

Online Payments Specification

Kenswitch

Kenswitch Web Service

Version 1.3

July 2011

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without express written permission of:

The Managing Director
[Kenswitch](#)
16th Floor Ambank House, University Way, Nairobi

[Kenswitch](#) is committed to ongoing research and development in order to track technological developments and customer in the market. Consequently, information contained in this document may be subject to change without prior notice.

[Postilion](#) is a registered trademark of [S1 Limited](#).

[Windows 2003](#), [Windows XP](#), [Windows 2000](#) and [SQL Server](#) are trademarks of [Microsoft Corporation](#).

Document Version Control

Date	Version	Comments
May 31, 2011	1.0	Initial release...
June 3, 2011	1.1	Made updates to....
July 1, 2011	1.2	Addition of Kenswitch Online Payment Gateway. Addition of CVV field.
September,19	1.3	Addition of “KenswitchWebServiceAuthTransaction” Web Service
September,22	1.3.1	Addition of ‘mname’ request parameter

INTRODUCTION.....	5
Scope.....	5
Context	5
BACKGROUND	5
USING WEB SERVICE.....	6
CONSIDERATIONS.....	6
Communications	6
Security.....	6
MESSAGE TYPE SUPPORT	6
MESSAGE FORMATS.....	7
Message Structure.....	7
Online iPayment request	8
Online iPayment Response	8
EMBEDDING THE KENSWITCH ONLINE PAYMENT GATEWAY FORM.....	9
Considerations	9
Communication.....	9
Security.....	10
Modes of payment.....	10
Requirements.....	11
APPENDIX.....	12
Sample SOAP messages:	12
Sample SOAP messages for Authentication web service:	14
Kenswitch online Payment Gateway Form.....	16
Field Definitions	16

Introduction

Scope

The scope of this document is to describe the implementation and functioning of Kenswitch Web Service.

Context

The specification has been designed for third party integration and implementation of the Kenswitch Web Service to enable payment transactions.

Background

The Web Service channel was designed to support the following transactions:

- Purchase (00)
- Cash Withdrawal (01)

The Web Service can be implemented and integrated using:

- Using Web Service.
- Embedding the Kenswitch Online Payment Gateway Form.

Using Web Service

Considerations

Communications

Merchant will connect to the Web Service via a socket based TCP/IP connection. The Address to be used when calling the web service is:

<http://41.215.139.59:8080/KenswitchWebService/IPaymentsService?wsdl>

The merchant application will connect as a client while web service acts as a server.

Security

Card and pin information entered on merchant website should be secured using SSL certificates from a trusted CA.

Merchant will be authenticated using a token and secret.

Message exchange between merchant web server and web service will be secured through firewall encryption.

Message Type Support

- iPayment request
- iPayment response

Message Formats

Message Structure

Client application will exchange messages with the web service via Simple Object Access Protocol (SOAP) over a secure channel.

Online iPayment request

A field denoted as “M” means that it is mandatory and must be populated with valid data; “C” is conditional and may be required to be provided under certain conditions and “O” is optional and may or may not be provided under all conditions.

If a field is “C” or “O” it should be submitted with an empty string if no value is passed to it.

FIELD NAME		REMARK
token	M	
secret	M	
pan	M	
expiryDate	M	
pin	M	
tranType	M	
amount	M	
referenceNo	M	
transmissionDateAndTime	M	
localDate	M	
localTime	M	
systemTraceNo	M	
forwardingInst	O	Used in transactions that require a mobile number
receivingInst	C	Used for routing specific transactions
merchantid	M	
CVV	O	For Visa Cards only

Online iPayment Response

FIELD NAME		REMARK
tranType	M	
amount	M	
terminalId	O	
nameAndLocation	O	
referenceNo	M	
localDate	M	
localTime	M	
acquiringInstIdCode	O	
currencyCode	M	
responseCode	M	
additionalAmount	C	
additionalData	C	
systemAuditNumber	M	
authorizationResponseId	C	

Embedding the Kenswitch Online Payment Gateway Form

Considerations

Communication

Merchant will call and embed the Kenswitch Online Payment Gateway Form on their Website.

