**Extending EIE Header to include**

**Business Individual Identifier**

Version 0.4

Contents

[2 Revision History 2](#_Toc536797050)

[3 Brief 3](#_Toc536797051)

[4 Solution Sketch 3](#_Toc536797052)

[5 EIE Header Changes 3](#_Toc536797053)

[5.1 EIE Header 4](#_Toc536797054)

[5.1.1 EIE Header Data Model 4](#_Toc536797055)

[5.1.2 DSV Service Definition 4](#_Toc536797056)

[5.1.3 Process Detail 5](#_Toc536797057)

[5.1.4 Response Definition 5](#_Toc536797058)

[5.1.5 Integration with SOR: 6](#_Toc536797059)

[5.2 Token Endpoint 7](#_Toc536797060)

[5.2.1 Endpoint Definition 7](#_Toc536797061)

[5.2.2 Request Definition 7](#_Toc536797062)

[5.2.3 Response Definition 7](#_Toc536797063)

[5.2.4 Process Detail 8](#_Toc536797064)

[5.2.5 Response Codes 8](#_Toc536797065)

[5.2.6 Error Response 9](#_Toc536797066)

[5.2.7 Samples 9](#_Toc536797067)

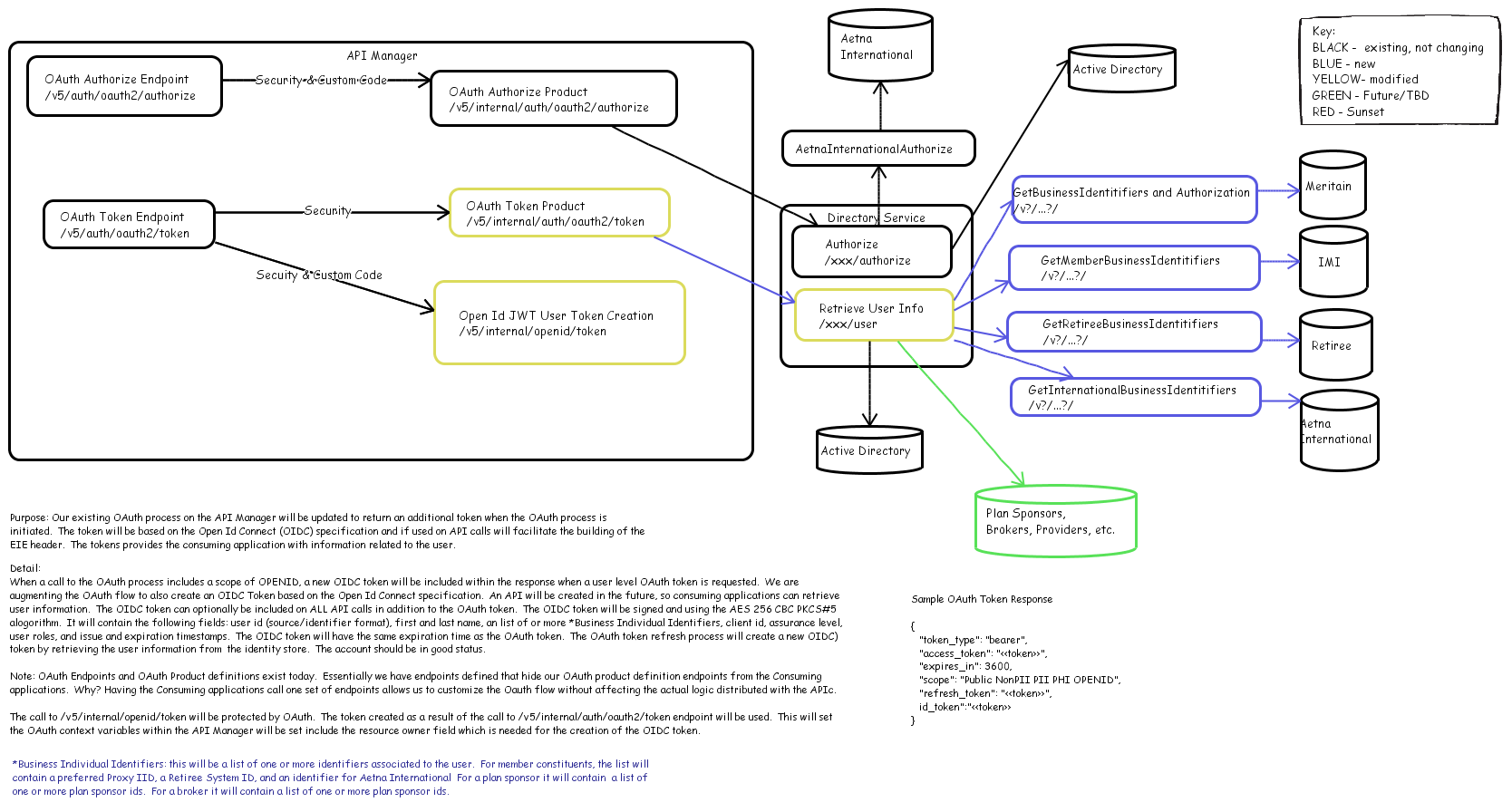
# Revision History

| **Version** | **Date**  (MM/DD/YYYY) | **Author** | **Description of Changes** |
| --- | --- | --- | --- |
| 0.1 | 10/15/2018 | Meister, Richard /Vamshi Varaganti | Initial Version |
| 0.2 | 01/30/2019 | Vamshi Varaganti | Updated the structure of Business Identifier as suggested by Andy. |
| 0.3 | 02/01/2019 | Vamshi Varaganti | Included Clint ID as a request parameter to Directory Service |
| 0.4 | 02/11/2019 | Vamshi Varaganti | Include CustNum as part of retrieveUserInfo service response |

