



DIGITAL INNOVATIONS COMPANY

---

**Identity as-a-service (IDaaS) Implementation for First American DBS - Approach**

**Date: March 21, 2020 (version 1.0)**

---

**Prepared for First American Corp**



*First American*

---

## Revision History

Version	Date	Author	Changes made
1.0	3/21/2020	Sanjeev Kuwadekar	Document Creation - 1st Draft

Please contact Sanjeev Kuwadekar regarding any matter contained with this document.

Sanjeev Kuwadekar

Mobile : 818-825-5024

Email: [sanjeev.k@infogen-labs.com](mailto:sanjeev.k@infogen-labs.com)

---

## 1. Background

First American DBS is looking for a secure and reliable cloud-based identity management solution to protect their customer's identities. Currently, First American Corporate has white labeled Azure IDaaS as EagleID, a First American branded, IDaaS service. First American Corporate built EagleID to meet mandate 4, no local user storage, of First American's Infosec mandates. However, specific to first American DBS is the directive that no First American branding be displayed on their products/services, so their non-First American customers like Fidelity, can white label them. EagleID is a First American branded service and does not meet the directive DBS has. First American DBS has been working with the FA EIM team to solve this issue but is in need of a back-up custom solution.

## 2. Requirements

First American DBS is looking for a secure and reliable cloud-based identity management solution to protect their customer's identities that . This solution needs to offer the following capabilities:

- FA DBA should be able to white label the solution and then allow their customers to white label further using their own branding
- User should be able to use their own Social IDs
- Supported on any device and OS
- Support for Multi-factor authentication
- Highly scalable
- 99.9% SLA
- No dependency on local user store
- Comply with all Infosec mandates

The current implementation of IDaaS is a white labelled version of Azure IDaaS, EagleID, which meets all the above requirements except one; it does not allow the customers of FA DBS to white label IDaaS using their own branding.

## 3. Approach

Below are a few of the top IDaaS solutions in the market:

Microsoft Azure Active Directory  
Okta Identity Management  
Oracle Identity Cloud Service  
IBM Cloud Identity  
AWS Identity Service  
OneLogin

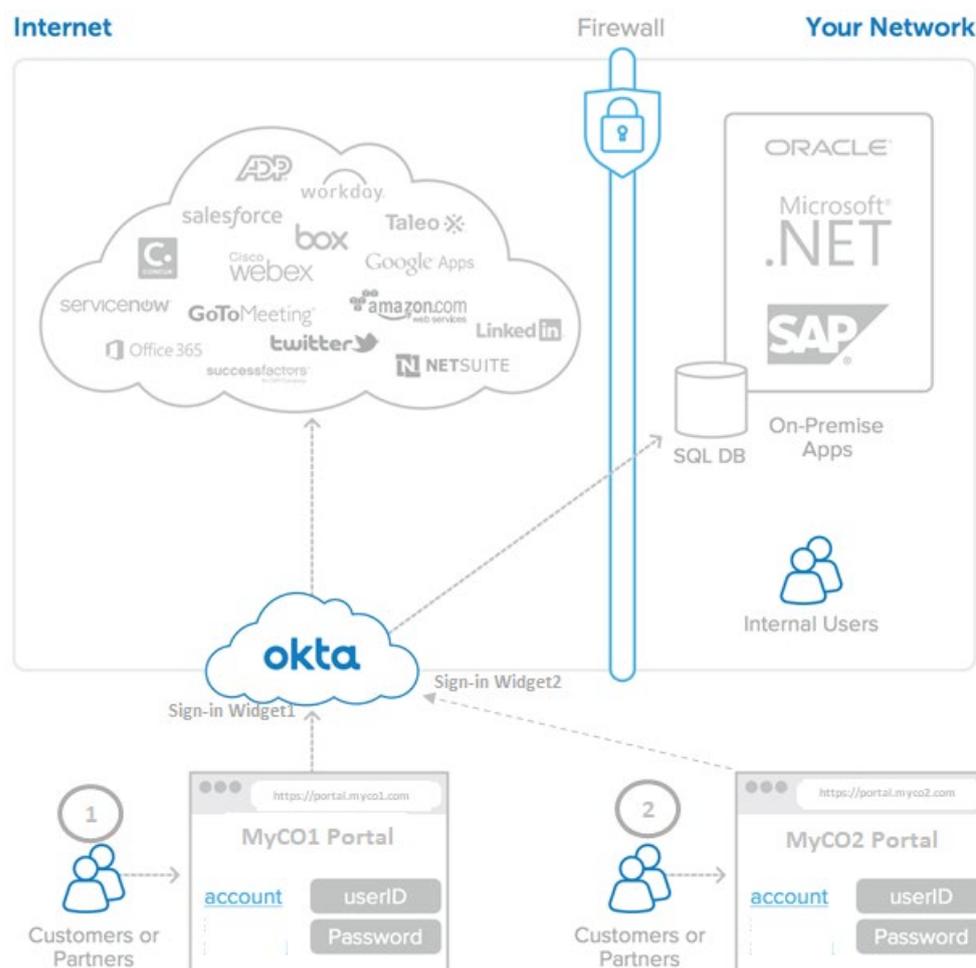
Gartner and other leading companies have named Okta as the leader in the IDaaS space:

Figure 1. Magic Quadrant for Access Management



Okta can be hosted in any of the leading cloud providers including Azure, AWS and Google. Okta can be easily integrated with Microsoft Azure AD services and all Microsoft products. In addition, Okta allows enterprises to customize (white label) their sign-on page so that companies can use their own branding.

The OKTA sign-in widget is a Javascript library. Developers can download its source code from git and modify it to customize sign-on experiences for their users. In order to allow FA DBS to offer white-labelled versions of Okta IDaaS service, multiple versions of this sign-on widget can be created – one for each customer. Creation of these widgets can also be automated. Okta can be configured to present the custom widget created for each customer based on the customer’s subdomain/domain as shown in the diagram below:



## 4. Next Steps

Further analysis is necessary to evaluate this approach. A short-term engagement with an Architectural consultant with IDaaS and Cloud experience is highly recommended. During this engagement, the following scenarios can be created and tested:

- Customized versions of the Okta sign-in widget to provide white-labelled experience for multiple tenants
- Okta integration with Azure Cloud Services
- Compliance with Infosec mandates.