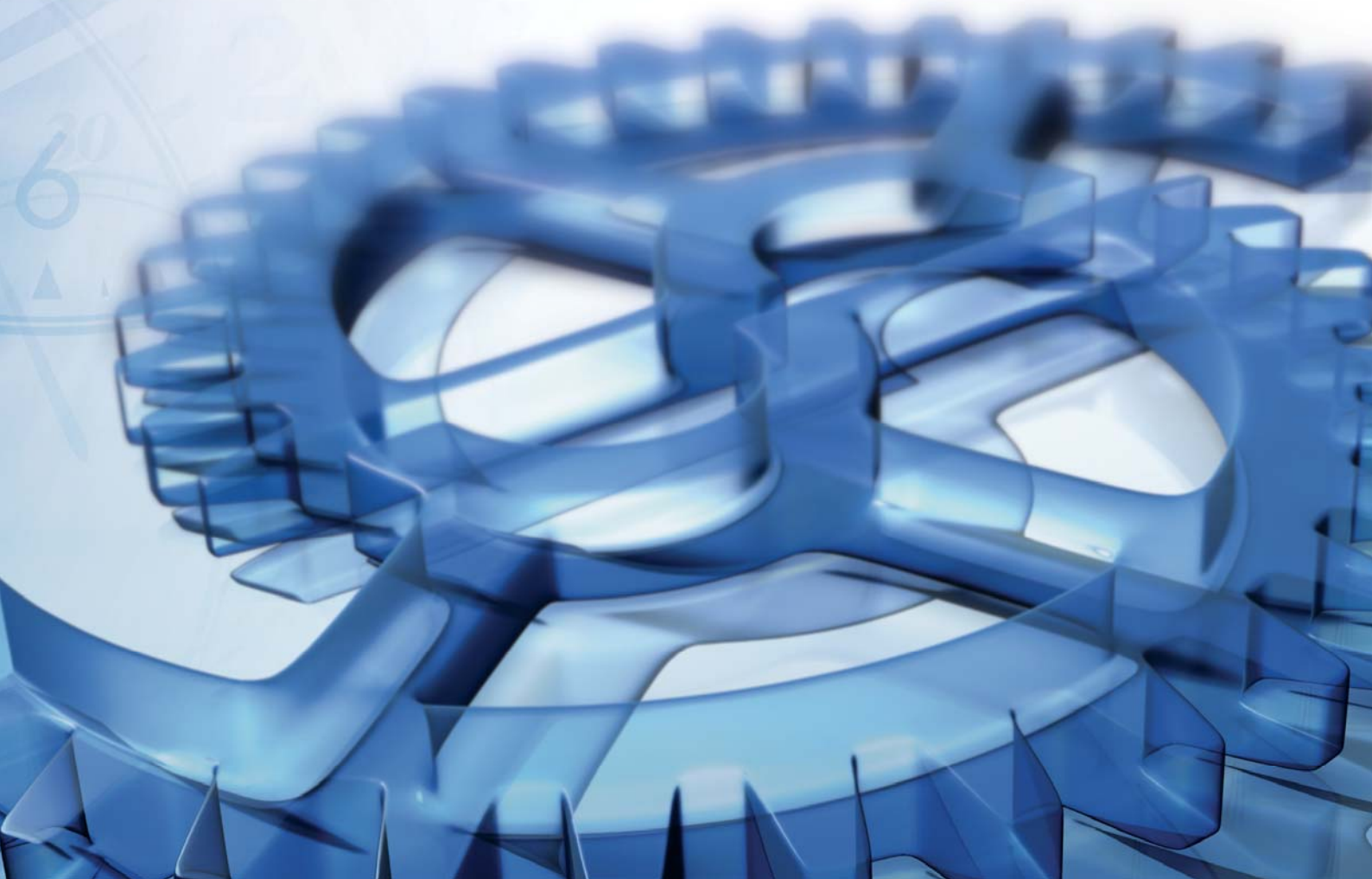
CHRONOPAY

a new gear of e-commerce

Integration Manual

Connection to ChronoPay's payment page v1.4



This document has been created by the ChronoPay. Its contents may be changed without prior notice.

Version 1.4
Last Updated: November 2007

Contact information
For questions relating to this document please contact:

ChronoPay B.V.
Strawinskylaan 1443
World Trade Center, C tower, 14th floor
1077 XX Amsterdam
Phone: +31 20 7940110
E-mail: sales@chronopay.com

1. Introduction

This instruction manual describes the technical aspects of payments processing using ChronoPay's hosted payment page.

ChronoPay is an online payment processor for e-commerce transactions and provides the following functions:

- Payment processing
- Merchant account
- Security of payment data
- Fraud management and screening
- Customer support during the initial process of payment and re-billing processing.
- Customer Refund service
- Chargeback monitoring service

The manual describes how a connection can be made with ChronoPay's hosted payment page.

2. Payment page

With this technical connection the customer is sent from the merchant's online shop to ChronoPay's payment page residing on our server. The customer fills in their payment details and is then redirected back to the merchant's website. You do not have to buy an SSL certificate. The payment page is HackerSafe certified. The payment page can be customized to the look and feel of your website.

2.1 Supported languages

Currently our standard payment interface is available in the following languages:

- English
- Dutch
- German
- Russian
- Spanish

Languages can be set via a submitting a specific language code.

If you would like the payment interface to be in a different language please contact your Account Manager.

2.2 Supported character sets

ISO-8859-1, cp-1251, iso-8859-13 page encodings are supported.

