Encryption API Documentation & Description

This document gives an overview of the characteristics and common features of the Encryption API.

Encryption Method Send Message

1. Overview

This technical document is intended for developers who wish to use the Encryption method for sending messages.

2. Introduction

To protect the end user's data against man-in-the-middle attack, reply attack, and snooping, our customer wishes to have an Edge-to-Edge encryption feature for the entire payload traveling from ProGate network. The feature shall be available over API only and does not cover campaign-based communication. It entails encryption of the following elements in the payload.

- End User's MSISDN
- Message Content
- Sender ID
- DLT Content ID

3. Getting Started

The following basic information will help you get started with using the interface. The message and other Payload parameter will be Encrypted along with an Encryption Key and an IV (Initial vector)

4. Basic comments

To send a message, the system will firstly need to authenticate you as a valid user. The preferred method of authentication is using username and password.

1. Token generation API would be separate for generation of the Token. Validity of the token is 12 hours (as per the standard process for the platform).
2. Separate API for sending the SMS will be provided, API will be on POST Method (Json) only, and the message body/ payload will be encrypted at client's end and the same will be decrypted at the platform level.
3. API response will also be in encrypted form, and client needs to decrypt the data value using the Jar that provided from us.

5. Encryption/Decryption Jar Details

Please find the below parameters for the jar file which used for payload encryption/decryption.

1. Class Name: com.enc.App
   - public static String decrypt (String encrypted, String key, String initVector)
   - public static String encrypt (String value, String key, String initVector)
2. Class Name: com.enc.EncryptorAesGcmPassword
   - public static String encrypt (byte [] pText, String password)
   - public static String decrypt (String cText, String password)
   - pText.getBytes(UTF_8)

Sample Values for User Credentials Encryption: **Class Name:** com.enc.EncryptorAesGcmPassword

```
Original String to encrypt –
{"username": "testuser","password": "Test@123","client_id": "apiclient"}

Encrypted (base64)-
MAk0ttYWK61mECFQ1jN2wGnhrw+pX7GgtcnKvnX23EbC6lnS25h8PnvlcbrZxiuo8jTji8SRixRWJg+5GTdZ47XWtfx7
Skha48etR6Q95i9VI7ssTG9vltzKjQ5IIUO4sbOpuWS+/yZfMuNb3lQ7lT3aaXjj
```

Note: Client_id (api_client) will be the default value for User name & Password encryption to Generate Token Code.

6. Generate Token API

Request Headers

Header Name	Header value
Content-Type	application/json
User	User id

Request Parameter

SN	Parameter	Description	Scope	Sample Values
1	Data	Payload encrypted with password (user id will be password)	M	{ "data": "3wWz5rY2/mqC8rM1H6gwpXgPJ4ncoc21yU9c9+icWSWTaAlhmrrJ/kD2p8UCEKhVa+tzG5xmzVDb+ELK69RVDl553njozjow4AMaNsG5S88t1MbgvJMKPkg7cQ==" } sample decrypted value of data - { "username": "testing", "password": "Test@123", "client_id": "api_client" }

Sample Request for Token Generation

```
curl -X POST "https://{Domain Name}/fe/api/v1/auth/login" -H "accept: /" -H "user:testing" -
H "Content-Type: application/json" -d
```

"{"data":"3wWz5rY2/mqC8rM1H6gwpXgPJ4ncoc21yU9c9+icWSWTaAlhmrrJ/kD2p8UCEKhVa+tzG5xmzVDb+ELK69RVDl553njozjow4AMaNsG5S88t1MbgvJMKPkg7cQ==}"

Response Parameter

SN	Parameter	Description	Scope	Sample Values
1	access_token	access token for http API	M	307e269c-627c-4d8d-8929-9b850ac76800
2	token_type	token type	M	bearer
3	expires_in	validity of token in sec	M	43200
4	Scope	token scope	M	read write
5	Eks	Encryption key	M	d94Yx81/VFHLZSuRROGUDQ==
6	Iv	Initialization vector	M	yQ37IRX4GusEtCR6S38PAQ==

Sample Encrypted Response value of Token

```
{
        "access_token": "307e269c-627c-4d8d-8929-9b850ac76800",
        "token_type": "bearer",
        "expires_in": 43200,
        "scope": "read write",
        "eks":"d94Yx81/VFHLZSuRROGUDQ==",
        "iv":"yQ37IRX4GusEtCR6S38PAQ=="
}
```

