Mobile VAS

Terra Carrier Billing

Integration Document

TERRA NETWORKS

Version 3.01

Contents

1. Introduction

Terra is the first Latin American Digital Media Company.

More than 15 years in the market, it has experience and connections with 50 carriers in 17 countries in Latin America and has more than 15 years of experience in mobile services. Currently, we have 32 integrations with carriers for doing carrier billing, the rest of them, are in being developed

Experience in the generation, development and management of content and multiplatform services (WAP, WEB, SMS, MMS, SatPush, SDK, APP/Site Creator & IVR) with more than 20 million mobile services subscribers.

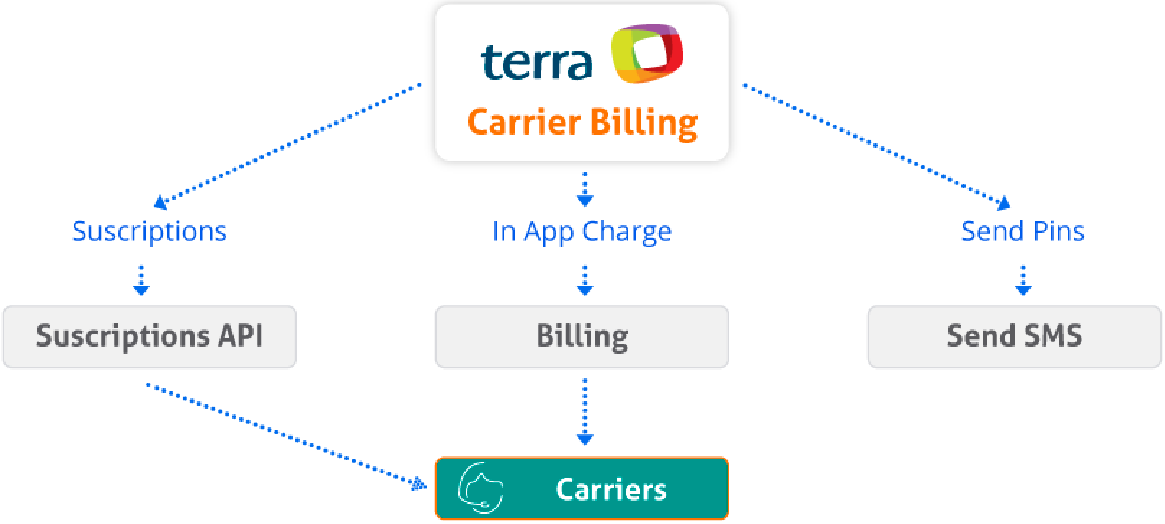
The aim of the Terra Carrier Billing Platform is to allow payments of "events" (subscriptions, content downloads, upselling, etc.) of a product (App 1, App 2, Wap 3, etc.) to mobile users directly from the balance of their cell phone bill. This way, we will access to a much bigger market different from the credit cards users but practically with the same possibilities of processing online payments.

1.1 Objective

This is a technical document and for that reason it is intended for the use of the IT team. The purpose of this document is to provide developers a guide about how to use the tools from Terra, as well as for them to know the different integration methods and to be able to select their best option.

1.2 Scope

The Carrier Billing system has 3 main functions:



- Subscriptions management. Registration and cancellation of MSISDN in a Subscription Service with automatic renewals, as well as verifications of Active Subscriptions.

- One time collections. It is in charge of collecting payments, in the local currency of the Operator, directly to the MSISDN account.

- Delivery of authentication pins. Its function is to validate that the number provided is really owned by the person accepting the collection or subscription.

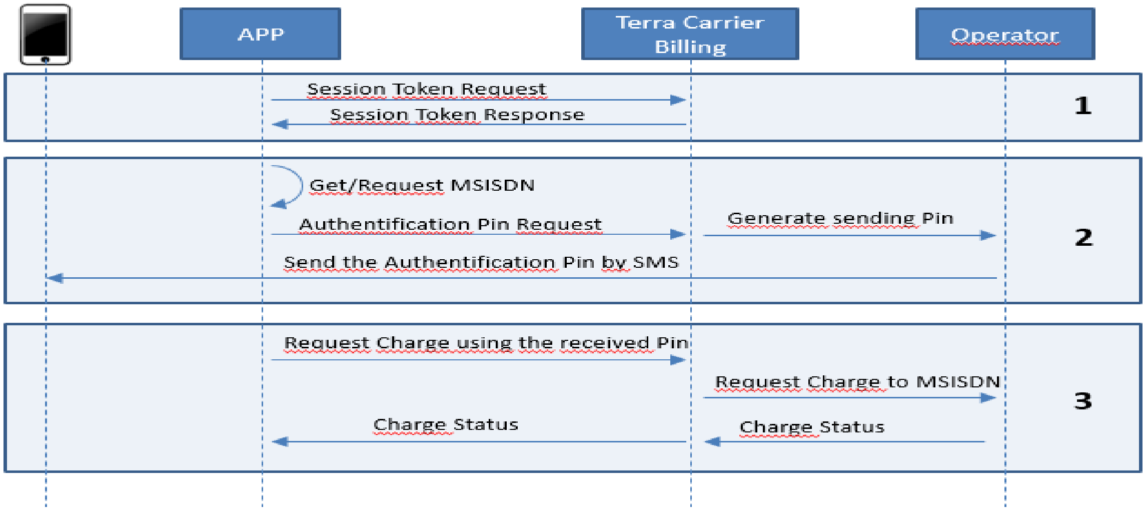
2. Architecture

Basic architecture of Terra Carrier Billing is a 3 layer architecture:

- Partner Application. This is the application or Wap/Web site of the Partner that requires collecting the payments or subscriptions from the users.
- Terra Carrier Billing. This is the Terra platform responsible of intercommunication between user requests and mobile carriers.
- Carrier. Mobile Carrier Company where users's charges are made.

According to the service flow, it can be classified as 3 stages:

- Authentication Token. This Token is necessary in order to communicate through the Web Service with Terra Carrier Billing. This Token has a configurable expiration date and it can be used for multiple calls while it is not expired, for that reason once it is obtained it can be kept to use it again.
- MSISDN validation. If the user is browsing through the data network of its Carrier Company, Terra Carrier Billing attempt to read the number automatically (if the operator provides this information), if isn't available this information, there is an alternate method to retrieve the number, this method is available in certain carriers and just when the user browse whitin the carrier's network. When there was not possible to get the phone number, there is another the way to validate a telephone number through the use of a validation PIN number sent to the user telephone. This PIN has a configurable expiration date and it can be used for multiple calls while it is not expired, for that reason once it is obtained it can be kept to use it again.
- Operation. It is how it will operate with Terra Carrier Billing, it could be collection of payments or a subscription registration/cancellation/verification.



3. Development Guide

3.1 Integration via API

3.1.1 Introduction

The API of the Terra Carrier Billing platform processes requests to its methods only via POST and has the ability to return the response in any of its methods in the following formats:

- XML, sending on the “Format Parameter of the Output Response”: Xml
- Json, sending on the "Format Parameter of the Output Response" Json

3.1.2 Security

As a safety feature of the platform, most of the data sent to the API methods should be encrypted with **AES 256**. *(Initial Vector: TerraNetworksMEX, Key Size: 256, Block size: 128 and ZeroBytePadding) and BASE64 encoded.*

Each Partner will be given to him a private encryption key and an initial vector, which will be used to encrypt data being sent to the API methods. *This key is unique and non-transferable and secrecy of it is the responsibility of Partner, so special emphasis is placed on the responsible management of the same.*

All calls to the API methods of the Terra Carrier Billing Platform require some kind of authentication to relate them to one of the Partners registered on the platform and thus can be correctly processed. Currently the platform has a three ways of authentication.

