**Workforce OKTA ASP.Net toolkit Playbook**

|  |
| --- |
|  |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version #** | **Date** | **Revised By** | **Description of Changes** |
| 1.0 | 10/01/2024 | Accenture | Initial Version |
| 1.1 | 2/8/2024 | Accenture, HPE IAM Engineering, HPE IAM Operations | Reviewed |
|  |  |  |  |
|  |  |  |  |

**Table of Contents**

[1 Purpose 3](#_Toc1157617201)

[2 Pre-requisites 4](#_Toc945872246)

[3 Scope 4](#_Toc1830549261)

[4 Functional overview 4](#_Toc1875183818)

[5 Integration Steps 5](#_Toc485362168)

[6 Appendix 7](#_Toc1213517859)

[6.1 Resources 7](#_Toc1326836355)

# **Purpose**

The purpose of this document is to describe the specification for the OIDC Library and migration of the Agentless Library to OIDC Library from PING to OKTA. The library will perform the authentication with OKTA.

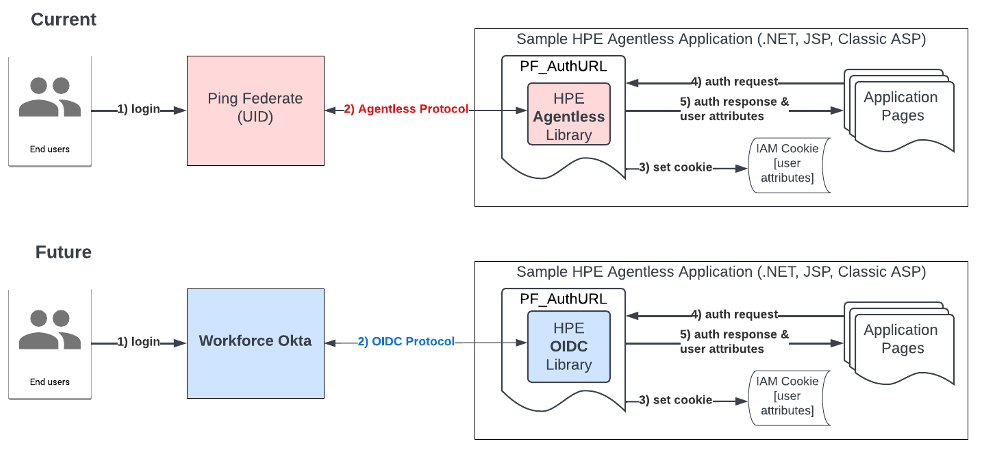
# **Pre-requisites**

1. To integrate application using ASP.NET Code with Okta we need these requirements:
2. Developer knowledge to ensure the application code and authentication code will work with each other.
3. Application server(s) running ASP.NET. (Internet Information Services i.e., IIS)
4. Access to the application server(s) to add files to “bin” folder of application.
5. Create OKTA OIDC application using the AOB portal. Please refer the [AOB OIDC Playbook](https://hpe.sharepoint.com/teams/WorkforceOkta/Shared%20Documents/AOB/OIDC%20AOB%20Playbook_V1.pdf?web=1) to know the details on how to access AOB portal and creating an OIDC application.
6. Access to the application server(s) to add files to “bin” folder of application.
7. .Net Framework 2.0 and above

# **Scope**

1. Ability to perform Authentication with OKTA.
2. Ability to parse user attributes after successfully authenticated.
3. Ability to redirect to OKTA to authenticate if token expires.

# **Functional overview**



# Integration Steps

1. Download the Agentless Kit from [IAM Workforce OKTA FAQ](https://hpe.sharepoint.com/teams/WorkforceOkta/) . It will be downloaded on your system as a .zip file.
2. Extract the zip file and import the dlls into the asp.net project.
3. Copy the following dll files into the bin folder of application to be integrated with OKTA.
4. (If working on the application you can reference these URL into your project by using the “Add Reference” option in the solution explorer.