Actual Encrypted Response -

KgdjmzN5W1HYgLucD7axwhsPx8bOtsA9NUoSlZchmw1dOIoap1MqsoHtjGIH7r0kDGAIwbnmApSkVpqPzbEwupV/ZA0Q8SASYXUsVTAIM2nDZNYSvQ7lU1A/oNQ7xTHn+IcQlffPGX4eB70Vr4HqKQouvWord8C1lZxxFPo3PFJgi01WoStkXdm+Nvpie3Gi8lNQs8CW0s2Kjb8kBL5gNUDnRxBORPzjvA7PiYZ4c73YxaVXvFR/+odcweFQ1M8CWiLIeYGqoRMrfoPm6CQdPEWXbmNJFcQTueYWAxrrdVTpLg==

7.Token based Send Message API

Request Headers

Header Name	Header value
Content-Type	application/json
Authorization	Bearer: 307e269c-627c-4d8d-8929-9b850ac76800

Request Parameter

Encryption API Documentation & Description

SN	Parameter	Description	Scope	Sample Value
1	Data	Payload encrypted with key and iv received in token request if encryption is on in user profile, else the json payload	M	Encrypted Data

Note:
Encrypted Data Value: {"data":"
Iqp0nsIVX5BTUwnusRnM5DTTjBuuMiSIh80RPLKbHPdGGH0aDvV+sN29b7jx06UwZaSl4WOK4pdKFJ4xMg36Qll5kM23sL8XFiXJztvNvE/zoyuab+u7NlHIi7CKrBeEJ7Z/W7zcQo0ootiixiREOes2+12I+2syLPHYACAcNjPXjSPEV/2ngB6g1y2wFQMIRr05tD/SCmevmhp8/toQ1QYpEr+qruOzoLA5tnMq7nQnU0YoPUu496RMDy3hOWcrEnXIVL4EmTYLbwIidj/dXZULSQhICzdXv7F6QIqTML3ZKcSK7aYslmrkacfDrN1ZGU4xbQBu4qsHP1X7iJ6xxykOjdyyKHd8u4UBEe68MjnYqcOt2C756Z5LBT5lijdX+IT58tKJSBPN9g/jOWIzmA==
"}

Sample Value for Message Payload encryption **Class Name: com.enc.App**

Encrypted Data Value: -

```
{
        "data":
"Iqp0nsIVX5BTUwnusRnM5DTTjBuuMiSIh80RPLKbHPdGGH0aDvV+sN29b7jx06UwZaSl4WOK4pdKFJ4xMg36Qll5kM2
3sL8XFiXJztvNvE/zoyuab+u7NlHIi7CKrBeEJ7Z/W7zcQo0ootiixiREOes2+12I+2syLPHYACAcNjPXjSPEV/2ngB6
g1y2wFQMIRr05tD/SCmevmhp8/toQ1QYpEr+qruOzoLA5tnMq7nQnU0YoPUu496RMDy3hOWcrEnXIVL4EmTYLbwIidj/
dXZULSQhICzdXv7F6QIqTML3ZKcSK7aYslmrkacfDrN1ZGU4xbQBu4qsHP1X7iJ6xxykOjdyyKHd8u4UBEe68MjnYqcO
t2C756Z5LBT5lijdX+IT58tKJSBPN9g/jOWIzmA=="
}
```

Actual Payload Value -

```
{
                "options": {
                        "dltContentId": "111113",
                        "dltTelemarketerId": "44343434444444444",
                        "dltPrincipalEntityId": "1701158271876955477"
                },
                "from": "Sender",
                "messageText": "Test Message",
                "recpients": [{
                        "corelationId": "id7000000001",
                        "mobile": "7000000001"
                }, {
                        "corelationId": "id7000000002",
                        "mobile": "7000000002"
                }],
                "unicode": "true/false",
                "campaignType": "pro/trans"
        }
}
```

