

# **eVoting Specification (DP)**

## Table of Contents

1. Introduction .....	3
2. Description.....	3
3. Process flow.....	4
4. e-Voting Application.....	4
5. Ecryption Algorithm Specification .....	6

## 1. Introduction

Web Interface for eVoting application

## 2. Description

The application is an interface that allows the Client to make an e-Voting request from CDSL web portal to ESP web portal.

- The investor (BO) will come to CDSL website to know the e-Voting for their respective portfolio ISIN and can directly go to the ESP for e-voting. Following are the three ways investor can do e-Voting using CDSL portal:

### 1. EASI Application.

1. Investor can log into EASI application.
2. After login, an evoting link/menu will be provided to the user.
3. On the click of this link/menu, a new tab with user portfolio page will be open.
4. On this page, if any of the ISIN's e-Voting is currently going on than the e-Voting link for that ISIN will be enable.
5. When user clicks on e-Voting link user will be re-directed to the ESP portal where user can actually cast their vote.

### 2. CDSLINDIA website.

1. A login page for eVoting will be provided on cdslindia website.
2. User has to enter BOID and PAN to verify BO details.
3. After verification, an OTP will be sent to BO registered mobile number with CDSL.
4. After entering and verifying OTP, user will be re-directed to their respective portfolio page.
5. On this page, if any of the ISIN's e-Voting is currently going on than the e-Voting link for that ISIN will be enable.
6. When user clicks on e-Voting link user will be re-directed to the ESP portal where user can actually cast their vote.

### 3. DP website

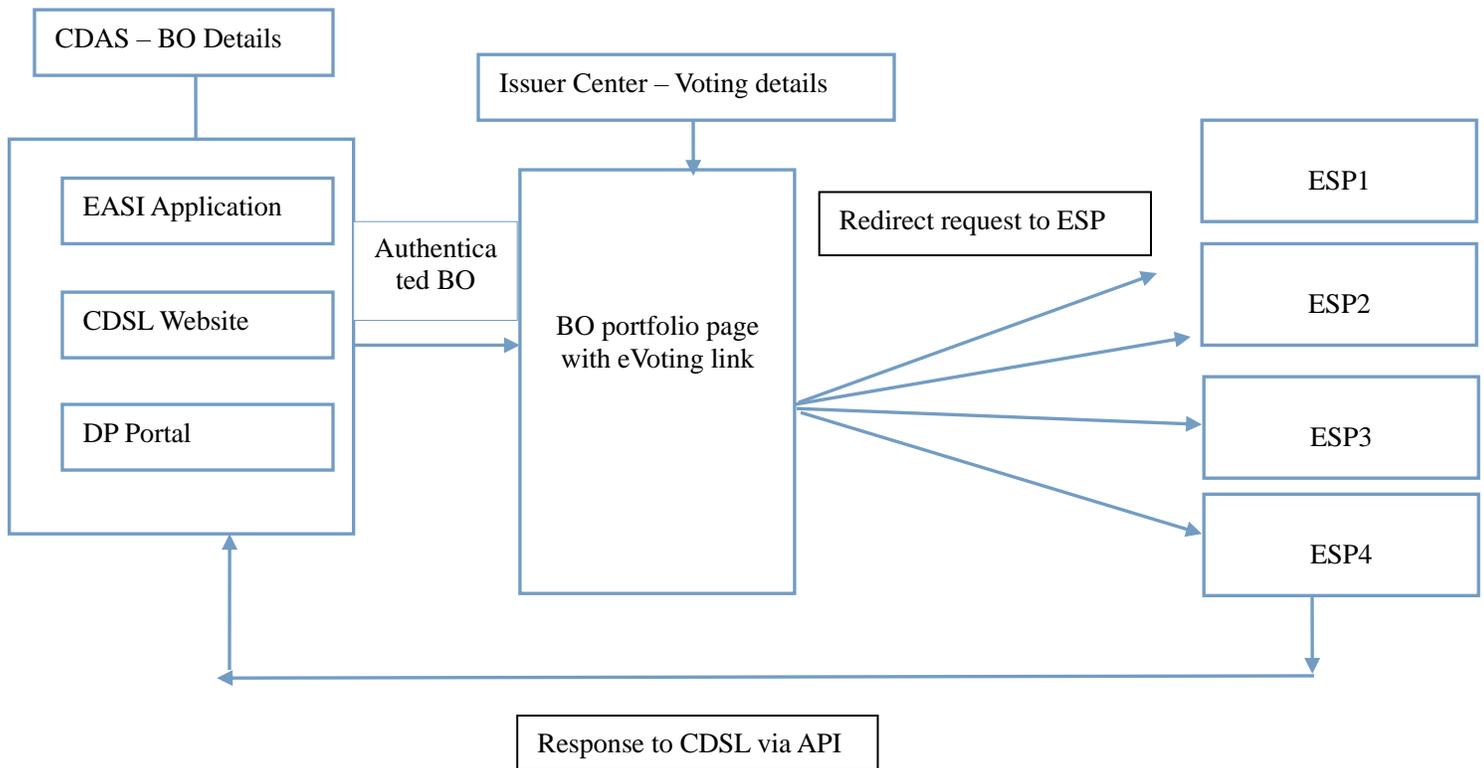
1. CDSL DP can provide e-Voting link on their website.
2. DP has to send investor details such as BOID, PAN number and DP user-id provided by CDSL to DP.
3. Once DP sends investor details, CDSL system will verify and after verification investor will be redirected to portfolio page.
4. On this page, if any of the ISIN's e-Voting is currently going on than the e-Voting link for that ISIN will be enable.
5. When user clicks on e-Voting link user will be re-directed to the ESP portal where user can actually cast their vote.