It is important to note that the partner must not use the encryption key in a way that expose it to be hacked using reverse engineering , view source, etc. The key must be handled server side.

1) *IP Address*

In the case the partner owns exclusive IP addresses for their products, the partner can provide to Terra a list of the Homologated (s) IP(s) where requests are made to the API. If a request for one of the API methods comes from any of the registered IPs in the Platform, this automatically links to the Partner that registered that IP and the request is processed without any other authentication. It is important to note that all the requests from this IP addresses will be processed and decrypted using the partner key. (there are just one key per partner)

2) *Session Token*

In case that the Partner does not have a fixed or static IP address, where they will make the call to the API, for example, if the calls are made from within a mobile application installed on the user's device, you have the option of using a session token to authenticate the call.

This is a security token such as “Bearer Token”, therefore it has to be sent to the HTTP Header “Authorization" that should contain the value “Bearer X”, where X is the string of the encrypted token with the private key of the Partner.

3) User/Password

This type of Authentication is only used in the method of generating a Session Token. The Partner must create at least one account with "API" characteristics from the Administration Console and the "User / Password" will allow you to generate a Session Token.

These tokens are designed by a Product, therefore Tokens created for a Product are invalid if you want to use them in another token different that the one that was used to create. Also, it is important to mention that the Token has a configurable lifetime per Product and it will automatically expire unless the Partner decides to renew it, which would give a period of life after the renovation. It’s important to note that the partner must follow security measures in order to protect its credentials and key, not storing them within the app or html code exposing them to reverse engineering, viewsource, etc. They must be handled server-side.

3.1.3 Getting Started

To run the API methods is necessary:

1) Authentication Request

For the call to a method of the API can be executed by the platform, this must be authenticated, either because the IP address from which the call Server Side is related to the Partner or because the call carries the Token Session in the Headers.

Or in case that the call is the reference method for the generation of a Session Token, the user/password will be sent to an account with Role API of the Partner.

2) Response Authentication (optional)

The Terra Carrier Billing platform provides the ability to authenticate that the answer comes from the correct source, avoiding spoofing responses. This validation is performed by sending a Verification Code on data of the request; this code will be encrypted in the response. The Partner has to decrypt with his private key the Verification Code and if the partner gets the info, that will be a pretty good indicator that the answer comes from the correct source.

3) Identification of the User Device

It is very important for Terra Carrier Billing Platform to identify the device from which the user makes use of the Platform. For this purpose it is required that in every call to each method, the HTTP Header related to the User Agent includes the real User Agent of the users' device.

It is very important to mention that any call to the methods of the API that do not carry this HTTP Header, will be rejected automatically.

4) *Calling a method*

The flow of the calls to any of the API methods follows a general scheme where we have the following guidelines:

- POST petition through HTTPS to the desire method
- Send the Header with the Session Token if needed.
- Use the encrypted token or data in multiples of the block size completing the remaining bytes (Ej. while(strlen($data) < 16) $data .= "\0";)
- Send the Header of the User Agent with the real User Agent of the user.
- If you want to authenticate the response of the API methods, you must send the item called "VERIFYCODE", this code will send a verification text generated by the Partner, which will be returned in the response and it must be encrypted. Therefore, the Partner must decrypt the "VERIFYCODE" of the response to compare with the one that was sent. This parameter is optional.
- The data required for each method can vary but necessarily all parameters are required (and its values too), except for those relating to the generation of the Session Token, these tokens must be inserted into an XML or JSON structure, according to the preference of the Partner.

    ○ XML format :

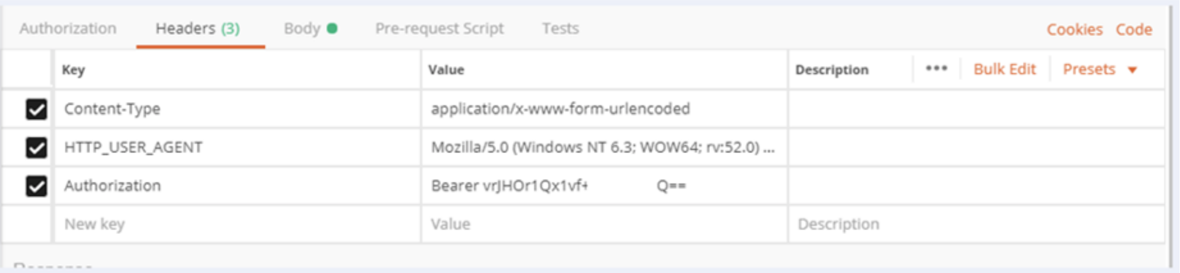
```
<REQUESTSET>
    <REQUEST>
            <PARAM1>trtrss</PARAM1>
            <PARAM2>435</PARAM2>
            <PARAM3>sdgdhf</PARAM3>
                    .
                    .
                    .
            <PARAMx>wegewrg</PARAMx>
    </REQUEST>
    <VERIFYCODE>123abc</VERIFYCODE>
        <OUTPUTFORMAT>xml</OUTPUTFORMAT>
</REQUESTSET>
```

    ○ JSON format:

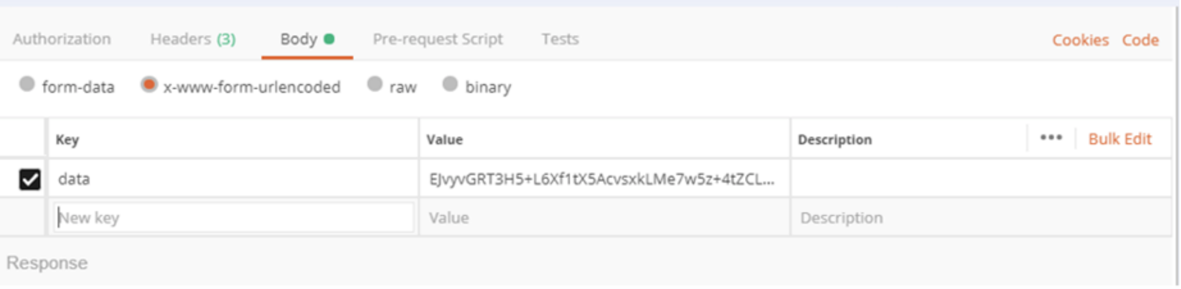
```
{
    "REQUEST": [ {
            "PARAM1": "trtrss",
            "PARAM2": 435,
            "PARAM3":" sdgdhf",
                    .
                    .
                    .
            "PARAMx": "wegewrg"

 } ],
    "VERIFYCODE": "123abc",
    "OUTPUTFORMAT": "xml"
}
```

The generated XML or JSON structure that contains all the necessary parameters for the API method must be encrypted using AES256 algorithm using the private key of the Partner (previously generated by Terra), and then it must be sent via POST in a parameter named **"data"**.

A sample request to a method must use the following use of headers and body:



	Key	Value	Description
☑	Content-Type	application/x-www-form-urlencoded	
☑	HTTP_USER_AGENT	Mozilla/5.0 (Windows NT 6.3; WOW64; rv:52.0) ...	
☑	Authorization	Bearer vrJHOr1Qx1vf+ Q==	
	New key	Value	Description



○ form-data ● x-www-form-urlencoded ○ raw ○ binary

	Key	Value	Description
☑	data	EJvyvGRT3H5+L6Xf1tX5AcvsxkLMe7w5z+4tZCL...	
	New key	Value	Description

3.1.4 API Reference Manual

API Methods

Generation of the Token *https://wstcb-mobile.terra.com/wstcb/Token.asmx/Gen*	This method generates a Session Token that relates the calls to the API methods of the Terra Carrier Billing Platform to a Partner, and therefore allows execution.
Token renewal *https://wstcb-mobile.terra.com/wstcb/Token.asmx/Upd*	This method performs the renewal of the duration of a Session Token.
Token revocation *https://wstcb-mobile.terra.com/wstcb/Token.asmx/Rvk*	This method is used to revoke an active Token.
MSISDN Auto Detection by SICOWEB *https://wstcb-mobile.terra.com/wstcb/Detect.asmx/BrVivoWho*	This method returns the MSISDN of the user even when the navigation header does not include it, it Works while the user browses using an internet conection through Vivo's network.