2.3 Transaction processing sequence

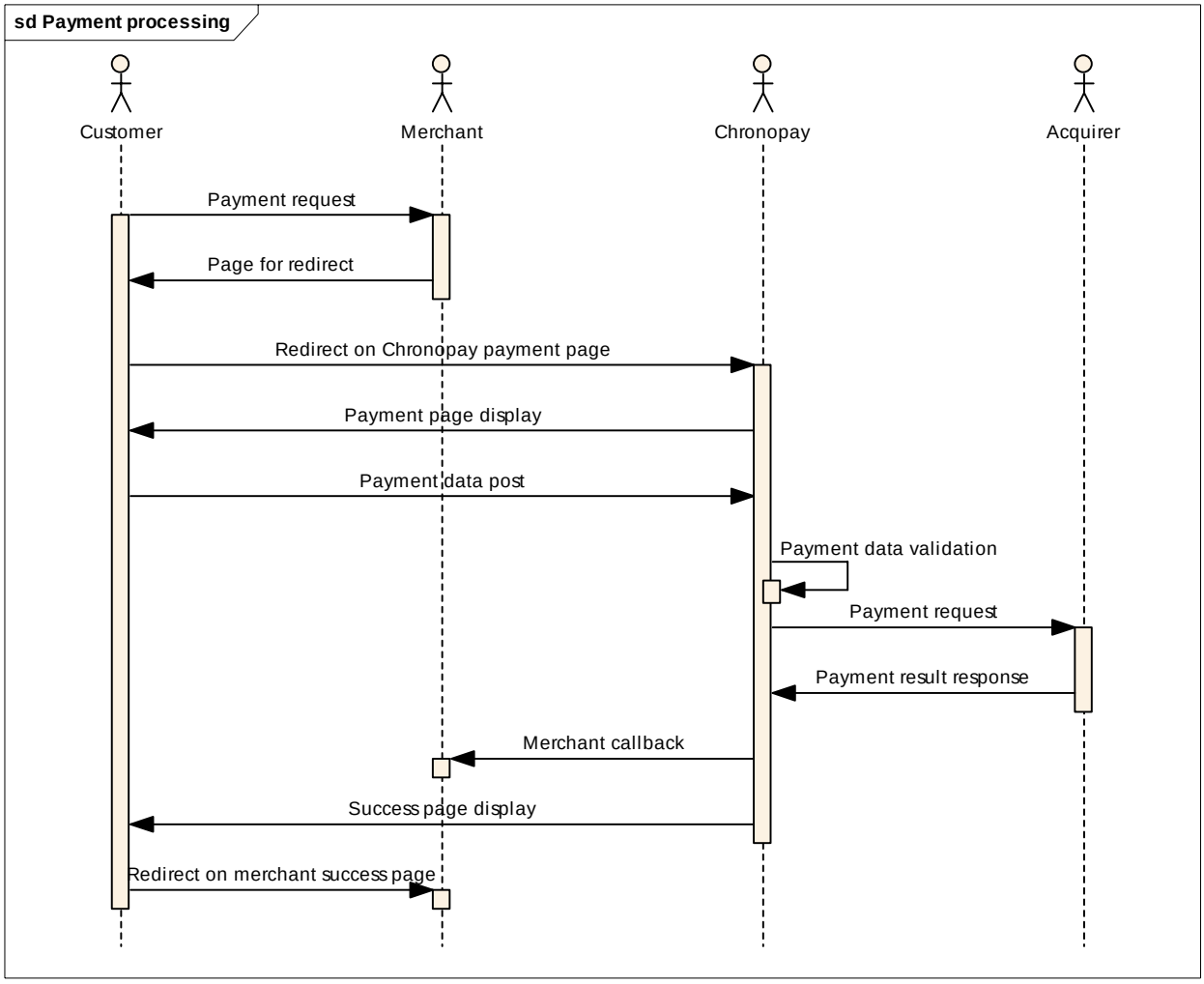


Fig. 1 Payment processing scheme

The payment process consists of the following steps:

1. The customer fills in an online form on the Merchant's website and sends a payment request.
2. The Merchant's website then redirects the Customer to the ChronoPay payment page. Required parameters are sent by the Customer's browser using GET or POST request.
3. ChronoPay displays the payment form based on the data provided by the Merchant.
4. After filling in the fields on the payment form, the transaction data are being passed onto the ChronoPay's system.
5. ChronoPay validates data and checks its integrity using sophisticated fraud prevention tools.
6. If all validations and fraud prevention checks are passed successfully, ChronoPay requests the payment from the Acquirer.
7. Acquirer returns a result code to ChronoPay.
8. ChronoPay invokes Client system to report the result of the payment. If the Customer's browser is still open and has JavaScript turned on, Customer will be redirected to the link sent in request parameter.

2.4 Example standard payment page

Below you can find an example of the standard ChronoPay's hosted payment page. The payment is both SSL and HackerSafe certified.

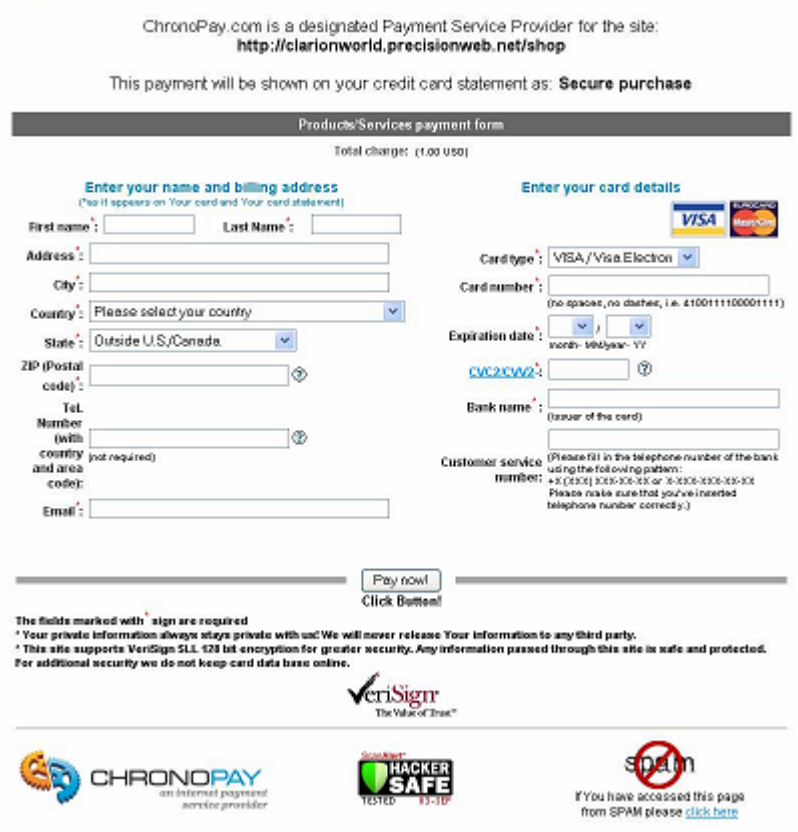


Fig. 2. Example standard payment page

This is a link to the live environment of the example payment page:

https://secure.chronopay.com/index_shop.cgi?product_id=003325-0001-0001&product_price=1

3. Client admin

3.1 Introduction

ChronoPay supplies merchants with a comprehensive and user-friendly interface that makes it possible to manage easily your transactions and update the account parameters.

ChronoPay's transaction management and reporting tool, provides full visibility of all payments across multiple accounts, payment methods and channels. The transactions are displayed in real time, allowing every transaction request to be enriched with additional data - such as transaction id, customer id, IP address and email address. It is easy and fast to find each transaction.

With SSL-encrypted access to the back office over the Internet, no software installation is necessary.

Your Account Manager will supply you with the login details in order to enable you to have access to the client admin. In the admin you are able to set various functions, such as recurring transactions.

This is the link to the client admin: https://clients.chronopay.com/

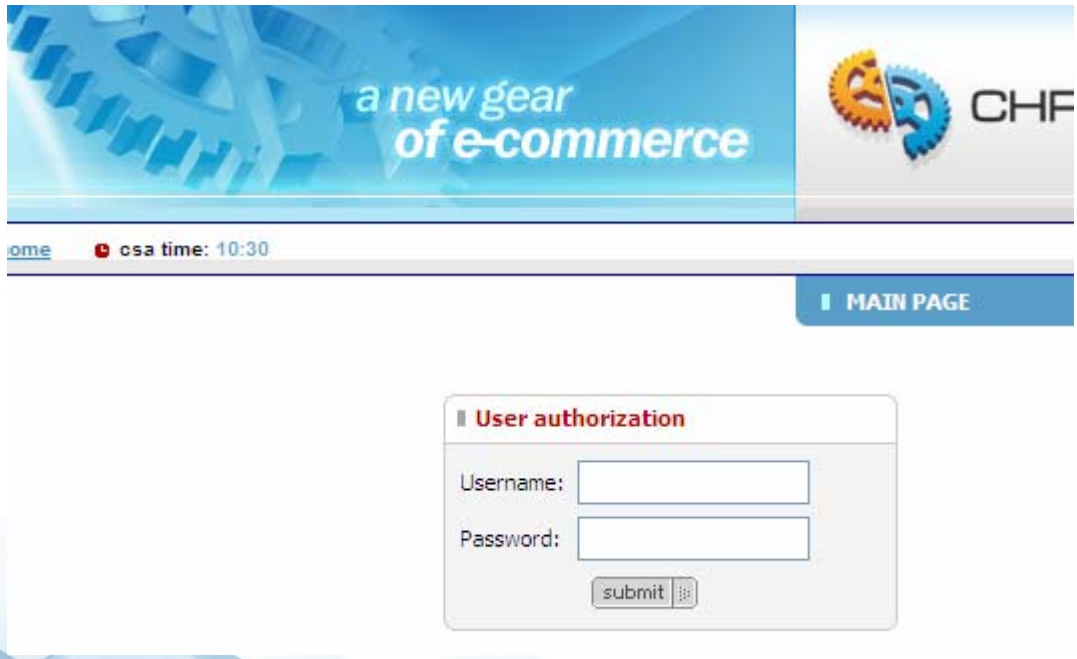


Figure 3. Back office entry

3.2 Sections within the client admin

The client admin consists of the following sections:

- **Sales**
- **Payout info**
- **Client support**
- **Set up**
- **Customer Service**
- **Rebills info**
- **Virtual terminal (optional)**

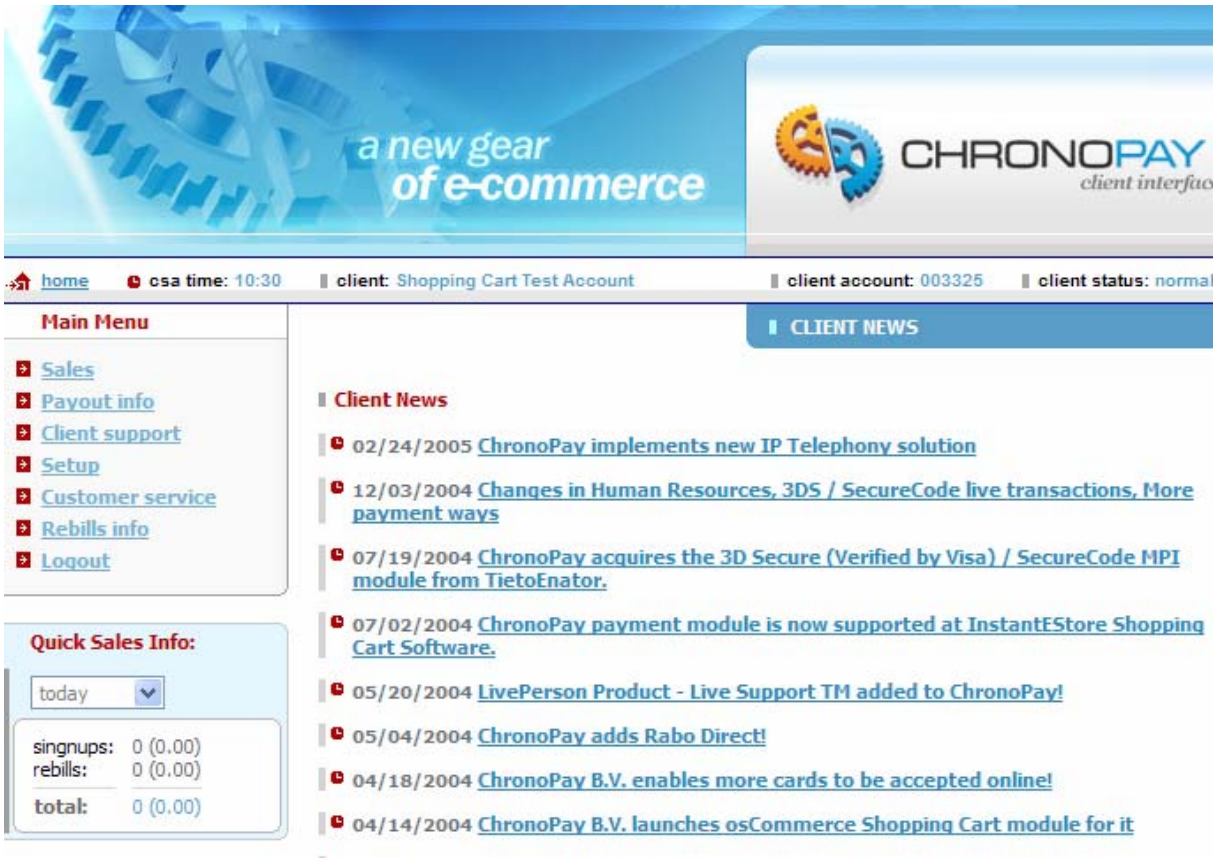


Fig. 4 Back office

Sales
This section provides you with sales statistics (total sales, detailed sales, expected rebills, chargebacks and refunds). Each choice is represented as a separate section with a submission button (grey one) on top. You are able to correct field values (represented by a default) and after clicking on appropriate submission button corresponding statistics will be shown.

Payout info
The payout information section will provide you with a list of invoices, approximate future payout calculations and the rolling reserve status. You are able to change the payouts set up.

Client Support

Through this link you will be able to open a ticket with ChronoPay Customer Support and a list of recently opened tickets will be showed.

Set up
The set up section allows you to view and update your personal details, sites and product list.

Customer service
This part of Interface is to be used for purchases history retrieval, rebill cancellation, transactions refund/reversal, clients e-mail list generation and manual addition of username/password (when it was not successful due to some reasons).

There are also functions used to refund or reverse transactions by a specified transaction ID. 'Refund' is used for transactions that were made one or more days ago, 'Reverse' is used for transactions that are made on present day.

Rebills info
In this section the merchant is able to activate and set recurring transactions.

Virtual terminal (optional)

This allows you to manually process credit or debit card numbers collected by telephone, fax or post. You can enter customer details and card numbers into a web based payment terminal.

For a complete overview of the back office functions you can take a look at the demo which is available on ChronoPay's website:

http://www.chronopay.com/demo-client-admin-en.html.

4. Test account

Any merchant planning to integrate ChronoPay's payment platform can test it with the use of a test account. It is recommended to do the integration first in our testing environment before upgrading it to the production environment. Our testing environment is a payment interface that works exactly like our live interface, except that no transaction request is sent to the credit card acquirer, and we do not bill you to use it. So you can freely make test payments, change the configuration of your account, fine-tune the integration of our payment system into your e-Commerce application before you start to process real payments.

4.1 Open your test account

Merchants can either choose to run test transactions via a dedicated test account or via the account which later will be set into live mode. In order to open a test account you can contact an Account Manager via sales@chronopay.com.

4.2 Configure your account

Your Account Manager will offer you a test account which is already configured.

4.3 Request activation

Once you have added a product and a site you can ask your Account Manager to activate your account. Usually you are already be provided with an active test account and you do not need to ask for activation.

4.4 Integration

Chapter 5 describes how a technical connection can be created with ChronoPay's payment page.

4.5 Make a test payment

Once the connection has been created you are able to test it. With the credit card details below you can make test transactions:

Credit card Visa #: 4296010582436758
CVV: any
Expiry date: now + 1 month

Please Note
These test transactions will not be shown in the client admin and can only be done in US Dollars. In the live mode other currencies will be activated as well.

When you fill in your email address in the payment form you will receive a transaction receipt by email. However, the transaction id will not be created in test mode and will therefore not been shown in the receipt.

