RSAConference2022
San Francisco & Digital | February 7 – 10

TRANSFORM

SESSION ID: **IDY-R05**

Demystifying the Identity Capabilities of AWS for Enterprise Practitioners

Jon Lehtinen

Jon Lehtinen
Director, Okta on Okta, Okta
@jonlehtinen

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

The views and opinions expressed in this presentation are my own and not necessarily shared nor endorsed by any current or former employers, organizations or affiliates.

RSAConference2022

AWS & Identity

The Enterprise Practitioner's Conundrum

What This is Not

Why Can identity on AWS Seem So Hard?

- Services with similar functionality
- Occasionally distinct application of identity across services
- AWS as IaaS (Infrastructure as a Service) vs. AWS as PaaS (Platform as a Service)

AWS as IaaS

You own/run/manage:

- Data
- Applications
- Runtime environment
- Middleware
- OS

AWS owns/runs/manages:

- Virtualization
- Hardware
- Storage
- Networking

AWS as PaaS

You own/run/manage:

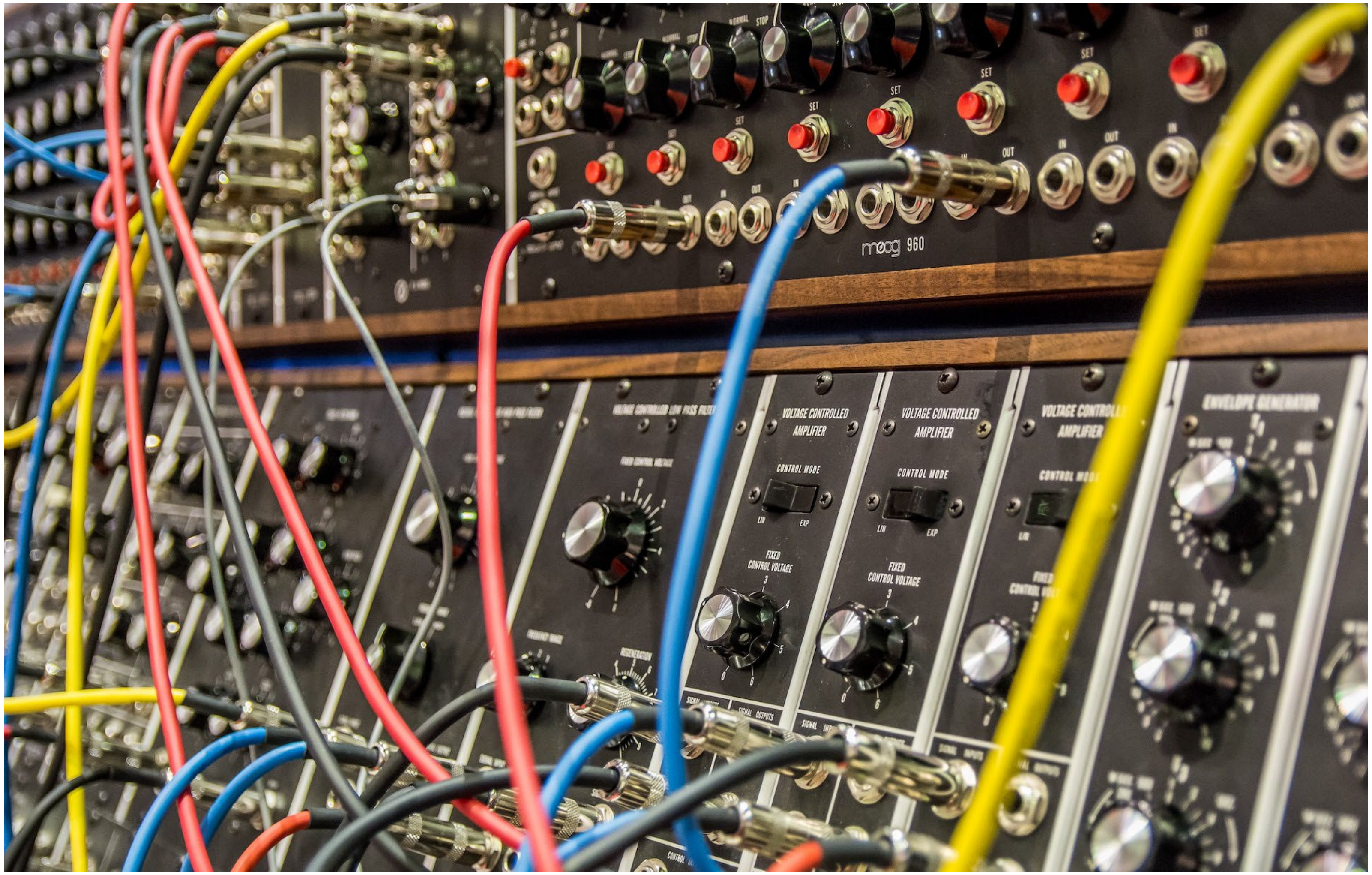
- Applications
- Data

AWS owns/runs/manages:

