carried out as one-off (without installments). </div>	
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, submit 0 or 1 or do not send the «Installments» parameter at all. <div>  Note: <p>Euronet Merchant Services provides the «BIN Web Service» 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.</p> </div>	Integer
TaxCardNumber	No value needs to be sent	String
DeviceID	For future use. For the time being, do not submit any value.	String
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

	<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: Visa card ▪ MasterCard: MasterCard card ▪ Maestro: Maestro card. Can be used <u>only if the 3D-Secure process is applied</u> ▪ DinersClub: DinersClub or Discover card ▪ AMEX: American Express card <div>  <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. ▪ Transactions with Diners/Discover or American Express card use a <u>different MerchantId value</u> than the Visa/Mastercard/Maestro transactions and with a <u>"null" value in the "AuthInfo" element</u> (parameters Cavv, Eci, Xid, etc. are included – see below) </div>	
CardNumber	<p>The transaction card number with 19 digits at most.</p> <p>For e-wallet transactions, the wallet DPAN token number is sent.</p>	String
ExpirationMonth	<p>The expiration month of the card.</p> <p>For e-wallet transactions, the wallet DPAN expiration month is sent.</p>	Short integer
ExpirationYear	<p>The expiration year of the card.</p> <p>For e-wallet transactions, the wallet DPAN expiration year is sent.</p>	Short integer
Cvv2	<p>The card verification code (CVV2 ṡ CVC) usually indicated on the rear side of the card.</p> <div>  <p>Note:</p> <p>Characters should not be visible when typed by the user in the cvv2 field (e.g. asterisks should be displayed instead).</p> </div>	String

AuthInfo DATA



Note:


The «AuthInfo» element should not be included into the request message if the 3D-Secure process is not applied (see [Annex 1](#) for the available messages)




Cavv	<p>Only for Visa/Mastercard/Maestro transactions that the 3D-Secure process has been applied. It contains the value of the "Cavv" parameter returned in the 3D Secure process (see section 4).</p> <p>For e-wallet transactions, the wallet cryptogram is sent.</p>	String
Eci	<p>Only for Visa/Mastercard/Maestro transactions that the 3D-Secure process has been applied. It contains the value of the "Eci" parameter returned in the 3D Secure process (see section 4).</p> <p>For e-wallet transactions, the wallet ECI is sent.</p>	String
Xid	<p>Only for Visa/Mastercard/Maestro transactions that the 3D-Secure process has been applied. It contains the value of the "Xid" field returned in the 3D Secure process (see section 4).</p>	String
Protocol	<p>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:</p> <ul style="list-style-type: none"> 1 (for 3D Secure version 1) 2 (for 3D Secure version 2 or EMV 3D Secure) 	String
DsTransID	<p>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" parameter returned in the 3D Secure process (see section 4).</p>	String
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>	String

	<ul style="list-style-type: none"> ▪ 0: In the case of a recurring transaction executed at regular intervals ▪ 1: In the case of a recurring transaction not executed at regular intervals. 	
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
WalletType	Used if the transaction is carried out via e-wallet. Potential values: <ul style="list-style-type: none"> ▪ 1: For transactions via Google Pay ▪ 2: For transactions via Apple Pay 	String
FT_SenderLastName	<p>Sender's last name.</p> <p>Only refers to digital wallet top up transactions. (RequestType = «FUNDSTRANSFER»).</p> <ul style="list-style-type: none"> ▪ Accepts Latin uppercase and lowercase alphanumeric characters and space. ▪ Must not be all spaces or 0's. <p>Must not contain special characters (?, @, #, \$, &, *, etc.).</p>	String (max. 35 characters)
FT_SenderFirstName	<p>Sender's first name.</p> <p>Only refers to digital wallet top up transactions. (RequestType = «FUNDSTRANSFER»).</p> <ul style="list-style-type: none"> ▪ Accepts Latin uppercase and lowercase alphanumeric characters and space. ▪ Must not be all spaces or 0's. <p>Must not contain special characters (?, @, #, \$, &, *, etc.).</p>	String (max. 35 characters)
FT_SenderAddressStreet	<p>Sender's address street.</p> <p>Only refers to digital wallet top up transactions. (RequestType = «FUNDSTRANSFER»).</p> <ul style="list-style-type: none"> ▪ Accepts Latin uppercase and lowercase alphanumeric characters and space. ▪ Must not be all spaces or 0's. <p>Must not contain special characters (?, @, #, \$, &, *, etc.).</p>	String (max. 50 characters)
FT_SenderAddressStreetNumber	<p>Sender's address street number.</p> <p>Only refers to digital wallet top up transactions.</p>	String (max. 5 characters)