- On clicking this e-Voting option, CDSL will redirect the user to ESPs website in a 'New browser window'. The session at CDSL end will be handled independently.
- During redirection from CDSL website, Unique Request ID, CDSL User-ID, DP ID, Client ID of the user, Customer's public IP and timestamp will reach ESP's e-Voting web-site through the user browser. The Data will encrypt by CDSL private key. These

details will be sent to ESPs over HTTPS.

- After vote casted on ESP website, ESP will send response by calling CDSL API. While calling CDSL URL, ESP should send parameter like Demat account detail, Unique Request ID, evoting response, timestamp. CDSL will send acknowledgement to the callback request and SMS/Email will be sent to BO. In case CDSL does not provide positive confirmation to ESP, ESP should call CDSLAPI again with new request.

### 3. Process Flow



### 4. e-Voting Application

This application will mainly have following components:

- Evoting through CDSL portal ( EASI , CDSLINDIA website) ,
- DP portal( Redirect Post Request to CDSL portal)
- Redirect Post Request to ESP portal.

- API for response from ESP.
- SMS/eMail to BO
- Issuer login to provide eVoting details ( Process flow for the same has yet to be decided)

## Format of Input Message Structure from DP to CDSL

Given below is proposed message structure.

### Request Structure

```
<form name="ESPREDIRECT" method="post" action="{UAT url}">
<input type="hidden" name="dpid" value="10600" />
<input type="hidden" name="request_id" value="requestid" />
<input type="hidden" name="encdata" value="vKsdr76uyV===:aGVsbG8gd29ybGQ=" />
</form>
```

{UAT url}:- <http://202.54.83.147:9003/EVoting/EvotingRequest>

{LIVE url}:- <https://evoting.cdslindia.com/EVoting/EvotingRequest>

The field 'encdata' contains IV followed by colon (:) and a json string in encrypted format with base64 encoding ie {IV base64 encoded}:{Encrypted Data base64 encoded}

Below is the format of the UnEncrypted json payload.

```
{
  "request_id":"testuser",
  "bo_id":"1201060001376451",
  "pan":"RCPAN3764Q"
}
```

### Data Mapping

S. N.	Data Type	Description	Details	TagName
	String	Encdata	Contains the JSON representation of the actual payload	encdata
1	String	Request ID	System generated unique request number	request_id
2	String	BO ID	BOID	bo_id
3	String	PAN	PAN	pan

## 5. Encryption Algorithm Specification

Type	AES
Mode	CBC
Padding	PKCS7