- Runtime
- Middleware
- OS
- Virtualization
- Hardware
- Storage
- Networking

AWS IAM Taxonomy

AWS IAM


moog 960
VOLTAGE CONTROLLED AMPLIFIER
CONTROL MODE
LIN
EXP
FIXED CONTROL VOLTAGE
VOLTAGE CONTROLLED AMPLIFIER
CONTROL MODE
LIN
EXP
FIXED CONTROL VOLTAGE
ENVELOPE GENERATOR
SET
IN
OUT

AWS IAM – Taxonomy

RESOURCES

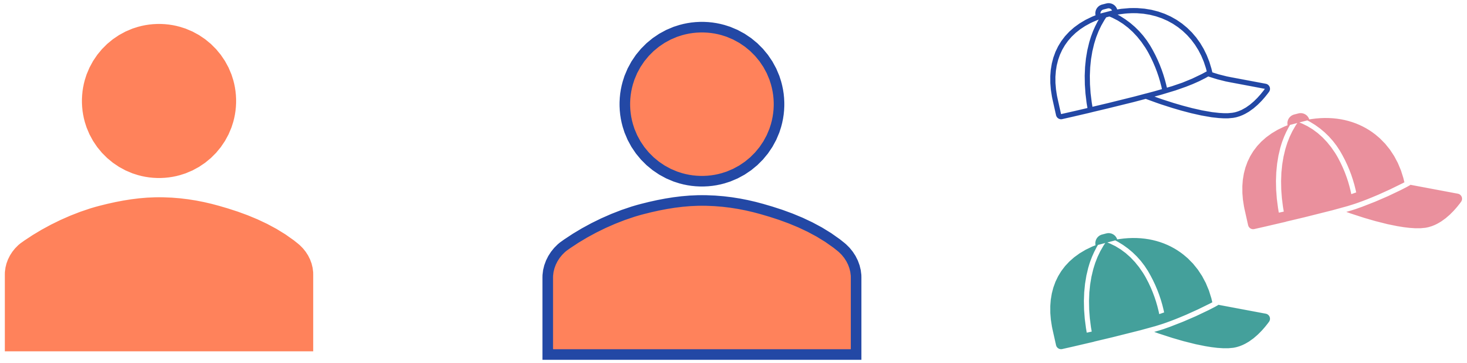
The “things” within AWS IAM, like users, roles, policies, and groups. Resources are also how other AWS objects are referred to, like S3 buckets, EC2 instances, etc.

AWS IAM – Taxonomy

IDENTITIES

“AWS IAM resource objects that are used to identify and group.” Think user objects, groups, and roles

