|  |  |
| --- | --- |
| *CES Web APIs App Registration* | |
| Document Title: | CES Web APIs OAuth Implementation |

|  |  |
| --- | --- |
| **Information Security Classification:** | *Confidential* |
| **Status:** | *Draft* |
| **Version Number:** | *1.2* |
| **Date:** | Dec-07-2020 |
| **Originator:** | Ashwani Kumar |
| **Supplier Approval:** |  |
| **Customer Approval:** |  |

Page Break

*Contents*

1. Introduction
2. Document Purpose

This document defines API resources between the Network Rail CES (CEFA Enabling Solution) solution and Supplier systems. The document includes list of client and backend app registration required for Oauth 2.0 security implementation for CES Web APIs

The detail agreed between Suppliers and Network Rail within this document for security implementation.

1. References

|  |  |  |
| --- | --- | --- |
| S.N0 | Documentation | Share point Link |
| 1 | ICD |  |
| 2 | DSD |  |

Page Break

1. Backend App Registration

1. Backend App Registration for OAuth 2.0 Implementation for Suppliers Web APIs Access

**Note**: The user required to access all backend Web APIs. Approach could be either claim or scope based.

Steps:

1. Login to azure portal and select Azure Active directory service
2. Click **Application Registration** under **Manage** section
3. Provide Name: **APIM\_CES\_SUPPLIERS\_BACKEND\_APP**
4. **Click Register**
5. Select **Expose an API** under **Manage** Section
6. Set the **Application ID URI**

Adding Application Role:

* Edit **Manifest**underthe **Manage** Section
* Replace **“appRoles”:[]** with below content

**Note: Open PowerShell and run command new-guid. Replace the id of appRoles with unique guid.**

  "appRoles": [

            {

                  "allowedMemberTypes": [

                        "Application"

                  ],

                  "description": "Allow client apps to send requests to the API.",

                  "displayName": "CES\_EXTERNAL\_API\_REQUEST",

                  "id": "93d44a2b-8d22-42b2-aac2-cfffc853c7fe",

                  "isEnabled": true,

                  "lang": null,

                  "origin": "Application",

                  "value": "API.ExtRequest"

            }

      ]

1. Backend App Registration for OAuth 2.0 Implementation for CES UI Web APIs Access

Steps:

1. Login to azure portal and select Azure Active directory service
2. Click **Application Registration** under **Manage** section
3. Provide Name: **APIM\_CES\_UI\_ BACKEND\_APP**
4. **Click Register**
5. Select **Expose an API** under **Manage** Section
6. Set the **Application ID URI**
7. Click**Add a Scope**
8. Name**:**CESAPIs.Read

Who can Consent**:** **Admin Only**

Admin consent display name: CES\_Dev\_API

Admin consent description: Read\_CES\_Dev\_API

User consent display name: CES\_Dev\_API

User consent description: Read\_CES\_Dev\_API

Click **Add scope**

Adding Application Role:

* Edit **Manifest**underthe **Manage** Section
* Replace **“appRoles”:[]** with below content

**Note: Open PowerShell and run command new-guid. Replace the id of appRoles with unique guid.**

  "appRoles": [

            {

                  "allowedMemberTypes": [

                        "Application"

                  ],

                  "description": "Allow client apps to send requests to the API.",

                  "displayName": " CES\_EXTERNAL\_API\_REQ",

                  "id": "e2cc8f9d-728c-45ee-b06b-a069841927f6",

                  "isEnabled": true,

                  "lang": null,

                  "origin": "Application",

                  "value": " API.ExtRequest "

            },

{

                  "allowedMemberTypes": [

                        "Application"

                  ],

                  "description": "Allow client apps to send requests to the API.",

                  "displayName": " CES\_INTERNAL\_API\_REQ",

                  "id": "813ff1a1-30dd-4c4b-960f-debd03f2a4d2",

                  "isEnabled": true,

                  "lang": null,

                  "origin": "Application",

                  "value": " API.IntRequest "

            }

      ]

1. Client App Registration

1. Client App Registration for Amey Rail

Steps:

1. Login to azure portal and select Azure Active directory service
2. Click **Application Registration** under **Manage** section
3. Provide Name: **APIM\_CES\_AMEYRAIL\_CLIENT\_APP**
4. **Click Register**
5. Click**Certificates & secrets**under**Manage**section
6. Create New Client Secret
7. Select Expire duration as 1 year.
8. Description – apim ces suppliers client service principal

**Note: After creation of the secret take backup/copy of the client secret value.**

1. Click **API permissions** under **Manage** section
2. Click Add a permission
3. Under **MyAPIs** tab select backend app -**APIM\_CES\_SUPPLIERS\_BACKEND\_APP**
4. Check the check box – Scope (**CES\_EXTERNAL\_API\_REQUEST**) and click**Add Permission.**
5. After adding the permission**– Click admin consent to provide consent.**

**Adding optional Claim:**

* Click **Token Configuration** under **Manage** section
* Click **+Add group claim.**
* Select the checkbox Groups**assigned to the application**

1. Client App Registration for CES UI

Steps:

1. Login to azure portal and select Azure Active directory service
2. Click **Application Registration** under **Manage** section
3. Provide Name: **APIM\_CES\_UI\_CLIENT\_APP\_DEV**
4. **Click Register**
5. Click**Certificates & secrets**under**Manage**section.
6. Create New Client Secret
7. Select Expire duration as 1 year.
8. Description – apim ces suppliers client service principal

**Note: After creation of the secret take backup/copy of the client secret value.**

1. Click **API permissions** under **Manage** section
2. Click Add a permission
3. Under **MyAPIs** tab select backend app -**APIM\_CES\_UI\_ BACKEND\_APP**
4. Check the check box – Scope (CES\_EXTERNAL\_API\_REQ***,***CES\_INTERNAL\_API\_REQUEST) and click**Add Permission.**
5. After adding the permission**– Click admin consent to provide consent.**

**Adding optional Claim:**

* Click **Token Configuration** under **Manage** section
* Click **+Add group claim**
* Select the checkbox  **Groups assigned to the application**