

---

**Developer Guide To The**

**viaKLIX**

**Virtual Terminal**

**Version 2.0  
June 19, 2003**

THIS VIAKLIX VIRTUAL TERMINAL USER GUIDE  
WILL FAMILIARIZE YOU WITH ALL THE TRANSACTION  
TYPES AND PROCEDURES YOU WILL USE. PLEASE TAKE SOME  
TIME TO THOROUGHLY REVIEW THIS MATERIAL

**NO PART OF THIS DOCUMENT MAY BE  
PHOTOCOPIED OR REPRODUCED IN ANY  
FORM WITHOUT PRIOR WRITTEN CONSENT FROM  
NOVA INFORMATION SYSTEMS, INC.**

THE INFORMATION CONTAINED IN THIS MANUAL IS  
SUBJECT TO CHANGE WITHOUT NOTICE.  
NOVA INFORMATION SYSTEMS, INC. SHALL NOT BE LIABLE  
FOR TECHNICAL OR EDITORIAL OMISSIONS MADE HEREIN;  
NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES  
RESULTING FROM THE FURNISHING OR USE OF THIS MATERIAL.



**NOVA NETWORK**

*The most reliable payment processing  
network in the industry*

**Copyright © 2003 NOVA Information Systems, Inc. All rights reserved.**

## *Table of Contents*

<b>General Overview</b>	<b>4</b>
<b>Flowchart</b>	<b>5</b>
<b>Payment Form</b>	<b>6</b>
viaKLIX Provided Form	6
Merchant Provided Form	8
<b>Receipt Options</b>	<b>11</b>
viaKLIX Provided Receipt	11
Merchant Provided Receipt	14
<b>Best Practices</b>	<b>17</b>
<b>What's New?</b>	<b>18</b>
<b>Appendices</b>	<b>20</b>
Appendix 1: Input values	20
Appendix 2: Response Codes	24
Appendix 3: viaKLIX Error Numbers and Messages	26
<b>Glossary of Terms</b>	<b>28</b>

## General Overview

viaKLIX is a payment gateway allowing merchants to submit credit card transactions via the Internet to the NOVA Network™ and have them authorized in real-time. This guide is designed to help you, the developer, write a Web site that will interface with viaKLIX to process these transactions. viaKLIX allows for a wide range of customization by utilizing both code and configuration through the administration section of your account at [www.viaklix.com](http://www.viaklix.com), to allow you to process transactions in the manner that best fits your particular business needs.

viaKLIX accepts information sent via HTTPS, either by a Get (along with the Query string in the URL) or Post (typically from an HTML Form) Method. The information you send, along with your viaKLIX settings, will determine how your transactions are handled. This information will determine user interface settings such as colors, images to display, field order and field selection. This information also will determine behavior. For example, if viaKLIX needs to display a form to collect additional customer information, the information you send and your viaKLIX settings will determine the type of receipt to display to the customer, and how information is sent back to you.

The first decision you need to make is how much work you want to do, and how much work you want to let viaKLIX do for you. viaKLIX can accept as little as two pieces of data from your Web site, and do the rest of the work on its own, by gathering information from your customer and using the settings that have been configured by your company in the viaKLIX administration section. On the other hand, you could go as far as using viaKLIX as a backend feature to your Web site, completely transparent to your customers, in which you write the page that gathers all of the pertinent customer information and the receipt page that displays the outcome of the transaction processing to the user. We find that most merchants fall somewhere in the middle of these scenarios, gathering some data from their customer's before sending them out to viaKLIX and then letting viaKLIX gather more information from the customer and displaying the receipt after credit card approval.

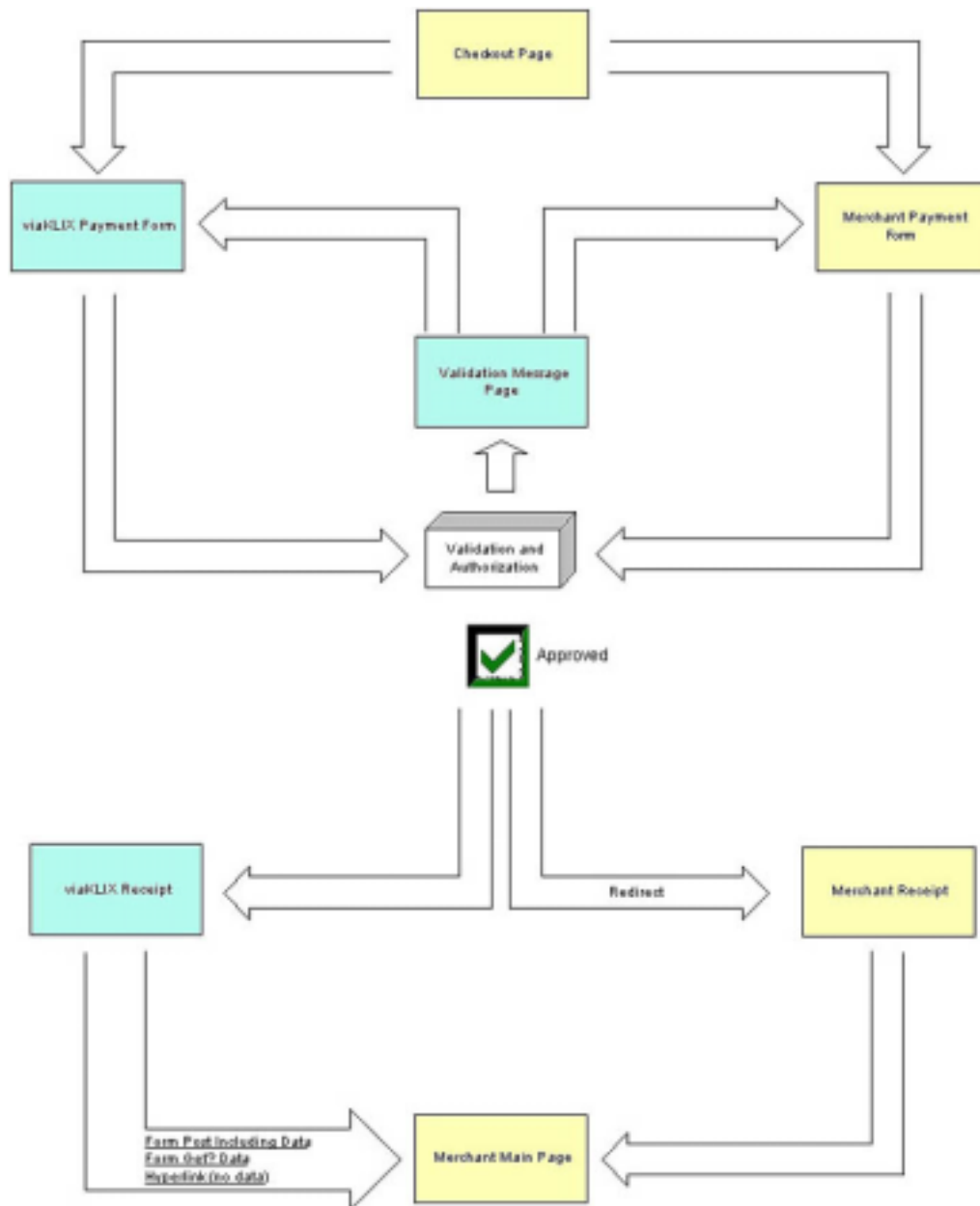
The viaKLIX program is easy to integrate with other payment systems. For more information on integration, please call **1-800-377-3962** or e-mail your question to: [internetproductsupport@merchantconnect.com](mailto:internetproductsupport@merchantconnect.com).

## Flowchart

Periodically throughout the entire viaKLIX Developer's Guide, you'll see a flowchart diagram to give you a visual aide to help you maintain your bearings as you navigate through the transaction process.