Request of the Authentication Pin *https://wstcb-mobile.terra.com/wstcb/Services.asmx/GetPin*	Request of the Authentication Pin to an indicated MSISDN which is able to transact for that mobile on Terra Carrier Billing.
External Authentication Pin Request *https://wstcb-mobile.terra.com/wstcb/Services.asmx/GetPin*	Method that makes the request to send a PIN to the user's telephone number as the first step of the subscription. It is only useful for the subscription.
Subscription using an Authentication Pin *https://wstcb-mobile.terra.com/wstcb/Services.asmx/SetPin*	Makes the subscription of a MSISDN to a service.
Validation of the Authentication Pin *https://wstcb-mobile.terra.com/wstcb/*Services.asmx/ChkPin	Validate whether the received PIN matches with the PIN generated in the last request, which by the way, was made by the same MSISDN for the same Product.
Subscription Verification *https://wstcb-mobile.terra.com/wstcb/Services.asmx/VrfSus*	Verifies the status of a MSISDN subscription to a service.
Multiple Subscription Verification *https://wstcb-mobile.terra.com/wstcb/Services.asmx/VrfMultSus*	Get the status of the suscription of a user and also the service associated.
List of subscribed Devices *https://wstcb-mobile.terra.com/wstcb/Services.asmx/GetDevices*	Gets the list of Devices to which the MSISDN is located in the Subscription Service.
Remove the device Subscribed *https://wstcb-mobile.terra.com/wstcb/*Services.asmx/RmvDevice	Removes an Authenticated Device from the registered devices list for the MSISDN/Service.
Unsubscribe using authentication PIN *https://wstcb-mobile.terra.com/wstcb/*Services.asmx/RmvSusc	Unsubscribe a MSISDN from service using authentication PIN from the user
Unsubscribe without using authentication PIN *https://wstcb-mobile.terra.com/wstcb/MSC.asmx/MscGateway*	Unsubscribe a MSISDN from service without using authentication PIN from the user
Send SMS *https://wstcb-mobile.terra.com/wstcb/Services.asmx/SndSms*	Allows to send an SMS to a MSISDN.

API Methods – Detailed description

3.1.4.1 Generation of the Session Token

This method generates a Session Token that relates the calls to the methods of the API of the Terra Carrier Billing Platform to a Partner, and therefore allows execution. This token will be sent to all calls to the APIs of the platform, except, of course, the methods concerning the Token.

One way to avoid handling this Session Token is that all calls to the API methods are made from fixed IPs, homologate, belonging to the Partner and prior notification to Terra.

URL
https://wstcb-mobile.terra.com/wstcb/Token.asmx/Gen

Required parameters, which must be sent via POST:

Name	*Type*	*Optional*	*Description*
u	Text	NO	User Name of an account with role “API” of the Partner.
c	Text	NO	Account Password of the Users "API".
p	Numeric	NO	ID Product that requires to process.
f	Text	Yes	Output Format Parameter Response, the default is " xml"

Return Data:

Name	*Type*	*Description*
TOKEN	Text	Session Token generated.
EXPIRES	Numeric	It indicates the number of seconds of life that this Token have.
STATUS	Text	Server Response Code.

Server Response Code:

Value	*Description*
OK	The Token was generated successfully.
NOK	It was not possible to generate the Session Token
ERR	An error occurred in the Terra Carrier Billing Platform which prevented the generation of Token.
FA	Execution of the Method not allowed by failing to identify the Partner (username/password invalid).

Response formats:

Format	*Example*

XML	<RESPONSESET>
	    <RESPONSE>
	        <TOKEN>LOG01G</TOKEN>
	        <EXPIRES>3600</EXPIRES>
	        <STATUS>OK</STATUS>
	    </RESPONSE>
	</RESPONSESET>

JSON	{
	“RESPONSE”:[{
	"TOKEN": "LOG01G",
	"EXPIRES": 3600,
	“STATUS”:”OK”
	}]
	}

3.1.4.2 Renewal of the Session Token

This method performs the renewal of the lifetime of a Session Token. Once renovated the Session Token, this extends the life time of the default Token, allowing the continued use indefinitely, as long as the renewal occurs when the Token is still active.

Once the session token expires you cannot renew it, if you want to do so, you would have to generate a new one.

URL
https://wstcb-mobile.terra.com/wstcb/Token.asmx/Upd

Send the Session Token that you want to renew in the corresponding Http Header.

Required parameters to send in a XML or JSON encrypted via POST on “data”.

Name	***Type***	***Optional***	***Description***
IDPRODUCT	Numeric	NO	ID Product required to process
OUTPUTFORMAT	Text	YES	Output Format Parameter of the Response, the default is "xml".
VERIFYCODE	Text	YES	Random verification text generated by the Partner.

Return data:

Name	***Type***	***Description***
EXPIRES	Numeric	It indicates the number of seconds of life that now has the renewed Token.
STATUS	Text	Server Response Code.
VERIFYCODE	Text	Verification text sent in response, but encrypted with the private key of the Partner. ONLY if it was sent in Request.

Server response codes:

Value	***Description***
OK	The Token was successfully renewed.
NOK	It was not possible to renew the Session Token.
DER	Error on input.
ERR	An error occurred in the Terra Carrier Billing Platform, which prevented the renewal of the Token.

FA	Execution of the Method not allowed by failing to identify the Partner (invalid or expired Token).

Response formats:

Format	*Example*
XML	<RESPONSESET> <RESPONSE> <EXPIRES>3600</EXPIRES> <STATUS>OK</STATUS> </RESPONSE> <VERIFYCODE>f99bQcY6u/jI6/arH0jjuw==</VERIFYCODE> </RESPONSESET>

JSON	{
	“RESPONSE”: [{
	"EXPIRES": 3600,
	“STATUS”:”OK”
	}],
	"VERIFYCODE":"f99bQcY6u\/jI6\/arH0jjuw=="
	}

3.1.4.3 Revocation of the Session Token

This method is used to revoke an active Token, which causes that the Session Token is no longer valid to run the calls to the API methods of the Terra Carrier Billing platform.

Only one active Session Token can be revoked, it is not necessary to revoke a Token that has already expired because the revocation process is basically the same as the expiration process.

URL
https://wstcb-mobile.terra.com/wstcb/Token.asmx/Rvk

Send the Session Token that you want to revoke in the corresponding Http Header.

Required parameters to send in a XML or JSON encrypted via POST on “data”.

Name	*Type*	*Optional*	*Description*
IDPRODUCT	Numeric	NO	ID Product required to process
OUTPUTFORMAT	Text	YES	Output Format Parameter of the Response, the default is "xml".
VERIFYCODE	Text	YES	Random verification text generated by the Partner.

Return Data:

Name	*Type*	*Description*

STATUS	Text	Server Response Code.
VERIFYCODE	Text	Verification Text sent in response, but encrypted with the private key of the Partner. ONLY if it was sent in Request.

Server response codes:

Value	***Description***
OK	The Token was successfully revoked.
NOK	It was not possible to revoke the Session Token.
DER	Data error entry
ERR	An error occurred in the Terra Carrier Billing Platform, which prevented the revocation of the Token.
FA	Execution of the Method not allowed by failing to identify the Partner (invalid or expired Token).