# Brief

The document details the changes to be implemented in directory service to pull the business identifiers from SOR (system of record), changes in API Token endpoint to accommodate business identifiers in the OIDC token.

# Solution Sketch



# EIE Header Changes

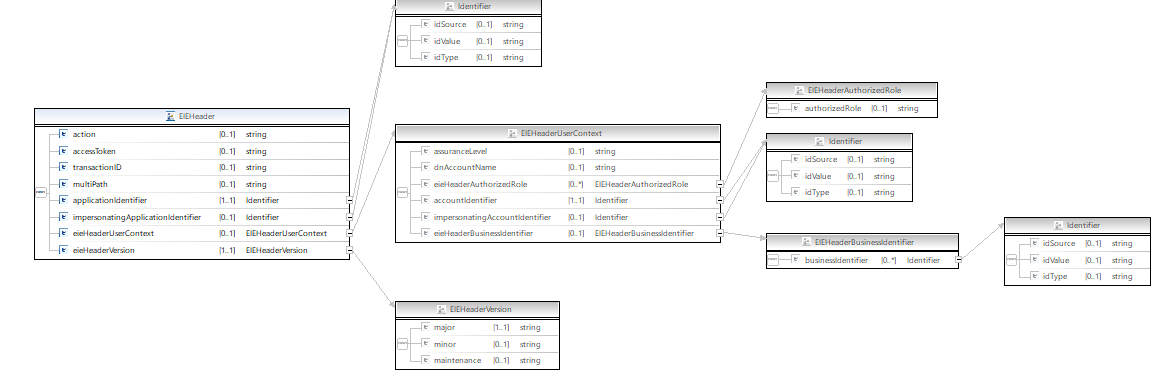
Existing EIE Header is being extended to include business Identifier associated with the user. Business Identifier constitutes a list of identifiers associated with the user’s system of record.

For member/ constituent the list will contain the preferred proxy Id, a Retiree system Id and an identifier from Aetna International. For Plan Sponsors, broker it would include the list of plan sponsor Ids.

As part of the current scope the solution would focus on integration with IMI and will be extended to integrate with Maritain, Aetna International, Retiree applications in future.

## EIE Header

### EIE Header Data Model



* businessIdentifier is of type Identifier and would accommodate the following,
  + IdSrouce
  + idValue
  + Idtype
* A new DSV service (DirectoryServiceV3/retrieveuserInfo/{id}/users) will be developed, this service will be invoked by APIC token end point , to fetch user details from active directory along with the business identifier.
* Token endpoint need to send the client Id as part of the request to DSV service.