4.5 Troubleshooting

In case of questions you can contact your Account Manager directly or via sales@chronopay.com.

5. Technical integration

After the sales process in which the merchant has applied for a merchant account/ IPSP solution, an account in our system will be created. You will not only receive login details for access to the client admin, but also your unique id's within our system. These id's are examples:

Client id	Unique client id	003325
Site id	Unique website id	003325-0001
Product id	Unique product id	003325-0001-0001

5.1 Set your account

Your account can be set within the client interface on https://clients.chronopay.com/. Within the "Set up" section your website(s) can be registered as well as your products.

5.1.1 Add sites to client admin

New account

Upon registration, the Merchant can register any necessary number of websites. The sites serve as a virtual storage area for products offered by the client, and their physical representation as a fixed link is not obligatory. Every

Every site id is linked to a website with processing for all credit cards. This can only be set for one specific currency. If you would like to process credit card payment in both EUR and USD two site id's will be created. Local payment methods, such as iDEAL, also have their own site id in our system. This will already be set when your Account Manager will send you the login details of your account.

Add new sites to existing account
When you already have an account with ChronoPay and you would like to process payments for a new website as well it is possible to add a website. One condition is that it must offer the same type of product as offered on the other website(s).

In this section of the Interface a list of sites is shown which are actually registered. In order to add the new website, login to the client admin and go to "Set up" and click on "List your sites". Subsequently click on "Add New Site". Once a new site is submitted, it has an 'inactive' status. When a site has been added, you will need to contact your Account Manager. He or she will contact our specialists from the Risk department who will review the submitted website and manually approve it.

The following fields will have to be filled in when you add a new website:

Site name
A name that identifies your project. The exact text structure represented in this field is not relevant (just for information).

Site main URL
The URL of the site where the product or services are being offered (e-commerce site). This URL will be visited by ChronoPay sales personnel for approval.

Password script URL
The URL of the script that is used additionally for the customers to the members/restricted zone of the site.

Password script secure key
A key (password) to identify the authority of ChronoPay for password addition.

FTP
The fields FTP, FTP username, FTP password are reserved for future use.

Does this site need login control?
To be checked if site is offering membership access, thus password management from ChronoPay is required.

In case you do not need to set up any restriction on access then the following can be filled in:

Password script URL:	"https://nothing.no
Password script secure key:	000
FTP:	ftp://nothing.no
FTP username:	ftp://nothing.no
FTP password:	none
Does this site need login control?:	none

5.1.2 Add products to client admin

The merchant's products do not need approval by one of our representatives - you can register as many products as you wish.

In regards to the products offered in its store, the merchant can choose to work via two possible technical set ups:

1. Predefined price product mode (a product id for each separate product)

The merchant will need to register all products separately in our system. This means that you have to transmit only a code of the product preliminarily registered in our system and our system will automatically charge customer's credit card with the required amount.

This mode operates via the https://secure.chronopay.com interface.

2. Generic price product mode (one product id representing many products)

The merchant will only register one product within the system. However, one product id represents many products. This means that product's price along with it's code will be transmitted by a script to our system and customer's credit card will be charged according to these parameters.

This mode operates via https://secure.chronopay.com/index_shop.cgi interface.

In most cases the second scheme is preferable. Not only is it the simplest solution, but

also it eliminates the need for continuous synchronization with the user website's set of products.

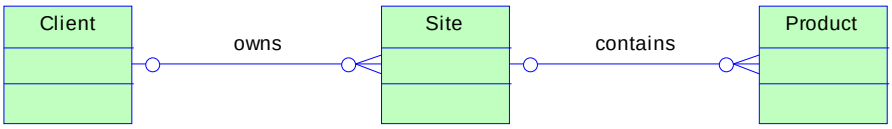


Illustration 4 Correlation of user information

In order to add a new product, login to the client admin and go to "Set up" and click on "List your products". Subsequently click on "Add New Product". Below are the descriptions of the required fields:

Site ID
A site from the "sites list" should be selected (list of approved sites).

Product name
If a mode with fixed prices is used, this name will appear on top of Payment Form. If customer provides price with index_shop.cgi, this field is not relevant and can be set as a 'generic product', for instance.

Description
Description of a product upon merchant's choice, just for information.

Product type
'Standard' is for products that are sold normally through credit cards processing
'Web900' is for products that are sold via Web-900 paid phones service (USA only).

Price
Oroduct price, to be used when index.cgi (fixed pricing model) is used. Not relevant if index_shop.cgi is used, but has to be filled in by some value in any case.

Period
Period in days when service sold (membership access) is active. Not used in index_shop.cgi model, but has to be set in any case (any value).

Rebill price
Price of a prolongation of the membership access service, if used, only for index.cgi model (predefined prices).

Rebill period
Period in days of prolongation of the membership access service. Rebills will be charged when possible after corresponding period of time until cancelled by customer.

Access URL
An URL that will be called after payment is completed by ChronoPay (next stage after ChronoPay Payment Form), if purchase has been made successfully your customers will be directed to the mentioned URL.

Support e-mail
An e-mail of customer's support service (not mandatory).

Does this product need Username / password management?
If this checkbox is checked, Username/password combination will be asked from you when ChronoPay Payment Form works.

Each purchase/recurrent payment is collected technically with a link of a corresponding product that was bought.

5.2 Parameters transmission from Client system to ChronoPay

The POST method is preferable for parameter transmission. It's used to prevent the end customer from changing parameters, thus minimizing the risks involved (minimizing, not eliminating).

Below is the example of the form, which is posted by Customer from client system site to ChronoPay payment system site.

```
<form action="https://secure.chronopay.com/ index_shop.cgi" method="POST"
name="payment_form">
<input type="hidden" name="product_id" value="NNNNNN-NNNN-NNNN">
<input type="hidden" name="product_name" value="Main Product">
<input type="hidden" name="product_price" value="10.0">
<input type="hidden" name="cs1" value="client value 1">
<input type="hidden" name="cs2" value="client value 2">
<input type="hidden" name="cs2" value="client value 3">
<input type="hidden" name="cb_url"
value="http://www.somesite.com/backoffice_sales_register.php">
<input type="hidden" name="decline_url"
value="http://www.somesite.com/payment_failed.php">
<input type="submit" value="Pay!">
</form>
```

5.3 Description of parameters accepted by ChronoPay payment form

As it was mentioned above, the products can be set in two different ways within the ChronoPay system. Depending on whether it is product with a fixed price or common product for all transactions, the Customer is being redirected to URL https://secure.chronopay.com/index.cgi or https://secure.chronopay.com/index_shop.cgi respectively.

It is important to note that redirect to https:// is obligatory, as payment systems require the use of SSL tools to enhance the security.

The input parameters are as follows:

Code field	Required		Description
	index	Index_shop	
product_id	Yes	Yes	Unique code of product or service. ChronoPay uses it to determine which Merchant site Customer belongs to.
product_name	No	Yes	Product (list of products) for payment.
product_price	No	Yes	Amount to be paid. Currency is set during product setup.
language	No	No	Interface language. Currently one of the following languages can be chosen: • EN – English (default). • RU – Russian. • NL – Dutch. • DE- German
f_name/s_name	No	No	Name of the Customer. This and consequent parameters, related to personal information of the Customer, are displayed to minimize recurring input of information already acquired by Client system.

