SSO Federated Overview

Smarter Balanced Assessment Consortium

Document Date: April 9, 2020

1 Document Control

1.1 Revision History

Version	Date	Author	Approver	Reason for version
1.0	4/9/2020	Peter Flores, Jeff Khoury		• Created and based-off document supplied from vendor (Okta) that assisted Smarter Balanced in establishing the Federated SSO solution

1.2 Document References

Ref No.	Referenced Item
1	

2 Introduction

2.1 Purpose

The purpose of this document is to capture the architectural framework for implementing federation with Okta for unified single sign-on with Smarter Balanced. This document entails how the users will securely authenticate and gain access to external facing applications..

2.2 Intended Audience

This document is intended for the implementation project teams:

- Project Manager - to define tasks for phases & milestones
- Architects - to define the implementation strategy
- Developers - to define any custom applications needed
- Business Analysts - to define user experience

2.3 Scope

Smarter Balanced has been asked to transform our SSO infrastructure into a federated model to allow member states to unify their authentication. The scope of this document is to present use cases for internal and external users to access Smarter Balanced resources. Okta has been selected as the SSO vendor because of its flexibility and the ability to easily integrate with widely varied identity providers (IdPs).

The Digital Library (DL), Tools for Teachers, the Reporting and Data Warehouse (RDW), and Test Item Management System (TIMS) systems have been integrated with Okta and are available to federated members.

3 Solution Overview

3.1 Business Goals and Objectives

Smarter Balanced provides an SSO solution for their members to give secured access to protected applications. The goal is to share authenticated application access that will provide different levels of secure access to Smarter Balanced members via a centralized, secure, highly available service.

3.2 Requirements Review

High level features include:

- Just in Time User creation through Identity Provider
    - Users will be provisioned within the Okta organization using Just in Time (JIT) provisioning once the user has been validated through the trusted Identity Provider. The Member Service Provider is responsible for maintaining an up-to-date directory of users and their associated authorization information.
    - The user will be automatically assigned to a group based upon the source IdP.
- Sign-In
    - Smarter Balanced Staff will use the standard Okta sign-in user interface (UI).
    - Users from member states will sign in through their federated IdP UI.
    - Once federated, the Okta sign-in UI will direct the users to their “home” IdP for login *if it is known.*
        - Note: If the account exists and it's not known what the person's home IdP is, they will continue to operate as a standalone user in Okta. If no account exists, then they MUST log in from their "home" IdP at least once in order to be provisioned.
- Application/Policy Assignment
    - Assignment by group
    - Assignment by tenancy chain

4 Architecture

4.1 Overview

Smarter Balanced provides a secure, single user data source for a federated single sign-on authentication for its members to their shared applications. Each member state must have its own IdP. Smarter Balanced employs Okta Identity Portal to be the authentication point for all applications. All applications use Okta for authentication.

Application and policy assignment are based on group assignments and the users' tenancy chains. A user's group assignment will be automatically assigned based on the identity provider at the time of creation using Okta's JIT provisioning process.

Since most users will be authenticating via inbound SAML federation, passwords are not stored within the Okta Universal Directory. Any locally created Okta accounts must adhere to the University of California's password policies (https://its.ucsc.edu/policies/password.html).