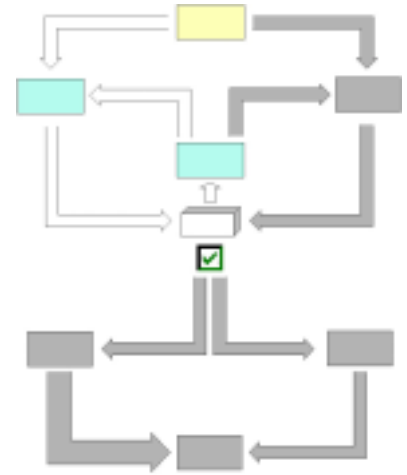
The blue boxes represent the viaKLIX process in the chart and the yellow boxes represent the merchant side of the transaction.

The flowchart will appear in its entirety throughout the document. You'll be able to determine your location in the transaction, as the corresponding section of the flowchart will appear in color. All other quadrants of the chart will appear shaded. The green checkmark in the middle represents an approved transaction and the red, crossed circle represents a declined transaction.



## Payment Form

The Payment Form is the place where your customer enters the necessary and/or required personal and credit card information required to process the transaction. It also is the page that will send the transaction on to the viaKLIX system for authorization processing. If viaKLIX is drawing the Payment Form for you, you will only need to give the system enough information to know who you are and any special information about your transaction that the customer is not going to be entering. If you are drawing your own Payment Form, then your form will need to send all of the necessary data to complete the transaction into viaKLIX.



### viaKLIX Provided Form

This section will tell you what you need to do to send information to viaKLIX in order to have viaKLIX present a payment form to your customer. This payment form will gather information from your customer such as the name displayed on their credit card, card number, expiration date, billing and shipping address, as well as other fields specified by you in your web page's code or in the Terminal Setup section of your viaKLIX account.

### Input

The first, and most basic, step is to submit the minimum information to viaKLIX. The minimum information required for viaKLIX to provide a payment form to your customer is the following two fields:

- Your `ssl_merchant_id` (sometimes referred to as your Account ID or your viaKLIX ID)
- `ssl_PIN` that matches your Account to the terminal you are using.

If you have more than one terminal assigned to your account, you need to make sure that the PIN you are using corresponds to the correct terminal. With these two pieces of information, viaKLIX can display a payment form based on the settings you have pre-determined in your viaKLIX account that will allow your customers to enter all of the transaction data including the amount. Although in most cases this is not practical, this could be used to accept on-line donations, for which the customer decides the amount of money he/she wishes to spend.

In a more likely scenario you will have some additional information to send to viaKLIX, including the transaction amount, a description, and perhaps other fields such as a customer code, or an invoice number. viaKLIX would then draw a payment form for your customer to enter their credit card information, and other information such as their billing address and any custom fields that you have created.

To integrate viaKLIX with a Web site that offers paid goods or services and wants to charge for those goods or services by credit card, the following procedure can be followed:

1. Create a form on your Web site
2. Set the action of the form to `https://www.viaKLIX.com/process.asp`
3. Set the method of the form to POST
4. Add a hidden field with the name `ssl_merchant_ID`. Set the value to the viaKLIX account ID.
5. Add a hidden field with the name `ssl_pin`. Set the value to the merchant PIN associated with the viaKLIX ID.
6. Add a hidden field with the name `ssl_amount`. Set the value to the desired amount.
7. Add a submit button.

## Example 1:

The following HTML code demonstrates the initiation of a minimal viaKLIX transaction, in which viaKLIX gathers all of the customers billing information:

```
<form action="https://www.viaKLIX.com/process.asp" method="POST">
  <input type="hidden" name="ssl_merchant_id" value="my_merchant_ID">
  <input type="hidden" name="ssl_pin" value="my_PIN">
  <input type="hidden" name="ssl_amount" value="14.95">
  <input type="submit" value="Click To Order">
</form>
```

This code creates a button with the label "Click To Order". When the button is clicked, the user is taken to the payment form on the secure viaKLIX servers.

**Please Note: In all of these examples, you will have to change the data values, such as "my\_merchant\_ID", "my\_PIN", and the amount of "14.95" to values that match your viaKLIX account and meet your Web site's needs.**

Version 2.0 of viaKLIX has added a user hierarchy to the application. Each account will have one Merchant Admin user and can have multiple Employee Users, who may or may not have access to run transactions on the terminal that is integrated with your Web site. When specifying a User ID, please make sure that the PIN that is submitted matches up with the User ID that you are submitting and the terminal on which you wish to run the transaction. When an account has more than one Terminal, it is the combination of ssl\_merchant\_id, ssl\_pin and ssl\_user\_id that viaKLIX will use to determine which of the terminals the transaction is being submitted to. The terminal itself will not be submitted to viaKLIX. When ssl\_user\_id is omitted, the User ID is assumed to be the same as the ssl\_merchant\_id, the merchant Admin User.

## Example 2:

The following HTML code demonstrates the initiation of a slightly more complex viaKLIX transaction in which the viaKLIX system will display a form to gather additional required customer information:

```
<form action="https://www.viaKLIX.com/process.asp" method="POST">
  <input type="hidden" name="ssl_merchant_id" value="my_merchant_ID">
  <input type="hidden" name="ssl_user_id" value="my_User_ID">
  <input type="hidden" name="ssl_pin" value="my_PIN">
  <input type="hidden" name="ssl_show_form" value="true"> <!-- Optional, Default Value = "true" -->
  <input type="hidden" name="ssl_test_mode" value="false"> <!-- Optional, Default Value = "false" -->
  <input type="hidden" name="ssl_invoice_number" value="Inv-123-ABC">
  <input type="hidden" name="ssl_amount" value="31.01">
  <input type="hidden" name="ssl_sales_tax" value="1.86">
  <input type="submit" value="Click Here to Complete Your Order">
</form>
```

This code creates a button with the label "Click Here to Complete Your Order." When the button is clicked, the customer is taken to the payment form on the secure viaKLIX servers to fill in the final details of their transaction.

## Behavior

In both of these examples, the output will be an HTML page from viaKLIX displayed on the customer's Web Browser. This page will either be a Payment Form for them to enter more information or an error message, indicating an error condition with the data sent to viaKLIX (such as when the ssl\_PIN doesn't match an existing terminal for the ssl\_merchant\_ID). See Appendix 3 for more about the Error Messages and Error Numbers

Your customer will use the Payment Form that is displayed to provide the final pieces of information needed to complete the transaction. This final information will include at least the credit card number and expiration date. Most likely, other information such as Billing Address, Shipping Address and e-mail will be included as well. The fields that are presented on the viaKLIX payment form are fully configurable from within the viaKLIX site itself. Please see the Merchant's Guide for more information on how to do this.

## Merchant Provided Form

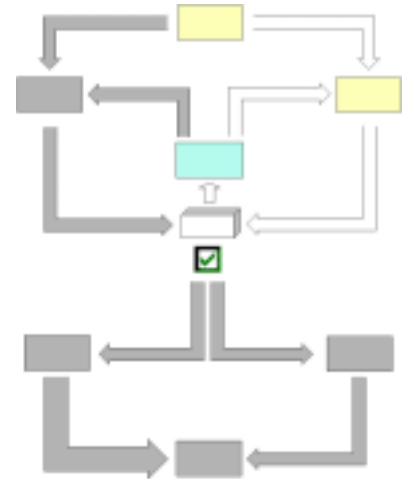
This section will tell you what you need to do to send information to viaKLIX in order to have viaKLIX process a credit card transaction without any additional input from your customer. Using this method, viaKLIX will only be visible to your customer before the transaction is processed if the data passed in is found to be invalid. Invalid data could consist of data such as a bad PIN or User ID that does not allow the transaction to be associated with your account, or it could be bad customer data such as a mal-formed credit card number or e-mail address.