Response formats:

Format	***Example***
XML	<RESPONSESET> <RESPONSE> <STATUS>OK</STATUS> </RESPONSE> <VERIFYCODE>f99bQcY6u/jI6/arH0jjuw==</VERIFYCODE> </RESPONSESET>

JSON	{
	“RESPONSE”: [{
	“STATUS”:”OK”
	}],
	"VERIFYCODE":"f99bQcY6u\/jI6\/arH0jjuw=="
	}

3.1.4.4 MSISDN Auto-detect using SICOWEB

This method returns the MSISDN of the user even when the navigation header does not include it, it Works while the user browses using an internet connection through Vivo’s network.

Available only for Operator VIVO Brazil.

This method returns the same MSISDN that is being validated and also a PIN, which can be used in other methods of Carrier Billing, for this reason you may store it in the application storage.

This values are returned encrypted, so you have to use the provided key to get the actual values.

We have 2 ways of calling this method, one to be used in apps and another to be used in web environments.

URL (For Apps)
https://wstcb-mobile.terra.com/wstcb/Detect.asmx/BrVivoWho

List of parameters, they must be provided using a XML o JSON structure, encrypted and via POST using the “data” parameter.

Name	***Type***	***Optional***	***Description***
IDPRODUCT	Numeric	NO	ID Product required to process
IDOPERATOR	Numeric	NO	ID of the operator or carrier that will be used.
OUTPUTFORMAT	Text	YES	Output Format Parameter of the Response, the default is "xml"
VERIFYCODE	Text	YES	Random verification text generated by the Partner.

Return data:

Name	***Type***	***Description***
E1	Text	Encripted MSISDN
E2	Text	Encripted PIN code
IDCOUNTRY	Numeric	ID Country
IDOPERATOR	Numeric	Operator/Carrier ID
IDPRODUCT	Numeric	ID Producto
EXPIRES	Numeric	Indicates the time window in seconds that the Pin will be active for collections. In case of being -1 it indicates that only can be used to make a single payment
STATUS	Text	Server response code
VERIFYCODE	Text	Verification Text sent in response, but encrypted with the private key of the Partner. ONLY if it was sent in Request

Server response codes:

Value	***Description***
OK	The phone number was returned successfully.
NA	The phone number is blacklisted
DER	Unable to identify the phone number.
ERR	An error occurred during the processing of your call.
FA	Invalid Partner (or invalid or expired Token).

Response formats:

Format	***Example***

XML	<RESPONSESET>
	        <RESPONSE>
	                <E1> pmRNWO1XbmZaXZggyBwyqA==</E1>
	                <E2> LsE5qneWUoAs0yPZfikNTA==</E2>
	                <EXPIRES>3600</EXPIRES>
	                <IDCOUNTRY>1</IDCOUNTRY>
	                <IDOPERATOR>334100</IDOPERATOR>
	                <IDPRODUCT>3</IDPRODUCT>
	                <STATUS>OK</STATUS>
	        </RESPONSE>
	        <VERIFYCODE>f99bQcY6u/jI6/arH0jjuw==</VERIFYCODE>
	</RESPONSESET>

JSON	{
	  "RESPONSE":[{

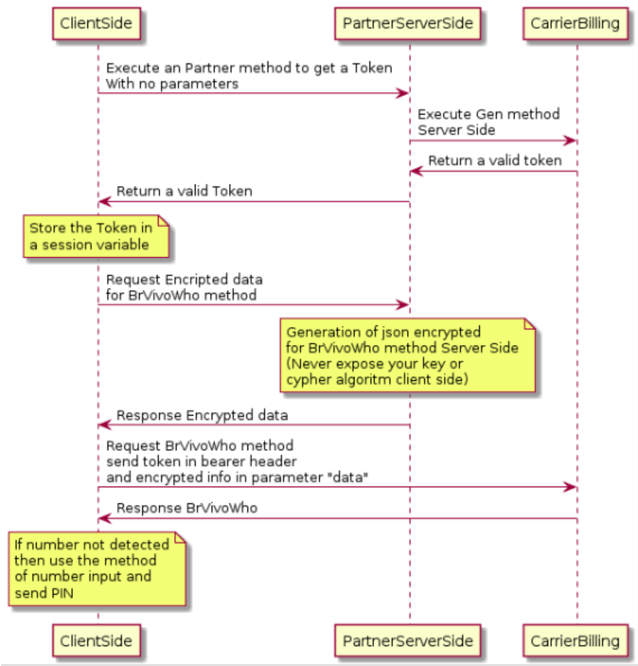
	"E1":"pmRNWO1XbmZaXZggyBwyqA==", "E2":"LsE5qneWUoAs0yPZfikNTA==", "EXPIRES":7767968, "IDCOUNTRY":1, "IDOPERATOR":334100, "IDPRODUCT":3, "STATUS":"OK" }], "VERIFYCODE":"9eme5XNiZQUShF5i7o9gt4HcL8vNxA2xngkdVHzOgRQ=" }

URL (*for WEB*)

For web the request must be GET, the data parameter should not be encoded, have to use javascript because JSONP will be used for the request, but always keep in mind that the encryption key should be managed server-side in order to not expose it.

https://wstcb-mobile.terra.com/wstcb/Detect.asmx/BrVivoWho?data=" + txtData + "&ttkn=" + encrypted token

Sample flow to use in a web environment:



3.1.4.5 Request of the Authentication Pin

This method makes the request to send a Pin to the user's phone number as the first step of authentication. The purpose of this Pin is to validate that the number provided by the user is actually his. The Pin generated is valid for a particular product, which could be several active Pins for the same MSISDN but for different products.

This generated Pin may have a validity window, depending on the Partner´s profile, of a certain amount of time, during which they can apply for multiple collections, using the same PIN of authentication. It should be noted that requesting a new PIN of authentication for the same MSISDN and Product, any Pin "active" for charges shall be automatically canceled.

Obtain a short dialing: It is possible to obtain, besides the confirmation of the PIN, the short dialing origin, in other words, the one in which the SMS will be delivered to the phone.

It's important to mention that we count with various security mechanisms to prevent the sending of PIN requests, as some form of attack. These mechanisms will not be discussed for security reasons.

URL
https://wstcb-mobile.terra.com/wstcb/Events.asmx/GetPin
https://wstcb-mobile.terra.com/wstcb/Services.asmx/GetPin

Required parameters to send in a XML or JSON encrypted via POST on “data”:

Name	***Type***	***Optional***	***Description***
MSISDN	Numeric	NO	User phone number including country code and area code, for example. 5511963889439
IDPRODUCT	Numeric	NO	ID Product required to process
IDOPERATOR	Numeric	NO	ID of the operator or carrier
SERVICE	Text	YES	For the specific case of Entel Chile needs to send the Service identifier related to the Product.
OUTPUTFORMAT	Text	YES	Output Format Parameter of the Response, the default is "xml".
VERIFYCODE	Text	YES	Random verification text generated by the Partner.
GETSHORTCODE	Numeric	YES	When the value is "1", the response will include the short dial from which you send the SMS of the PIN. Any other value will be ignored.

Return Data:

Name	***Type***	***Description***
STATUS	Text	Server Response Code.
EXPIRES	Numeric	Indicates the time window in seconds that the Pin will be active for collections. In case of being -1 it indicates that only can be used to make a single payment.
SHORTCODE	Numeric	In case of sending the “GETSHORTCODE" = 1 parameter, the dialing with the SMS which contains the authentication pin, will be delivered to the mobile.
VERIFYCODE	text	Verification Text sent in response, but encrypted with the private key of the Partner. ONLY if it was sent in Request.

Server response codes:

Value	***Description***
OK	The Token was successfully sent.
NOK	Could not send the PIN authentication.
NA	The MSISDN is in the Blacklist

DER	Data error entry
ERR	An error occurred in the Terra Carrier Billing Platform which prevented the sending of the Pin.
FA	Execution of the Method not allowed by failing to identify the Partner (invalid or expired Token).