	(RequestType = «FUNDSTRANSFER»).	
	<ul style="list-style-type: none"> Accepts Latin uppercase and lowercase alphanumeric characters and space. Must not be all spaces or 0's. <ul style="list-style-type: none"> Must not contain special characters (?, @, #, \$, &, *, etc.). 	
FT_SenderAddressPostalCode	Sender's address Postal Code. Only refers to digital wallet top up transactions. (RequestType = «FUNDSTRANSFER»).	String (max. 5 characters)
	<ul style="list-style-type: none"> Accepts Latin uppercase and lowercase alphanumeric characters and space. Must not be all spaces or 0's. Must not contain special characters (?, @, #, \$, &, *, etc.).	
FT_SenderAddressCity	Sender's address city. Only refers to digital wallet top up transactions. (RequestType = «FUNDSTRANSFER»).	String (max. 50 characters)
	<ul style="list-style-type: none"> Accepts Latin uppercase and lowercase alphanumeric characters and space. Must not be all spaces or 0's. Must not contain special characters (?, @, #, \$, &, *, etc.). 	
FT_SenderAddressCountry	Sender's address country. Only refers to digital wallet top up transactions. (RequestType = «FUNDSTRANSFER»).	String (max. 2 characters)
	<ul style="list-style-type: none"> ISO Alpha-2 e.g., GR for Greece Must not be all spaces or 0's. Must not contain special characters (?, @, #, \$, &, *, etc.).	
FT_SenderCommunicationPhone	Sender's communication phone number. Only refers to digital wallet top up transactions. (RequestType = «FUNDSTRANSFER»).	Numeric (max. 15 characters)
	<ul style="list-style-type: none"> Accepts numeric characters. Must not be all spaces or 0's. 	

The parameters submitted as a response, are as follows:

RESPONSE PARAMETERS		
Parameter name	Description	Type
HEADER DATA		
MerchantID	The merchant identification (merchant id) submitted with the request.	Integer
SRID	<p>[Support Reference ID] Reference id of the submitted request. There is a different value per request (even if the transaction failed).</p> <div>  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. </div>	Long integer
BODY DATA		
StatusFlag	<p>The parameter value indicating whether the transaction was successful. Possible values:</p> <ul style="list-style-type: none"> ▪ 0: <u>Transaction approved</u>. The transaction response code and the corresponding description are included in «ResultCode» and «ResultDescription» parameters. ▪ 1: <u>Transaction not approved by the card Issuer</u>. The response code and the corresponding description are included in «ResultCode» and «ResultDescription» parameters. ▪ 2: There was a transaction data problem or a technical problem at epay eCommerce, so <u>the transaction was not processed by epay eCommerce</u>. Information on the nature of the problem is included in «ResultCode» and «ResultDescription» parameters. 	Integer
ResultCode	<ul style="list-style-type: none"> ▪ If StatusFlag = 0 or 1 It takes the transaction response code. The «ResultDescription» parameter contains the corresponding description. The response codes for approved transactions are: 00, 08, 10, 11, 16. ▪ If StatusFlag = 2 It takes the error code corresponding to the reason the transaction was not processed. The «ResultDescription» parameter contains the corresponding description. 	String

	 Note: The most frequent «ResultCode» values are shown in Annex 2 .	
ResultDescription	<p>The description corresponding to the «ResultCode» parameter value.</p>  Note: <ul style="list-style-type: none"> ▪ This information should not 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 relevant rule codes that may be returned. 	String
MerchantReference	The transaction reference submitted with the request.	String
ApprovalCode	If a successful transaction has been executed (i.e. when StatusFlag=0), it takes the transaction approval code.	String
TransactionID	<p>If a transaction has been executed, it takes a unique transaction id generated by epay eCommerce.</p>  Note: This value is necessary in the «TransactionReferenceID» parameter for the following transactions: <ul style="list-style-type: none"> ▪ Preauthorisation settlement ▪ Preauthorization voiding ▪ 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, sale or digital wallet top up «TransactionID»).</p>	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 StatusFlag = 0 or 1), it takes the	DateTime

	transaction execution date and time. Its value expresses the number of milliseconds after Jan 1, 1970 00:00:00 GMT in the following format e.g. : «/Date(1357219425000 +0200)/».	
TraceID	Transaction reference code generated by Visa/Mastercard; it is recommended that this code be stored by the merchant's system. <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). (For transaction types SALE, AUTHORIZE, FOLLOW_UP, FUNDSTRANSFER)	String (max. 50 characters)
Token	Tokenized transaction card (with format 888888*****) (For transaction types SALE, AUTHORIZE, FOLLOW_UP, FUNDSTRANSFER)	String
Masked Card	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). Masked Card data returned when the transaction is successful. (For transaction types SALE, AUTHORIZE, FOLLOW_UP, FUNDSTRANSFER)	String
Card Expiration Date	The expiration date of the card used in the transaction in "MM-YYYY" format, e.g. 10-2025. (For transaction types SALE, AUTHORIZE, FOLLOW_UP, FUNDSTRANSFER)	String

**Note:**

- The «**SRID**» 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**», «**ApprovalCode**» parameter values.
- The transaction decline or technical error message («**ResultDescription**») should not appear as such on the user page.

The table below shows the «Rest Web Service» parameters that must be used in the request of any transaction type.