### Input

If you want to collect all of the data from the customer on your Web site, and only send the information to viaKLIX after it has all been gathered you can do so. To hide the Payment Form you will need to send the parameter "ssl\_show\_form" with a value of "False".

If you are presenting the payment form, and not asking your customers to input any additional fields on a viaKLIX provided Web page, you must include some additional information. The three additional required fields that you must pass to viaKLIX are:

- ssl\_amount
- ssl\_card\_number
- ssl\_exp\_date



### Example 3:

This example shows a very basic form that collects and passes the minimum required data for a complete viaKLIX transaction that will not display the viaKLIX payment form:

```
<form action="https://www.viaKLIX.com/process.asp" method="POST">
  Your Total: $5.00 <br/>
  <input type="hidden" name="ssl_amount" value="5.00">
<br/>
  <input type="hidden" name="ssl_merchant_id" value="my_merchant_ID">
  <input type="hidden" name="ssl_pin" value="my_PIN">
  <input type="hidden" name="ssl_show_form" value="false">
  Credit Card Number: <input type="text" name="ssl_card_number"> <br/>
  Expiration Date (MMYY): <input type="text" name="ssl_exp_date" size="4"> <br/>
```



```
<br/>

</form>
```

This code creates a form displaying the customer's total, and asking for their credit card number and expiration date, with a button labeled "Continue." After the user enters the information and the button is clicked, the transaction is processed by the secure viaKLIX servers. Then the user is taken directly to a receipt or result form, displaying the outcome of the transaction.

**Please Note: In all of these examples, you will have to change the data values, such as "my\_merchant\_ID", "my\_PIN", and the amount of "5.00" to values that match your viaKLIX account and meet your Web site's needs.**

Version 2.0 of viaKLIX has added a user hierarchy to the application. Each account can have one Merchant Admin user and can have multiple Employee Users, who may or may not have access to run transactions on the terminal that is integrated with your website. When specifying a User ID, please make sure that the PIN that is submitted matches up with the User ID that you are submitting and the terminal on which you wish to run the transaction. When an account has more than one Terminal, it is the combination of ssl\_merchant\_id, ssl\_pin, and ssl\_user\_id that viaKLIX will use to determine which of the terminals the transaction is being submitted to. The terminal itself will not be submitted to viaKLIX. When ssl\_user\_id is omitted, the User ID is assumed to be the same as the ssl\_merchant\_id, the merchant Admin User.

## Using Address Verification Service (AVS)

AVS is a service that is performed by the credit card issuer. It compares the street address and zip code supplied with the credit card number with the address and zip code on file. The following three system fields are used by viaKLIX to handle the AVS:

- ssl\_avs\_address
- ssl\_avs\_zip
- ssl\_avs\_response

The first two fields are visible by default on the payment form under the names "Address" and "Zip Code" and control the input to the AVS. If you are collecting address information on your Web site or already have this information in a customer database, before displaying the viaKLIX form, you can pass the information to viaKLIX as variables in the same fashion that the PIN and ID's are sent. The last field contains the response of the AVS and is stored with the transaction, as well as included in the receipt.

viaKLIX may also return a space, in which case AVS was not performed. The most likely reasons for this are:

- No address or zip code was supplied
- AVS not supported by card issuer

See Appendix 3: AVS Response Codes for more detail.

**Please Note: A failed AVS check will NOT result in a Decline response for the transaction itself.**

## Using CVV2/CVC2

CVV2 and CVC2 are fraud-prevention measures implemented by VISA and MasterCard. These numbers are located on the back of your credit card and are generally three- or four-digit numbers listed after your credit card number. CVV2 refers to the VISA number and CVC2 refers to MasterCard's implementation.

By being able to provide this number, virtual (Internet) cardholders can help prove they have the physical card in hand when completing the transaction. This helps eliminate the possibility of someone using a stolen card number on your Web site.

The following three system fields are used by viaKLIX to handle CVV2/CVC2:

- ssl\_cvv2
- ssl\_cvv2cvc2
- ssl\_cvv2\_response

VISA implements two fields when using CVV2: the CVV2 Indicator (ssl\_cvv2) and the CVV2 Data (ssl\_cvv2cvc2). The indicator is one of the following:

- Present
- Bypassed
- Not Present
- Illegible

The CVV2 Data indicates the actual number on the card. When passing the CVV2 data, you must also pass the CVV2 indicator, or the transaction will be rejected by viaKLIX.

MasterCard does not implement an indicator like VISA. The CVC2 data (ssl\_cvv2cvc2) is all that is necessary. When you pass a MasterCard number, CVV2 indicator and CVC2 data, the indicator is ignored. This is by design.

See Appendix 4: CVV2/CVC2 Response Codes for more detail.

**Please Note: A failed CVV2/CVC2 check WILL result in a Decline response for the transaction.**

### Example 4:

To pass AVS data and CVV2 data or CVC2 data, use the following syntax:

```
<form action="https://www.viaKLIX.com/process.asp" method="POST">
  <input type="hidden" name="ssl_merchant_id" value="my_merchant_ID">
  <input type="hidden" name="ssl_user_id" value="my_User_ID">
  <input type="hidden" name="ssl_pin" value="my_PIN">
  <input type="hidden" name="ssl_card_number" value="0000000000000000">
  <input type="hidden" name="ssl_exp_date" value="0000">
  <input type="hidden" name="ssl_amount" value="12.77">
  <input type="hidden" name="ssl_show_form" value="false">
  <input type="hidden" name="ssl_cvv2" value="present"> <!--CVV2 Indicator -->
  <input type="hidden" name="ssl_cvv2cvc2" value="1234"> <!--CVV2 Data -->
  <input type="hidden" name="ssl_avs_address" value="123 Main St."> <!--AVS Postal Address -->
  <input type="hidden" name="ssl_avs_zip" value="01234"> <!--AVS ZIP Code -->
  <input type="submit" value="Donate Now">
</form>
```

### Behavior

In both Example 3 and Example 4, the output will be an HTML Receipt page describing the outcome of the transaction displayed to the customer. This page will either be a Receipt or result page drawn by viaKLIX, a viaKLIX error message indicating an error condition with the data sent to viaKLIX (such as when the ssl\_PIN doesn't match an existing terminal for the ssl\_merchant\_ID) or a Receipt page developed by you. See Appendix 3 for more about the Error Messages and Error Numbers and see the next two chapters for more information on Receipt pages.

## Receipt Options

The Receipt is the customer's documentation of the outcome of the transaction authorization. It also is the page that can send the transaction information back to your Web site, based on the customer's actions. If viaKLIX is drawing the Receipt for you, then your Web site will not need to include logic to parse through the viaKLIX result, but your customer might not return to your Web site when the transaction is complete. If you are drawing your own Receipt, then your form will need to handle the data received from viaKLIX in order to correctly communicate to your customer the outcome of their transaction.

### viaKLIX Provided Receipt

This section will instruct you on the methodology of allowing viaKLIX to display the receipt to your customer. The receipt has quite a few configuration possibilities that can be driven by code or by choices made in the Administration section of the viaKLIX Web site. Please see the Merchant's Guide for more information on how to use viaKLIX Web site to configure your Receipt options.