AWS IAM – Taxonomy



ENTITIES

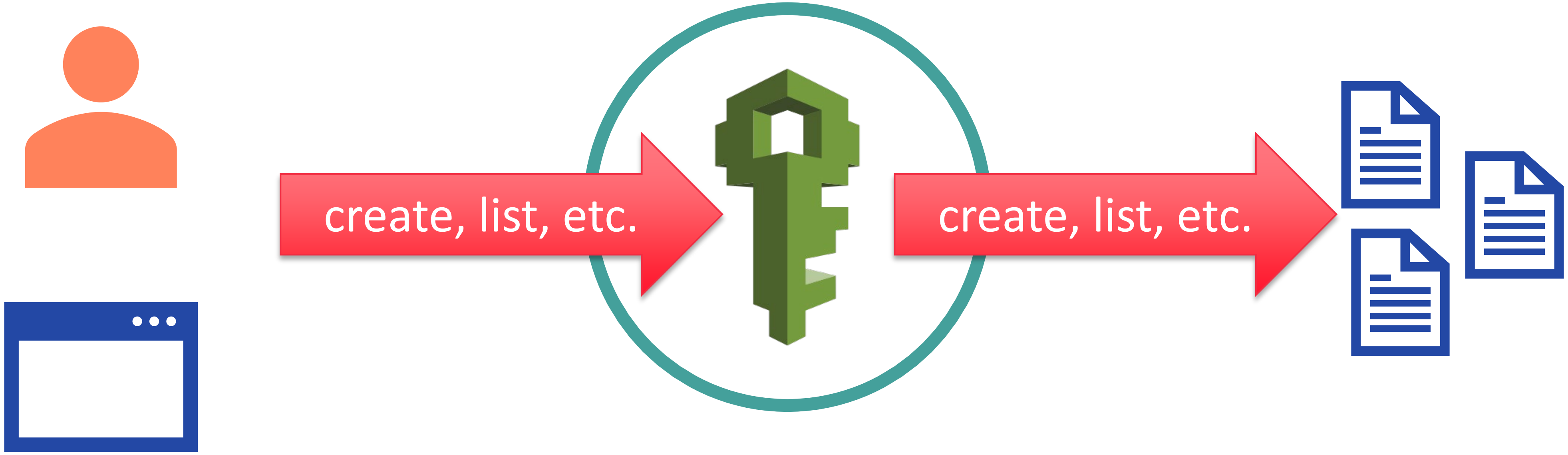
The AWS IAM resource object that AWS IAM authenticates as part of an identity transaction, e.g. AWS IAM user objects, federated users/their assumed AWS IAM roles.

AWS IAM – Taxonomy

PRINCIPALS

“The person or applications that uses […] an IAM user, or an IAM role to sign in and make requests to AWS.”

AWS IAM – Taxonomy



ACTIONS

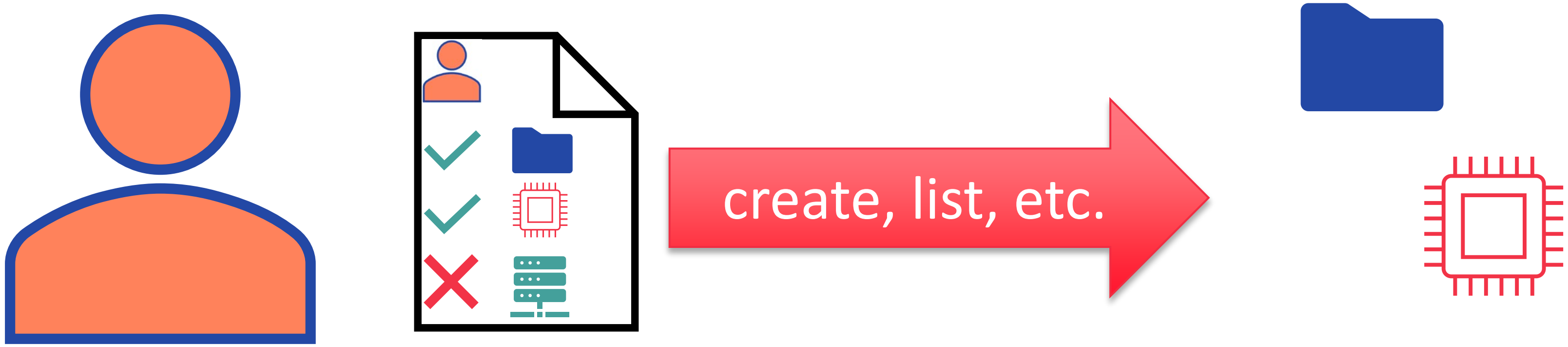
What the principal gets to do to a resource after having been authenticated and authorized by AWS IAM

AWS IAM – Service Capabilities

- User & Group object management
- Authentication of entities
- Credential management, including:
  - Password management and policy
  - Multifactor authentication and token management
  - Programmatic credentials
- Identity federation (inbound)
- Authorization and authorization policy management