Code field	Required		Description
	index	Index_shop	
street	No	No	Street of residence.
city	No	No	City of residence.
state	No	No	State of residence (US only).
zip	No	No	ZIP code.
country	No	No	Country of residence.
phone	No	No	Phone.
email	No	No	E-mail.
cs1/cs2/cs3	No	No	Merchant system parameters relative to payment. Free-form data format up to 255 symbols. It is stored along with other customer information and returns with successful payment report and transaction report query.
cb_url	No	No	Merchant system URL script handling payment result notification. This script must validate authenticity of requesting system over its IP. Request is sent by ChronoPay system regardless of Customer's presence.
cb_type	No	No	G or P value for GET or POST notification methods respectively.
decline_url	No	No	URL for redirecting the Customer in case of declined transaction. URL for redirecting in case of successful payment is set as product parameter (access url).

All payment data are filled in solely at ChronoPay's side.

5.4 Description of callback parameters

In case cb_url/cb_type fields in the payment request are filled in, after a successful payment (for certain categories of clients also in case of decline from ChronoPay/Acquirer) the payment result notification will be sent. The data format for the callback is as follows:

Parameter code	Description
transaction_type	Transaction type: • initial – initial payment. • onetime – onetime payment. • decline – decline of payment.
customer_id	Unique customer identifier.
site_id	Site identifier.
product_id	Product identifier.
date	Payment date (m/d/Y H:i:s).
time	Payment time (H:i:s).
transaction_id	Transaction identifier.
email	E-mail.
country	Country of residence.
name	Name as stated on credit card.
city	City.
street	Street.
phone	Phone number.
state	State.
zip	ZIP code.
language	Language of Payment form interface

Parameter code	Description
cs1/cs2/cs3	Client system parameters relevant to payment. No changes from ChronoPay.
username	Username chosen by Customer or generated by ChronoPay.
password	Password chosen by Customer or generated by ChronoPay.
total	Total amount to be charged with additional payments included (VAT, etc).
currency	Payment currency.

5.5 Set landing page after a successful payment

After a successful payment the shopper will be redirected to a specific page. This can be set as well in the client admin. It can be set per product id individually and is called the "Access URL". Another name for this URL is the "Success URL". This can be set in the client admin;
- go to "set up",
- click on "List Your Products"
- click on your site ID
- click on "update"
- You can change the "access URL".

5.6 Description of export parameters

The merchant can obtain a transaction report. For this purpose ChronoPay's system generates a query to https://clients.chronopay.com/exp/index.cgi with the following parameters:

Parameter code	Description
site_id	Identification code of site for which transaction report has to be retrieved.
bdate	Starting date of report (current date is set by default).
btime	Start time (00:00:00 is set by default).
fdate	Ending date of report (current date is set by default).
ftime	End time (23:59:59 is set by default).
rs	Line separator sequence. (\n is set by default).

It should be considered that in provided reports and generated queries server time is shown as Eastern Standard Time. It is strongly recommended to use *btime* and *ftime* parameters, because an overload of the export system is not allowed. Furthermore, we do not allow for queries exceeding 60 days in time span and queries with same parameters more frequent than one in 58 minutes.

Output is provided in comma separated format in following sequence:

```
transaction_type;transaction_id;customer_id;site_id;product_id;name;email;customer_ip;date;total;currency;cs1;cs2;cs3;username;password;payment_type;reference
```

Its description corresponds with previously given and with following additions:

Parameter code	Description
transaction_type	Type of transaction: • rebill – recurrent transaction (follows initial). • refund – money return (transaction cancel), initiated by Merchant or ChronoPay. • chargeback – chargeback. • reversal – cancel of authorization before pre-authorization confirmation.
customer_ip	IP address of the Customer, which conducted the payment. Registered by ChronoPay payment form.
payment_type	Type of payment document: • CHECK – online check. • CARD – credit card.
reference	Reference to paired transaction. Applicable to onetime/initial, refund, reversal, chargeback transaction.

In case there are no data for specified period return will be the following:

NO DATA

5.7 Troubleshooting

In case of questions you can contact your Account Manager directly or via sales@chronopay.com

6. Support of 3D Secure

With some of our acquirers it is also possible to process payments with 3D secure enabled.

6.1 What is 3D Secure?

Visa has developed a technology to increase the security of the credit card transactions that you accept. Now provided by both Visa and MasterCard, 3D Secure technology is offered under the "Verified by Visa"and "MasterCard SecureCode" brand name.

The basic concept of the protocol is to tie the financial authorization process with an online authentication. This authentication is based on a 3 domain model (that is the 3-D in the name). The three domains are: Acquirer Domain (the commerce), the Issuer Domain (the bank issuer of the credit card) and finally the Interoperability Domain (Worldwide credit card and support).

6.2 What are the advantages of 3D Secure?

With 3D Secure, the risk of fraud and payment loss due to card misuse is significantly reduced.

Cardholders are protected from misuse of their credit card numbers because they have to produce confirmation of identity (i.e., by entering a code, before making a payment). The code is checked directly by the card issuer in real-time, before allowing the transaction to continue.

Both MasterCard SecureCode and Verified by Visa protect the merchant. Because of the secure password requirement, the cardholder's identity was confirmed prior to the purchase and the liability is shifted away from the merchant.

The benefits for merchants are:

- 3-D secure can be readily integrated into existing e–commerce systems
- Real–time cardholder authentication at time of purchase
- Improved profitability through increased sales and reduced costs
- Substantially reduced rates of fraudulent transactions and chargebacks
- Increased cardholder confidence leads to increased sales
- Minimal impact on the existing checkout process

6.3 How does 3D Secure work?

A. When enrolled shoppers choose to pay online, a prompt from their card issuer appears and requests their personal password (similar to visiting an ATM machines). Within seconds, the card issuer confirms the identity of the shopper and allows the purchase to continue.

6.4 How to integrate 3D Secure

Please contact you account manager to find out whether or not the acquiring bank you have an account with supports processing of 3D Secure transactions. Once you have chosen in the sales process to accept 3D Secure transactions it will depend on your acquiring bank how this security check can be activated. With some acquirers is is being activated automatically on the acquirer's side. With other banks you will need to add an additional script. Please contact your Account Manager for further details.

7. Additional functions

7.1 Refunds

It is necessary that the Customer's transactions can be refunded (money returned to the Customer's Card Account or the Account when Customer claims for that). If there are tangible goods involved in a sales procedure, Customer must return all purchased goods prior to starting the refund process. If the Customer has bought services (online access etc.) he/she may claim for refund even in case when there was no satisfaction from services usage. 'Refund' is a term used for transactions that were made one or more days ago, 'Reverse' is a term which is used for transactions that are made on present day.

Merchant should use the Client Admin in order to perform refund for a particular operation when required by the Customer. It is suggested that Customer will be asked for some of the data as described above (customer login name, customer name, transaction amount) that will uniquely identify a particular Customer and a particular transaction. It normally takes less than 1 (one) day for a refund to be completed (money returns to Customer's Credit Card Account) and this may depend on the Customer's bank terms and conditions. Once the refund is completed, it is not guaranteed that the same Customer with the same Card will be able to make a similar purchase in the future, because refund usage increases negative points on the Customer's Fraud Screening Profile. Negative transactions databases authorities may also be informed on the refund operation performed by a particular Customer.

Customers are also able to make refunds themselves through ChronoPay Customer Support (contact data are available on Payment Form).