Response formats:

Format	***Example***
XML	<RESPONSESET> <RESPONSE> <STATUS>OK</STATUS> <EXPIRES>60</EXPIRES> <SHORTCODE>3000</SHORTCODE> </RESPONSE> <VERIFYCODE>f99bQcY6u/jl6/arH0jjuw==</VERIFYCODE> </RESPONSESET>

JSON	{
	“RESPONSE”: [{
	“STATUS”:”OK”,
	“EXPIRES”:60,
	“SHORTCODE”:3000
	}],
	"VERIFYCODE":"f99bQcY6u\/jl6\/arH0jjuw=="
	}

3.1.4.6 External Authentication Pin Request

This method makes the request to send a PIN by SMS to the user's telephone number as the first step of the subscription. The SMS is sent directly from the operator to the user's mobile.

It is only useful for subscription and can only be used for one subscription at a time. Terra will inform Partner in a timely manner of the cases in which it should be used.

URL
https://wstcb-mobile.terra.com/wstcb/Events.asmx/GetPin
https://wstcb-mobile.terra.com/wstcb/Services.asmx/GetPin

Required parameters to send in a XML or JSON encrypted via POST on “data”:

Name	***Type***	***Optional***	***Description***
MSISDN	Numeric	NO	User phone number including country code and area code, for example. 5511963889439
IDPRODUCT	Numeric	NO	ID Product required to process
IDOPERATOR	Numeric	NO	ID of the operator or carrier
SERVICE	Text	NO	Service code, related with Product.
OUTPUTFORMAT	Text	YES	Output Format Parameter of the Response, the default is "xml".

VERIFYCODE	Text	YES	Random verification text generated by the Partner.
GETSHORTCODE	Numeric	YES	When the value is "1", the response will include the short dial from which you send the SMS of the PIN. Any other value will be ignored.

Return Data:

Name	***Type***	***Description***
STATUS	Text	Server Response Code.
EXPIRES	Numeric	Indicates the time window in seconds that the Pin will be active for collections. In case of being -1 it indicates that only can be used to make a single payment.
SHORTCODE	Numeric	In case of sending the “GETSHORTCODE" = 1 parameter, the dialing with the SMS which contains the authentication pin, will be delivered to the mobile.
VERIFYCODE	text	Verification Text sent in response, but encrypted with the private key of the Partner. ONLY if it was sent in Request.

Server response codes:

Value	***Description***
OK	The Token was successfully sent.
NOK	Could not send the PIN authentication.
NA	The MSISDN is in the Blacklist
DER	Data error entry
AS	Already subscribe-
OP	Subscription on process.
RV	The MSISDN Subscription to the product is in renewal process.
FD	The amount of active Devices has exceded the limit for the Service.
ERR	An error occurred in the Terra Carrier Billing Platform which prevented the sending of the Pin.
FA	Execution of the Method not allowed by failing to identify the Partner (invalid or expired Token).

Response formats:

Format	***Example***
XML	<RESPONSESET> <RESPONSE> <STATUS>OK</STATUS> <EXPIRES>60</EXPIRES> <SHORTCODE>3000</SHORTCODE> </RESPONSE> <VERIFYCODE>f99bQcY6u/jI6/arH0jjuw==</VERIFYCODE> </RESPONSESET>

JSON	{
	“RESPONSE”: [{
	“STATUS”:”OK”,
	“EXPIRES”:60,
	“SHORTCODE”:3000

	}], "VERIFYCODE":"f99bQcY6u\/jI6\/arH0jjuw==" }

3.1.4.7 Subscription using the authentication PIN

The purpose of this method is to make the subscription of a MSISDN to one Service (Product), making the collection of the payment or request of it through the Clubs Terra Platform.

It is placed in local currency from the Operator to the mobile bill of the requester user, only if, the PIN is sent to the corresponding method generated by the previous request of "PIN request" for the MSISDN/Product.

The definition of the Club (Collections, automatic renewal, grace period, etc.) is configured entirely outside this API, for that reason the Partner should previously manage the configuration of this Club in the Clubs Terra Platform before using this method.

URL
https://wstcb-mobile.terra.com/wstcb/Services.asmx/SetPin

List of parameters sent within an XML or JSON encryption via POST in "data".

Name	***Type***	***Optional***	***Description***
MSISDN	Numerical	NO	User telephone number including country code and area code, for example: 5511963889439
PIN	Numerical	NO	The verification PIN sent via SMS.
ORDER	Text	NO	Unique identifier of the order in the Partner system.
IDPRODUCT	Numerical	NO	Product ID required for processing.
IDOPERATOR	Numerical	NO	Operator or Carrier ID
SERVICE	Text	NO	Service identifier related to the Product.
DESCRIPTION	Text	NO	Service description related to the Product from the Partner, for example: “AllGames Subscription”
DEVICEID	Text	NO	User device unique identifier. This value is used to limit the number of different devices the user can have logged in. It is recommended to use IME or MAC address.
SOURCE	Text	YES	Origin of the transaction. Valid values are 'WEB' AND 'APP'. For Vivo BR they are mandatory.
MEDIA	Text	YES	The Partner will be informed by Terra when required and the value to be used.
OPERKW	Text	YES	Valid values are 'WEB' AND 'APP'. For Vivo BR they are mandatory.
DEVICENAME	Text	YES	Friendly name for the device in case of not sending it the same value of DEVICEID will be used.

SECURE	Text	YES	Extra security code sent directly to the MSISDN by some Operators and required to allow the Subscription.
OUTPUTFORMAT	Text	YES	Reply output format parameters, “xml” is the default one.
VERIFYCODE	Text	YES	Random verification text generated by the Partner.

Return data:

Name	***Type***	***Description***
ID	Numerical	Transaction ID of the Operation in the Terra Carrier Billing platform.
MSISDN	Numerical	User telephone number including country code and area code, for example: 5511963889439
ORDER	Text	Unique identifier of the transaction in the Partner system.
STATUS	Text	Server response code for the transaction, for example: “NOK”
MESSAGE	Text	If there is a relevant message for the transaction, for example "Time Out”.
EXPIRES	Numerical	Indicates the remaining time window, in seconds, that the PIN will be active to collect payments. In case of being 0, it indicates that the PIN is no longer useful to make another collection.
VERIFYCODE	Text	Verification text sent in the reply message but encrypted with the private key of the Partner. ONLY if the Request was sent.

Server Response Codes:

Value	***Description***
OK	Subscription done correctly.
NOK	It was not possible to make the Subscription of the MSISDN to the Service.
NA	The MSISDN in in the Blacklist.
NEQ	The PIN sent does not correspond with the generated one.
NAP	There is no PIN active for the partner MSISDN / Product.
AS	The MSISDN is already Subscribed to the Service.
OP	The MSISDN Subscription to the product is in process. This could be due the user isn’t have enough money to complete the Subscription, or due we depend on third party to register the user in the Service, in this case you should check the User status in the Service.
RV	The MSISDN Subscription to the product is in renewal process.
SR	If this response code is received then you have to execute SetPin methid again but including the SECURE parameter, this parameter refers to the Security code sent to the MSISDN by the Operator.
FD	The amount of active Devices has exceeded the limit for the Service.
DER	Data input error
ERR	A mistake in the Terra Carrier Billing Platform that impeded the Request processing.
AP	Previously transaction processed. This case happens when an ID “Order” is sent to the Partner that was already sent.
FA	Method execution not allowed because it was not identified by the Partner (invalid/expired Token and not recognized IP).