### Input

There are four primary variables that dictate how Receipts are processed:

- `ssl_result_format`
- `ssl_receipt_link_method`
- `ssl_receipt_link_url`
- `ssl_receipt_link_text`

You also have the option to split the last three of these up to allow for a different type of receipt for Approvals vs. Declines. If you use the variables above, they will take precedence over the following parameters:

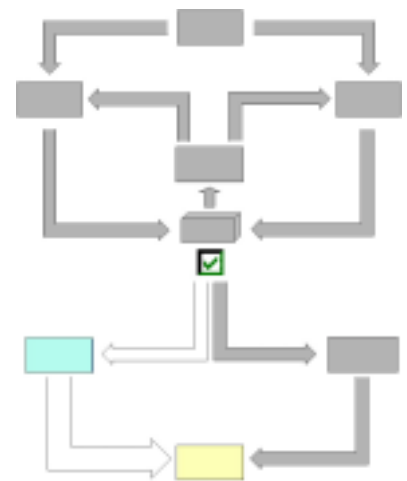
- `ssl_receipt_decl_method`
- `ssl_receipt_decl_get_url`
- `ssl_receipt_decl_post_url`
- `ssl_receipt_decl_text`
- `ssl_receipt_apprvl_method`
- `ssl_receipt_apprvl_get_url`
- `ssl_receipt_apprvl_post_url`
- `ssl_receipt_apprvl_link_text`

`Ssl_result_format` has acceptable values: ASCII and HTML. If you do not specify the format, an HTML receipt will be returned. If you specify ASCII, only a list of key/value pairs will be returned, the other Receipt related parameters you have sent in would be ignored. The ASCII format is intended to be called on by a separate application that will process the data, instead of directly by a web page used by customers initiating transactions.

There are four options for the various `ssl_receipt_link_method` variables:

- GET
- POST
- LINK
- REDG. GET
- POST

Your choice can be made by utilizing the button at the bottom of the Receipt for the customer to select so that they may return to your Web site. These two options will pass the transaction's data back to your site via the method chosen. LINK presents a hyperlink at the bottom of the viaKLIX receipt page, and does not transmit data back to your Web site. REDG (RE-Direct Get) is covered in more detail in the next section.



## Example 5:

To pass receipt options, use the following syntax:

```
<form action="https://www.viaKLIX.com/process.asp" method="POST">
  Your Total: $5.00 <br/>
  <input type="hidden" name="ssl_amount" value="5.00">
  <br/>
  <input type="hidden" name="ssl_merchant_id" value="my_merchant_ID">
  <input type="hidden" name="ssl_user_id" value="my_User_ID">
  <input type="hidden" name="ssl_pin" value="my_PIN">
  <input type="hidden" name="ssl_show_form" value="false">
  <input type="hidden" name="ssl_invoice_number" value="123-ABC">
  <input type="hidden" name="ssl_email" value="test@test.com">
  Credit Card Number: <input type="text" name="ssl_card_number"> <br/>
  Expiration Date (MMYY): <input type="text" name="ssl_exp_date" size="4"> <br/>
  <input type="hidden" name="ssl_result_format" value="HTML">
  <input type="hidden" name="ssl_receipt_decl_method" value="POST">
  <input type="hidden" name="ssl_receipt_decl_post_url" value="http://www.website.com/decline.asp">
  <input type="hidden" name="ssl_receipt_apprvl_method" value="GET">
  <input type="hidden" name="ssl_receipt_apprvl_get_url" value="http://www.website.com/approval.asp">
  <input type="hidden" name="ssl_receipt_link_text" value="Continue">
  <input type="submit" value="Continue">
</form>
```

Producing a receipt that includes the following code for an Accepted transaction:

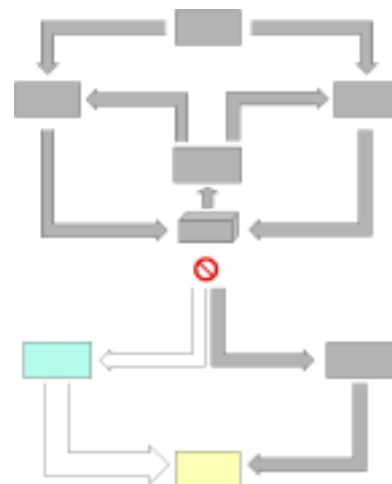
```
This is your Receipt<br><br>
...
<!--The visible portion of your receipt will appear here, according to the configuration settings you applied
in the viaKLIX administrative Web site.-->
...
<form action="http://www.website.com/approval.asp" method="GET">
<input type="hidden" name="ssl_result" value="0">
<input type="hidden" name="ssl_result_message" value="APPROVED">
<input type="hidden" name="ssl_txn_id" value="99C7884A-EDB6-4256-BE69-4547B8859D5B">
<input type="hidden" name="ssl_approval_code" value="N29032">
<input type="hidden" name="ssl_cvv2_response" value="">
<input type="hidden" name="ssl_avs_response" value="">
<input type="hidden" name="ssl_transaction_type" value="SALE">
<input type="hidden" name="ssl_invoice_number" value="123-ABC">
<input type="hidden" name="ssl_amount" value="5.00">
<input type="hidden" name="ssl_email" value=" test@test.com">
<br>
<input type="submit" value="Continue" class="smallbutton">
</form>
```

And producing a result form that includes the following code for a Declined transaction:

```

<b>An Error Occurred</b><br><br>
    Number : 1<br>
    Message : This transaction request has not been approved.
    You may elect to use another form of payment to complete this
    transaction or contact customer service for additional options.<br>
    <form action="http://www.website.com/decline.asp" method="POST">
    <input type="hidden" name="ssl_result" value="1">
    <input type="hidden" name="ssl_result_message"
    value="DECLINED">
    <input type="hidden" name="ssl_txn_id" value="B6637C93-CA38-
    41C5-951A-C995BFFBD708">
    <input type="hidden" name="ssl_approval_code" value="    ">
    <input type="hidden" name="ssl_cvv2_response" value="">
    <input type="hidden" name="ssl_avs_response" value="">
    <input type="hidden" name="ssl_transaction_type" value="SALE">
    <input type="hidden" name="ssl_invoice_number" value="123-ABC">
    <input type="hidden" name="ssl_amount" value="5.00">
    <input type="hidden" name="ssl_email" value=" test@test.com">
    <br>
    <input type="submit" value="Continue" class="smallbutton">
    </form>

```



**Please Note:** In all of these examples, you will have to change the data values, such as “my\_merchant\_ID”, “my\_PIN”, “123-ABC” and the amount of “5.00” to values that match your viaKLIX account and meet your Web site’s needs.

## Behavior

An HTML page will be displayed to your customer containing information as to whether the transaction was approved or not. If the transaction was approved, then the receipt will also display the data elements that make up the transaction. A link back to your Web site is displayed at the bottom of the page. This link is configured based on the parameters you set or the configuration settings you applied in the viaKLIX administrative Web site. If you choose, you can set the format to ASCII or override the receipt link parameter in your code. Also, it is possible to specify the behavior for the approvals separate from the behavior of the declines.

Example 5, above, shows two possible outcomes for a viaKLIX Receipt. **A receipt containing ssl\_result=0 represents an Approved transaction. A receipt containing any other value for ssl\_result represents a Declined transaction, or a transaction that had an error, preventing it from being authorized.** See Appendix 2 for other possible response codes.

## Merchant Provided Receipt

This section will tell you what you need to do to show your customer a receipt of your own creation for a viaKLIX transaction. The receipt has quite a few configuration possibilities that can be driven by code, or by choices made in the Administration section of the viaKLIX Web site. Please see the Merchant's Guide for more information on using the viaKLIX Web site to configure your Receipt options.

