Integration of eBG Event Request API
V 1.1
API Integration Document

API for eBG Event Request

Introduction:

This API will be used by the Beneficiaries who are availing DDE eBG service. Beneficiaries who receive huge number of eBGs and prefer to raise the eBG event requests through the API mode can trigger this API instead of logging to the NeSL IU portal every time.

Request URL:

Below is the end point URL for eBG Event Request API on which the data is to be submitted:
https://stg.nesl.co.in/DDEeBGEventAPI/eBGEventRequest/request

- There is an OAuth implementation in the API considering *JWT token* as an input to the authorization.
- Below is the URL to generate the JWT token:
  https://stg.nesl.co.in/TokenGenerationAPI/authenticate
- There is a Basic Auth implementation in the API considering *userid:password* as an input to Basic Authentication. The *userid* and *password* will be shared by NeSL.
- The generated authorization token will need to be passed as a request header parameter - *authToken* in the eBG Event Request API along with the request payload.

Request Parameters:

Below are the request parameters:

Sl No	Field Name	Field Description	Field Type	Mandatory	Field data type
1	txnid	This will be a unique transaction ID that will be associated with the request.	Alphanumeric	M	Varchar(50)
2	ebgrefno	This will be the eBG number for which the request is being submitted	Alphanumeric	M	Varchar(30)
3	crdtsubtyp	Credit sub-type (Debt Facility Type)	List of values	M	**Values:** • GRNT • HeBG (For HeBG, the first event should be either amendment or renewal)

4	requestorrltnship	Relationship of the Requestor Party to the eBG	List of values	M	**Values:** • Beneficiary • Debtor
5	bankuin	Bank PAN	Alphanumeric	M	Varchar(10)
6	requestorentity	Name of the requesting entity	Alphanumeric	M	Varchar(100)
7	requestoruser	Name of the requestor	Alphanumeric	M	Varchar(100)
8	typofrequest	Type of request	List of values	M	**Values:** • Invocation • Partial Invocation • Amendment • Renewal • Closure • Cancellation • Extend or Pay
9	invctnamnt	The invocation amount of the eBG. This will be applicable only in case of invocation, partial invocation and Extend or Pay events.		CM	Numeric(16,2)
10	extperiod	The extension period of the eBG. This will be applicable only in case of Renewal and Extend or Pay events.	Date	CM	Date format (yyyy-MM-dd)
11	accholdername	Beneficiary account holder name. This will be applicable only in case of invocation, partial invocation and Extend or Pay events.	Alphanumeric	CM	Varchar(100)
12	accnumber	Beneficiary Account Number. This will be applicable only in case of invocation, partial invocation and Extend or Pay events.	Numeric	CM	Varchar(50)
13	bankname	Beneficiary Bank Name. This will be applicable only in case of invocation, partial invocation and Extend or Pay events.	Alphanumeric	CM	Varchar(50)

14	ifsccode	Beneficiary Bank IFSC Code. This will be applicable only in case of invocation, partial invocation and Extend or Pay events.	Alphanumeric	CM	Varchar(30)
15	cnctprsnnm	Name of the person who can be contacted	Alphanumeric	O	Varchar(100)
16	dept	Department of the contact person	Alphanumeric	O	Varchar(30)
17	cnctnumber	Mobile Number of the contact person	Numeric	O	Int(10)
18	emailid	Email Address of the contact person	Alphanumeric	O	Varchar(100)
19	docData	This will have the base 64 encoded value of the digitally signed documents that requestor wishes to submit as part of the event request. The request will get rejected if the document is not digitally signed.	Alphanumeric	O	Base64 encoded value of PDF document
20	rmrks	Remarks from the beneficiary about the event request, if any.	Alphanumeric	O	Varchar(500)

Request JSON Payload:

```json
{
    "txnid" : "ABCD1234",
    "ebgrefno" : "eBG1234",
    "invctnamnt" : "100000.00",
    "typofrequest" : "Invocation",
    "crdtsubtyp" : "GRNT",
    "requestorrltnship" : "Beneficiary",
    "requestorentity":"sfdggvsjdjssj",
    "bankuin" : "XXXXX1111X",
    "requestoruser" : "hdfsajshjdhf",
    "extperiod" : "2023-07-01",
    "accholdername" : "ghgsdhaghs",
    "accnumber" : "564674785895",
    "bankname" : "XXX Bank",
    "ifsccode" : "FGHJY0000023",
    "cnctprsnnm" : "gdgfhdshjhsjdh",
    "dept" : "dgshghgshashjsh",
    "cnctnumber" : "9898989998",
    "emailid" : "abc@abc.co.in",
    "docData" : "Base 64 encoded value of the digitally
    signed document.",
    "rmrks" : "Invoked",
}
```