Reply formats:

Format	***Example***

XML	<RESPONSESET>
	    <RESPONSE>
	        <ID>1242345345435</ID>
	        <MSISDN>8181504000</MSISDN>
	        <ORDER>Partner Order ID</ORDER>
	        <STATUS>NOK</STATUS>
	        <EXPIRES>47</EXPIRES>
	        <MESSAGE>Time Out</MESSAGE>
	    </RESPONSE>
	    <VERIFYCODE>f99bQcY6u/jl6/arH0jjuw==</VERIFYCODE>
	</RESPONSESET>

JSON	{
	  “RESPONSE”: [{
	    "ID": "1242345345435",
	    “MSISDN”: 8181504000,
	    "ORDER": "Partner Order ID",
	    "STATUS": "NOK",
	    "EXPIRES": 47,
	    "MESSAGE": "Time Out"
	  }],
	  "VERIFYCODE":"f99bQcY6u\/jl6\/arH0jjuw=="
	}

3.1.4.8 Validation of PIN Verification

Method that validates if the received PIN corresponds to the one generated in the last request made by the same MSISDN for the same Product.

Different from the methods “Events.asmx/SetPin” and “Services.asmx/SetPin”, because in this one there is no payment or subscription transaction made.

It is important to mention that there are different security mechanisms to avoid a brute force attack to verify a PIN. These mechanisms will not be mentioned due to security measures.

URL
https://wstcb-mobile.terra.com/wstcb/Services.asmx/ChkPin

List of parameters sent within an XML or JSON encryption via POST in "data".

Name	***Type***	***Optional***	***Description***
MSISDN	Numerical	NO	User telephone number including country code and area code, for example: 5511963889439
PIN	Numerical	NO	The verification PIN sent via SMS.
IDPRODUCT	Numerical	NO	Product ID required for processing.
IDOPERATOR	Numerical	NO	Operator or Carrier ID
OUTPUTFORMAT	Text	YES	Reply output format parameters, “xml” is the default one.
VERIFYCODE	Text	YES	Random verification text generated by the Partner.

Return data:

Name	***Type***	***Description***
MSISDN	Numerical	User telephone number including country code and area code, for example: 5511963889439
STATUS	Text	Server response code for the transaction, for example: “NOK”
EXPIRES	Numerical	This indicates the remaining time window, in seconds, that the PIN will be active to collect payments. If it is 0 it will indicate that the PIN cannot be used to collect another payment.
MESSAGE	Text	If there is a relevant message for the transaction, for example "Time Out”.
VERIFYCODE	Text	Verification text sent in the reply message but encrypted with the private key of the Partner. ONLY if the Request was sent.

Server Response Codes:

Value	***Description***
OK	Correct PIN.
NOK	Verification attempts limit reached.
NEQ	The PIN sent does not correspond with the generated one.
NAP	There is no PIN active for the partner MSISDN / Product.
NA	The MSISDN in in the Blacklist.
DER	Data input error
ERR	A mistake in the Terra Carrier Billing Platform that impeded the Request processing.
FA	Method execution not allowed because it was not identified by the Partner (invalid/expired Token and not recognized IP).

Reply formats:

Format	***Example***

XML	<RESPONSESET>
	    <RESPONSE>
	        <ID>1242345345435</ID>
	        <MSISDN>8181504000</MSISDN>
	        <STATUS>NEQ</STATUS>
	        <EXPIRES>47</EXPIRES>
	        <MESSAGE>Time Out</MESSAGE>
	    </RESPONSE>
	    <VERIFYCODE>f99bQcY6u/jI6/arH0jjuw==</VERIFYCODE>
	</RESPONSESET>

JSON	{
	  “RESPONSE”: [{
	    "ID": "1242345345435",
	    “MSISDN”: 8181504000,
	    "STATUS": "NOK",
	    "EXPIRES": 47,
	    "MESSAGE": "Time Out"
	  }],
	  "VERIFYCODE":"f99bQcY6u\/jI6\/arH0jjuw=="
	}

3.1.4.9 Subscription Verification

This method is especially designed for the Service (Products) Subscription with automatic renewal, for which the verification of a number still subscribed to the product is a very important part of the service.

URL

https://wstcb-mobile.terra.com/wstcb/Services.asmx/VrfSuc

List of parameters sent within an XML or JSON encryption via POST in "data".

Name	***Type***	***Optional***	***Description***
MSISDN	Numerical	NO	User telephone number including country code and area code, for example: 5511963889439
IDPRODUCT	Numerical	NO	Product ID required for processing.
IDOPERATOR	Numerical	NO	Operator or Carrier ID
SERVICE	Text	NO	Service identifier related to the Product.
DEVICEID	Text	NO	User device unique identifier. This value is used to limit the number of different devices the user can have logged in. It is recommended to use IME or MAC address.
DEVICENAME	Text	YES	Friendly name for the device in case of not sending it the same value of DEVICEID will be used.
OUTPUTFORMAT	Text	YES	Reply output format parameters, “xml” is the default one.
VERIFYCODE	Text	YES	Random verification text generated by the Partner.

Return data:

Name	***Type***	***Description***
STATUS	Text	Server Response Codes:
VERIFYCODE	Text	Verification text sent in the reply message but encrypted with the private key of the Partner. ONLY if the Request was sent.

Server Response Codes:

Value	***Description***
OK	The MSISDN is already Subscribed to the Service.
NO	The MSISDN is not Subscribed to the Service.
NA	The MSISDN in in the Blacklist.
RV	The MSISDN Subscription to the product is in renewal process.
OP	The MSISDN Subscription to the product is in process.
FD	The amount of active Devices has exceeded the limit for the Service.
NOK	It was not possible to verify the status of the Subscription.
DER	Data input error
ERR	A mistake in the Terra Carrier Billing Platform that impeded the Request processing.

FA	Method execution not allowed because it was not identified by the Partner (invalid/expired Token and not recognized IP).

Reply formats:

Format	***Example***

XML	<RESPONSESET>
	        <RESPONSE>
	                <STATUS>OK</STATUS>
	        </RESPONSE>
	        <VERIFYCODE>f99bQcY6u/jI6/arH0jjuw==</VERIFYCODE>
	</RESPONSESET>

JSON	{
	  “RESPONSE”: [{
	   “STATUS”:”OK”
	  }],
	  "VERIFYCODE":"f99bQcY6u\/jI6\/arH0jjuw=="
	}

3.1.4.10 Multiple Subscription Verification

This method returns all the subscriptions associated with the product and the user provided as parameters in the call.

URL
https://wstcb-mobile.terra.com/wstcb/Services.asmx/VrfMultSuc

List of parameters, they must be provided using a XML o JSON structure, encrypted and via POST using the “data” parameter.

Name	***Type***	***Optional***	***Description***
MSISDN	Number	NO	User telephone number including country code and area code, for example: 5511963889439
IDPRODUCT	Number	NO	Product ID required for processing.
IDOPERATOR	Number	NO	Operator or Carrier ID
SERVICE	Text	NO	Service identifier related to the Product.
DEVICEID	Text	NO	User device unique identifier. This value is used to limit the number of different devices the user can have logged in. It is recommended to use IME or MAC address.
DEVICENAME	Text	YES	Friendly name for the device in case of not sending it the same value of DEVICEID will be used.
OUTPUTFORMAT	Text	YES	Reply output format parameters, “xml” is the default one.
VERIFYCODE	Text	YES	Random verification text generated by the Partner.

Return data:

Nombre	*Tipo*	*Descripción*
SERVICE	Text	Identificador del Servicio relacionado al Producto.
STATUS	Text	Server response code associated with the service, ej. “NOK”
MESSAGE	Text	If there is a relevant message for the transaction, for example "Time Out”.
VERIFYCODE	Text	Verification text sent in the reply message but encrypted with the private key of the Partner. ONLY if the Request was send.

