ERI API Specifications

Integrated e-filing and CPC 2.0 Project

API Name	Login
API Description	APIs for performing User Authentication

Version History

Version	Date	Description
1.0	29-10-2021	Initial Draft
1.1	17-11-2021	Exception scenarios added

Table of Contents

1. Overview

Electronic Return Intermediaries shall begin the interaction with the eFiling system by establishing a session by invoking the login APIs. As noted in the ERI Specifications document, type-2 ERIs shall create a session using their own credentials while the Type-3 ERIs shall use the taxpayer or ERI-Type1 credentials.

2. About API

Requester	Type-2 or Type-3 ERI
Provider	LoginApi
Description	Login API supports multiple modes of authentication which can be broadly classified into two categories 1. Single Call (Password Based) - There will be single call for ERI 2 2. Multiple Calls (OTP Based) - There will be multiple calls for individual taxpayers when ERI 3 In the second category, the caller needs to make two calls, first to request for an OTP and subsequent call to submit the OTP. The request payload shall be common for both the calls. The system shall intelligently interpret the intent based on the parameters passed. For e.g. if the password is supplied, then the system will assume that the caller intends to login using password. If the password and otp is missing, then the system shall treat it as a request for an OTP. Finally, if the password is blank and OTP is supplied, the system shall attempt to log the user in using the OTP.
Mode of Integration (Real time / Batch)	Real Time
Processing Details	All validations regarding User Id, Password, OTP must be passed for successful authentication
Pre-Processing Details	User should be registered with e-filing portal and should have active profile
Service Name	EriLoginService
API URL	TBD

3. Target Audience and Pre-requisites

This is technical document and is target to ERIs working in their application and interested to integrate their application with IEC 2.0 platform.
The pre-requisites to call this API is that ERI is already registered with IEC 2.0 platform. They have valid credentials to call the API.

4. login API Details

This service is used to login and stablish the session with eFiling system from ERI application.

4.1 API Usage Scenario

ERI application pass their credentials to login API to get the session stablish with eFiling system. This is required to call any other eFiling API from ERI application. ERI user must be registered with eFiling system and should have valid credentials.

4.2 API Request process

ERI application must pass the ERI credential to establish the login session. Application will initiate addClient request as below:

1. ERI application will pass ERI user id and password to login API.
2. Login API will validate the credentials and respond with authToken.
3. ERI can use the auth token to call subsequent APIs after post login.

4.3 API Protocol

addClient API is exposed as REST API over the HTTPS. The input data should be sent as JSON document using Content-Type "application/json".

4.4 Request Parameters

The request will consist of request header and request body:

4.4.1 Request Header:

Header is mandatory and will consists of following values:

Mandatory Request Header Parameters:

Header Name	Header Value
Content-type	application/json
clientId	clientId value which is provided to ERI as part of the registration
clientSecret	clientSecret value which is provided to ERI as part of the registration
accessMode	"API"

4.4.2 Request Body: Description

Request body will consist of below attributes:

data: data attribute will be Base64 encoded string of API request json. Details of request json attributes are explained in request data element details.

signature:

- The API request data attribute should be digitally signed for the message integrity and non-repudiation purposes.
- Digital signing should always be performed by the ERI from value of data attribute which was generated from request json.
- The signature should be generated using a valid X.509 certificate
- signature value should be generated from data field using ERI's DSC private key.
- ERI should share their DSC public key with ITD to validate the signature.

eriUserId:

- It is mandatory and valid value is user ID of the ERI

4.4.3 Details of data attribute:

Below are the request parameters, which is request json used to create data attribute as explained above data attribute of the request body:

Name of the Parameter	Data type	Max length	Is Mandatory	Description
serviceName	String	60	yes	It is mandatory value is "EriLoginService"
entity	String	10	yes	ERI user Id for ERI 2 taxpayer user ID/PAN for ERI 3
pass	String	50	yes	Encrypted Password associated with the User using symmetric key

otpSourceFlag	String	1	no	**This is mandatory only for ERI 3** Checks for Option user has selected for otp: "**E**" for eFiling OTP "**A**" for Aadhaar OTP
otp	String	6	no	**This is only for ERI 3** where taxpayer will pass OTP after receiving OTP. It is not mandatory. It is mandatory when Transaction Id is provided.
transactionId	String	20	No	**This is only for ERI 3** where taxpayer will pass OTP after receiving OTP. It is mandatory when otp is provided. Transaction no. which was provided while OTP generation

Request Parameter logic for different flows:
Login API supports multiple modes of authentication which can be broadly classified into two categories

1. Single Call (Password Based) There will be single call for ERI 2
2. Multiple Calls (OTP Based) There will be multiple calls for individual taxpayers when ERI 3

In the second category, the caller needs to make two calls, first to request for an OTP and subsequent call to submit the OTP. The request payload shall be common for both the calls. The system shall intelligently interpret the intent based on the parameters passed. For e.g. if the password is supplied, then the system will assume that the caller intends to login using password. Below is the details of password and OTP options:
Option 1: UserId/password validation: If password is provided, then it will be considered as password to be validated.
Option 2: UserId/password and OTP request: If password and otpSourceFlag both are provided, then password will be validated and on successful userid/password then otp will be sent to taxpayer based on the value of otpSourceFlag
Option 3: OTP validation: If OTP is provided, then it will be considered as OTP to be validated. In this case value of otpSourceFlag and transactionId to be provided. When OTP value is provided then password should not be provided.