REQUEST PARAMETERS	SALE	PREAUTHORIZATION	PREAUTHORIZATION SETTLEMENT	PREAUTHORIZATION VOIDING	REFUND	FOLLOW_UP	FUNDSTRANSFER
AcquirerID	✓	✓	✓	✓	✓	✓	✓
MerchantID	✓	✓	✓	✓	✓	✓	✓
User	✓	✓	✓	✓	✓	✓	✓
Password	✓	✓	✓	✓	✓	✓	✓
MerchantReference	✓	✓	✗	✗	✗	✓	✓
TransactionReferenceID	✗	✗	✓	✓	✓	✗	✗
CurrencyCode	✓	✓	✓	✓	✓	✗	✓
Amount	✓	✓	✓	✓	✓	✗	✓
Installments	(1)	(1)	✗	✗	✗	✗	✗
TaxCardNumber	✗	✗	✗	✗	✗	✗	✗
DeviceID	✗	✗	✗	✗	✗	✗	✗
CardType	✓	✓	✗	✗	✗	✗	✓
CardNumber	✓	✓	✗	✗	✗	✗	✓
ExpirationMonth	✓	✓	✗	✗	✗	✗	✓
ExpirationYear	✓	✓	✗	✗	✗	✗	✓
Cvv2	✓	✓	✗	✗	✗	✗	✓
Cavv	(2) (5)	(2)	✗	✗	✗	✗	(2)
Eci	(2) (5)	(2)	✗	✗	✗	✗	(2)
Xid	(2)	(2)	✗	✗	✗	✗	(2)
Protocol	(2)	(2)	✗	✗	✗	✗	(2)

DsTransID	(2)	(2)	×	×	×	×	(2)
RecurringInd	(3)	(3)	×	×	×	×	×
TraceID	(4)	(4)	×	×	×	×	×
WalletType	(5)	×	×	×	(5)	×	×
FT_SenderLastName	×	×	×	×	×	×	✓
FT_SenderFirstName	×	×	×	×	×	×	✓
FT_SenderAddressStreet	×	×	×	×	×	×	✓
FT_SenderAddressStreetNumber	×	×	×	×	×	×	✓
FT_SenderAddressPostalCode	×	×	×	×	×	×	✓
FT_SenderAddressCity	×	×	×	×	×	×	✓
FT_SenderAddressCountry	×	×	×	×	×	×	✓
FT_SenderCommunicationPhone	×	×	×	×	×	×	✓

Explanation of symbols	
Symbol	Explanation
✓	A value must be submitted
✗	The parameter should not be submitted
(1)	A value is submitted only for an installment transaction
(2)	If the 3D-secure process is not applied, the «AuthInfo» element is not submitted; otherwise, the parameter value depends on the cardholder authentication process result («3d-secure» process) – see section 4
(3)	A value is submitted in case of a recurring transaction.
(4)	A value is submitted after the second recurrence of a recurring transaction.
(5)	A value is submitted in case of an e-wallet transaction.

The chart below shows the sequence in which the various transaction types may be used. As shown on the chart, specifically, the following applies:

- A preauthorization may either be settled for an amount lower than or equal to the preauthorization amount, or voided for an amount equal to the preauthorization amount.
- A preauthorization that has been settled, may be refunded 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 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 digital wallet top up transaction («FUNDSTRANSFER»), may be cancelled (REFUND) for an amount equal to the top up amount.
- A FOLLOW_UP transaction may be used at any time to return the details of a request already submitted provided that a cancellation/refund has not been carried out for that transaction.



Note:

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

- Preauthorization settlement
- Preauthorization voiding
- Sale or settlement or digital wallet top up 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.