Server response codes:

Value	*Description*
OK	The MSISDN is already Subscribed to the Service.
NO	The MSISDN is not Subscribed to the Service.
NA	The MSISDN in in the Blacklist.
RV	The MSISDN Subscription to the product is in renewal process.
OP	The MSISDN Subscription to the product is in process.
FD	The amount of active Devices has exceeded the limit for the Service.
NOK	It was not possible to verify the status of the Subscription.
DER	Data input error
ERR	A mistake in the Terra Carrier Billing Platform that impeded the Request processing.
FA	Method execution not allowed because it was not identified by the Partner (invalid/expired Token and not recognized IP).

Response formats:

Format	*Examples*

XML	<RESPONSESET>
	        <RESPONSE>
	                <STATUS>OK</STATUS>
	                <SERVICE>ServiceCode01</SERVICE>
	        </RESPONSE>
	        <RESPONSE>
	                <STATUS>OP</STATUS>
	                <SERVICE>ServiceCode02</SERVICE>
	        </RESPONSE>
	        <VERIFYCODE>f99bQcY6u/jI6/arH0jjuw==</VERIFYCODE>
	</RESPONSESET>

JSON	{
	    "RESPONSE": [{
	      "STATUS": "OK",
	      "SERVICE": "ServiceCode01"
	  },
	{
	      "STATUS": "OP",
	      "SERVICE": "ServiceCode02"
	    }],
	   "VERIFYCODE":"f99bQcY6u\/jI6\/arH0jjuw=="
	}

3.1.4.11 Subscribed Devices List

List of Devices for which there is an authentication of an MSISDN in a Subscription Service. This list is useful in case of reaching the limit of allowed Devices by the Service, so that the Partner can show the list to the user and he or she can choose which device´s authentication wants to eliminate so that he can continue registering a new one.

URL
https://wstcb-mobile.terra.com/wstcb/Services.asmx/GetDevices

List of parameters sent within an XML or JSON encryption via POST in "data".

Name	***Type***	***Optional***	***Description***
MSISDN	Numerical	NO	User telephone number including country code and area code, for example: 5511963889439
IDPRODUCT	Numerical	NO	Product ID required for processing.
IDOPERATOR	Numerical	NO	Operator or Carrier ID
SERVICE	Text	NO	Service identifier related to the Product.
OUTPUTFORMAT	Text	YES	Reply output format parameters, “xml” is the default one.
VERIFYCODE	Text	YES	Random verification text generated by the Partner.

Return data:

Name	***Type***	***Description***
DEVICEID	Text	User device unique identifier. This value is used to limit the number of different devices the user can have logged in. It is recommended to use IME or MAC address.
DEVICENAME	Text	Friendly name for the device in case of not sending it the same value of DEVICEID will be used.
IDPRODUCT	Numerical	Product ID.
SERVICE	Text	Service identifier related to the Product.
DATE	Text	Date of the purchase with the format “YYYY-MM-DD hh:mm:ss” in GMT 0
VERIFYCODE	Text	Verification text sent in the reply message but encrypted with the private key of the Partner. ONLY if the Request was sent.

Reply formats:

Format	***Example***
XML	<RESPONSESET> <RESPONSE> <DEVICEID>xxx-yyy-zzz</DEVICEID> <DEVICENAME>Cel de X</DEVICENAME> <IDPRODUCT>123</IDPRODUCT> <SERVICE>Weekly Subscription</SERVICE> <DATE>2014-01-01 16:32:15</DATE> </RESPONSE> <RESPONSE> <DEVICEID>xxx-yyy-uuu</DEVICEID> <DEVICENAME>Cel de U</DEVICENAME> <IDPRODUCT>123</IDPRODUCT>

	<SERVICE>Weekly Subscription</SERVICE> <DATE>2014-01-02 07:02:13</DATE> </RESPONSE> <VERIFYCODE>f99bQcY6u/jI6/arH0jjuw==</VERIFYCODE> </RESPONSESET>

JSON	{
	“RESPONSE”: [{
	"DEVICEID": "xxx-yyy-zzz",
	"DEVICENAME": "Cel de X",
	"IDPRODUCT": 123,
	"SERVICE": "Weekly Subscription",
	"DATE": "2014-01-01 16:32:15"
	},
	“RESPONSE”: {
	"DEVICEID": "xxx-yyy-uuu",
	"DEVICENAME": "Cel de U",
	"IDPRODUCT": 123,
	"SERVICE": "Weekly Subscription",
	"DATE": "2014-01-02 07:02:13"
	}],
	"VERIFYCODE":"f99bQcY6u\/jI6\/arH0jjuw=="
	}

3.1.4.12 Delete a Subscribed Device

This method is used to delete a verified Device from the Registered Device List for the MSISDN / User Service. When a device is deleted from a list of verified devices the user will be able to unbind a device in order to add other devices in the future, for that reason it will be possible to add a new device to the list in order to permit its use.

URL
https://wstcb-mobile.terra.com/wstcb/Services.asmx/RmvDevice

List of parameters sent within an XML or JSON encryption via POST in "data".

Name	***Type***	***Optional***	***Description***
MSISDN	Numerical	NO	User telephone number including country code and area code, for example: 5511963889439
IDPRODUCT	Numerical	NO	Product ID required for processing.
IDOPERATOR	Numerical	NO	Operator or Carrier ID
SERVICE	Text	NO	Service identifier related to the Product.
DEVICEID	Text	NO	User device unique identifier. This value is used to limit the number of different devices the user can have logged in. It is recommended to use IME or MAC address.
OUTPUTFORMAT	Text	YES	Reply output format parameters, “xml” is the default one.
VERIFYCODE	Text	YES	Random verification text generated by the Partner.

Return data:

Name	*Type*	*Description*
STATUS	Text	Server Response Codes:
VERIFYCODE	Text	Verification text sent in the reply message but encrypted with the private key of the Partner. ONLY if the Request was sent.

Server Response Codes:

Value	*Description*
OK	The Device was deleted from the Service.
NOK	The Device was not deleted from the Service.
NE	The Device is not registered for the Service.
DER	Data input error
ERR	A mistake in the Terra Carrier Billing Platform that impeded the Request processing.
FA	Method execution not allowed because it was not identified by the Partner (invalid/expired Token and not recognized IP).

Reply formats:

Format	*Example*
XML	<RESPONSESET> <RESPONSE> <STATUS>OK</STATUS> </RESPONSE> <VERIFYCODE>f99bQcY6u/jl6/arH0jjuw==</VERIFYCODE> </RESPONSESET>

JSON	{
	“RESPONSE”: [{
	“STATUS”:”OK”
	}],
	"VERIFYCODE":"f99bQcY6u\/jl6\/arH0jjuw=="
	}

3.1.4.13 Subscription Cancellation Request using authentication PIN

Method to request the cancellation of a subscription purchased by a MSISDN.

URL
https://wstcb-mobile.terra.com/wstcb/Services.asmx/RmvSusc

List of parameters sent within an XML or JSON encryption via POST in "data".

Name	*Type*	*Optional*	*Description*
MSISDN	Numerical	NO	User telephone number including country code and area code, for example: 5511963889439
PIN	Numerical	NO	The verification PIN sent via SMS.

IDPRODUCT	Numerical	NO	Product ID required for processing.
IDOPERATOR	Numerical	NO	Operator or Carrier ID
SERVICE	Text	NO	Service identifier related to the Product.
ORDER	Text	NO	Unique identifier of the transaction in the Partner system.
DESCRIPTION	Text	NO	Service description related to the Product from the Partner, for example: “AllGames Subscription”
OUTPUTFORMAT	Text	YES	Reply output format parameters, “xml” is the default one.
VERIFYCODE	Text	YES	Random verification text generated by the Partner.