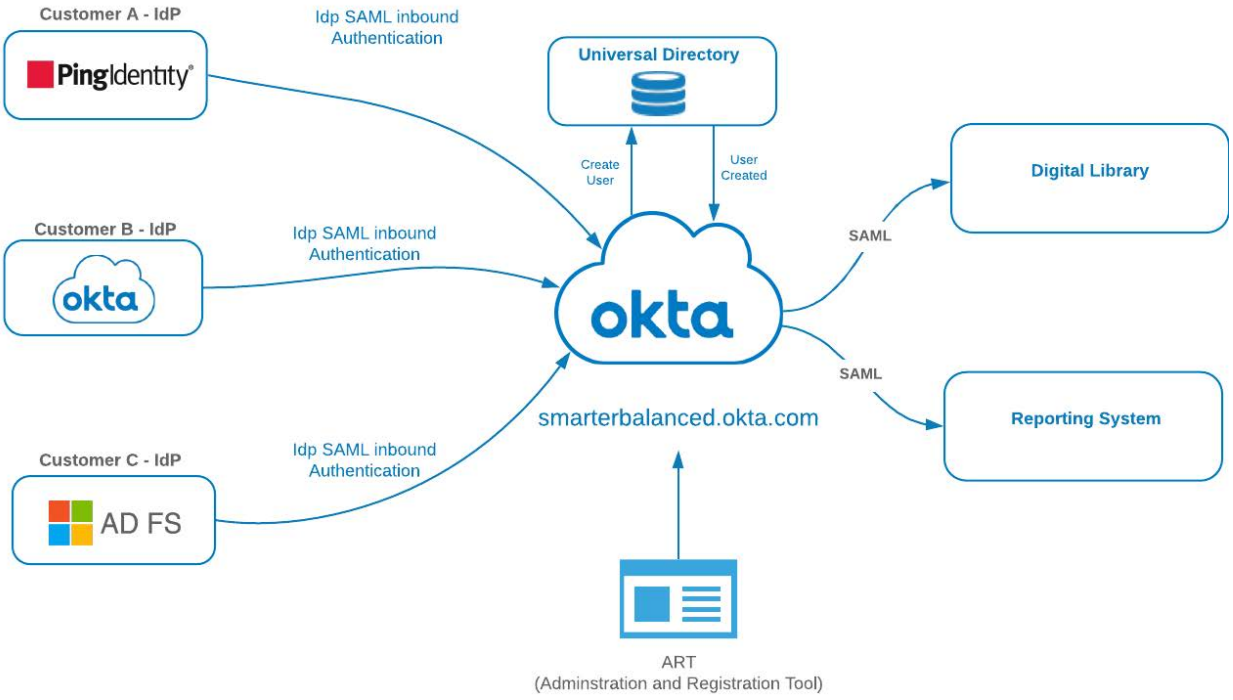
Okta supports a federated authentication for the web applications using the SAML / WS-Fed protocols. Each user will authenticate to Okta and will be redirected to the application using SAML authentication flow. Application assignment will be granted based on the user's group membership and tenancy chain.

Okta requires 5 attributes per user account:

- Username (in email format)
- Email address (same as username)
- Firstname
- Lastname
- Tenancy Chain (a string array attribute)

4.2 Target Architecture

Below is an overview diagram of the Okta architecture as it relates to the infrastructure in its final state:



Target State Architecture

- Digital Library, RDW instances, and Tools for Teachers (not pictured), will be configured to use Okta as their IdP

4.3 Environments

There are two Okta environments, one for "Production" and one for "Staging" (Integration testing with applications and member states).

4.4 Detailed Architecture Views

In this section, each requirement shall be associated with a specific implementation(s).

4.4.1 Login / Username

The **Email address** will be used as the consistent username across platforms. The email addresses are verified during the account activation/verification process.

Note: Okta recommends using email address as username going forward to reduce complexity.

4.4.2 Just-In Time User Creation

If the user does not have profile data in Okta and they authenticate from their federated IdP, and account will be automatically provisioned based on the data in the SAML payload. The user will seamlessly have an account created, activated and added to their respective IdP group.

See User Attribute Section.

The User profile must contain the 4 basic attributes:

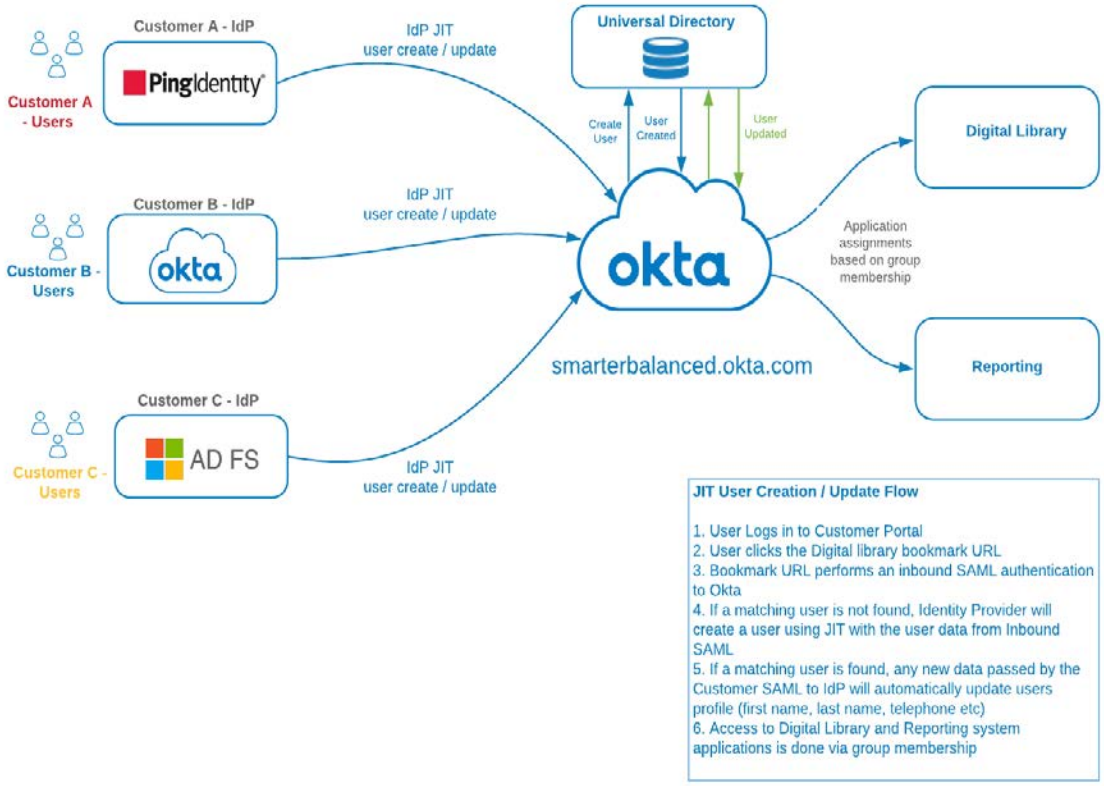
- Username (in email format)
- Email
- Firstname
- Lastname