The address to be used when calling the form is:

[http://www.kenswitch.com/TestKenswitchPaymentGateway/KenswitchPaymentGateway.aspx?trant=\[value1\]&tid92012=\[value2\]&mid=\[value3\]&tamt=\[value4\]&recins=\[value5\]&trace=\[value6\]&reference=\[value7\]&tdt=\[value8\]&ldate=\[value9\]&time=\[value10\]&mail=\[value11\]&anonymous=\[value12\]&mname=\[value13\]](http://www.kenswitch.com/TestKenswitchPaymentGateway/KenswitchPaymentGateway.aspx?trant=[value1]&tid92012=[value2]&mid=[value3]&tamt=[value4]&recins=[value5]&trace=[value6]&reference=[value7]&tdt=[value8]&ldate=[value9]&time=[value10]&mail=[value11]&anonymous=[value12]&mname=[value13])

The various parameters and their values should be passed as above.

Once the Customer has filled in card/mobile payment details and clicked on the “pay” button, Kenswitch will effect payment and redirect the customer to the merchant’s transaction completion page. Kenswitch will pass 3 parameters: Reference number, Transaction amount and System trace number.

As / When Kenswitch redirects to **merchant’s** transaction completion page, the merchant will (on the background) call the Authentication web service (via Simple Object Access Protocol (SOAP)) to validate the transaction.

The URL for the Authentication web service is:

<http://41.215.139.59:8080/KenswitchWebServiceAuthTransaction/AuthTransaction?wsdl>

When calling the Authentication web service, the merchant will pass the following parameters:

	PARAMETER NAMES
Reference number	refNo
Transaction amount	amount
System trace number	sysTraceNo
Transmission date and time	transDateTime

Kenswitch will in turn respond by passing the following parameters:

	PARAMETER NAMES
Transaction amount	amount
Reference number	refNo
Response code	responseCode
System trace number	sysTraceNo
Transmission date and time	transDateTime

Depending on the response code, the merchant will build the logic for completing the payment.

The merchant will in turn receive an email.

The reference number will be used to track the transactions carried out.

Security

Card and pin information entered on Kenswitch Online Payment Gateway Form will be secured using SSL certificates from a trusted CA.

Merchant will be authenticated using a token and secret.

Pin Encryption is by triple DES.

Pin, mPin and CVV values on the form will be input using an online pin pad.

Modes of payment

The client will be able to make payment using either of the following:

- Kenswitch Card – Cards from any Kenswitch member banks
- Kenswitch Mobile – Client has to be registered for Kenswitch Mobile
- Visa Card-Local and International Visa Cards

Requirements

The merchant will be required to pass the following parameters:

	PARAMETER NAMES	REMARKS
Transaction Type	trant	(00) Purchase (01) Cash Withdrawal
Token	tid92012	
Merchant Id	mid	
Merchant Name	mname	
Amount	tamt	Total amount to be paid by the client
Receiving Institution	recinst	
System Trace No.	trace	
Reference No.	reference	
Transmission Date and Time	tdt	
Local Date	ldate	
Local Time	ltime	
Secret	anonymous	
Email	mail	The merchant's email address to which the response message will be sent

Appendix

Sample SOAP messages:

REQUEST:

```
POST http://192.168.5.224:8080/KenswitchWebService/IPaymentsService
HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; MS Web Services Client Protocol
2.0.50727.4959)
Content-Type: text/xml; charset=utf-8
SOAPAction: ""
Content-Length: 794
Expect: 100-continue
Proxy-Connection: Keep-Alive

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <PaymentOperation xmlns="http://webservices.kenswitch.org/">
      <parameter xmlns="">
        <amount>0</amount>
        <CVV />
        <expiryDate>1207</expiryDate>
        <forwardingInst/>
        <localDate>0630</localDate>
        <localTime>013517</localTime>
        <merchantid>0000000000000000</merchantid>
        <pan>5041580050001156</pan>
        <pin>9228</pin>
        <receivingInst/>
        <referenceNo>063001351711</referenceNo>
        <secret>defaultpass</secret>
        <systemTraceNo>013517</systemTraceNo>
        <token>default</token>
        <tranType>00</tranType>
        <transmissionDateAndTime>0630013517</transmissionDate
AndTime>
      </parameter>
    </PaymentOperation>
  </soap:Body>
</soap:Envelope>
```

RESPONSE:

HTTP/1.1 200 OK

Server: Apache-Coyote/1.1

Content-Type: text/xml; charset=utf-8

Transfer-Encoding: chunked

Date: Thu, 30 Jun 2011 10:30:38 GMT

<?xml version='1.0' encoding='UTF-8'?>

<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">

<S:Body>

<ns2:PaymentOperationResponse xmlns:ns2="http://webservices.kenswitch.org/">

<return>

<acquiringInstIdCode>000000000</acquiringInstIdCode>

<additionalAmount></additionalAmount>

<additionalData></additionalData>

<amount>0</amount>

<authorizationResponseId></authorizationResponseId>

<currencyCode>404</currencyCode>

<localDate>0630</localDate>

<localTime>013517</localTime>

<nameAndLocation>RUIRU THIKA

THKE</nameAndLocation>

<referenceNo>063001351711</referenceNo>

<responseCode>00</responseCode>

<systemAuditNumber>013517</systemAuditNumber>

<terminalId>1111111</terminalId>

<tranType>0630013517</tranType>

</return>

</ns2:PaymentOperationResponse>

</S:Body>

</S:Envelope>

Sample SOAP messages for Authentication web service:

REQUEST:


524: Client to Server (505 bytes, Incomplete last line)
 <?xml version="1.0" encoding="utf-8"?><soap:Envelope
 xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema"><soap:Body>
 <AuthenticateTransaction
 xmlns="http://authtransaction.webservice.kenswitch.org/">
 <parameter xmlns="">
 <amount>100</amount>
 <refNo>091403285811</refNo>
 <sysTraceNo>032858</sysTraceNo>
 <transDateTime>0914032858</transDateTime>
 </parameter>
 </AuthenticateTransaction>
 </soap:Body>
 </soap:Envelope>

RESPONSE:

524: Server to Client (602 bytes)
 HTTP/1.1 200 OK
 Server: Apache-Coyote/1.1
 Content-Type: text/xml; charset=utf-8
 Transfer-Encoding: chunked
 Date: Mon, 19 Sep 2011 09:06:23 GMT

<?xml version='1.0' encoding='UTF-8'?><S:Envelope
 xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"><S:Body>
 145
 <ns2:AuthenticateTransactionResponse
 xmlns:ns2="http://authtransaction.webservice.kenswitch.org/">
 <return>
 <amount>100</amount>
 <refNo>091403285811</refNo>
 <responseCode>06</responseCode>
 <sysTraceNo>032858</sysTraceNo>
 <transDateTime>0914032858</transDateTime>
 </return>
 </ns2:AuthenticateTransactionResponse>
 </S:Body>
 </S:Envelope>

Kenswitch online Payment Gateway Form



WELCOME TO KENSWITCH PAYMENTS GATEWAY
Please verify the payment amount and then select your preferred payment method.
Merchant :
Amount (KES):

Choose preferred mode of payment :

☐ Kenswitch Card
 ☐ Kenswitch Mobile
 ☐ Visa Card

Pay using your Kenswitch ATM card with a secured pin.

Card Number :

Card Expiry Date :

Card Pin : (use pin pad below)

Register for Kenswitch Mobile to receive payments alerts.

Register for Kenswitch Mobile? ☐

Mobile Number :

5

8

9

4

7

2

3

0

1

6

Clear

PIN PAD

Field Definitions

FIELDS	DESCRIPTION	FORMAT
Token	This is a username provided by Kenswitch to the merchant	

	for authentication purposes.	
Secret	This is a password provided by Kenswitch to the merchant for authentication purposes.	
Primary Account Number (Pan):	This is a number identifying the cardholder .Typically it is printed/embossed on the front of a card (e.g. An ATM card).	19 numeric digits
Expiry Date	The month and year after which the card expires. It should be the format MMYY.	4 numeric digits
Pin	The number assigned to a cardholder intended to uniquely identify that cardholder.	4 numeric digits
Transaction Type	Indicates the type of the transaction as indicated below: Debits 00 Purchases 01 Cash withdrawal	2 numerical digits
Amount	The funds requested by the cardholder in the local currency of the source location of the transaction exclusive of transaction fees. Values are expressed in the minor denomination (e.g. cents). For example, KES 1,500.00 is represented as 000000150000	12 numerical digits
Reference Number	A reference number supplied by the system retaining the original source information and used to assist in locating that information or a copy thereof.	An12
Transmission Date and Time	The date and time, when this message is sent by the message initiator. It should be in the format MMDDhhmmss e.g 0321034534	10 numerical digits
System Trace Audit Number	A number assigned by a transaction originator to assist in identifying a transaction uniquely.	6 numeric digits
Amount (In Response)	The transaction amount that was approved in the local currency of the acquirer or source location of the transaction exclusive of transaction fees. Values are expressed in the minor denomination (e.g. cents).	12 numerical digits
Terminal ID	A unique code identifying a terminal at the card acceptor location	Ans 8
Name and Location	The name and location of the card acceptor (such as a merchant or an ATM).	Ans40
Local Date	The local date at which the transaction takes place. It should in the format MMDD	4 numerical digits
Currency Code	The local currency of the acquirer or source location of the transaction.	3 numeric digits
Response Code	A code that defines the disposition of a transaction T1 Timed Out E1 Internal System Error 00 Approved or completed successfully	An2