AWS IAM Authorization

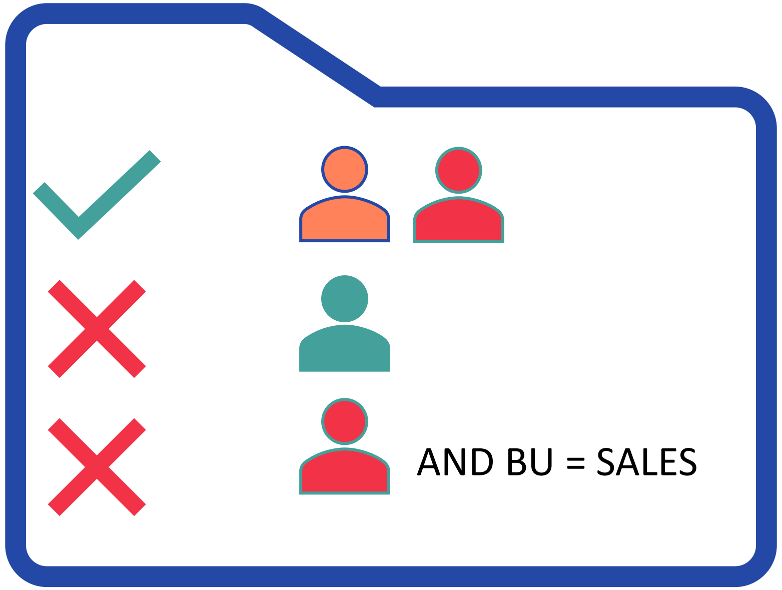
AWS IAM – Authorization Policy Types



IDENTITY POLICIES

Policies which can be attached to identity objects to determine what the principal can do to a resource, may be AWS-managed or customer-managed.

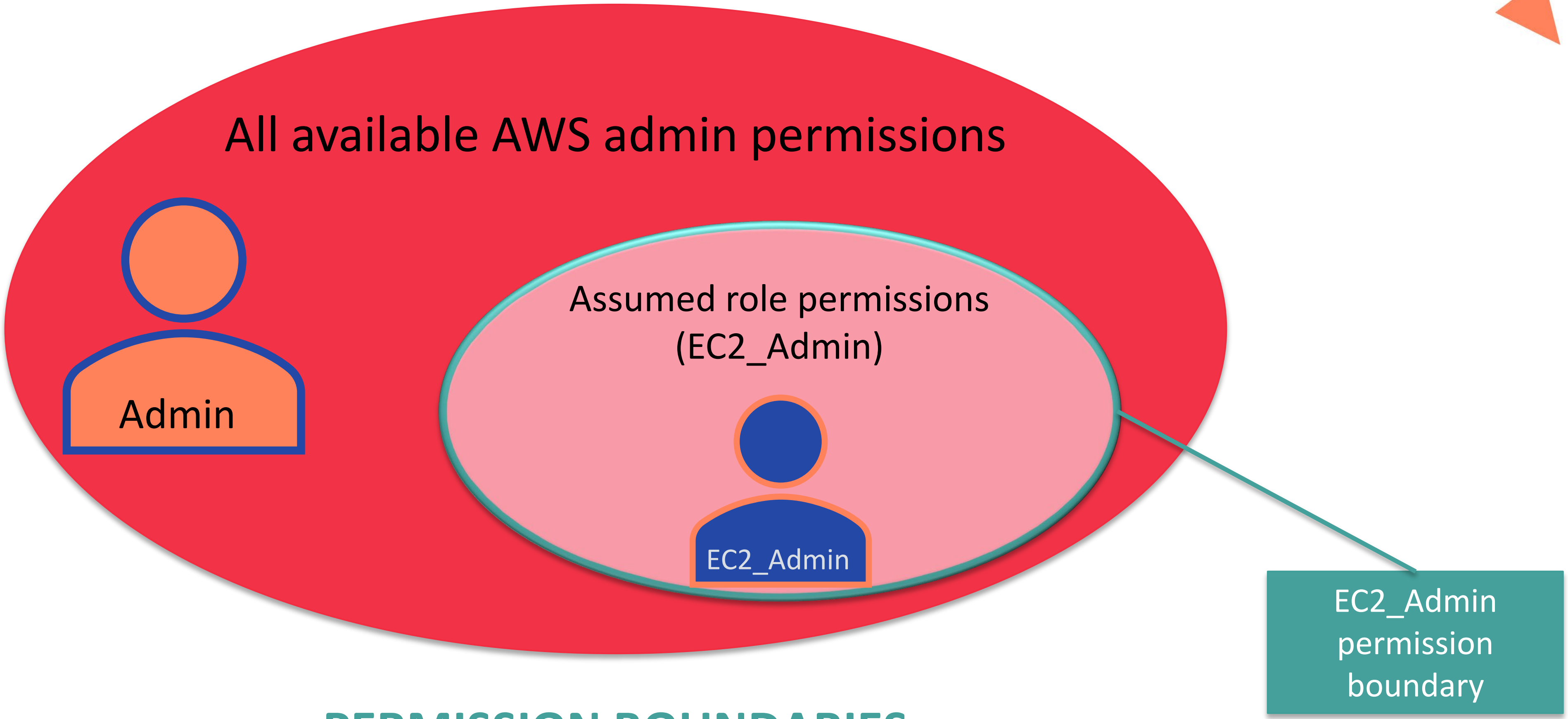
AWS IAM – Authorization Policy Types



INLINE POLICIES

Policies applied directly to a resource where they are written, becoming intrinsic characteristics of the resource.