**bin folder**

1. Interop.MSXML2.dll
2. Newtonsoft.Json.dll
3. PFAuth.dll
4. OktaAuthAppWeb.dll
5. Copy the below files in the main application folder where the web.config is present
   1. PF\_Auth.aspx
   2. Test.aspx
   3. Test.aspx.cs
6. Edit you application Web.Config with the okta app settings details. The settings template is provided web.config file that is available as part of the zip file.
7. Update the app settings values with your application details provided by OKTA

<appSettings>  
<!--generate this keys using ?pfcmd=keys in PF\_Auth.aspx-->  
<add key="PF\_Key" value=""/>  
<add key="PF\_IV" value=""/>  
<add key="PF\_Sign" value=""/>  
<!--fill this with information from UID team-->  
<add key="PF\_ExpTime" value="120"/>  
<!--This can't be greater than 480 minutes-->  
<!--fill this with OKTA Configuration settings-->  
<add key="okta:ClientId" value=""/>  
<add key="okta:ClientSecret" value=""/>  
<add key="okta:OrgUri" value="["/>](https://mylogin-dev.hpe.com/oauth2/aus74nxnh4dr3VRn91d7/v1/authorize%22/%3e)<add key="okta:TokenUri" value="["/>](https://mylogin-dev.hpe.com/oauth2/aus74nxnh4dr3VRn91d7/v1/token%22/%3e)<add key="okta:RedirectUri" value="["/>](http://localhost:60242/PF_Auth.aspx%22/%3e)<add key="okta:Scopes" value="openid profile"/>  
<add key="okta:State" value=""/>  
<!-- pingoktamapping is used the map the ping attributes that are no configured in okta but can map to alternate attributes provided by Okta-->  
<add key="pingoktamapping" value ="c:country;cn:name;subject:mail"/>  
</appSettings>

1. The Okta configuration details can be fetched using the AOB tool once the application is onboarded.

A screenshot of a computer

Description automatically generated

**okta:ClientId :** Client Id of the okta application that has been created

**okta:ClientSecret:** Client secret obtained from AOB tool

**Okta:OrgUri:** this is the Authorization server URI ("authorization\_endpoint") value from the metadata file from AOB tool. Example : https://mylogin- dev.hpe.com/oauth2/aus74nxnh4dr3VRn91d7/v1/authorize

**Okta:TokenUri:** this is the token URI ("token\_endpoint") value from the metadata file from AOB tool. Example: <https://mylogin-dev.hpe.com/oauth2/aus74nxnh4dr3VRn91d7/v1/token>

**Okta:RedirectUri:** this should be the applications PF\_auth.aspx url. This depends on application where the PF\_Auth.aspx is available. Example: https://{URL}/PF\_AUTH.aspx

**Okta:Scopes:** values will be “openid profile groups”

**Okta:state:** a random key please see example above.

**Pingoktamapping:** this is the mapping keyvalue pair to map the ping attributes that are missing in the OKTA attributes. Just in case. Example in this case the attribute “c” is mapped the value of “country” of the okta attribute.

1. If you don’t have it already you can generate the key, IV and PF\_Sign by using the following URL and use them in the web.config