Additional non-Okta required attributes

- sbacTenancyChain

Optional attributes

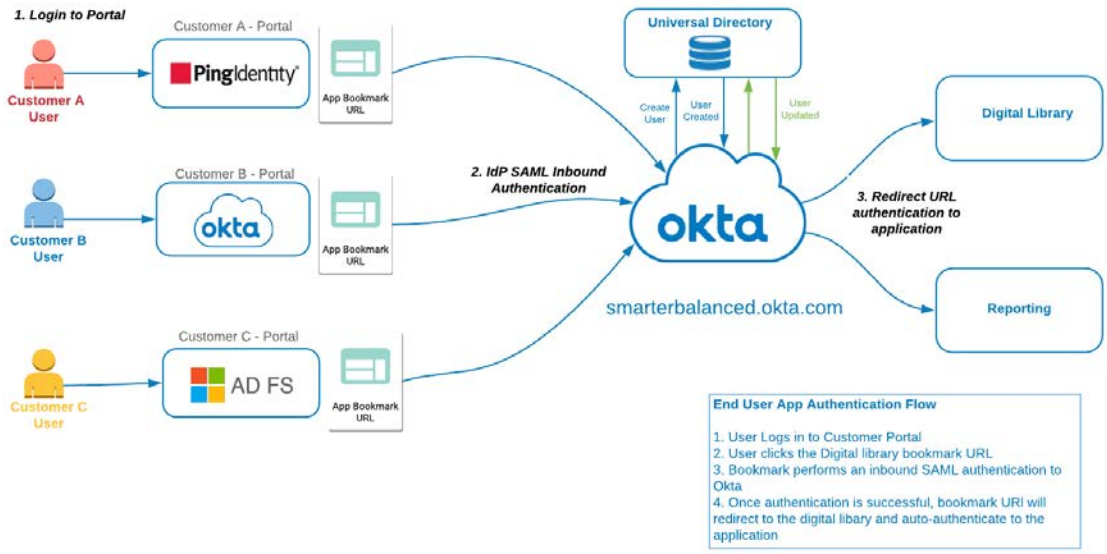
- telephone
- sbacUUID



JIT User Creation / Update

4.4.3 User Sign-In

The customer will utilize Inbound SAML to authenticate to the Okta Org. Local Users will utilize the Okta UI for standard authentications.



Authentication Flow

4.5 Identity Provider

Each Smarter Balanced Member will have its own IdP and that will be the authoritative source for user creation/updates. From the perspective of the member's IdP, Okta will be configured as a Service Provider. This is referred to as Inbound SAML, which allows users from external identity providers to SSO through Okta and on to their application. The matching criteria to link any existing user will be performed using email address.

If no match is found, the new user will be created 'on the fly' in Okta Universal Directory. All profile attributes will be mastered by the payload from the member Identity Provider.

Below is a sample data mapping that will need to be configured for each Identity Provider.