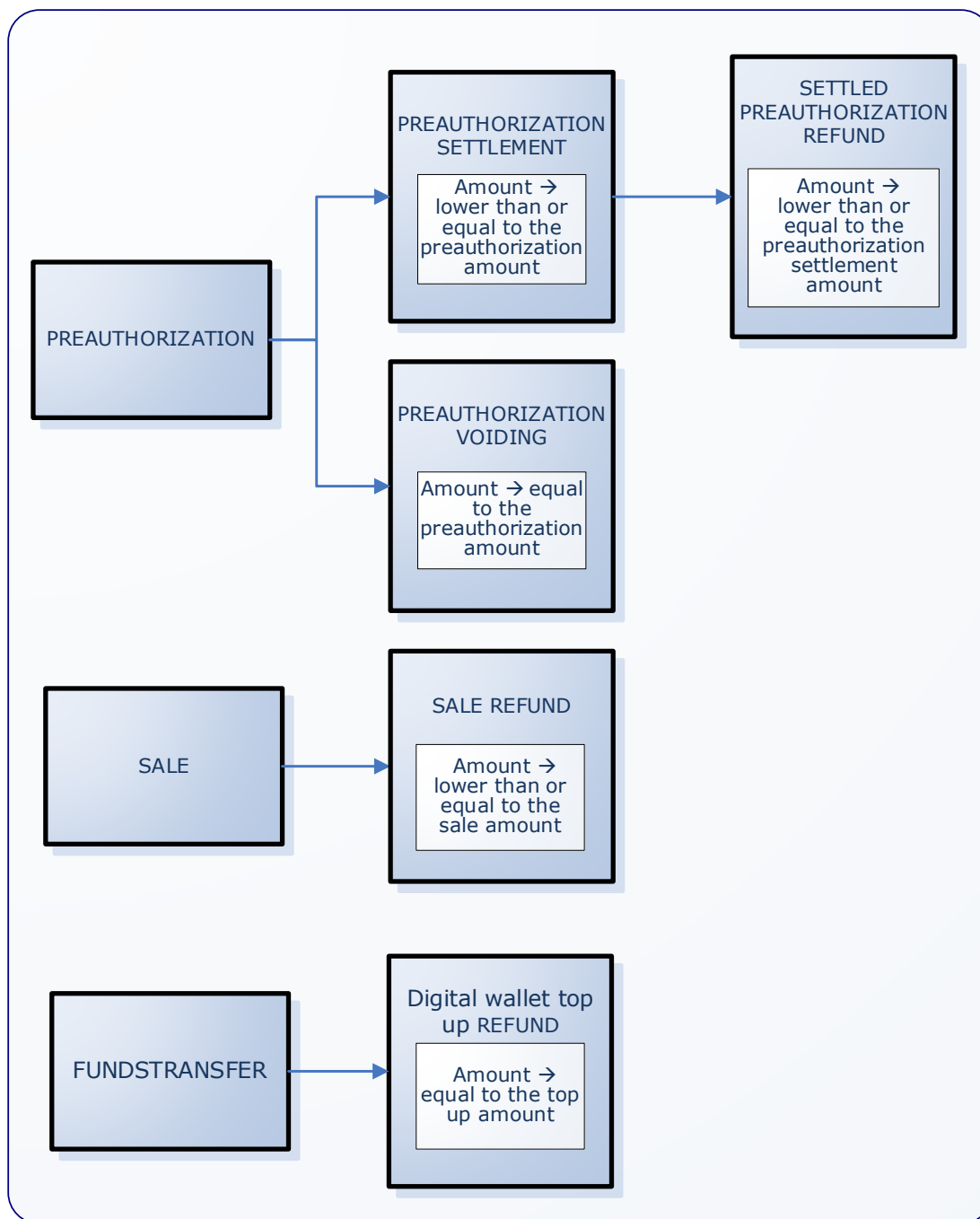


Chart 2: Transaction sequence



6. Merchant Application Action Flow

Following the analysis of the individual process modules to be implemented (cardholder authentication process and transaction submission to epay eCommerce), the flow of actions to be performed by the merchant application in collaboration with epay eCommerce, for a transaction to be executed, is illustrated in the flowchart below.

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.