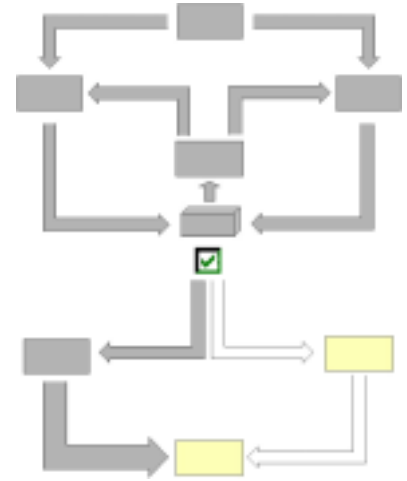
### Input

There are four primary variables that dictate how Receipts are processed:

- ssl\_result\_format
- ssl\_receipt\_link\_method
- ssl\_receipt\_link\_url
- ssl\_receipt\_link\_text

You also have the option to split the last three of these up to allow for a different type of receipt for Approvals vs. Declines. If you use the variables above, they will take precedence over the following parameters:

- ssl\_receipt\_decl\_method
- ssl\_receipt\_decl\_get\_url
- ssl\_receipt\_decl\_post\_url
- ssl\_receipt\_decl\_text
- ssl\_receipt\_apprvl\_method
- ssl\_receipt\_apprvl\_get\_url
- ssl\_receipt\_apprvl\_post\_url
- ssl\_receipt\_apprvl\_link\_text



### Result Format

Ssl\_result\_format has acceptable values:

- ASCII
- HTML

If you do not specify the format an HTML receipt will be returned. If you select ASCII, only a list of key/value pairs will be returned, the other Receipt related parameters you have set are ignored. The ASCII format is recommended if you are using an intermediary application to send transactions to viaKLIX rather than sending transactions to viaKLIX directly from an HTML form on a Web page that is driven by your customer's actions. The ASCII format will allow you to easily parse through the transaction data and choose what to display to your customer, and what data to use in other ways for your own application.

### Example 6:

To pass receipt options requesting an ASCII response, use the following syntax:

```
<form action="https://www.viaKLIX.com/process.asp" method="POST">
  Your Total: $5.00 <br/>
  <input type="hidden" name="ssl_amount" value="5.00">
  <br/>
  <input type="hidden" name="ssl_merchant_id" value="my_merchant_ID">
  <input type="hidden" name="ssl_user_id" value="my_User_ID">
```

```

<input type="hidden" name="ssl_pin" value="my_PIN">
<input type="hidden" name="ssl_show_form" value="false">
<input type="hidden" name="ssl_invoice_number" value="123-ABC">
<input type="hidden" name="ssl_email" value="test@test.com">
Credit Card Number: <input type="text" name="ssl_card_number"> <br/>
Expiration Date (MMYY): <input type="text" name="ssl_exp_date" size="4"> <br/>
<br/>
<input type="hidden" name="ssl_result_format" value="ASCII">
<input type="submit" value="Continue">
</form>

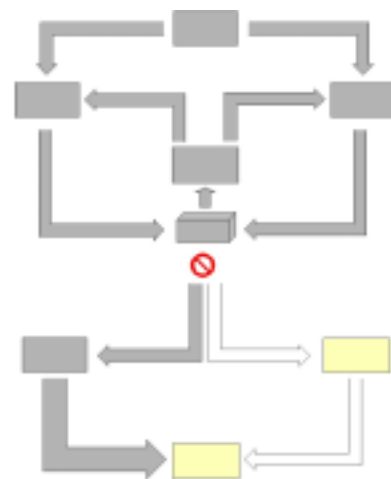
```

Producing a receipt that includes the following key/value pairs for an Accepted transaction:

```

ssl_result=0
ssl_result_message=APPROVED
ssl_txn_id=9621F9AD-E49E-4003-91BD-5C1B08569959
ssl_approval_code=N54032
ssl_cv2_response=
ssl_avs_response=
ssl_transaction_type=SALE
ssl_invoice_number=123-ABC
ssl_amount=5.00
ssl_card_number=00*****0000
ssl_exp_date=0000
ssl_email=test@test.com

```



And producing a receipt that includes the following key/value pairs for a Declined transaction:

```

ssl_result=1
ssl_result_message=This transaction request has not been approved. You may elect to use another form
of payment to complete this transaction or contact customer service for additional options.

```

Example 6 (above) shows 2 possible outcomes for an ASCII viaKLIX Receipt. **A receipt containing `ssl_result=0` represents an Approved transaction. A receipt containing any other value for `ssl_result` represents a Declined transaction, or a transaction that had an error, preventing it from being authorized.**

### Receipt Link Method: Re-direct Get

There are four options for the various `ssl_receipt_link_method` variables. To display a receipt of your own, you must use REDG (RE-Direct Get). REDG will redirect the customer's Browser to the URL of your choosing as soon as the transaction is processed by viaKLIX.

Using the various `ssl_receipt_link_url` variables viaKLIX gives you the option of sending approved and declined transactions to the same URL or to different URLs to handle them separately. If you are using the REDG method and wish to have separate approved and declined behaviors, you will want to use the "get" versions of the `ssl_receipt_link_url` variables, to specify the destination URL. Specifically:

- `ssl_receipt_decl_get_url`
- `ssl_receipt_apprvl_get_url`

## Example 7:

To pass receipt options for redirecting the customer to your own receipt, use the following syntax:

```
<form action="https://www.viaKLIX.com/process.asp" method="POST">
  Your Total: $5.00 <br/>
  <input type="hidden" name="ssl_amount" value="5.00">
  <br/>
  <input type="hidden" name="ssl_merchant_id" value="my_merchant_ID">
  <input type="hidden" name="ssl_user_id" value="my_User_ID">
  <input type="hidden" name="ssl_pin" value="my_PIN">
  <input type="hidden" name="ssl_show_form" value="false">
  <input type="hidden" name="ssl_invoice_number" value="123-ABC">
  <input type="hidden" name="ssl_email" value="test@test.com">
  Credit Card Number: <input type="text" name="ssl_card_number"> <br/>
  Expiration Date (MMYY): <input type="text" name="ssl_exp_date" size="4"> <br/>
  <br/>
  <input type="hidden" name="ssl_result_format" value="HTML">
  <input type="hidden" name="ssl_receipt_decl_method" value="REDG">
  <input type="hidden" name="ssl_receipt_decl_get_url" value="http://www.website.com/decline.asp">
  <input type="hidden" name="ssl_receipt_apprvl_method" value="REDG">
  <input type="hidden" name="ssl_receipt_apprvl_get_url" value="http://www.website.com/approval.asp">
  <input type="submit" value="Continue">
</form>
```

Redirecting to “http://www.website.com/approval.asp” for an Accepted transaction or to “http://www.website.com/decline.asp” for a Declined transaction. The transaction data will be passed along as Get variables in the query string of the URL.

## Behavior

In examples 6 and 7, your customer will see the receipt page you provide. Either your application will have received the transaction data in an ASCII format, and must then re-present that information to your customers in whatever fashion you determine, or their browser will be redirected to the page you have specified with transaction data being passed in the query string.



## Best Practices

This section will indicate some of the Best Practices for using version 2.0. Some of these items are features that existed in version 1.0. Developers and merchant administrators may find the information presented here valuable when writing and configuring applications and Web sites that will interface with viaKLIX, but Merchant Admins may find this information valuable as well. These best practices focus on ways to increase security and reduce the chance of fraudulent activity.