A Chargeback is a different type of a reversal transaction, which is reported to the Customer's bank (not to ChronoPay) by the Customer itself as a result of a transaction that neither Customer wishes to pay or which was not made by Customer itself (third party activity is suggested). ChronoPay will not obtain any information about the fact that the Customer's transaction has been declined. It will immediately be reported as a chargeback. This information will be sent to ChronoPay only after all chargeback stages passed, starting from the Customer's report to the credit card issuer organization till blocking of the Customer's credit card account which will lead to the re-issuing of the card. Negative transactions databases authorities will also be informed on chargeback operations performed by particular Customer.

How to initiate a refund?

Refunds of transactions can be done in the Client Admin. In order to initiate a refund you will need to go to the "Sales" section. In the Detailed Sales section you select the period in which the original sale was made. Subsequently you select the specific transaction and the corresponding transaction ID. With the transaction ID you go from the menu to the Customer service and go to Refund Transaction, once you have entered the transaction ID and have clicked submit then the transaction has been refunded.

7.2 Pre-authorization

Pre-authorization is an optional feature. It is a method by which an amount of funds is reserved for a period of time to await sales completion.

The principal scheme of pre-auth is the following:

1. Customer makes a purchase;

2. ChronoPay will send a request to bank and they block the requested amount on a cardholders account;

3. Merchant approves a transaction in their clients interface;

4. ChronoPay sends a request to bank to confirm pre-authorization (to capture the blocked amount) card holders account on a previously blocked amount.

If the Merchant does not approve a transaction the block is deactivated and money do not charged from cardholders account.

IMPORTANT: Cancelled transactions would not be indicated in cardholder bank statement.

All this action should be made during three days since cardholders placed an order. There is 3 days period which is used by our acquirers. If no action was made on transaction during three days period, this transaction would be automatically considered as VOID and automatically be cancelled.

7.3 Virtual terminal

The access to a Virtual Terminal is an optional feature and will only be offered to merchants who process payments for at least 3 months with ChronoPay. This tool allows a merchant to manually process credit card numbers received by telephone, fax or mail order. You can use the Virtual Terminal in addition to (or instead of) accepting credit card transactions from your website. The terminal can be visited via the client admin. No installation is required.

Appendix A Frequently asked questions

This section contains answers on the most frequently asked questions from merchants related to the connection procedures with the ChronoPay's payment system and the interaction with the client admin.

Question: Should all products have a description? All new products too?
Answer: Descriptions of products and services are not visible to the customer, therefore they are optional.

Question: The password script URL, the password script secure key, — what do these parameters mean?
Answer: The URL, which is used to send a request for a customer login and an additional password and secret password in script accordingly.

Question: I need to automate the addition process of new products in processing. How can I proceed with it?
Answer: The current version of the system doesn't support such automation.

Question: Can I entrust registration of new products to my shop developer? Can I change the access parameters in the processing interface after the development work is finished?
Answer: Yes, access parameters in the processing interface can be changed at any time. Please contact ChronoPay technical support.

Question: What cards are accepted for payments?
Answer: All cards mentioned at our site are available for payments acceptance except those that needs to invoke online authorization and a magnetic stripe read (as mentioned in the contract).

Question: After the Customer has entered the Credit Card Details and the attempt failed (three times), will the Customer be redirected to the URL specified in the "decline_url"? Will this session then keeps all its parameters?
Answer: Yes, the session usually keeps all parameters.

Question: If the transaction is successful, what will the URL specified in the "cb_url" do?
Answer: The Merchant site may show, for example a message that the transaction is successful.

Question: What is the main purpose of using of Access URL specified in the Administrative Interface?
Answer: Use this URL to redirect the customer in case of successful transaction.

Question: Once the payment is successful, what exactly details will return as parameter?
Answer: Unique transaction identifier will be returned in server response.

Question: I have set the retry_count field to 1 (one) and made an attempt to use a knowingly invalid card, but the system didn't redirect it to decline and offered to enter the card number once again. Only after second attempt has been made, the system has redirected the customer to the decline URL. How could it be possible that the system will redirect the customer to the decline URL just after the first attempt, when an invalid card was being used?

Answer: Try to set retry_count = 0.

Question: What is the purpose of the fields "Period", "Rebill price" and "Rebill period" in the form?

"Update your product info"? How should it be filled in if we need to accomplish rebilling every 1, 3 or 6 month for example without a period restriction?
Answer: — Period- time before re-bill has began, Re-bill price — price of single re-bill, Re-bill period — time between re-bill procedures.

Question: It is written in document that: fname — first name* lname — last name cardholder — cardholder. What does cardholder mean in this case?
Answer: cardholder — holder of the card as mentioned on the card surface.

Question: Country — 3 symbols country code* Usually country denoted by two symbols. Why are there 3 symbols here?
Answer: Two symbols can be entered, but not more than three.

Question: Product_id — product code* Describe this parameter. In my opinion it does not have any meaning and may be filled with anything you like?
Answer: product_id is a unique product or service identifier issued by the ChronoPay system after the product or service registration.

Question: How does the gateway determines the source of transaction, because client_id is not entered anywhere? Can you bind the server IP address (connected to gateway) to each client_id?
Answer: — Gateway determines the source of transaction by a unique product identifier — product id.

Question: What is the procedure for a refund action?
Answer: The refund procedure may be accomplished by using a transaction gateway of the ChronoPay system as described above or via the administrative interface.

Appendix B Glossary

ABA Routing Number- a specific bank code used for banks in the USA.

Acquirer (Acquiring bank) – financial organization providing credit card processing services to online merchants. Merchants are supposed either to sign up an agreement with Acquirer Bank or to grant PSP with the corresponding authority.

Automatic Check Handling (ACH) - ACH can also mean Automatic Clearinghouse. ACH is a form of epayment or electronic payment. There are two ways payments can be transferred: (1) by wire transfer, or (2) through an automated clearinghouse. Wire transfer is an e-payment system that is designed to handle high-dollar, time-crucial payments, usually between large banks. ACH is designed to be an e-check or electronic check. Unlike the wire transfer, it is usually used to process higher volumes or small-dollar payments for settlement issues within 1 to 2 business days. All ACH transactions are settled pretty much the same way checks are. The clearinghouse takes all of the ACH files received daily from member banks, it then divides them by the originating bank (where the check was either cashed or deposited) and the paying bank (the bank where the check was drawn), then it totals the accounts, and credits or deducts the accounts accordingly.

Address Verification Service (AVS)- in 1996, VISA/MasterCard headquarters introduced a new regulation requiring all businesses who manually key in the majority of their credit card transactions to have a special fraud prevention feature on their credit card processing equipment. This feature is referred to as an address verification system (it checks to see that the billing address given by the customer matches the credit card).

Administrative interface- Web-based tool allowing Merchants to track their sales with customers.

Approval- confirmation code, sent by bank to confirm the fact that the credit card of buyer exists, is suitable to the use and the inquired sum is within the limits of the permissible limit.

Authorization- with authorisation is meant the communication between the customer's bank on the one hand and the bank of the Merchant on the other hand. The aim is to find out whether or not the customer has enough money to pay for the products and services offered by the Merchant. The customer's bank reserves a certain amount of money for the transaction and supplies the Merchant bank with the necessary authorisation code.

Authorization code- this code consists of letters and numbers and is sent to the bank to confirm the authorisation.

Bank Identification Number (BIN)- the numbers on the credit card, which unambiguously determine the issuing bank. Usually these are the first six numbers.