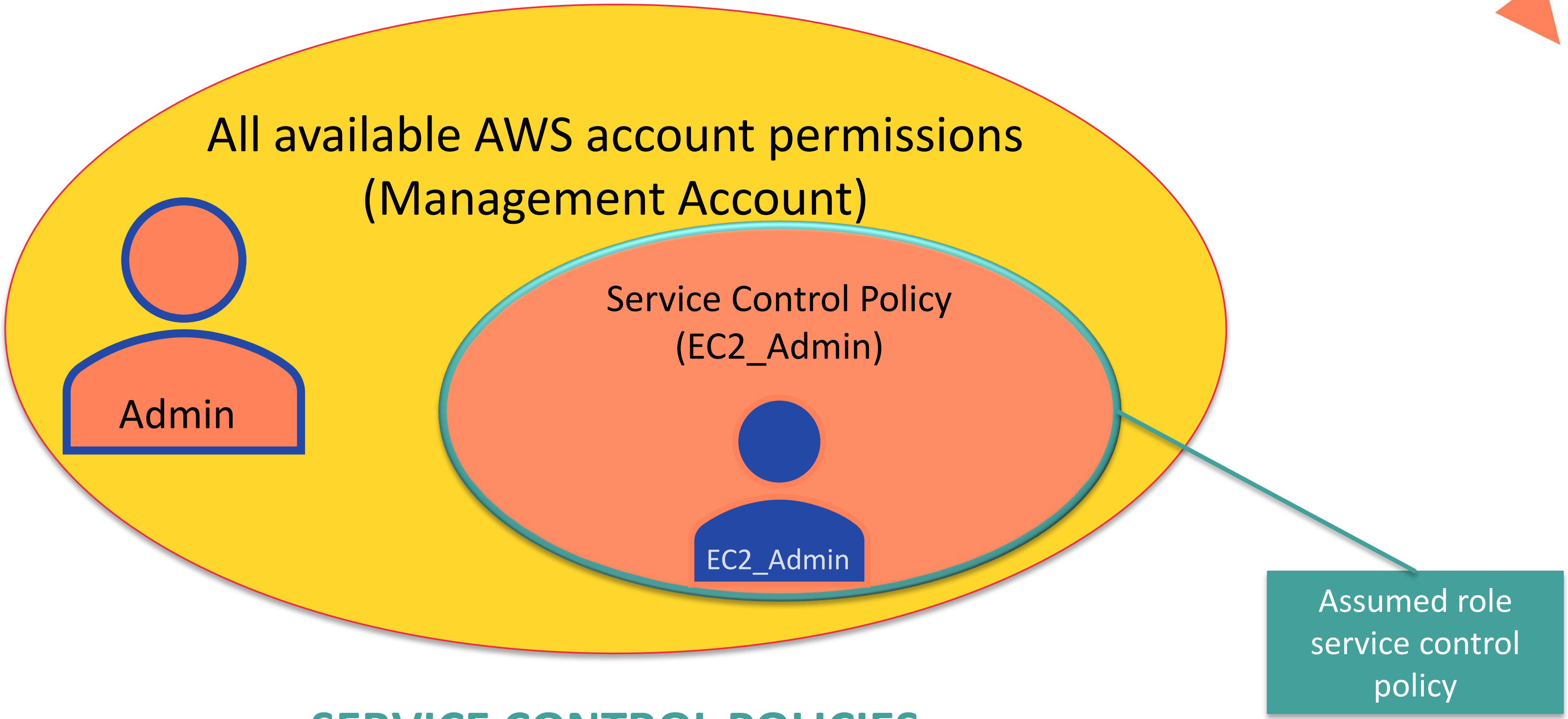
AWS IAM – Authorization Policy Types


All available AWS admin permissions
Admin
Assumed role permissions (EC2_Admin)
EC2_Admin
EC2_Admin permission boundary

PERMISSION BOUNDARIES

The *maximum* entitlements which may be applied to an identity object, regardless what other policies say.