Okta	Sample Value	Customer Identity Provider	Sample Value
Username	John.Smith@gmail.com	Username	John.Smith@gmail.com
Email	John.Smith@gmail.com	Email	John.Smith@gmail.com
First Name	John	First Name	John
Last Name	Smith	Last Name	Smith
TelephoneNo		TelephoneNo	
Institution	California		

Okta UID	Auto generated		
sbacUUID	584efee2e4b0e6709dfc6aa8	-	-
sbacTenancyChain	|TS101|DL_EndUser|DISTRICT|1000|ART_DL|||TS|TEST STATE|||TS101|Test State 101|||||	-	-

4.5.1 Multi-Factor Authentication

Note: MFA will not be used at this time. MFA is supported and may be added.

4.5.2 Application Embed Link

Application bookmarks will be available to give Federated Users access to applications within the Okta org. This is accomplished through inbound SAML federation using the Identity Provider and redirecting the user (once authenticated) to the target application embed link. Each Okta application has a defined app embed link that can be used for direct access. The user must have a valid Okta session token and be assigned the application in order to properly use the link.

4.5.3 SAML SSO

SAML has been widely used as the single sign-on protocol by many ISVs and is supported by many identity management solutions. Okta provides comprehensive guidance for developers to implement a proper SAML service provider.
https://help.okta.com/en/prod/Content/Topics/Security/Identity_Providers.htm

4.5.3.1 SAML Sequence

Ref: http://developer.okta.com/standards/SAML/

5 Security

5.1 Multiple Factors

Note: This project will not include MFA for External users at this time.

5.2 Password Policy

All Passwords, either created in Okta, or used by the members' IdPs should comply with the University of California security policy.

5.2.1 Self-Serve Password Management (for Local Accounts)

Password management is configurable by group driven policies. This includes complexity, history, or self-serve functions. The self-serve methods and recovery token duration are configurable.

The steps below represent a typical forgotten password flow for Okta local users:

- Present form to acquire username
- Check user state
    - Should be ACTIVE
    - If DEACTIVATED OR SUSPENDED, return message to call for assistance
- Generate a local recovery token
- Store recovery token locally or in Okta profile for user
- Send recovery token and Okta user ID in link to user in custom branded email
- Receive link
- Verify recovery token
    - Valid duration has not expired
    - Token matches stored data
- Present form to get new password and confirm
- Use Okta API to set password

Note: For inbound federated users, no passwords are associated with these users. Any locally created Okta users would have the password policies applied to them (SBAC staff and non-federated states).

5.3 Session Policy

The session inactivity timeout is set to 2 hours.

6 User Attributes

The highlighted items below are the Okta required attributes. All other attributes are not required by Okta but represent common data and are available by default.

6.1 Attribute Mapping

Normalized data avoids duplication, simplifies integration and aids in maintenance and troubleshooting.
Data available or required at the source needs to be identified. Sources include;

- CSV import applications
- registration applications
- profile update applications

Data required for the applications needs to be identified. Any transformations from the Okta org level attributes for a specific application needs to be identified.

* Indicates field is required *(sbacUUID is required if an organization has a proprietary ID that they would like to use to track user account information)*

Attribute	Source	Description	Data Type	Destination 1	Destination 2
Login*					
Email*					
secondEmail					
firstName*					
lastName*					
middleName					
honorificPrefix					
honorificSuffix					
title					
displayName					
nickName					
profileUrl					
primaryPhone					
mobilePhone					
streetAddress					
city					
state					
zipCode					
countryCode					
postalAddress					
preferredLanguage					

locale					
timezone					
userType					
employeeNumber					
costCenter					
organization					
division					
department					
managerId					
manager					
sbacUUID*					
sbacTenancyChain*					
Custom3		TBD			
Custom4		TBD			

6.2 Role and Tenancy Chain Information

6.2.1 Role Information

The roles used by the **RDW** are provided in the table below:

Role	Description
ASMTDATALOAD	Allows user to load data into the RDW via the API
Custom Aggregate Reporter	Allows an administrator to generate aggregate reports of student assessment results within the institution to which the user is.
Embargo Admin	Allows an administrator to control the release of summative test results within the institution to which the user is assigned.
GROUP_ADMIN	Allows a school or district administrator to create/manage groups within the school or district to which they are assigned.
Instructional Resource Admin	Allows a state, district, or school administrator to create/manage links to instructional resources within the institution to which the user is assigned.
PII	Allows access to reports and personally identifiable information (PII) for the students in institutions (school, district, state) to which the user is assigned. This role is intended for administrators and others responsible for reporting at the institutional level.
PII_GROUP	Allows access to reports and personally identifiable information (PII) for the students in groups to which the user was assigned. This role is intended for teachers.
State Coordinator	Allows access to ART in order to create other State Coordinator accounts as well as District Coordinator, School Coordinator, and Test Administrator accounts. They can upload data across all districts and institutions within their states.