4.5 Response Parameters

Name of the Parameter	Data type	Max length	Is Mandatory	Description
entity	String	60	yes	User id used for Login

messages	Array		yes	This is an array which has 4 sub parameters – code, type, desc, fieldName
code	String	7	yes	Error/message code depending on validation response
type	String	10	yes	It describes type of message
desc	String	50	yes	It describes Error/message if validation is passed/failed
fieldName	String	50	no	It describes the field name, when not applicable null will be returned
transactionId	String	20	yes	Transaction no. generated post successful login
autkn	String	32	yes	It is random number generated to authorize user for post login services

4.6.login API - Sample Request format

{
"data": "",
"sign": "",

"eriUserId:""
}

data tag will be Base64Encoded string from following request json

{
"serviceName": "EriLoginService",
"entity": "ERA2343353",
"pass": " TXlwYXNzd29yZEAxMjM="
}

login API - Sample Response format

{
"messages": [
{
"code": "EF00000",
"type": "INFO",
"desc": "OK",
"fieldName": null
}

],
"errors": [],
"entity": " ERA2343353",
"desc": "",
“transactionId” “”,
"autkn": "dGVzdFVzZXJEZXY4QGluZm9zeXMuY29t”
}

Logout API Details

This service is used to logout the ERI session from ERI application.

4.7 API Usage Scenario

ERI application already have logged in and has auth token. ERI application wants to logout from eFiling system

4.8 API Request process

ERI application already have auth token and wants to logout from the eFiling system. Application will initiate addClient request as below:

1. ERI application will auth token and call the logout API.
2. Login API will remove the validity of the auth token and kill the session for given auth token. Once logout then same auth token cannot be used to validate the session.

4.9 API Protocol

Login API is exposed as REST API over the HTTPS. The input data should be sent as JSON document using Content-Type "application/json".

4.10 Request Parameters

The request will consist of request header and request body:

4.10.1 Request Header:

Header is mandatory and will consists of following values:

Mandatory Request Header Parameters:

Header Name	Header Value
Content-type	application/json

clientId	clientId value which is provided to ERI as part of the registration
clientSecret	clientSecret value which is provided to ERI as part of the registration
authToken	Auth token from the Login Flow
accessMode	"API"

4.10.2 Request Body:

Request body will consist of below attributes:

data: data attribute will be Base64 encoded string of API request json. Details of request json attributes are explained in request data element details.

sign:

- The API request data attribute should be digitally signed for the message integrity and non-repudiation purposes.
- Digital signing should always be performed by the ERI from value of data attribute which was generated from request json.
- The signature should be generated using a valid X.509 certificate
- signature value should be generated from data field using ERI's DSC private key.
- ERI should share their DSC public key with ITD to validate the signature.

eriUserId: It is mandatory and valid value is user ID of the ERI

4.10.3 Details of data attribute:

Below are the request parameters, which is request json used to create data attribute as explained above data attribute of the request body:

Name of the Parameter	Data type	Max length	Is Mandatory	Description
serviceName	String	60	yes	It is mandatory and valid value is **"EriLogoutService"**
entity	String	10	yes	Valid User Id for ERI 2 Valid PAN for taxpayer in case of ERI3
pan	String	10	Yes	Valid PAN of the taxpayer

4.11 logout API - Sample Request format

{
"data": "",
"sign": "",
"eriUserId": ""
}
data tag will be Base64Encoded string from following request json
{
"serviceName": "**EriLogoutService**",
"entity": "ERIP124345",
"pan": ""
}

4.12 logout API Response

There is no response data. Caller must check the HTTP status of 200.

5. API Exception Details

Scenario	Error code	Error string	detail	Message Type
Successful scenario	EF00000	OK	If in response, we get this code then user navigates to next page else we show corresponding error message	INFO
When User enters PAN in user ID	EF00036	PAN does not exist, please register this PAN or try with some other PAN.	This means user id is PAN and user does not exist	REMARK
When User enters Aadhaar Number in user ID	EF00026	This Aadhaar number is not linked to any registered PAN. Please link your registered PAN with this Aadhaar number to login through Aadhaar number. Else, login through PAN	This means user id is Aadhaar Number and it is not linked to any active PAN profile	ERROR

When User enters OTP to validate	EF00016	The OTP has expired, on clicking of OK button you will be navigated to the previous screen to generate new OTP.	If User enters any OTP which has already expired	REMARK
When User enters OTP to validate	EF00028	Invalid OTP, please retry.	When user enters wrong OTP	ERROR
When User Id is entered	EF00032	Your UserId has been deactivated, kindly contact helpdesk for more information.	userId/account entered by user is deactivated	REMARK
When user enters password	EF00042	Your User Id/account has been locked, you can try after <4 hours> or contact e-filing helpdesk to unlock your account	When user enters Incorrect password for continuous 6 times	REMARK
too many invalid credentials attempts and account locked	EF00079	Your e-filing account has been locked\deactivated. Please contact e-filing helpdesk <Helpdesk Toll Free number>		ERROR
When PAN entered is inactive	EF00098	The PAN entered is inactive. Please contact your Accessing Officer to activate the PAN.	When user enter a PAN which is inactive (will be applicable for Type 3)	ERROR
When invalid userId/password is entered	EF500060	Invalid UserId/Password	Incorrect UserId/Password	ERROR
When attributes are incorrect in json request data	EF20123	Invalid Request Data	When request data is invalid	ERROR
When any attributes are missing in request JSON	EF40000	JSON data invalid.	JSON data invalid.	ERROR