http://{your application host}/PF\_Auth.aspx?pfcmd=keys

1. Output will be look like below. Below values are just an example

A screenshot of a computer code

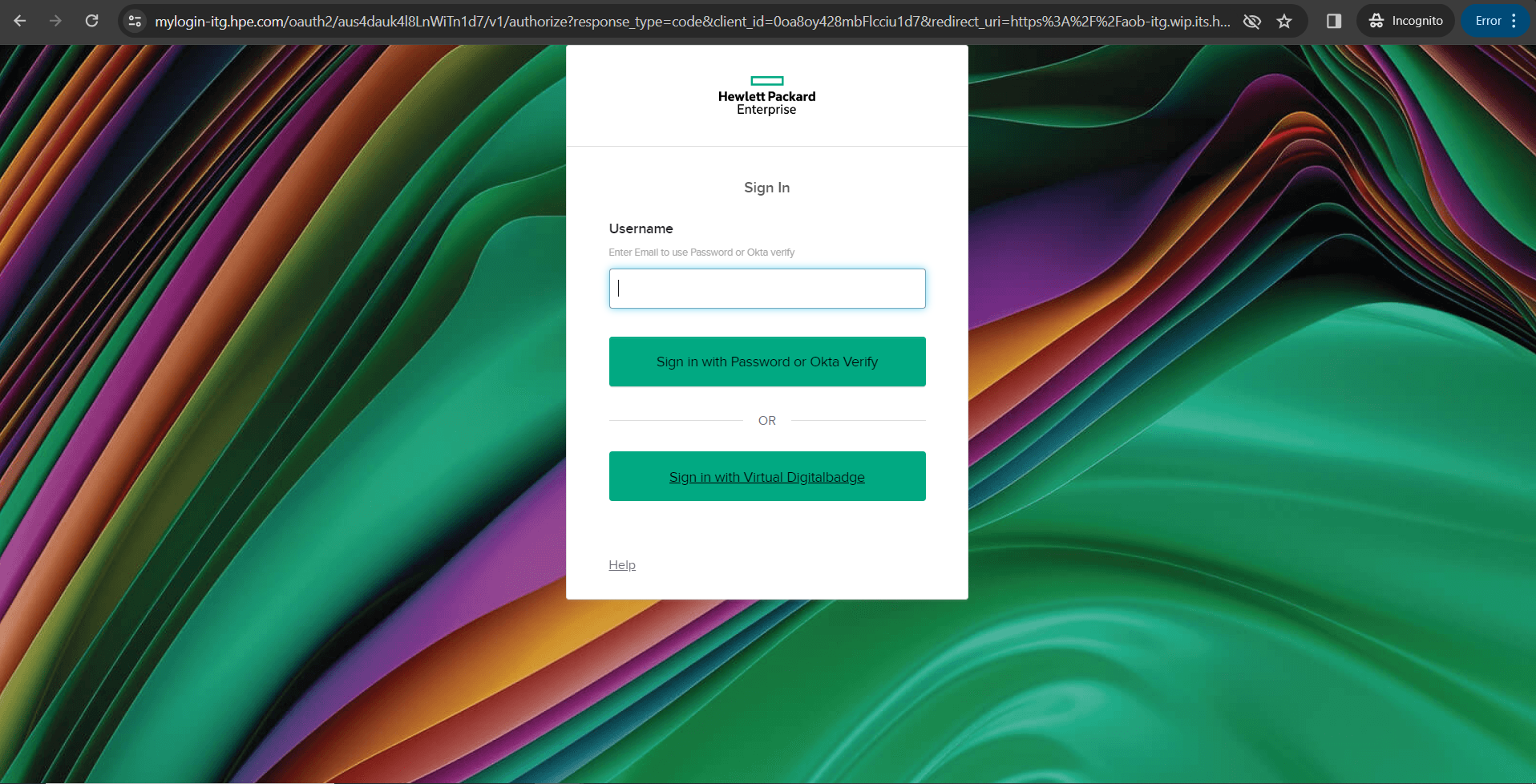
Description automatically generated

1. Test.aspx page is provided to check an example on how the attributes values can be accessed and authentication can be initiated to protect the pages in your application. Use this across the pages where that needs protection.

string uid = HPUID.PF\_Authentication("{your host}/PF\_Auth.aspx", "uid");

1. Access the test.aspx or start page of your application where you are using the authentication attributes.

If the application is not authenticated, the user will be navigated to authentication page as below



1. Once the user logs into OKTA successfully the user will be redirected the application page that was requested.
2. Use the URL https://{host}/PF\_AUTH.aspx to check all the OKTA authentication attributes that are available across the application

A close-up of a document

Description automatically generated

# **Appendix**

## **Resources**

[**WORKFORCE FAQ**](https://hpe.sharepoint.com/teams/WorkforceOkta/)