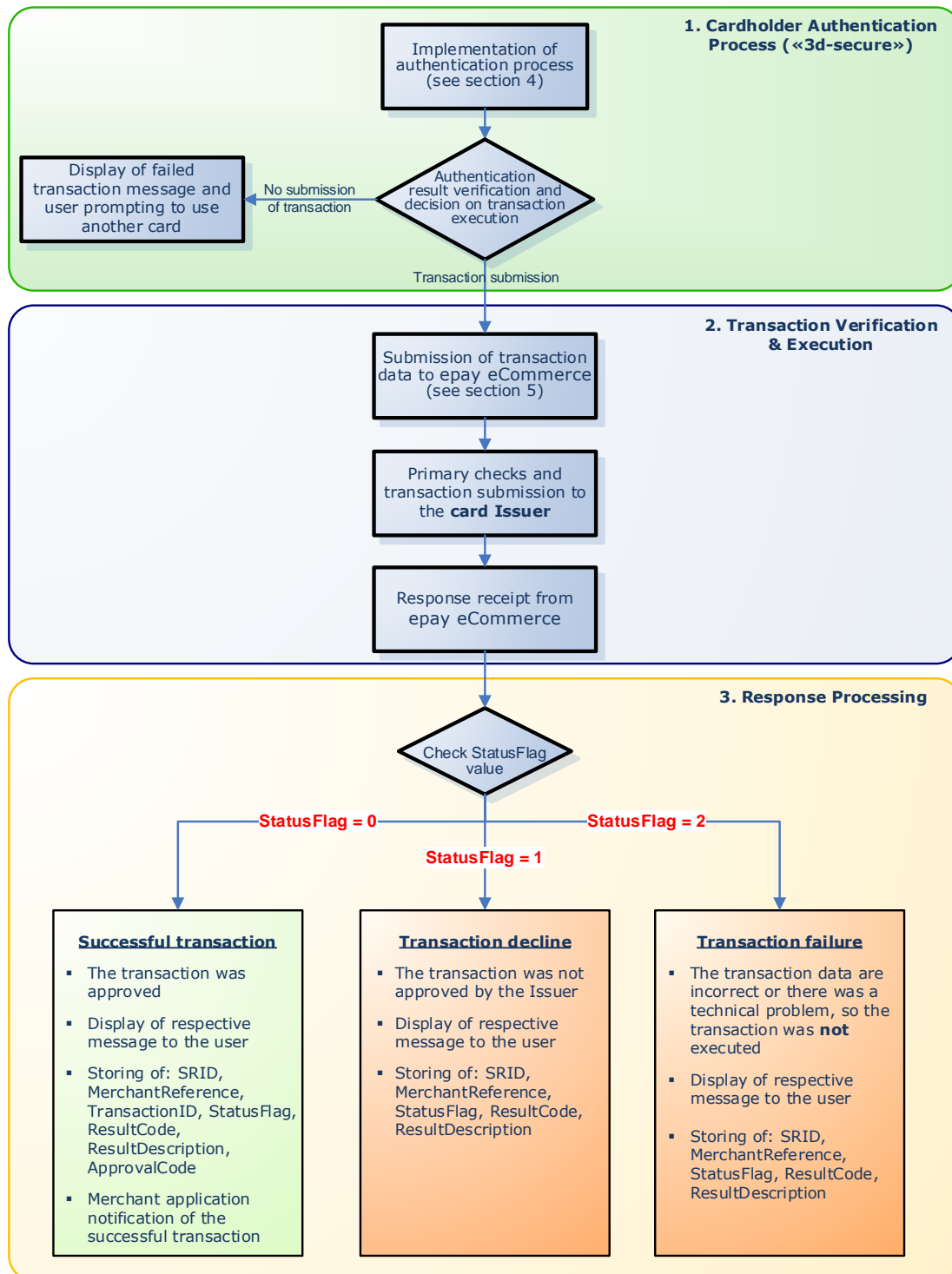


Chart 3: Merchant application actions

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

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

For preauthorization, sale or digital wallet top up transactions using a Visa, Mastercard or Maestro card, the strong customer authentication process is carried out (see section 4). Depending on the authentication process result, the merchant application decides whether to submit the transaction to epay eCommerce or not.



Attention!

The authentication process is only used for online **sale, preauthorization** or **digital wallet top up** transactions with Visa, Mastercard or Maestro card.

2. Transaction Verification & Execution

The merchant system uses the «Rest Web Service» to submit the transaction data to epay eCommerce (see section 5). 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 StatusFlag = «0»**, then **the transaction was successful**, thus the transaction information, such as SRID, MerchantReference, TransactionID, StatusFlag, ResultCode, ResultDescription, ApprovalCode should be stored and the merchant system notified of the successful transaction.
- **If StatusFlag = «1»**, then the transaction was executed but **not approved by the card Issuer**. If necessary, the details of the unsuccessful transaction (SRID, MerchantReference, StatusFlag, ResultCode, ResultDescription) are stored in the merchant system.
- **If StatusFlag = «2»**, 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 (SRID, MerchantReference, ResultCode, ResultDescription) are stored in the merchant system.



Attention!

The «SRID» 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 message («ResultDescription») should not appear as such on the user page.



7. Rest 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 Rest 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.

If the 3d-secure process is used, it must be applied first (see 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
Test case 16	APPROVED FUNDSTRANSFER	NO

The following applies to all test cases:

- The «AcquirerID», «MerchantID», «User» and «Password» parameter values are provided by Euronet Merchant Services.
- The URL that the request is submitted depends on the transaction type (see section 5).
- The «Amount» parameter may take any valid value (see section 5).
- The «Installments», «CurrencyCode», «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 Rest Web Service) **within 30 days** for the transaction to be settled.

**Test Case 1: APPROVED TRANSACTION (VISA)****MANDATORY**

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

**It is applicable:**

When StatusFlag=0

**Input parameters:**

Parameter	Value
Currency	978
Installments	0 or do not send it
CardType	VISA or UNKNOWN
CardNumber for sale	490845555555557
CardNumber for preauthorization	4020680000000098
ExpirationMonth	01
ExpirationYear	Any future year
CVV2	123

**Response parameters:**

Parameter	Value
StatusFlag	0
ResultCode	00

**Merchant application actions:**

- Display of transaction approval message on the user page
- Storing of SRID, MerchantReference, TransactionID, StatusFlag, ResultCode, ResultDescription, ApprovalCode parameter values
- Merchant application update for the successful transaction



Test Case 2: DECLINED TRANSACTION

MANDATORY

Scenario: Decline of a transaction



It is applicable:

When StatusFlag=1



Input parameters:

Parameter	Value
Currency	978
Installments	0 or do not send it
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
StatusFlag	1
ResultCode	12



Merchant application actions:

- Display of transaction decline message received from Issuer on the user page
- Storing of SRID, MerchantReference, StatusFlag, ResultCode, ResultDescription 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 = 2 and ResultCode = 1048



Input parameters:

Parameter	Value
Currency	978
Installments	0 or do not send it
CardType	VISA or UNKNOWN
CardNumber for sale	490845555555557
CardNumber for preauthorization	4020680000000098
ExpirationMonth	03
ExpirationYear	<i>Any future year</i>
CVV2	123



Response parameters:

Parameter	Value
StatusFlag	2
ResultCode	1048



Merchant application actions:

- Display of a transaction failure message on the user page
- Storing of SRID, MerchantReference, StatusFlag, 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 StatusFlag=2 and ResultCode = 50x (i.e. 500, 501 etc.)