Batch- a group of records considered a single unit for purposes of processing. A batch can be processed automatically as well via a POS terminal.

Batch Processing- type of data processing; it processes a group of transaction as one entity.

Billing address- the address of the person, who have purchased the goods and services.

Capture- the submission of a credit card transaction for processing and settlement. POS terminals and real-time processing software capture transactions to submit to merchant account providers or credit card processors.

Card Issuer- financial institution (or its agent) which issues the card.

Card-Not-Present- the situation in which the seller does not have the possibility to see the buyer as well as the credit card; this will result for instance in the situation that information can not be retrieved from the magnetic strip of the credit card, to verify signature or to look at the hologram. In order to increase, in this case, the reliability of the payment system, Address Verification Service is used.

Card –Unblocking- the action of unblocking the credit card

Certification Authority- the institute**,** which is in charge of the issuing of open keys.
Chargeback- a reversal of a credit card transaction, typically initiated by the transaction card issuer at the cardholder's request. Chargebacks can occur for any number of reasons, including: customer disputes, potential or actual fraud (on the part of merchants, sales associates and/or customers), processing errors and authorization issues. Chargebacks are governed by a complex set of rules and time limits that can be costly to merchants and their banks if disregarded.

Chargeback Reason Code- a two digit number, through which the reason of the chargeback is indicated.

Check Guarantee- a service (commonly offered to merchants) guaranteeing that a check writer has sufficient funds on his deposit to cover the payment.

Chip Card- a smart card, a plastic card, that is equipped with a microprocessor on which electronic money can be stored.

Commerce Server- a Web server that contains the software that is necessary for processing customer orders via the Web, including shopping cart programs, dynamic inventory databases, and online payment systems. Commerce servers are usually also secure servers.

Confirmation Letter- the electronic letter, which is sent to the Merchant and contains information regarding the processed batch files.

Creditcard- This is a type of bank card that can be widely used all around the world as a form of payment. The credit card holder must then reimburse the credit card company for the amount of the total sales the holder had charged on that particular credit card.

Credit card Processors (Third Party Processors)- merchant services providers that handle the details of processing credit card transactions between merchants, issuing banks, and merchant account providers. Website operators usually must first establish their own merchant account before contracting for credit card processing services.

Customer- end customer (buyer) performing electronic shopping.

CVV2/CVC2- this is the check number, which consists of three numbers, which is printed on the reverse side of bank card. The introduction of this number helps to ascertain that the card is used by a real owner. CVV2 classification is used for VISA cards. CVC2 classification is used for MasterCard cards.

Debit card- a financial instrument used by consumers instead of cash. Unlike a credit card, debit card purchases are deducted automatically from the cardholder's account, like a check. Visa and MasterCard now offer debit cards through banks and other financial institutions.

Decline- the decline of a credit card transaction.

Deposit- the moment at which the Merchant creates a batch file and sends the transactions for processing.

Deposit bank- the bank to which the money of the customer will be transferred to.

Digital signature- this signature is needed to determine the integrity of the source.

Digital wallet- a consumer account set up to allow e-commerce transactions through a particular credit card processing system. Before the consumer can make a purchase, he or she must first establish an account with the credit card processor, who provides an ID and password. These can then be used to make purchases at any Web site that supports that transaction system.

Discount rate - This is a fee that the major credit cards charge for handling a transaction.

E-commerce- the processing of economic transactions, such as buying and selling, through electronic communication. E-commerce often refers to transactions occurring on the Internet, such as credit card purchases at Websites.

Electronic Data Interchange (EDI)- a global computer network, separate from the Internet, used to handle financial transactions between banks and other institutions.

Electronic Data Capture- the use of a POS terminal for validating and submitting credit card transactions to a merchant account provider or other credit card processor. In online credit card processing, software takes the place of the POS terminal.

Electronic Cash Register (ECR)- electronic cash register, in other words, the combination of cash register and POS- terminal. Frequently ECR - this is the program application, is established on a personal computer.

Electronic Draft Capture (EDC)- the system, in which the transactions are transferred from different places to the central computer (Host Computer) for the storage and the processing. The transactions accumulated during the period are then transferred to the processor of payments.

Electronic Money (e-money)- digital available amount of money. It is stored in electronic form on a computer or a microprocessor. Digital available amounts can be purchased and remain on a special storage device.

Electronic Wallet- software that enables a cardholder to conduct online transactions, manage payment receipts and store digital certificates.

Electronic purse- a smart card on which electronic money can be stored.

Factoring- the purchase of debts owed, or "accounts receivable," in exchange for immediate payment at a discount. In e-commerce, the term is often applied to ISO's that offer to process credit card transactions through their own merchant account rather than through an account established by the merchant, in exchange for a percentage of the transaction or other fee. Factoring of credit card debts is illegal.

Fraud screening -all procedures intended to prevent customers from using of fake or stolen credit cards.

Front-end- information, which the buyer sees on the website of the merchant. Front-End makes it possible for buyers to interact with the electronic basket, the data base, and to also pay purchases.

Hold back (reserve account)- a portion of the revenue from a merchant's credit card transactions, held in reserve by the merchant account provider to cover possible disputed charges, chargeback fees, and other expenses. After a predetermined time, holdbacks are turned over to the merchant.

Host capture- the automatic composition of a batch- file for the processor of payments or the payment gateway

Host computer- the computer responsible for the authorisation and completion of the transaction.

Interchange- a standard format for sharing or transferring data electronically between parties that do not share a common application. Usually a format that is platform-independent is agreed upon as a standard. Examples of common interchange formats include EDI (electronic data interchange), ASCII (American Standard Code for Information Interchange), and GIF (graphics interchange format).

Independent Sales Organization (ISO) - This is an organization that processes merchants online credit card transactions in exchange for a percentage of the sales or transaction fees.

Issuer (Issuing bank)- the bank or other institution that issues a credit card or debit card to an individual.

Key- numbers which are applied for cryptographic algorithms.

Key length- the length of a key, expressed in bytes.

Limited-purpose prepaid card- a smart card, which only can be used in particular points of sale.

Load- the activity to load digital available amount of money into the digital purse.

Load log- a file containing the most recent loads

Local review- the ability of salesman to see from its terminal or ECR the contents of a batch- file after the completion of transaction.

Locking (Card blocking)- the blocking of a smart card after which it can not be used.

Magnetic stripe- can be found at the back of the credit card and contains coded information about the card.

Manual Entry (Key entry)- the operation of manual entering of the parameters of card with the use of the keyboard of computer or a POS- terminal.

Member- financial establishment - the member of the association of international pay system.

Merchant- E-commerce Web-site owner providing electronic sales function.

Merchant Account- a bank account established by a merchant to receive the proceeds of credit card purchases. By establishing a merchant account, the merchant bank agrees to pay the merchant for valid credit card purchases in exchange for the right to collect on the debt owed by the consumer.

Merchant Account Provider (MAP)- a institution that hosts merchant accounts and processes online credit card transactions. The term is also often used broadly to include any credit card processing service, including ISOs.

Merchant Agreement- the written agreement between the salesman and the bank (is possible, between the salesman, the bank and ISO), that establishes rights, responsibilities and guarantees of sides in the process of the card payments methods.

Merchant Bank- the bank, which offers merchant accounts.

Merchant Category Code- the code which indicates the type of activities of the Merchant.