- **HTTP Referrer** – Setting up the use of HTTP Referrers in the admin site tells viaKLIX to only accept transactions from a pre-approved list of Web sites. While requiring more work to implement, this action will prevent fraudulent users from submitting transactions from their Web site, claiming to be you.
- **Server Side Code** – Your users can read HTML source code from your Web pages when they are downloaded to the Web browser. Although our simple examples in the document show this as a method for passing data to viaKLIX, we do not recommend this for your production web site. All sensitive merchant data, including transaction amount and your viaKLIX credentials, should be placed in server side code, rather than of just hidden value fields on an HTML form. This will reduce the ability for malicious users to edit and use this data for their own fraudulent purposes.
- **Auto Pend** – We recommend that you use the Auto-Pend feature for any account that is set to Auto-Settle. This gives you the chance to review each transaction before it becomes finalized. This will help you avoid settling fraudulent transactions or transactions that you are unable to fulfill.
- **Merchant Admin** – The Merchant Admin account has full rights and access to each terminal in your system. We recommend that you use this account sparingly. We suggest that you create one or more separate accounts to manage day-to-day activity, including but not limited to: processing transactions from your web site, processing Virtual Terminal transactions, reviewing transactions and settling transactions. We recommend you do this even in the case of an Account with only one terminal.
- **Password Security** – Do not set your password to be the same value (or a similar value) as any other data associated with your viaKLIX account. This includes your viaKLIX PIN used for submitting transactions to process.asp. This PIN is not designed as a security feature. It is only used to ensure that transactions sent into viaKLIX are assigned to the correct Account, User and Terminal. Unlike the passwords, the PIN is not stored as encrypted data in our database. Your password is a highly confidential piece of data and is treated as such. Our administrators do not have access to your password data. You should make all of your Accounts' passwords as difficult to guess as possible.
- **Settings in Admin site** – We recommend that whenever possible you set Terminal options in the Administrative site, instead of setting equivalent parameters in code on your Web page. This will make it easier to maintain and will reduce the amount of data that is passed across the Internet with each of your transactions.

## What's New?

This section outlines the new features in version 2.0. It is intended as a guide to assist the merchants and developers who have used viaKLIX version 1.0. The information here is targeted at Developers writing applications and Web sites that will interface with viaKLIX, as well as Merchant Admins who manage individual viaKLIX accounts.

- **HTTP Referrer** – The HTTP Referrer feature is used to tell viaKLIX to accept only transactions from a pre-approved list of Web sites. This will prevent fraudulent users from submitting transactions from their Web site, claiming to be you. In version 1.0, any transaction sent in with the correct viaKLIX ID and PIN was accepted as coming from that merchant, regardless its origin.
- **Separate Decline Receipt Approved Receipt Options** – The split Receipt feature allows viaKLIX to handle Approved and Declined transactions differently. And more importantly, it allows you to tell viaKLIX about these differences. You can specify different URLs for your own custom receipts; allow viaKLIX to pass different transaction information back to you and much more. In version 1.0, Declined transactions simply presented a decline message to the user. Aside from an optional e-mail, there was no way for the merchant to learn about the decline in order to help the customer through this situation.
- **Multiple Terminals per VID** – viaKLIX accounts are now capable of having multiple terminals assigned to them. This allows you keep all of your viaKLIX transactions together. Whether you have multiple Web sites, a MO/TO call center, or multiple retail store locations, you can now manage all of your accounts from a single viaKLIX account. In version 1.0, each viaKLIX account was limited to one Terminal.
- **MO/TO and Retail Terminals** – viaKLIX now supports terminals for the MO/TO and Retail market place, as well as the Internet. This allows you to take advantage of better Interchange rates for transactions in those Market Segments. In version 1.0, only Internet Terminals were supported.
- **User Hierarchy including user Rights, and Terminal association** – The new User hierarchy allows you to assign different user ID's to each person using your account on viaKLIX. This allows to you assign different rights and functions to specific people in your organization. This feature also will allow you track which people are making new sales. In version 1.0, each viaKLIX account only had one user. That user had full access to all of that account's data and all of the different functions that could be performed on that data.
- **Disabling HTTP Transactions** – Terminals can now be set to deny all HTTP transactions from process.asp. This way if a terminal is only accessed from the viaKLIX Virtual Terminal, viaKLIX will know not to accept transactions for this terminal sent into process.asp from Web sites on the Internet. In version 1.0, all terminals allowed HTTP Transactions from process.asp, even if the terminal was not associated with a Web site.
- **Advanced Headers/Footers** – viaKLIX now allows you to use a special viaKLIX Markup Language to present custom headers and footers to your customers on e-mails, the payment form and the receipt page. True HTML tags are not allowed for security reasons, but the text and tags you enter will be translated into HTML to allow you to present more advanced content to your customers. In version 1.0, all headers and footers for e-mails, payment forms and receipts had to be in plain text.
- **Card Swipe** – The new Card Swipe feature allows viaKLIX to accept card data from a Magnetic Card Reader input device attached to your computer. This will allow you to process face to face retail transactions using the Virtual Terminal. Along with the added convenience to both you and your customers, these types of transactions result in the lowest Interchange Rates possible! In version 1.0, there were no features to handle retail transactions of any kind.

- **Serial Receipt Printer** – To add to the new capabilities to handle Retail Terminals, printed receipts for transactions are now supported. This includes the ability to interface with a Serial Receipt Printer with options to specify paper type, headers and footers, as well as the ability to print out your own custom fields. In version 1.0, there were no features to handle retail transactions of any kind.
- **More complex PINs** – To help prevent PIN cracking, the PINs can now be longer, and contain more data than before. PINs can be up to six characters in length and contain full alphanumeric data. In version 1.0, All PINs were just four-digit numeric pieces of data.
- **Error Configuration** – You can now customize some error messages that the system displays. This allows you to specify contact information, helpful tips, multi-language instructions, or other information that you didn't have the option to present to your customer before. In version 1.0, all messages were determined by the system.

## Appendices

### Appendix 1: Input values

Field Name	Size	Default (when not present)	Comments
<b>Transaction Data</b>			
ssl_test_mode	0	FALSE	optional, when set to TRUE, transactions will not be forwarded to the credit card processor, but instead will always return an "APPROVED" result.
ssl_transaction_type	10	SALE	required, SALE; CREDIT; or FORCE
ssl_merchant_id	15		required, viaKLIX merchant id
ssl_pin	6		required, viaKLIX merchant pin
ssl_user_id	15	ssl_merchant_id	required, viaKLIX user id
ssl_amount	10		required, amount of the transaction
ssl_salestax			optional, amount of sales tax
ssl_card_number	19		required, customer's credit card number
ssl_exp_date	4		required, customer's credit card expiration date
ssl_cv2	11		CVV2 Indicator
ssl_cv2cvc2	4		CVV2/CVC2 Data
ssl_description	255		optional, transaction description
ssl_invoice_number	10		optional, transaction information
ssl_customer_code	20		optional
ssl_company	50		optional, customer's company name
ssl_first_name	20		optional, customer's first name
ssl_last_name	30		optional, customer's last name
ssl_avs_address	30		optional, customer's address used to process AVS
ssl_address2	30		optional, customer's address
ssl_city	30		optional, customer's city
ssl_state	10		optional, customer's state
ssl_avs_zip	10		optional, customer's zip code and zip code used to process AVS
ssl_country	50		optional, customer's country
ssl_phone	20		optional, customer's phone number
ssl_email	100		optional, customer's E-mail address
ssl_ship_to_company	50		optional, customer's company name
ssl_ship_to_first_name	20		optional, customer's first name
ssl_ship_to_last_name	30		optional, customer's last name
ssl_ship_to_address	30		optional, customer's address
ssl_ship_to_city	30		optional, customer's city
ssl_ship_to_state	10		optional, customer's state
ssl_ship_to_zip	10		optional, customer's postal code
ssl_ship_to_country	50		optional, customer's country
<b>Email</b>			
ssl_email_header	4000	set in admin	Customer order confirmation email header; If present, overrides values for ssl_email_apprvl_header_html and ssl_email_decl_header_html