Sample Request for Send Message

```
curl -ivX POST "https://{domainname}/fe/api/v1/sendMessage" -H "accept: */*" -H "Content-
Type: application/json" -H "Bearer:3ab20277-097e-47b6-959d-d96626c8de14" -d
'{"data":"Fpkahss63chDmFyanQHt9Sse9FMMZy6nQXmpCdpEESXNrnX0vJZNsTqZbJvZHpS/8KYmtkHWNx8MV9aMSZ
kosveBYCYkMa/WqZeutMJFK1iBaJoIsWrbQfw6ayf/qaVULB0oXXAr/0m58W3rhET1ElkludlyXY5f/qW1cityN3L9r7
eWCNcGoPwaQDKD+UG1ooddL1n15rDPgPQ0WDp7zBVc6uWHQk/p7v8+WNwSha/T5JOCJdqjqUM//LX91lt3QH7lfkSq/v
LWdXPcrFvOKXENy6VjD5ks6KqByWglX+DPzF7EM1cOUB6rWMQDkPqNbXUoj5f5KvaY6NXI+LT8SBCwL//F1NnH6Y4+Pd
ht+39ZARKYEb43pUXvEzlBDAhbxQzmczer/pgQtOJjcPN2TJIBes4BeKSMyiTcaqqCwSDNq/6CiGFzQ0OZ7vMSIHCHji
rAMVynGhAwxASvFgAJmQ=="}'
```

Sample Encrypted Response Data Value: -

```
gpNSkE2YQVhc4f08JSFCC/bLzceu6vF9fSehrr0z/gVJk8t2H6nHvFIwMXpPwbeEOCXqAhRZe9x48Bl42fooT5EP7IP9
ewVTP20z2XNEg1Uc0D9a2XFGUW79zNWH8wXHRMcd23mfE5btYSF0SXjLQlaHoo7K02z2skZGdKbDQ+aGcjPDCFEY4h4I
uvKRQGHmSf/gHnhaekhPG4DUGg0chQgnM61lmZApj7ZAoarK7cdDTifP6NXzR+dzZCuDtbJ93g/JhJnE2SI2t8YfQAOd
Q+CoTWQf8AHmdu9A7ACghftAITxqj1M1puuczZOlnTcy2fVtMpW3I8zO4WxOoYv/N/zu7/3TXL95mTaRlo/gs5g5RIk7
vI1H3Ocwqb0Hn9D7OzMzDhvX4/TyCdnb87A6vWVlGyJc0Xrgc1sS4tQN0Ft4kAJjjehfao6Pff5W3ki1ut5LUymR5dgm
VGYEW/VbXyCoHBy708++feWweFljYESfTWZFVTKlttZs5oEegtZFk34lEjZELsjm0mAvf9Mu9Q==
```

Actual Response Value (Decrypted)-

```
{
        "submitResponses": [{
                "transactionId": 1137258625,
                "state": "SUBMIT_ACCEPTED",
                "description": "Message accepted successfully",
                "pdu": 1,
                "corelationId": "122222",
                "statusCode" : "",
                "dltPEId" : ""
        }]
}
```

Response Parameter

SN	Parameter	Description	Scope	Sample Values
1	encrypted value of if encryption is on else submit Responses	List of response containing, transaction id, state, description, number of PDU and corelation id if any	M	{"submitResponses": [{ "transactionId": 1137258625, "state": "SUBMIT_ACCEPTED", "description": "Message accepted successfully", "pdu": 1, "corelationId": "122222" }] }

Parameter	Value	Required?	Description
Username	Username	YES	Your username
Password	GUI Password	YES	Your password.
Unicode	true/ false	YES	Unicode value to be true in case of vernacular message or in any regional language, in case of English content it should be false.
From	6 Alpha/Numerical characters	YES	A Sender ID to appear on the recipients mobile (Cannot contain any special characters).
To	Recipient number with or without country code (91 for India)	YES	Recipient mobile number with or without country code eg:919876543210
Text	Text message	YES	Message to recipients mobile (URL Encoded)
DLTContent ID	Approved Content id (length of 4-19)	YES	Content Template ID: - This ID is assigned to a message template when the same is registered with DLT.
DLT TelemarketerID	Numeric TMID of length 12-19	Optional	Optional Parameter
DLT PEID (Principal Entity ID)	Approved PEID (Numeric DLT Principal Entity Id of length 12-19)	Optional	Principal Entity ID: - This is corresponding to the Header (Sender ID), For every Sender_ID registered in the DLT system

Other responses in case of an error:

Response	Description	Reason
"statusCode":2051	“Sender [xxxxxx] doesn’t exist”.	When the API request contains nonregistered SENDER ID on User Panel
"statusCode":2070	Authentication failure	Invalid Username/Password/Account expired
"statusCode":2054	Invalid Msisdn [xxxxxxxxx] [IN]	When the MSISDN is not in 10- or 12-digits length (with IN country code 91)
"statusCode":6001	Insufficient Balance!	Zero Credit
"statusCode":7001	DLT_Content_ID not found	DLT Content ID missing in API request