Input parameters:

Parameter	Value
Currency	978
Installments	0 or do not send it
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
StatusFlag	2
ResultCode	500



Merchant application actions:

- Display of a transaction failure message on the user page (with a prompt to try again later)
- Storing of SRID, MerchantReference, StatusFlag, ResultCode, 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 StatusFlag=2 and ResultCode = 981



Input parameters:

Parameter	Value
Currency	978
Installments	0 or do not send it
CardType	VISA or UNKNOWN
CardNumber for sale	4908455555555557
CardNumber for preauthorization	4020680000000098
ExpirationMonth	05
ExpirationYear	<i>Any future year</i>
CVV2	123



Response parameters:

Parameter	Value
StatusFlag	2
ResultCode	981



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 SRID, MerchantReference, StatusFlag, ResultCode, 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 StatusFlag=2 and ResultCode = 1045



Input parameters:

Parameter	Value
Currency	978
Installments	0 or do not send it
CardType	VISA or UNKNOWN
CardNumber for sale	4908455555555557
CardNumber for preauthorization	4020680000000098
ExpirationMonth	06
ExpirationYear	Any future year
CVV2	123



Response parameters:

Parameter	Value
StatusFlag	2
ResultCode	1045



Merchant application actions:

- Display of a transaction failure message on the user page (with a prompt to try again later)
- Storing of SRID, MerchantReference, StatusFlag, ResultCode, 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 StatusFlag=2 and ResultCode = 1072



Input parameters:

Parameter	Value
Currency	978
Installments	0 or do not send it
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
StatusFlag	2
ResultCode	1072



Merchant application actions:

- Display of a transaction failure message on the user page (with a prompt to try again later)
- Storing of SRID, MerchantReference, StatusFlag, ResultCode, 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 StatusFlag=2 and ResultCode = 1



Input parameters:

Parameter	Value
Currency	978
Installments	0 or do not send it
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
StatusFlag	2
ResultCode	1



Merchant application actions:

- Display of a transaction failure message on the user page (with a prompt to try again later)
- Storing of SRID, MerchantReference, StatusFlag, ResultCode, 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 StatusFlag=0



Input parameters:

Parameter	Value
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
StatusFlag	0
ResultCode	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 SRID, MerchantReference, TransactionID, StatusFlag, ResultCode, ResultDescription, ApprovalCode 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 StatusFlag=0



Input parameters:

Parameter	Value
Currency	978
Installments	0 or do not send it
CardType	MasterCard or UNKNOWN
CardNumber for sale and for preauthorization	519499333333335
ExpirationMonth for sale	01
ExpirationMonth for preauthorization	02
ExpirationYear	<i>Any future year</i>
CVV2	123



Response parameters:

Parameter	Value
StatusFlag	0
ResultCode	00



Merchant application actions:

- Display of transaction approval message on the user page
- Storing of SRID, MerchantReference, TransactionID, StatusFlag, ResultCode, ResultDescription, ApprovalCode 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 StatusFlag=0



Input parameters:

Parameter	Value
Currency	978
Installments	0 or do not send it
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 not include the «AuthInfo» element (it contains the Cavv, Eci, Xid elements – see section 5.)



Response parameters:

Parameter	Value
StatusFlag	0
ResultCode	00



Merchant application actions:

- Display of transaction approval message on the user page
- Storing of SRID, MerchantReference, TransactionID, StatusFlag, ResultCode, ResultDescription, ApprovalCode 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 StatusFlag=0



Input parameters:

Parameter	Value
Currency	978
Installments	0 or do not send it
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 not include the «AuthInfo» element (it contains the Cavv, Eci, Xid elements – see section 5.)



Response parameters:

Parameter	Value
StatusFlag	0
ResultCode	00



Merchant application actions:

- Display of transaction approval message on the user page
- Storing of SRID, MerchantReference, TransactionID, StatusFlag, ResultCode, ResultDescription, ApprovalCode 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 StatusFlag=0



Input parameters:

Parameter	Value
Currency	978
Installments	0 or do not send it
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 not include the «AuthInfo» element (it contains the Cavv, Eci, Xid elements – see section 5.)