Field Name	Size	Default (when not present)	Comments
ssl_email_apprvl_header_html			Customer order confirmation email header for approvals
ssl_email_decl_header_html			Customer order confirmation email header for declines
ssl_email_footer	4000	set in admin	Customer order confirmation email footer; If present, overrides values for ssl_email_apprvl_footer_html and ssl_email_decl_footer_html
ssl_email_apprvl_footer_html			Customer order confirmation email footer for approvals
ssl_email_decl_footer_html			Customer order confirmation email footer for declines
ssl_do_customer_email	1	set in admin (TRUE   FALSE)	TRUE : viaKLIX will send email to customer FALSE : viaKLIX will not send email to customer
ssl_do_merchant_email	1	Set in admin (TRUE   FALSE)	TRUE : viaKLIX will send email to merchant FALSE : viaKLIX will not send email to merchant
ssl_merchant_email	100	Set in admin	Merchant's email address
<b>Colors and Text</b>			
ssl_header_color	20	Set in admin	any valid HTML color value
ssl_text_color	20	Set in admin	any valid HTML color value
ssl_background_color	20	Set in admin	any valid HTML color value
ssl_table_color	20	Set in admin	any valid HTML color value
ssl_link_color	20	Set in admin	any valid HTML color value
<b>Payment Form</b>			
ssl_show_form	5	TRUE	optional, when set to FALSE viaKLIX will not present the payment form but process the transaction directly.
ssl_header_html	4000	set in admin	payment form header ignored when ssl_show_form=FALSE
ssl_footer_html	4000	set in admin	payment form footer ignored when ssl_show_form=FALSE
<b>Receipt Input</b>			
ssl_result_format	5	HTML	optional, when set to ASCII viaKLIX will generate a plain text key-value document.
ssl_receipt_header_html	4000	set in admin	Receipt form header ignored when ssl_result_format=ASCII
ssl_receipt_apprvl_header_html	4000	set in admin	Receipt form header for Approved Transaction. Ignored when ssl_result_format=ASCII
ssl_receipt_decl_header_html	4000	set in admin	Receipt form header for Declined Transaction. Ignored when ssl_result_format=ASCII
ssl_receipt_footer_html	4000	set in admin	Receipt form footer Ignored when

Field Name	Size	Default (when not present)	Comments
			ssl_result_format=ASCII
ssl_receipt_apprvl_footer_html	4000	set in admin	Receipt form footer for Approved Transaction. Ignored when ssl_result_format=ASCII
ssl_receipt_decl_footer_html	4000	set in admin	Receipt form footer for Declined Transaction. Ignored when ssl_result_format=ASCII
ssl_receipt_link_method	4	Set in admin (LINK   GET   POST   REDG)	Type of link to generate at the bottom of the receipt. Ignored when ssl_result_format=ASCII. If present, overwrites ssl_receipt_apprvl_method and ssl_receipt_decl_method
ssl_receipt_apprvl_method	4	Set in admin (LINK   GET   POST   REDG)	Type of link to generate at the bottom of the receipt for an approved transaction. Ignored when ssl_result_format = ASCII.
ssl_receipt_decl_method	4	Set in admin (LINK   GET   POST   REDG)	Type of link to generate at the bottom of the receipt for a declined transaction. Ignored when ssl_result_format = ASCII.
ssl_receipt_link_url	255	set in admin	Target of the Redirect or the link generated at the bottom of the viaKLIX drawn receipt. Ignored when ssl_result_format=ASCII; If present, overwrites ssl_receipt_apprvl_method and ssl_receipt_decl_method
ssl_receipt_apprvl_post_url		set in admin	Target of the link generated at the bottom of the receipt for an approval using the "POST" method. Ignored when ssl_result_format=ASCII
ssl_receipt_decl_post_url		set in admin	Target of the link generated at the bottom of the receipt for a declined transaction using the "POST" method. Ignored when ssl_result_format=ASCII
ssl_receipt_apprvl_get_url		set in admin	Target of the link generated at the bottom of the receipt for an approval using the "GET" method, or the Target of the redirect for an approval using the "REDG" method. Ignored when ssl_result_format=ASCII
ssl_receipt_decl_get_url		set in admin	Target of the link generated at the bottom of the receipt for a declined transaction using the "GET" method, or the Target of the redirect for a declined transaction using the "REDG" method. Ignored when ssl_result_format=ASCII

Field Name	Size	Default (when not present)	Comments
ssl_receipt_link_text	100	Set in admin	Text in the link / on the submit button generated at the bottom of the receipt page. Ignored when ssl_result_format=ASCII; If present, overwrites ssl_receipt_apprvl_text and ssl_receipt_decl_text
ssl_receipt_apprvl_text		set in admin	Text that appears on the receipts of approved transactions
ssl_receipt_decl_text		set in admin	Text that appears on the receipts of declined transactions
<b>Receipt Output</b>			
ssl_result	1	0	Result code for the transaction: a result of 0 indicates an approval; any other result means that the transaction was not approved.
ssl_result_message	8	APPROVED	Result message for the transaction: a result of "APPROVED" indicates an approval; any other result means that the transaction was not approved.
ssl_txn_id	36		Unique transaction identifier
ssl_approval_code	10		Return code generated by credit card processor
ssl_cvv2_response	1		Return code generated by service. See Appendix 3: CVV2/CVC Response Codes
ssl_avs_response	1		Return code generated by service. See Appendix 2: AVS Response Codes
<b>AVS Specific Fields</b>			
ssl_avs_address	30		optional, customer's address used to process AVS
ssl_avs_zip	10		optional, customer's zip code and zip code used to process AVS
ssl_avs_response	1		Return code generated by service. See Appendix 2: AVS Response Codes
<b>CVV2/CVC2 Specific Fields</b>			
ssl_cvv2	11		CVV2 Indicator (PRESENT / NOT PRESENT / MISSING / ILEGILE)
ssl_cvv2cvc2	4		CVV2/CVC2 Data
ssl_cvv2_response	1		Return code generated by service. See Appendix 3: CVV2/CVC Response Codes

## Appendix 2: Response Codes

### Authorization Response Codes

This is a list of the values that may be returned during an authorization request.

Authorization Response Codes		
Code	Message	Definition
AA	APPROVAL	Approved
AA	ACCEPTED	Frequency Approval
NC	PICK UP CARD	Pick up card
ND	AMOUNT ERROR	Tran Amount Error
ND	DECLINED	Do Not Honor
ND	DECLINED-HELP 9999	System Error
ND	EXPIRED CARD	Expired Card
ND	INVALID CARD	Invalid Card
ND	INVALID TERM ID	Invalid Terminal ID
ND	INVLD TERM ID 1	Invalid Merchant Number
ND	INVLD TERM ID 2	Invalid SE Number
ND	INVLD VOID DATA	Invalid Data
ND	SERV NOT ALLOWED	Invalid request
NR	CALL AUTH. CENTER	Refer to Issuer
NR	CALL REF.; 999999	Refer to Issuer
N7	DECLINE CVV2	Do Not Honor; Declined due to CVV2 mismatch \ failure



## AVS Response Codes

An **AVS Response Code** will be returned in Authorization Response Message when AVS information is present in the transaction authorization request.

AVS Response Codes	
Code	Definition
<b>A</b>	Address matches - Zip Code does not match.
<b>B</b>	Street address match, Postal code in wrong format. (International issuer)
<b>C</b>	Street address and postal code in wrong formats
<b>D</b>	Street address and postal code match (international issuer)
<b>E</b>	AVS Error
<b>G</b>	Service not supported by non-US issuer
<b>I</b>	Address information not verified by international issuer.
<b>M</b>	Street Address and Postal code match (international issuer)
<b>N</b>	No Match on Address (Street) or Zip
<b>O</b>	No Response sent
<b>P</b>	Postal codes match, Street address not verified due to incompatible formats.
<b>R</b>	Retry, System unavailable or Timed out
<b>S</b>	Service not supported by issuer
<b>U</b>	Address information is unavailable
<b>W</b>	9 digit Zip matches, Address (Street) does not match.
<b>X</b>	Exact AVS Match
<b>Y</b>	Address (Street) and 5 digit Zip match.
<b>Z</b>	5 digit Zip matches, Address (Street) does not match.