Micro payment- micro-payment, very small sum, possibly, can be lower than the cent

MID (Merchant Identification Number)- unique identifier issued by Acquirer Bank in order to track and collect Merchant's online payments.

Monthly minimum - This is the amount of fees you must meet each and every month. If month sales do not make the monthly minimum the merchant account holder must make up the difference.

MOTO Discount rate (Mail Order/ Telephone Order)- the discount rate charged by the merchant account provider for credit card transaction in which the actual credit card was not available to the merchant. MOTO discount rates are generally higher than swipe discount rates to account for the increased chance of fraud or non-payment.

Non-Qualified- the designation of the transaction, which is characterized by an increased risk (for example, in the case, when transaction is achieved with the aid of the transfer of the parameters of bank map with the physical impossibility of access to it).

Payment form- web-based electronic form provided by ChronoPay PSP to Customers where Customers have to enter their personal and credit card data in order to perform payment using Credit Card.

Payment processing- a process of attempting to charge some value from customer's credit card.

Payment system- financial organization (or association of financial organizations) providing financial services to customers and allowing them to use credit cards that are identified by its number and some supplementary information.

Pc Pos Application- computer is a program application, which unites two functions from the list: cash register, the calculation of values, bookkeeping program, program for authorization and method of credit card payments.

PIN (Personal Identification Number)- an alphanumeric or numeric code used to verify the identity of an individual attempting to use a credit card, debit card, or other account.

POS Terminal (Point of Sale)- an electronic device used for verifying and processing credit card transactions. If the credit card is available, the merchant can swipe the card through the terminal. See also swipe discount rate and MOTO discount rate.

Post authorization- the transaction, which precedes the vocal authorization.

Pre-paid card- a smart card on which electronic money is stored.

Prior Authorized Sale- the transaction, for which first authorization is needed. Salesman authorizes credit card before granting to products and services.

Private information- a combination of credit card (Account) number with customer's name and some other private data.

Private Key- the secret key, to which only its owner has access to. The open key corresponds to a secret key.

Processor- the processor of payments, a computer center, which generates master operations of payments.

PSP- Payment Processing Provider (means ChronoPay PSP).

Public Key- the open key, the non-secret part of the pair of two keys in asymmetric cryptography.

Public Key Certificate- the certificate of the open key. Information about the open key, as a rule, which includes the key itself, signed by a digital signature of physical face or organization. Certificate protects the integrity of the key, if person or organization, that signed him, is well known, and their open keys are widespread.

Public Key Cryptography- the diagram of coding, which does not require confidential channel for establishing the confidential connection.

Public Key Encryption- the method of coding, developed for the purpose of overcoming the main disadvantage in symmetrical cryptography - the need for having reliable channel for the transfer of key to addressee.

Real-Time Processing- the verification and processing of credit card transactions immediately following a purchase. Real-time verification on the Web usually takes less than five minutes. Real-time verification is especially important for websites that sell products and services that consumers expect immediately, such as memberships to the site or software downloads.

Receipt- the check, which contains the description of the purchase with the credit card, usually includes the following information: date, name and the address of salesman, sum, unique number and the code of authorization.

Recurring Fees- regular, usually monthly, charges for maintaining a merchant account. Recurring fees include the discount rate, transaction fees, statement fee, and monthly minimum.

Recurring Transaction- the periodic removal of money from the account of buyer, proceeding on the basis of agreement.

Retrieval Request (Copy Request)- the requirement to a salesman to present documentation about the concrete transaction. Usually it comes from bank, when the holder of the card disputes a transaction.

Secure Server- a Web server or other computer connected to the Internet that is capable of establishing encrypted communication with clients, generally using SSL or SET.

Session Key- the key for the symmetrical coding, which is used for a limited time, is more frequent used for a protected connection, for example, on protocol SSL.

SET (Secure Electronic Transaction)- the system of providing safety of payments for bank cards, developed by the companies VISA, MasterCard, Microsoft and by several leading banks, based on the coding with the open key of the information, connected with the parameters of the card, and with the separation of information between participants in the transaction in such a way that none of the participants in the calculations possesses information wholly. With the aid of standard SET, the buyer and salesman can unambiguously identify each other, after exchanging the digital SET- certificates.

Settlement (Draft Capture)- a process of completing fund transfers so that all parties in a transaction are paid for their goods or services.

Setup Fee- one-time pay, collected for the creation of the Merchant Account.

Shopping Basket - As you shop online, you add items to your 'virtual' shopping basket. The basket is simply a list of the items you have selected to buy, together with the necessary details (number selected, price of each item etc). You can review what's in your basket at any time as you shop.

Shopping cart - Software used to aid customers when ordering a number of products/services from a merchants web site.

SIC Code- the code of standard business- classification (Standard Industry Classification). This is the four-place number, which determines the type of activity.

Smart Card- a plastic card containing a computer chip that can store electronic "money". Unlike a credit card, a smart card can only spend out the dollar amount its owner has already put into the card account. It's similar in function to a prepaid calling card but is available for all purchases.

SSL (Secure Socket Layer)- a system for encrypting data sent over the Internet, including e-commerce transactions and passwords. With SSL, client and server computers exchange public keys, allowing them to encode and decode their communication.

Statement Fee- - the fixed periodic pay for the use of a Merchant Account.

Surcharges- additional charge for the method of payments of the bank cards.

Swipe Discount Rate- the discount rate charged by a merchant account provider for transactions in which a credit card is available for inspection by the merchant. Swipe discount rates are generally lower than MOTO discount rates because the merchant can match signatures and perform other checks for fraud or miss-use.

Symmetric Cryptography- symmetrical cryptography or cryptography with the closed gate. The cryptographic algorithm, in which for the coding and the decoding is used one and the same key.

Third Party Processor- a company that processes transactions on behalf of the banks or other participants to those transactions.

Ticket Only- the monetary value of an order placed by credit card.

Terminated Merchant File (TMF) - Merchants with excessive chargebacks are stripped of their merchant account and the ability to accept credit card orders. The merchant is then placed on the TMF match list that all Merchant Service Providers have access to. Being placed on this file can keep you from obtaining another merchant account for several years.

Transaction - This is any action between a cardholder and a merchant that results in activity on the account, such as an authorization and settlement. Merchants and financial institutions also conduct follow-on transactions that affect the cardholders' account, such as a capture and credit.

Transaction fee - A fee charged by a merchant account provider for each credit card transaction completed.

Transaction File (Vendor File)- the file, into which the processor of payments places all transactions, carry out in the previous day.

Transaction Log- the transactions, recorded by the state of accomplishment.

Turn-key - A solution a firm offers in which they provide an individual with a fully e-commerce enabled web site. Usually complete with shopping cart, web design, hosting and merchant account

Virtual Terminal - This tool allows a merchant to manually process credit card numbers received by telephone, fax or mail order. You can use the Virtual Terminal in addition to (or instead of) accepting credit card transactions from your website.

Voice Authorization- vocal authorization. It applies, when there is no suitable device for conducting the authorization, for example, of POS- terminal.

Void- the refusal of the buyer's payment after successfully passed authorization. The transactions, marked as Void, are not included into the batch and are not presented to further payment.

XML- a meta language containing a set of rules for constructing other markup languages. With XML, people can make up their own tags, which expands the amount and kinds of information that can be provided about the data held in documents. It enables designers to create their own customized tags to provide functionality not available with HTML. For example, XML supports links that point to multiple documents, as opposed to HTML links, which can reference just one destination each.