### DSV Service Definition

End Point :: DirectoryServiceV3/retrieveuserInfo/{id}/users?clientId={clientId}&domain={domain}:: GET

|  |  |  |  |
| --- | --- | --- | --- |
| **Parameter** | **Required?** | **Data Type** | **Description** |
| id | Yes | String | Login ID associated with the user, in the format idsource~idvalue. |
| clientId | No | String | Client id of the application used to pull the associated network groups. |
| domain | No | String | Business domain associated with the user. |

### Process Detail

1. The directory service accepts loginId and business domain associated with the user and provides the user account details (similar to the existing DSV User Search Service - GET /users?userid={id}).
2. Apart from the basic user information required to construct a user token, the services will also fetch business identifier details associated with the user.
3. Directory service will identify the SOR using domain name, businessCategory, healthCareRoles and OU (org Unit) attributes of the associated user in Active Directory, the service integrates with corresponding SoR and fetches the business identifier associated with the user.
4. Directory service will provide the business identifier in the following format,

Ex: "businessIdentifier": [

{ "identifierType":"preferredProxyId", "identifier":"15~7SLBBBQBBPXY" },

{ "identifierType":"retireeId", "identifier":"idSrouce~idValue" }

]

1. Directory service will have to validate the number of preferred proxy Ids received as part of the API response, it’s expected to have a single preferred proxy Id for a given loginId. If IMI service returns multiple preferred proxy Ids, directory service can ignore passing the business identifier to the consumer.
2. Every instance, where directory service receives multiple preferred proxy Id for a given login Id has to be logged in splunk. The report generated in splunk can to be shared with support team (AD, IMI) for necessary data correction.

### Response Definition

The response sent by the DSV service to APIC would be as below,

{

"userInfoResponse": {

"userName": {

"firstName": "firstName",

"lastName": "lastName",

"middleName": "middleName"

},

"userId": "john@email.com",

"userDOB": "12/12/1921",

"userAccountStatus": "enabled",

"userUUID": "11111",

"domain": {

"domainId": "1",

"domainName": "AD"

},

"distinguishedName": "CN=xxx,..",

"userHealthCareRole": "membersubscriber1",

"userSAMAccountName": "xxxxx",

"userAddress": {

"zip": "11111"

},

"userLanguage": "English",

"userAssuranceLevel": "1",

"userClassification": "User",

"businessCategory": "USHC}ART",

"userCustNum": ["XXXXX", " XXXXX"],

"userEmailId": "Charlotte@aetna.com",

 "userAuthorizationRoles": [

      "NavDevRead",

      "NavAdmin",

      "NavDevWrite"

    ],

"businessIdentifier": [

{ "identifierType":"preferredProxyId", "identifier":"15~7SLBBBQBBPXY" },

{ "identifierType":"retireeId", "identifier":"idSrouce~idValue" }

]

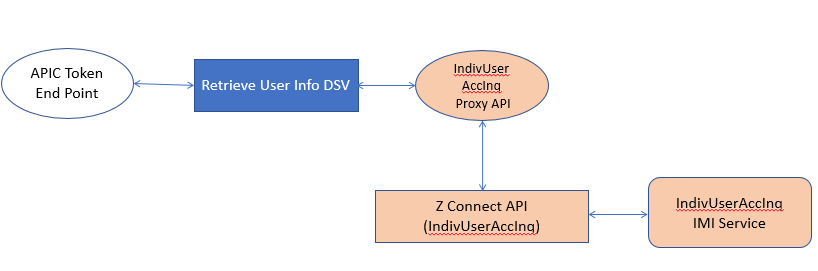
}

}

### Integration with SOR:

* As part of the first phase of the implementation – we would integrate DSV with IMI to obtain individual proxy identifier, in the next phases we would extend DSV service to integrate with other SORs including Aetna International, Retiree, Meritain Systems.
* IMI exposes IndivUserAccInq service through a proxy API, which could be used to fetch the individual preferred proxy Id using the associated loginId.

The below diagram explains the solution approach to be followed by DSV to fetch Preferred Proxy Id from IMI.



* API Token endpoint invokes the new DSV service that would call the IMI service User Account Inq. getProxyIIDByUserLoginId.
* Individual User Account Inq will be extended to include a new operation (getProxyIIDByUserLoginId) which will be used to fetch the preferred proxy Id of the member using login ID. The IMI service is being exposed through ZConnect RESTful endpoint.