Response parameters:

Parameter	Value
StatusFlag	0
ResultCode	00



Merchant application actions:

- Display of transaction approval message on the user page
- Storing of SRID, MerchantReference, TransactionID, StatusFlag, ResultCode, ResultDescription, ApprovalCode 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 StatusFlag=0



Input parameters:

Parameter	Value
Currency	826
Installments	0 or do not send it
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



Response parameters:

Parameter	Value
StatusFlag	0
ResultCode	00



Merchant application actions:

- Display of transaction approval message on the user page
- Storing of SRID, MerchantReference, TransactionID, StatusFlag, ResultCode, ResultDescription, ApprovalCode 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 StatusFlag=0



Input parameters:

Parameter	Value
Currency	840
Installments	0 or do not send it
CardType	VISA or UNKNOWN
CardNumber for sale and for preauthorization	4908456666666663
ExpirationMonth for sale	03
ExpirationMonth for preauthorization	04
ExpirationYear	<i>Any future year</i>
CVV2	123



Response parameters:

Parameter	Value
StatusFlag	0
ResultCode	00



Merchant application actions:

- Display of transaction approval message on the user page
- Storing of SRID, MerchantReference, TransactionID, StatusFlag, ResultCode, ResultDescription, ApprovalCode parameter values
- Merchant application update for the successful transaction



Test Case 16: APPROVED FUNDSTRANSFER

OPTIONAL

Scenario: Approval of digital wallet top up transaction (funds transfer)



It is applicable:

When StatusFlag=0



Input parameters:

Parameter	Value
Currency	978
CardType	VISA or UNKNOWN
CardNumber	490845555555557
ExpirationMonth	12
ExpirationYear	<i>Any future year</i>
CVV2	123



Response parameters:

Parameter	Value
StatusFlag	0
ResultCode	00



Merchant application actions:

- Display of transaction approval message on the user page
- Storing of SupportReferenceID, MerchantReference, TransactionID, StatusFlag, ResultCode, ResultDescription, ApprovalCode 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:

- It is strongly recommended to use a client certificate in order for Euronet Merchant Services to authenticate and authorize the merchant application that submits transactions to epay eCommerce.
- 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 it's about a web application, 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.
- If it's about a web application, the use of ssl on the card details entry page 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.
- 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

It is necessary to display the icons of supported cards on the mobile application. Furthermore, if the cardholder authentication process is applied («3D-Secure» – see section 4), the relevant icons should be displayed on the page where the user enters his card details.

All relevant material can be downloaded from the following link:

<https://www.epayworldwide.gr/wp-content/uploads/2022/10/Icons.zip>

Specifically:

Supported cards 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>)

3D-Secure icons

If the 3D-Secure process is applied, the following icons must be displayed:

- **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 can optionally be displayed on the application. The relevant icons are included in the icons/epay folder.

10. Tips

Below, there are some remarks-tips which must be taken into account:


- 💡 A **preauthorization transaction** can be completed by the merchant (either via the epay eCommerce AdminTool or by calling the Rest Web Service) within **30 days**. After that period of time, the preauthorization cannot be either completed or cancelled.
- 💡 **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 «Rest Web Service» (see section 5) must be sent encrypted with the MD5 hashing algorithm.
- 💡 The «**MerchantReference**» parameter in the «Rest Web Service» should be unique for each successful sale, preauthorization or digital wallet top up 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 Rest 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 «**SRID**» parameter should be stored with every attempt and be available to the merchant managers, so that it may be used in the communication with Euronet Merchant Services to solve potential problems. The same parameter must be sent by technical managers to Euronet Merchant Services in the event of problems during the test transactions.
- 💡 Interest-free installments are supported only for some cards issued by Greek banks (depending on the BIN, i.e. the first 6 digits of the card). Euronet Merchant Services provides the «BIN Web Service» 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 epay eCommerce is interrupted and no response is received by the merchant system, a «REFUND» request may be submitted

sending a value in the «**MerchantReference**» parameter instead of the «**TransactionReferenceID**» parameter. This functionality is available only for transaction cancellations (i.e. cancellations of transactions in an open batch).



> 11. Implementation Checklist

	TASK
1.	CONTRACT SIGNING Signing of acquiring contract for the «Rest 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 «Rest Web Service»
3.	TEST ACCOUNT INFORMATION SUBMISSION Submit the required information to Euronet Merchant Services to create a test account (see section 3)
4.	PERFORMANCE OF TEST TRANSACTIONS <ul style="list-style-type: none">■ Euronet Merchant Services forwards test account details:<ul style="list-style-type: none">■ AcquirerID■ MerchantID■ User■ Password■ <u>Only if the 3D-Secure process is applied</u>: Execution of all test cases of the 3D Secure process (see relevant documentation).■ Perform test transactions using the «Rest Web Service» (see section 7).
5.	USE OF ICONS Post the necessary icons on the merchant application (see section 9)
6.	COMPLETION OF TEST TRANSACTIONS <ul style="list-style-type: none">■ Inform Euronet Merchant Services about the successful completion of the test transactions and the use of icons and ssl (if it's about a web application) submit the test transactions data to be checked by Euronet Merchant Services. In particular, submit the following:<ul style="list-style-type: none">○ the "MerchantReference" value for each test case of the 3D Secure process (see relevant documentation).