## CVV2/CVC Response Codes

The **CVV2 Response Codes** are returned in an Authorization Response Message when the CVV2 data is present in the transaction authorization request.

CVV2 Response Codes	
Code	Definition
<b>M</b>	CVV2 Match
<b>N</b>	CVV2 No match
<b>P</b>	Not Processed
<b>S</b>	Issuer indicates that CVV2 data should be present on the card, but the merchant has indicated that the CVV2 data is not resent on the card
<b>U</b>	Issuer has not certified for CVV2 or Issuer has not provided Visa with the CVV2 encryption Keys.

## Appendix 3: viaKLIX Error Numbers and Messages

A **viaKLIX Error Number and Error Message** is returned when the transaction fails to be authorized. This could be the result of a data or system error, or if the transaction is “Declined.” For backwards compatibility, the non-unique v1 error number is currently returned.

viaKLIX Error Messages and Numbers		
V2 Number	V1 Number	Error Message
3000	3	Error, no response.
3001	3	<i>NOVALINK ERROR MESSAGE</i>
4000	2	The viaKLIX ID was not supplied in the authorization request.
4001	N/A	The viaKLIX ID, User ID and/or PIN supplied in the authorization request is invalid.
4002	N/A	HTTP POST transactions are not allowed for this account.
4003	N/A	HTTP POST transactions are not allowed for this HTTP Referrer.
4005	5	The Email Address supplied in the authorization request appears to be invalid.
4006	1000	CVV2 Data was supplied, but the CVV2 indicator was not identified in the authorization request.
4007	1000	CVV2 check cannot be performed as no data was supplied in the authorization request.
4009	2	A required field was not supplied in the authorization request.
4010	4	An invalid Transaction Type was supplied in the authorization request.
4012	7000	The viaKLIX ID and/or User ID supplied in the authorization request is invalid.
4013	8000	The PIN was not supplied in the authorization request.
4014	7000	This account is not permitted to process transactions.
4015	7000	The PIN supplied in the authorization request is invalid.
4016	4016	This account does not have permission to process <b>TRANSACTIONTYPE</b> transactions.
5000	4000	The Credit Card Number supplied in the authorization request appears invalid.
5001*	5000	The Credit Card Expiration Date supplied in the authorization request appears invalid.
5002	7000	The amount supplied in the authorization request appears invalid.
5003	8000	A FORCE Approval Code was supplied for this transaction, however the transaction type is not FORCE.
5004	2	The FORCE Approval Code supplied in the authorization request appears invalid or blank. The

		FORCE Approval Code must be 6 or less alphanumeric characters.
5005	N/A	The value for the <b>DISPLAYNAME</b> field is too long. <b>XX</b> characters (maximum) are allowed. Your entry contains <b>XXX</b> characters.
5006	N/A	Invalid Transaction The refund amount for this transaction (\$ <b>XX.XX</b> ) may not exceed \$ <b>XX.XX</b> .
5007*	6000	The Credit Card Expiration Date supplied in the authorization request appears invalid or blank.
60XX	1	This transaction request has not been approved. You may elect to use another form of payment to complete this transaction or contact customer service for additional options.

\* The difference between the V2 errors 5001 and 5007 is that 5001 corresponds to a check in V1 (V1 error number 5000) for the correct length of the expiration date passed in while 5007 corresponds to the V1 validity check of the expiration date (numeric, first two digits map to month; V1 error number 6000).

## Glossary of Terms

### Address Verification

The process of verifying customer addresses with the issuing bank to minimize fraudulent transactions.

### Authorization

The process of having credit card transactions approved by the issuing bank through communication with the NOVA Network.

### Auto-Pend Transaction

A transaction option that automatically "Pends" Sale transactions submitted through the viaKLIX payment form.

### Auto-Settle

An option that automatically settles all "unpending" transactions in the Unsettled Transaction batch at a specified time each day.

### Card Verification Value

The process of verifying the Card Verification Value with the issuing bank to minimize fraudulent transactions. The CVV2 value is a three or four-digit value that is printed in reverse italics on the backside of the card. This additional value is not embossed upon the front of the card, nor is it contained upon the magnetic stripe on back.

### Comma-Separated Value

A text file format in which all data elements within the file are separated by a comma. This format is also referred to as a comma delimited file.

### Filter

A function that allows you to enter specific parameters to narrow a search for transaction information in a particular file. You can search for a specific card number, within a specific date range, etc.

### Force Transaction

A transaction with a previously obtained authorization that needs to be entered in the current batch.

### GBOK Number

A successful settlement batch with the NOVA Network.

### HTTP Referrer

The HTTP Referrer Web site that sent the customer to viaKLIX. This can be used to allow traffic into viaKLIX for a given terminal to be limited only to the merchant's website. This will prevent a malicious hacker from masquerading as a given merchant and running transactions through their terminal.

### Merchant Admin

The default user account for the viaKLIX account; the **Merchant Admin User ID (MID)** is the same as the **viaKLIX Account ID**. This special user cannot be deleted, always has all user rights and all terminal associations.

**Peer User**

A user who shares the same supervisor as you.

**Pend Transaction**

A transaction status option that will not allow the transaction to be submitted for settlement. To change the status of the transaction to allow it to be submitted for settlement, it must be **"Unpending"**.

**Refund Transaction**

A transaction used to refund a previous purchase.

**Sale Transaction**

A transaction in which an authorization is obtained and the transaction is entered into the unsettled batch.

**Scope of user rights**

Virtual Terminal and Terminal Setup rights apply to your ability to do things in the context of any terminal in your Terminal Associations list. User Management rights apply to your ability to do things to your subordinates and to your peers' subordinates. If you have the Edit Terminal Associations right, you may only add terminal associations that you, yourself have.

**Settlement Process**

The process of sending a batch of previously authorized transactions for settlement to the NOVA Network.

**Subordinate**

This is anyone who is directly below you in the user hierarchy, or any of their **subordinates**.

**Supervisor**

This is the person directly above you in the user hierarchy.

**Tab-Delimited Value**

A text file format in which all data elements within the file are separated by the Tab character.

**Terminal Association**

Where your user rights refer to something you can do involving a terminal (make a sale or settle a transaction), your user must be associated with that terminal and you must have selected that terminal context in viaKLIX. See the chapter on User Management for details on how to make or edit **Terminal Associations**.

**Terminal Friendly Name**

Terminals are referred to in viaKLIX by a **Friendly Name** configured by NOVA's Internet Product Support, for instance, "Web site Terminal."

**Terminal ID**

A number used to identify the source of a transaction to the NOVA Network. This corresponds to a physical credit card terminal in a traditional POS solution, but for viaKLIX, this is a virtual ID. You may have more than one terminal for use within your viaKLIX account. Each **Terminal ID (TID)** is associated with certain features as dictated by your NOVA merchant agreement. "Merchant Information" in Terminal Setup can be different for each terminal so that, for instance, the address printed on a receipt is correct for that location. See the chapter on Terminal Setup for details on configuring your terminal.

## Unpend Transaction

A transaction status option that will allow the transaction to be submitted for settlement. To prohibit the transaction from being submitted for settlement, it must be "**Pended**".

## User Account

The **user** you use to sign in to viaKLIX; the **User ID** is case sensitive

## User Rights

The things that your **User Account** can do in viaKLIX; there are three areas of **User Rights**: Virtual Terminal, User Management and Terminal Setup. See the chapter on User Management for details on how to make or edit **User Rights**

## viaKLIX Account

The **viaKLIX Account** your company has with the NOVA Network.

## Developer Guide

06-19-03



**NOVA NETWORK**

*The most reliable payment processing  
network in the industry*