District Coordinator	Allows access to ART in order to create other District Coordinator accounts as well as School Coordinator and Test Administrator accounts. They can upload data across all institutions within their districts.
School Coordinator	Allows access to ART in order to create other School Coordinator and Test Administrator accounts. They are able to upload data for their institution only.
DL_EndUser	Allows access to the Digital Library (Tools for Teachers).

The role necessary for accessing the **Digital Library** (and in June 2020, **Tools for Teachers**)

Role	Description
DL_EndUser	Allows access to the Digital Library (Tools for Teachers).

The role value is what is passed through in the tenancy chain. Attached below is what multiple tenancy chain values look like in the SAML payload from ART:

6.2.2 Tenancy Chain Information

The Tenancy Chain is a multi-value string attribute that is used to provide authorization to, and control access to specific data within Smarter Balanced applications. The specifications for the sbacTenancyChain are available on GitHub in the OpenDJ repository:
https://github.com/SmarterApp/IM_OpenDJ/blob/master/SBAC_SSO_Design.pdf
Page 13 of the PDF lists the data elements that go into the pipe delimited string. A user may have many entries in this attribute, but the entire SAML assertion cannot exceed 1MB in size.

Below are some examples of tenancy chain elements.
Note: Attributes are case-sensitive.
The following are not real values, these are examples of how a tenancy chain may look.

For *Digital Library* or *Tools for Teachers*, an example would be:
`|NV|DL_EndUser|STATE|1000|ART_DL|||NV|NEVADA|||||||||`

For *Reporting Data Warehouse* and access to PII for an entire state, see the below example:
`|NV|PII|STATE|1000|ART_DL|||NV|NEVADA|||||||||`

Reporting access at the district level:
`|02|PII|DISTRICT|1000|ART_DL|||NV|NEVADA|||02|Clark|||||`

Reporting at a school level:
`|19687336819087|PII|INSTITUTION|1000|ART_DL|||NV|NEVADA|||19647830000000|Whoville Unified School District|||19647386019087|Whoville Elementary|`


sbacTenancyChainExample.xml

The chain position explanations are:

Chain position	Position name	Sample Value	Notes
1	RoleID (May also be referenced as Org ID)	31750853130150	This value is identical to the ID code for which the role is assigned.
2	Name	PII	Smarter Balanced role (ex: PII, PII_GROUP, GROUP_ADMIN, Custom Aggregate Reporter)
3	Level	INSTITUTION	Level in which the role is assigned. Allowed values are 'INSTITUTION', 'DISTRICT', 'STATE'
4	ClientID	1000	Code of the system generating the tenancy chain. For Smarter Balanced systems, the value of 1000 corresponds to ART
5	Client	ART_DL	Name of the system generating the tenancy chain. For Smarter Balanced systems, the value of 'ART_DL' corresponds to ART
6	GroupOfStatesID	1	ID of the group of states. I have not seen this position used.
7	GroupOfStates	Western US	Name of the group of states. I have not seen this position used.
8	StateID	NV	ID of the state. Should be the two-character state code. If the permission level is at the state, this value should appear in the RoleID position.
9	State	NEVADA	Name of the state. Should be in upper case
10	GroupOfDistrictsID		ID of the group of districts. I have not seen this position used.
11	GroupOfDistricts		Name of the group of districts. I have not seen this position used.
12	DistrictID	31750850000000	ID of the district. If the permission level is at the district, this value should appear in the RoleID position. If the permission level is State, this value should be blank.
13	District	Whoville Unified School District	Name of the district. If the permission level is State, this value should be blank.

14	GroupOfInstitutionsID	54879	ID of the group of institutions. I have not seen this position used.
15	GroupOfInstitution	East Whoville Schools	Name of the group of institutions. I have not seen this position used.
16	InstitutionID	31750853130150	ID of the school. If the permission level is at the institution, this value should appear in the RoleID position. If the permission level is State or District, this value should be blank.
17	Institution	Whoville High	Name of the school. If the permission level is at the institution, this value should appear in the RoleID position. If the permission level is State or District, this value should be blank.