	<ul style="list-style-type: none"> ○ The "SupportReferenceID" value of each test case where the Rest 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 . ■ Send to Euronet Merchant Services an email address belonging to the merchant; this email address will be used for informational purposes about epay eCommerce. ■ The technical manager informs the merchant about the completion of the test transactions
7.	<div>➡ LIVE ACCOUNT RECEIPT</div> <ul style="list-style-type: none"> ■ Euronet Merchant Services forwards live account details: <ul style="list-style-type: none"> ■ AcquirerID ■ MerchantID ■ User ■ Password ■ Replace the test account details with the live account details. <div>  Note: The URLs of Rest Web Service are the same for both test and live transactions (see section 5). </div>

Annex 1


Samples of all possible JSON request and response messages that may be sent/received by Rest Web Service are included in the **RestWS samples** folder in the technical specifications.


> Annex 2

The table below shows the most frequent values of the «ResultCode» parameter in case the transaction was not carried out due to a technical problem (i.e. the «ResultCode» parameter expresses an error code → StatusFlag = 2), as well as in case the transaction was normally processed (i.e. the «ResultCode» expresses a response code → StatusFlag = 0 or 1).

ResultCode FREQUENT VALUES WHEN StatusFlag=2 (Error Codes)			
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» and/or «Password» parameter	Use correct values in «Username» 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 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	Check if the preauthorization is finally settled using epay eCommerce AdminTool.

		which has 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 provided by	Check the server's IP address and if it's necessary, contact Euronet Merchant Services in order to change the IP

		the technical Manager to Euronet Merchant Services	address that corresponds to the specific merchant id.
1042	Refund maximum allowed period exceeded	Attempted refund after the allowed period.	Contact Euronet Merchant Services .
1045	Duplicate transaction references are not allowed	The request sent had the same «MerchantReference» value 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 error code «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	<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>

		with the merchant, Euronet Merchant Services will provide the relevant rule codes that may be returned.	
9150	Wallet transaction in request message is not supported	<p>The request was sent:</p> <ul style="list-style-type: none"> ▪ with unsupported wallet type ▪ with unsupported card type ▪ with unsupported transaction type ▪ with installments ▪ with recurring payments indicator 	Re-send the transaction using correct values in parameters.
9151	Wrong FundsTransfer Parameters	<p>Refers to digital wallet top up transactions. («FUNDSTRANSFER»). No value or value that does not meet the requirements at one or more of the following parameters:</p> <ul style="list-style-type: none"> ▪ FT_SenderLastName ▪ FT_SenderFirstName ▪ FT_SenderAddressStreet ▪ FT_SenderAddressStreetNumber ▪ FT_SenderAddressPostalCode ▪ FT_SenderAddressCity ▪ FT_SenderAddressCountry FT_SenderCommunicationPhone 	Re-send the transaction using correct values in parameters.
9152	FundsTransfer in request message is not supported	<p>Refers to merchant that doesn't support digital wallet top up («FUNDSTRANSFER»). The request was sent with unsupported transaction type.</p>	Contact Euronet Merchant Services.

9156	Transaction Type in request message is not supported	Refers to merchant that only supports digital wallet top up («FUNDSTRANSFER»).	Contact Euronet Merchant Services.
9153	Loyalty is not supported for FundsTransfer	Refers to merchant that only supports digital wallet top up («FUNDSTRANSFER»).	Contact Euronet Merchant Services.
9154	Installments are not supported for FundsTransfer	The request was sent with unsupported transaction type.	
9155	Recurring Transactions are not supported for FundsTransfer	Refers to merchant that only supports digital wallet top up («FUNDSTRANSFER»).	Contact Euronet Merchant Services.
		The request was sent with Loyalty data.	
		The request was sent with installments.	
		The request was sent with recurring payments indicator	

ResultCode FREQUENT VALUES WHEN StatusFlag=0 or 1 (Response Codes)				
ResponseCode	ResponseDescription	Explanation	Action	Transaction approval
00, 08, 10, 16	Approved or completed successfully	Transaction approval	Sale approval	Yes
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 Organization (Visa, Mastercard etc)	Try again later when the problem has been rectified	No
12	Installment amount bellow allowed minimum	It concerns installment transactions; the	Use o lower number of installments	No

		individual installment value is lower than the allowed minimum		
--	--	--	--	--



Note:

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

> Annex 3

Below there is a list of all 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. In this case, Euronet Merchant Services.
BIN	The first 6 digits of a card designating the Issuer Bank.
Live account	The merchant account through which live transactions are executed. It is made up of the following components: <ul style="list-style-type: none">▪ AcquirerID▪ MerchantID▪ User▪ Password
Merchant id	The «merchant identification».
Test account	A test account provided by Euronet Merchant Services to enable test transactions. It is made up of the same components as a «live account» but has different values.
Rest Web Service	Euronet Merchant Services Web Service via which transactions are submitted to epay eCommerce.
epay eCommerce	Euronet Merchant Services' e-payment system.