#### **Chi tiết luồng xác thực sử dụng giao thức OpenIDConnect**

Các bước cơ bản xác minh người dùng sử dụng tài khoản Viettel AI SSO:

Bước 1: App khởi tạo một link đăng nhập với Viettel AI SSO và chuyển hướng người dùng tới link này

Bước 2: Người dùng đăng nhập với tài khoản Viettel AI SSO và xác nhận cho phép app truy cập thông tin của mình

Bước 3: Viettel AI SSO redirect người dùng về địa chỉ nằm trong param redirect\_uri trong link đăng nhập, kèm theo một authorize code

Bước 4: App gửi request để đổi code này thành token của người dùng

***Khởi tạo link đăng nhập***

App tạo ra một link đăng nhập (với base URL là địa chỉ của hệ thống IAM) rồi redirect người dùng đến link có cấu trúc như sau:

<https://sso.viettelai.vn/oauth/authorize>

?client\_id=<CLIENT\_ID>

&redirect\_uri=<RIDIRECT\_URI>

&response\_type=code

&scope=openid email profile phone

&state=<STATE>

&code\_challenge=<CODE\_CHALLENGE>

&code\_challenge\_method=S256

Trong đó:

client\_id : Định danh ứng dụng của vendor trên hệ thống ViettelAISSO . Admin của ViettelAISSO sẽ khai báo ứng dụng lên hệ thống và gửi lại client\_id cho app owner

redirect\_uri : Là địa chỉ đường dẫn mà hệ thống ViettelAISSO sẽ chuyển hướng tới sau khi xác thực người dùng thành công

state : Là một xâu ngẫu nhiên gồm 10 ký tự chữ cái tiếng Anh viết thường, viết hoa và chữ số ([a-zA-Z0-9]), dùng để định danh request đăng nhập

code\_challenge : Là một xâu base64-encoded được generate theo các bước trong hướng dẫn ở đây: <https://www.oauth.com/oauth2-servers/pkce/authorization-request/>

Chú ý:

1. REDIRECT\_URI là địa chỉ quản lý bởi app, có chức năng verify thông tin sau khi người dùng hoàn tất xác thực trên ViettelAISSO và được chuyển hướng về trang này
2. Giá trị STATE cần được lưu lại trong session để sau khi người dùng được redirect về, app có thể xác nhận phiên đăng nhập trên hệ thống IAM là khớp với authorization request mà app đã tạo ra
3. Giá trị CODE\_VERIFIER dùng để generate CODE\_CHALLENGE cũng cần được lưu lại trong session để verify code khi trao đổi code lấy token tại bước 3

(Chi tiết về cách thức xử lý trên trang REDIRECT\_URI sẽ được đề cập cụ thể ở mục [Verify code và lấy id token từ code](#_Verify code và lấy id token từ code))

***Viettel AI SSO xác thực người dùng***

Người dùng chưa đăng nhập cần cung cấp credentials của họ cho hệ thống để xác thực danh tính. Sau khi xác thực danh tính thành công, người dùng được redirect lại về địa chỉ nằm trong parameter redirect\_uri trong link đăng nhập với các tham số sau:

<REDIRECT\_URI>?code=<CODE>&state=<STATE>

Trong đó:

REDIRECT\_URI : Là địa chỉ được truyền vào tham số redirect\_uri của login link

CODE : Là thông tin định danh phiên xác thực thành công mà IAM cung cấp, app cần dùng code này để đổi lấy access token của người dùng tại bước 4

STATE : Là thông tin định danh request đăng nhập mà app truyền vào khi khởi tạo login link

***Verify code và lấy id token từ code***

Địa chỉ REDIRECT\_URI là địa chỉ quản lý bởi app, trang này có chức năng chính là verify code mà ViettelAiSSO trả về, đồng thời exchange code đó thành token của người dùng để tiếp tục verify và thực hiện các nghiệp vụ cần thiết phía sau.

Các bước xử lý bao gồm:

1. Lấy về param state từ URL, nếu param này khác giá trị được tương ứng lưu trong session thì trả về trang lỗi 404
2. Lấy về param error từ URL mà IAM chuyển hướng về, nếu param này có được set thì hiển thị trang lỗi 403
3. Lấy về param code từ URL và sử dụng code này để gửi request tới IAM để verify và exchange token

Request exchange token là một HTTP POST request có khuôn dạng như sau:

URL: <https://sso.viettelai.vn/oauth/token>

Body:

grant\_type=authorization\_code

client\_id=<CLIENT\_ID>

code=<CODE> : Là giá trị code trong URL param ViettelAISSO trả về

redirect\_uri=<REDIRECT\_URI>

code\_verifier=<CODE\_VERIFIER>

Sau khi verify thành công response trả về như sau:

{  
 “id\_token”:“eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI5YWNmZjgwNi1kMzJlLTQyZDEtYTkzOC00OTZiYzEwMzgwZjgiLCJp...”,

“access\_token”:“eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI5YWNmZjgwNi1kMzJlLTQyZDEtYTkzOC00OTZiYzEwMzgwZjgiLCJp...”

}

Thông tin người dùng được encoded trong trường id\_token , dưới định dạng một base64-encoded JWT token. Nội dung sau khi decode như sau:

{

"aud": "9acff806-d32e-42d1-a938-496bc10380f8",

"iss": "https://sso.viettelai.vn",

"iat": 1702437523.0938,

"exp": 1702441123.0938,

"sub": "30790",

"email": "lien@gmail.com",

"email\_verified": true,

"name": "Nguyen Văn B",

"family\_name": "Công ty TNHH 2 thành viên",

"phone\_number": "0365878952"

}