TERMINOLOGY

A

AD (Active Directory) – is a cluster of services and resources that run on a Windows Server, being a Microsoft Product; it helps administrators manage access of identity and permissions distributed to users, generally speaking, but has lots of other features that evolve around access control;

Assertion Consumer Service URL (ACS) – public endpoint disclosed by the SP side where SAML responses got displayed, it can be the SP login URL;

Admin (Administrator) – Privileged user who tends to have more permissions than a normal user account; there can be different types of admins, differentiated in terms of permissions;

Admin’s Dashboard – here, refers to the center of control, the UI that allows an admin to structure the organization, hence the Okta Universal Directory, as he pleases;

Agent – Software that allows Okta to communicate with a resource beyond the firewall. Usually realizes Cloud to On-Prem / On-Prem to Cloud connections;

AIW (Application Integration Wizard) – Tool in the Admin Dashboard that allows the creation of Custom Apps (SAML, SWA, etc.);

API (Application Program Interface) – set of HTTP verbs (mainly CRUD types are used, but there are much more) that allow the secure creation of users / manipulation of data / etc. by means of an API token;

App (Application) – usually a website that has several functions (permitted actions) implemented in it’s front-end (GUI) and in its connected backend;

Assertion – Data identified within a SAML information exchange flow that can contain a clear statement that there is a user that successfully authenticated, a timestamp of several actions, attribute values of a user beside his mandatory username provided and perhaps even a decision pertaining to a user allowed or not to access a specific resource;

Attribute – data representing a characteristic of a user / person it might represent;

Audience Restriction – data showing who the assertion is intended for;

Authentication – process of verifying an identity; *"You are who you say you are"*

Authorization – process of allowing the user authenticated to do some action(s); *"You are allowed to do what you need to do"*

! Authentication is different than Authorization **!**

B

Backend – part of a system not directly accessed by a user;

C

CDN (Content Delivery Network) – set of server endpoints that store information about an app. Can be multiple servers, hence multiple IPs usually - and is a common and best-practice to be like that. Those servers deliver content over the internet;

CRUD (Create, Read, Update, Delete / Deactivate) – CRUD types of API / HTTP verbs that can help you create an entity, read some data from an entity, modify it or even delete / deactivate the entity (can be a user, for example);

D

Deprovisioning – act of deactivating a user that can even mean removing roles from it, licenses, etc.;

Domain – Group of servers that can be accessed under specific terms / data provided; may refer to a website / URL / URI;

E

End user – Person using a product; normally, an account which is not an admin;

Endpoint – A node in a LAN / WLAN that sustains communications back and forth across that network;

Entity ID – Unique value that identifies a service;

External ID – Unique ID usually coming from an external resource (SP) into the (IDP) and tacks provisioning to a specific user with it;

F

Federated – entity upon which a specific autonomy of actions and monopole of actions is implied;

Frontend – directly access functions from a user's perspective (structures that make the GUI);

G

Group – way of organizing users / apps for ease of distributing elements within a targeted context;

H

HTTP (HyperText Transfer Protocol) – underlying protocol used by the internet for data formatting and transmission

HTTP verb – API methods – as examples are the aforementioned CRUD ones;

I

IDP (Identity Provider) – system that copes with identity management and distribution; Okta is an IDP, mainly;

IDP-initiated SSO – Single Sign On process initiated from the IDP side;

IDP-initiated SLO – Single Log Out process initiated from the IDP side;

IP (Internet Protocol Address) – numerical way of identifying a device connected to a network;

Immutable ID – value that cannot be changed as long as the object it refers to exists;

IWA (Integrated Windows Authentication) – way of accessing Okta without inputting Okta credentials, but by a level of trust between Okta and the device you're logging into, with the use of a Kerberos token;

J

JIT Provisioning (Just is Time Provisioning) – creation of a user at the exact moment a required action is completed;

K

KB (Knowledge Base) – or KB article, usually, document / website that either describes something or teaches you something;