Encrypted Request JSON:

Clients will digitally sign the unencrypted request payload using their private certificate.

```json
{
    "sessionId" : "ghegjskjakjkJAKJaksdsdghjhg",
    "ciphertext" :
"hdgydfryewtysYFAYSGYDFGDGSGAgashdegfgdgGuarogfjdzsyugiirur,

"digisign" :
"sdjgfjksdfjwelhrowernsdfbsdkljfjasb2342asklfbsdklbfsdlfsdl;
fsdlfsdklfbksdbfsdklfbksdfbksdbf;sdfwsehrowehrlsdbnfkbsdfbsd
kfbsdkfbsdkfbsdkl"

}
```

sessionId	The session ID is a randomly generated value. This session ID will be encrypted using RSA algorithm using NeSL's public certificate and the encrypted session ID will be passed as part of the request payload
Ciphertext	Client will encrypt the request json object using a 32-bit unencrypted session ID as the key using AES algorithm with CBC mode and IV parameter of length 16. IV parameter can be determined by taking the first 16 bytes of the decoded session ID value.
Digisign	This is the digital signature value by taking the hash of the unencrypted request json payload. This will be done using the Clients's private key.

Response Parameters:

Below are the response parameters:

Field Name	Description
txnid	This is the same txn_id that was passed as part of the request
ebgrefno	This is the same ebg_ref_no that was passed as part of the request
responsecode	This will have one of the following values: • 1 [In case of Success] • Appropriate Error code will be returned in case of failure
responsemsg	Corresponding message based on the response code

Response Payload:

Success response :
```
{
    "txnid" : "ABCD1234",
    "ebgrefno" : "eBG1234",
    "responsecode" : "1",
    "responsemsg" : "Success"
}
```

Failure response :

```
{
   "txnid" : "ABCD1234",
   "ebgrefno" : "eBG1234",
   "responsecode" : "ER001",
   "responsemsg" : "Not an Authorised user."
}
```

Encrypted Response JSON

NeSL will digitally sign the unencrypted response payload using NeSL's private certificate.

```
{
"sessionId" : "ghegjskjakjkJAKJaksdsdghjhg",
"ciphertext" :
"hdgydfryewtysYFAYSGYDFGDGSGAgashdegfgdgGuarogfjdzsyugiirur,

"digisign" :
"sdjgfjksdfjwelhrowernsdfbsdkljfjasb2342asklfbsdklbfsdlfsdl;
fsdlfsdklfbksdbfsdklfbksdfbksdbf;sdfwsehrowehrlsdbnfkbsdfbsd
kfbsdkfbsdkfbsdkl"

}
```

sessionId	The session ID is a randomly generated value. This session ID will be encrypted using RSA algorithm using Client's public certificate and the encrypted session ID will be passed as part of the response payload
Ciphertext	NeSL will encrypt the response json object using a 32-bit unencrypted session ID as the key using AES algorithm with CBC mode and IV parameter of length 16. IV parameter can be determined by taking the first 16 bytes of the decoded session ID value.
Digisign	This is the digital signature value by taking the hash of the unencrypted response json payload. This will be done using the NeSL's private key.

List of error codes:

Sl No	Error code	Error description
1	ER001	Not an Authorised user.
2	ER002	Missing input parameters.
3	ER003	Invalid input parameters.
4	ER004	Duplicate transaction id.
5	ER005	Invalid JSON request.
6	ER006	Unable to raise the event request, since you are not a {0} for this eBG Reference number.
7	ER007	Invalid Digital Signature.
8	ER008	Unable to process the request.
9	ER009	Unable to verify Signed pdf, since signature is not valid or signature is not available.
10	ER010	Unable to raise the event request, since the eBG Reference number is not found against the specified Issuing Bank.
11	ER011	Existing eBG event should be completed before processing new event.
12	ER012	eBG has already been cancelled or closed.
13	ER013	The eBG request is in progress or already invoked.
14	ER014	{{ebgEvent}} request cannot be raised as eBG has already crossed the claim expiry date