## Token Endpoint

### Endpoint Definition

* The endpoint URI will be defined as follows:

POST:: /v7/auth/oauth/token

* Requests sent to the endpoint must be sent securely using the HTTPS protocol.
* The endpoint will allow the following scope to be requested:
  + Public
  + NonPII
  + **PII**
  + PHI
  + **openid**

### Request Definition

|  |  |  |  |
| --- | --- | --- | --- |
| **Header** | **Required?** | **Data Type** | **Description** |
| Authorization | Yes | string | client\_id:client\_secret in the standard Basic Authorization format |
| Content-type | No | string | Default: application/json |

|  |  |  |  |
| --- | --- | --- | --- |
| **Parameter** | **Required?** | **Data Type** | **Description** |
| redirect\_URI | Required | url | Provided by the client application when the client application is defined within the API Portal |
| grant\_type | Required | string | Constant Value: ‘authorization\_code’ |
| code | Required | string | The authorization code received in the prior step. |

### Response Definition

|  |  |  |
| --- | --- | --- |
| **Field** | **Data Type** | **Description** |
| token\_type | String | “Bearer” |
| access\_token | String |  |
| expires\_in | String | “3600” |
| scope | String | “Public NonPII **PII** PHI **openid**” |
| refresh\_token | String |  |
| id\_token | String |  |

### Process Detail

* API Manager issues OAuth tokens following the OAuth 2.0 specification
* Token flow would generate an OIDC token based on the data obtained from DSV service.
* Token flow returns OAuth token and OIDC token based on the IDP source system ID and the subject.
* List of claims including the Aetna specific custom claims is documented below (information included within all OIDC tokens issued at Aetna):
  + iss: <<http://openid.aetna.com/consumer>>
  + sub: <Active Directory GUID>
  + aud: <[client id]>
  + exp: the expiration time of the token
  + lat: the issue time of the token
  + given\_name: <first name>
  + family\_name: last name
  + acr: level of assurance (URL format)
  + ae\_dgn: distinguished name
  + ae\_hcr: healthcare roles
  + ae\_accountId: identifies the user (in identifier format, src~value)
  + ae\_busIndId: business identifier of the associated individual (in identifier format, src~value)
  + ae\_version
* For impersonation flow, there would be additional fields included as part of the token as listed below,
  + ae\_impAUD – client id used with the impersonation process, if applicable.
  + ae\_impHCR - healthcare roles related to the person being impersonated.
  + ae\_impACR – Level of Assurance of the user being impersonated.
  + ae\_impDGN – distinguished name of the user being impersonated.
  + ae\_impAcountId – account identifier of the user being impersonated.
  + ae\_impBusIndId – list of business individual identifier related to the user being impersonated.
  + Ae\_impGranted LOA – the authorization level of assurance – the LOA granted to the user performing the impersonation. (for future use)
* The token endpoint would populate the identifier value in the EIE Header in the format idsource~idvalue.

### Response Codes

|  |  |
| --- | --- |
| **Code** | **Description** |
| 200 | Returned on success. |
| 401 | Unauthorized |
| 500 | Internal server errors. The service response was not completed. Additional detail on the error response can be found in the response body. |

### Error Response

1. The authorization server responds with an HTTP 400 (Bad Request) status code (unless specified otherwise).
2. Refer the specification at <https://tools.ietf.org/html/rfc6749#section-5.2> for further details.
3. The parameters are included in the entity-body of the HTTP response using the "application/json" media type.
4. Error response includes the following attributes,
   1. error code
   2. error\_description (optional)
   3. error\_uri (optional)

### Samples

#### SAMPLE REQUEST

POST https://<token endpoint>

HTTP/1.1

Accept-Encoding: gzip,deflate

Content-Type: application/x-www-form-urlencoded

Authorization: Basic <encrypted client\_id:client\_secret>

Connection: Keep-Alive

User-Agent: Apache-HttpClient/4.1.1 (java 1.5)

code=<code>&grant\_type=authorization\_code&redirect\_uri=<redirect\_uri>

#### SAMPLE RESPONSE

A sample JSON response is shown below:

{

"token\_type":"bearer",

"access\_token":"{access\_token}",

"expires\_in":"3600",

"scope":"{scopes}",

"refresh\_token":"{refresh token}",

"id\_token":"{id\_token}"

}

#### SAMPLE error RESPONSE

A sample JSON error response is shown below:

HTTP/1.1 400 Bad Request  
 Content-Type: application/json;charset=UTF-8  
 Cache-Control: no-store  
 Pragma: no-cache

{  
 "error":"invalid\_grant"  
}