Kerberos – Computer-Nertwork authentication protocol;

L

LAN (Local Area Network) – interconnected computers within a limited area;

LDAP (Lightweight Directory Access Protocol) – open standard for accessing and maintaining data from a server; tends to be more familiar within Linux servers, but the underlying part of AD itself works of LDAP queries either;

License – accreditation given to a user for accessing specific parts of an app;

Lifecycle Management – evolution of users; their creation process, provisioning process, attribute-creation / deletion / modification process, deactivation process, etc.;

M

Metadata – data sends towards the IDP or the SP in an .xml format;

MFA (Multi Factor Authentication) – refers to a second layer of authentication (2FA), so usually an addition of information supplied beside the credentials (username, password); but the difference between 2FA and MFA tends to be in the form of having a set of different factors from which you can choose one or even more that may coexist when speaking of MFA, and only one (usually; there can be more but they won't coexist activated for the same user) when referring to 2FA;

O

OAuth – open standard authorization protocol that define how totally unrelated servers can trust each other in exchanging information;

OIDC (OpenID Connect) – authentication layer that comes on top of OAuth; hence the difference explained above between authentication and authorization;

OIN (Okta Integration Network) – database of pre-integrated apps within Okta Dashboard that you can quickly configure for your own particular use;

ORG (Organization) – here, the Okta account for your Organization; tenant;

P

Python 2 / Python 3 – Python programming language and its most known versions;

Provisioning – act of data distribution from an IDP towards an SP;

R

Relay State – usually, a structure within a URL which identifies a different endpoint that the initial one the action was started for;

Role – describes the part a user is responsible with, within an org.;

S

SaaS (Service as a Software) – a provider hosting an app and making it available over the internet;

SAML (Security Assertion Markup Language) – xml based standard for authentication of authorization between two applications (IDP – SP);

SLO (Single Log Out) – Act of getting an endpoint or multiple endpoints to lose the session once the session of a specific SP or IDP entity has been terminated;

SP (Service Provider) – the target application a user wants to access;

SP-initiated SLO – Single Log Out initiated from within the SP (target application);

SP-initiated SSO – Single Sign On initiated from within the SP (target application);

SSL (Secure Sockets Layer) – protocol designed for sending information over the internet in a secure way;

SSO (Single Sign On) – Act of getting an endpoint or multiple endpoints to instantly create a session for a user that currently has a valid session for their IDP service, once the endpoint for the app has been hit with a GET type of API request (READ HTTP verb);

SSO URL (Single Sing On URL / SAML Endpoint / Identity Provider Single Sign On URL) – endpoint provided by Okta when setting up SAML, information that SP needs for a proper SAML trust configuration to be realized;

Super Admin – Admin that has absolute control over the GUI, has access to all of the features, unlike an App Admin or Group Admin, Read-Only Admin, etc.;

SWA (Secure Web Authentication) – SSO system developed by Okta which uses a plugin to securely inject credentials into a website;

T

Tenant – can refer to an 'ORG', the Okta URI you have for your OKTA account / the Okta account itself with all it provides in terms of GUI / backend;

TLS (Transport layer Security) – cryptographic protocol designed to send data over the internet; SSL being its deprecated predecessor;

Token – here, API token – used to authenticate requests to the Okta Cloud, the same as an HTTP cookie is used to authenticate requests to the Okta Application;

U

UI / GUI (User Interface / Graphical User Interface) –

URI – string of characters identifying a domain; usually refers to the subdomain / domain part of a URL and not its possible string extensions / parameters;

URL – the full web address in the form of a string of characters;

Universal Directory – Okta's database of user attributes pertaining to either Okta or different applications, provisioning attributes towards the Okta - which retains them and creates a database of attributes from different mediums within a user's profile;

W

WLAN (Wireless Local Area Network) – network of computers that communicate with each other via wi-fi signals;

Z

Zone – here, Network Zone – range(s) of IPs defined in a specific cluster named zone;