	01 Refer to card issuer 02 Refer to card issuer, special condition 03 Invalid merchant 04 Pick-up card 05 Do not honor 06 Error 07 Pick-up card, special condition 08 Honor with identification 09 Request in progress 10 Approved, partial 11 Approved, VIP 12 Invalid transaction 13 Invalid amount 14 Invalid card number 15 No such issuer 16 Approved, update track 3 17 Customer cancellation 18 Customer dispute 19 Re-enter transaction 20 Invalid response 21 No action taken 22 Suspected malfunction 23 Unacceptable transaction fee 24 File update not supported 25 Unable to locate record 26 Duplicate record 27 File update edit error 28 File update file locked 29 File update failed 30 Format error 31 Bank not supported 32 Completed partially 33 Expired card, pick-up 34 Suspected fraud, pick-up 35 Contact acquirer, pick-up 36 Restricted card, pick-up 37 Call acquirer security, pick-up 38 PIN tries exceeded, pick-up 39 No credit account 40 Function not supported 41 Lost card 42 No universal account 43 Stolen card 44 No investment account	
--	--	--

	51 Not sufficient funds 52 No check account 53 No savings account 54 Expired card 55 Incorrect PIN 56 No card record 57 Transaction not permitted to cardholder 58 Transaction not permitted on terminal 59 Suspected fraud 60 Contact acquirer 61 Exceeds withdrawal limit 62 Restricted card 63 Security violation 64 Original amount incorrect 65 Exceeds withdrawal frequency 66 Call acquirer security 67 Hard capture 68 Response received too late 75 PIN tries exceeded 77 Intervene, bank approval required 78 Intervene, bank approval required for partial amount 90 Cut-off in progress 91 Issuer or switch inoperative 92 Routing error 93 Violation of law 94 Duplicate transaction 95 Reconcile error 96 System malfunction 98 Exceeds cash limit 99 Reserved for future Postilion use A1 ATC not incremented A2 ATC limit exceeded A3 ATC configuration error A4 CVR check failure A5 CVR configuration error A6 TVR check failure A7 TVR configuration error B1 MAC error Co Unacceptable PIN C1 PIN Change failed C2 PIN Unblock failed	
Additional Amount	Information on up to 6 amounts and related account data for which specific data elements have not been defined. Each amount is a fixed length field consisting of 5 data elements:	An..120

	<ul style="list-style-type: none"> Account type Amount type Currency code Amount sign Amount 	
Additional Data	Used to provide linked account or mini-statement information for a linked account inquiry or a mini-statement inquiry.	Ans..99
Authorization Response ID	A code assigned by the authorizing institution indicating approval.	Anp6
Forwarding Institution	A code identifying the institution that forwards the transaction in an interchange system en route to the card issuer.	11 numeric digits. Variable in length
Receiving Institution	A code identifying the financial institution that should receive a request or advice.	11 numeric digits. Variable in length
Merchant ID	A code identifying the merchant.	Ans15
CVV	The printed Visa CVV2 value.	3 numeric digits

a	Alphabetic character, A through Z and a through z
n	o through 9
p	Pad character, space
ans	Alphabetic, numeric and special characters
DD	Date, 01 through to 31
MM	Month, 01 through to 12
YY	Year, 00 through to 99 no apparent allowance for the turn of the century.
hh	Hour, 00 through 23
mm	Minute, 00 through 59
ss	Second, 00 through 59
..11	variable length up to 11

Note – all fixed length “n” elements are presumed to be right justified with leading zeroes. All other fixed length data elements are left justified with trailing spaces.