Return data:

Name	***Type***	***Description***
ID	Numerical	Transaction ID of the Operation in the Terra Carrier Billing platform.
MSISDN	Numerical	User telephone number including country code and area code, for example: 5511963889439
ORDER	Text	Unique identifier of the transaction in the Partner system.
STATUS	Text	Server Response Codes:
MESSAGE	Text	If there is a relevant message for the transaction, for example "Time Out”.
EXPIRES	Numerical	This indicates the remaining time window, in seconds, that the PIN will be active to collect payments. If it is 0 it will indicate that the PIN cannot be used to collect another payment.
VERIFYCODE	Text	Verification text sent in the reply message but encrypted with the private key of the Partner. ONLY if the Request was sent.

Server Response Codes:

Value	***Description***
OK	The Telephone Number was cancelled from the Service Subscription.
NOK	The Telephone Number could not be cancelled from the subscription of the Service.
NS	The Telephone Number was not subscribed to the Service.
DER	Data input error
ERR	A mistake in the Terra Carrier Billing Platform that impeded the Request processing.
FA	Method execution not allowed because it was not identified by the Partner (invalid/expired Token and not recognized IP).

Reply formats:

Format	***Example***
XML	<RESPONSESET> <RESPONSE> <ID>100</ID> <MSISDN>5511963889439</MSISDN> <ORDER>OR_585445</ORDER> <STATUS>NOK</STATUS> <MESSAGE>TimeOut</MESSAGE>

	<EXPIRES>0</EXPIRES> </RESPONSE> <VERIFYCODE>f99bQcY6u/jI6/arH0jjuw==</VERIFYCODE> </RESPONSESET>

JSON	{
	"RESPONSE": [{
	"ID": 100,
	"MSISDN": 5511963889439,
	"ORDER": "OR_585445",
	"STATUS": "OK",
	"MESSAGE": "TimeOut",
	"EXPIRES": 0
	
	}],
	"VERIFYCODE":"f99bQcY6u\/jI6\/arH0jjuw=="
	}

3.1.4.14 Subscription Cancellation Request without using authentication PIN

Method to request the cancellation of a subscription purchased by a MSISDN without using PIN from the user.

URL
https://wstcb-mobile.terra.com/wstcb/MSC.asmx/MscGateway

List of parameters, they must be provided using a XML o JSON structure, encrypted and via POST using the “data” parameter.

Nombre	***Tipo***	***Opcional***	***Descripción***
IDOPERATOR	Numérico	NO	ID de Operadora o carrier.
IDPRODUCT	Numérico	NO	ID Producto asignado en la plataforma Carrier Billing.
ACTION	Texto	NO	Valor fijo: RmvSusc
MSISDN	Numérico	NO	Número telefónico. Incluye código de país y código de área, ej. 5511963889439
OPERKW	Texto	SI	Identificador de la aplicación o plataforma origen.
SOURCE	Texto	NO	Identificador de la aplicación o plataforma origen. Importante para estadísticas y métricas.
MSCPARTNER	Numérico	NO	Identificador numérico del partner en la plataforma MSC
MSCSERVICE	Numérico	NO	Identificador numérico del club o servicio en la plataforma MSC
OUTPUTFORMAT	Texto	SI	Parámetro de Formato de Salida de la Respuesta, el default es “xml”
VERIFYCODE	Texto	SI	Texto de verificación aleatorio generado por el Partner.

Return data:

Nombre	*Tipo*	*Descripción*
STATUS	texto	Código de respuesta del Server para la Transacción, ej. “NOK”
MESSAGE	texto	Si existiera, mensaje relevante a la transacción, por ejemplo, “Time Out”
VERIFYCODE	texto	Texto de verificación enviado en la respuesta pero encriptado con la llave privada. SOLO si se envió en Request.

Response codes:

VALOR	*DESCRIPCIÓN*
OK	Request processed succesfully.
ERR0	An exception error ocurred
ERR1	Invalid Partner at MSC plattform
NA	The MSISDN is blocked due to be in blacklist.
NOK	Too many retries
ERR2	Error at MSC plattform
NS	MSISDN not suscribed.
DER	Incorrect parameter.
ERR	Carrier Billing API exception.
FA	Unable to identify the partner (expired/expired token, invalid IP address, etc).

Response formats:

Formato	*Ejemplo*

XML	<RESPONSESET>
	        <RESPONSE>
	                <STATUS>NOK</STATUS>
	                <MESSAGE>Time Out</MESSAGE>
	        </RESPONSE>
	        <VERIFYCODE>f99bQcY6u/jl6/arH0jjuw==</VERIFYCODE>
	</RESPONSESET>

JSON	{
	   “RESPONSE”: [{
	     "STATUS": "NOK",
	     "MESSAGE": "Time Out"
	   }],
	  "VERIFYCODE":"f99bQcY6u\/jl6\/arH0jjuw=="
	}

3.1.4.15 SMS Messaging

Method that allows to send a SMS to a specific number.

URL
https://wstcb-mobile.terra.com/wstcb/Services.asmx/SndSms

List of parameters sent within an XML or JSON encryption via POST in "data".

Name	***Type***	***Optional***	***Description***
MSISDN	Numerical	NO	User telephone number including country code and area code, for example: 5511963889439
SMSTEXT	Text	NO	Text sent in the SMS. - Maximum 150 characters. - It is not allowed to include special characters (for example, ç,ñ,¿,&,%,^,Õ,Ü)
IDPRODUCT	Numerical	NO	Product ID.
IDOPERATOR	Numerical	NO	Operator or Carrier ID
OUTPUTFORMAT	Text	YES	Reply output format parameters, “xml” is the default one.
VERIFYCODE	Text	YES	Random verification text generated by the Partner.

Return data:

Name	***Type***	***Description***
MSISDN	Numerical	User telephone number including country code and area code, for example: 5511963889439
STATUS	Text	Server response code for the transaction, for example: “NOK”
MESSAGE	Text	If there is a relevant message for the transaction, for example "Time Out”.
VERIFYCODE	Text	Verification text sent in the reply message but encrypted with the private key of the Partner. ONLY if the Request was sent.

Server Response Codes:

Value	***Description***
OK	SMS sent successfully.
NOK	It was not possible to send the SMS.
NA	The MSISDN is in the Blacklist.
DER	Data input error
ERR	A mistake in the Terra Carrier Billing Platform that impeded the Request processing.
FA	Method execution not allowed because it was not identified by the Partner (invalid/expired Token and not recognized IP).

Reply formats:

Format	***Example***
XML	<RESPONSESET> <RESPONSE> <MSISDN>8181504000</MSISDN> <STATUS>NOK</STATUS> <MESSAGE>Time Out</MESSAGE> </RESPONSE> <VERIFYCODE>f99bQcY6u/jI6/arH0jjuw==</VERIFYCODE>

	</RESPONSESET>

JSON	{
	  “RESPONSE”: [{
	    “MSISDN”: 8181504000,
	    "STATUS": "NOK",
	    "MESSAGE": "Time Out"
	  }],
	  "VERIFYCODE":"f99bQcY6u\/jI6\/arH0jjuw=="
	}

4. Next Steps

Once the tests for all the different actions are completed, Terra will generate the Partner’s registration in the Terra Carrier Billing operation platform.

Terra will also be responsible in generating all the needed configurations for all the required actions required by the Partner (the different prompt charges, the different subscription services, etc.).

Once the Partner registration is active, Terra will provide the Partner the necessary data to make use of the API and the Terra Carrier Billing SDK.

5. Contacts & Support

For any question or consultation about the Terra Carrier Billing platform, you can contact any of the following persons.

Contact	***Area***	***Email***	***Skype***
Daniel Cattaneo	Commercial	daniel.cattaneo@corp.terra.com	danielamcatt
Arnoldo Chereti	S&D	arnoldo.chereti@corp.terra.com	achereti
Rene Charles	Engineering	rene.charles@corp.terra.com	rene.charlesmx
Fernanda Loaiza	Engineering	fernanda.loaiza@corp.terra.com	fernandailg