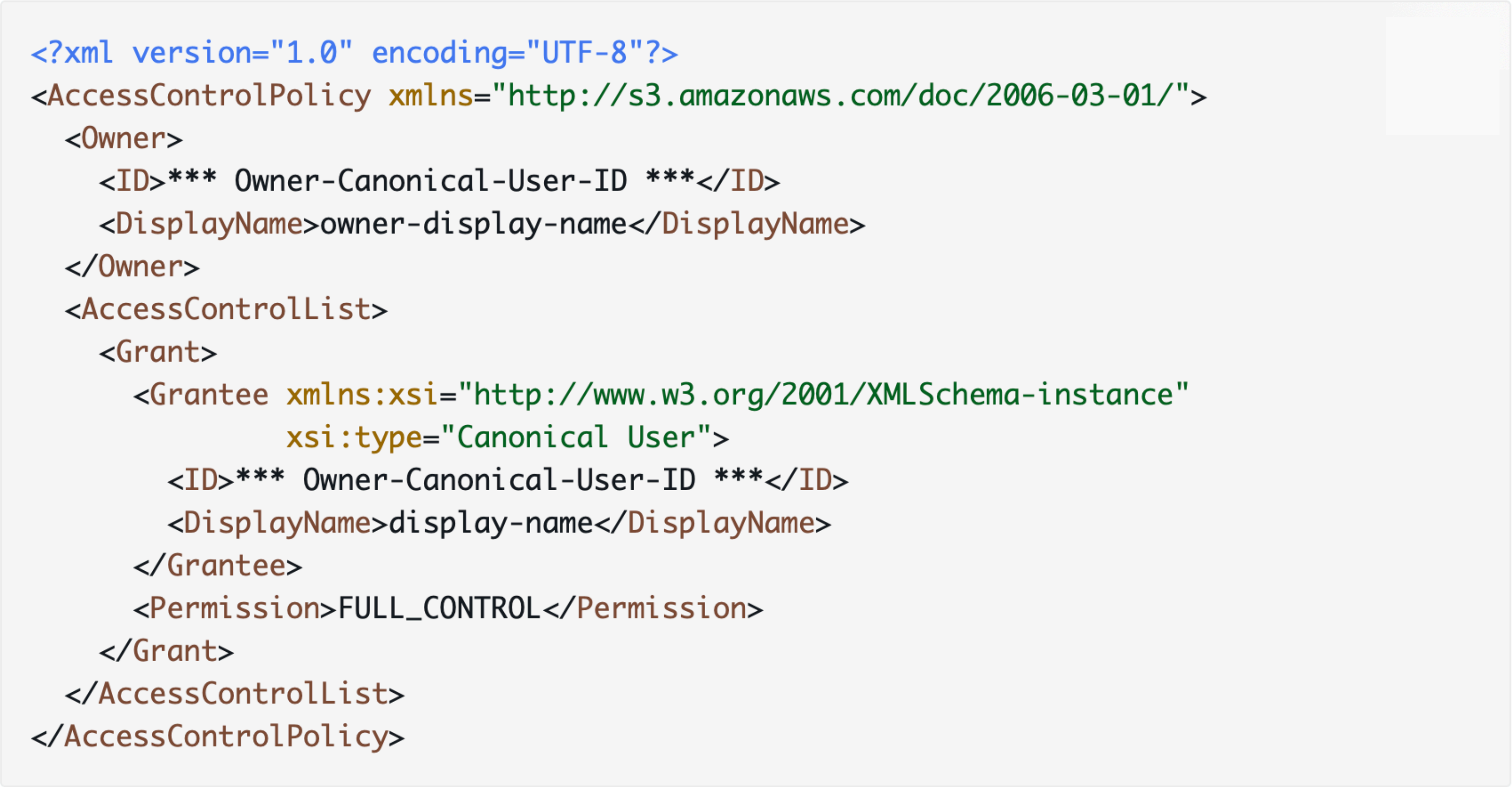
AWS IAM – Authorization Policy Types


All available AWS account permissions (Management Account)
Admin
Service Control Policy (EC2_Admin)
EC2_Admin
Assumed role service control policy

SERVICE CONTROL POLICIES

Similar to permission boundaries but applied to member accounts within an AWS Organization.

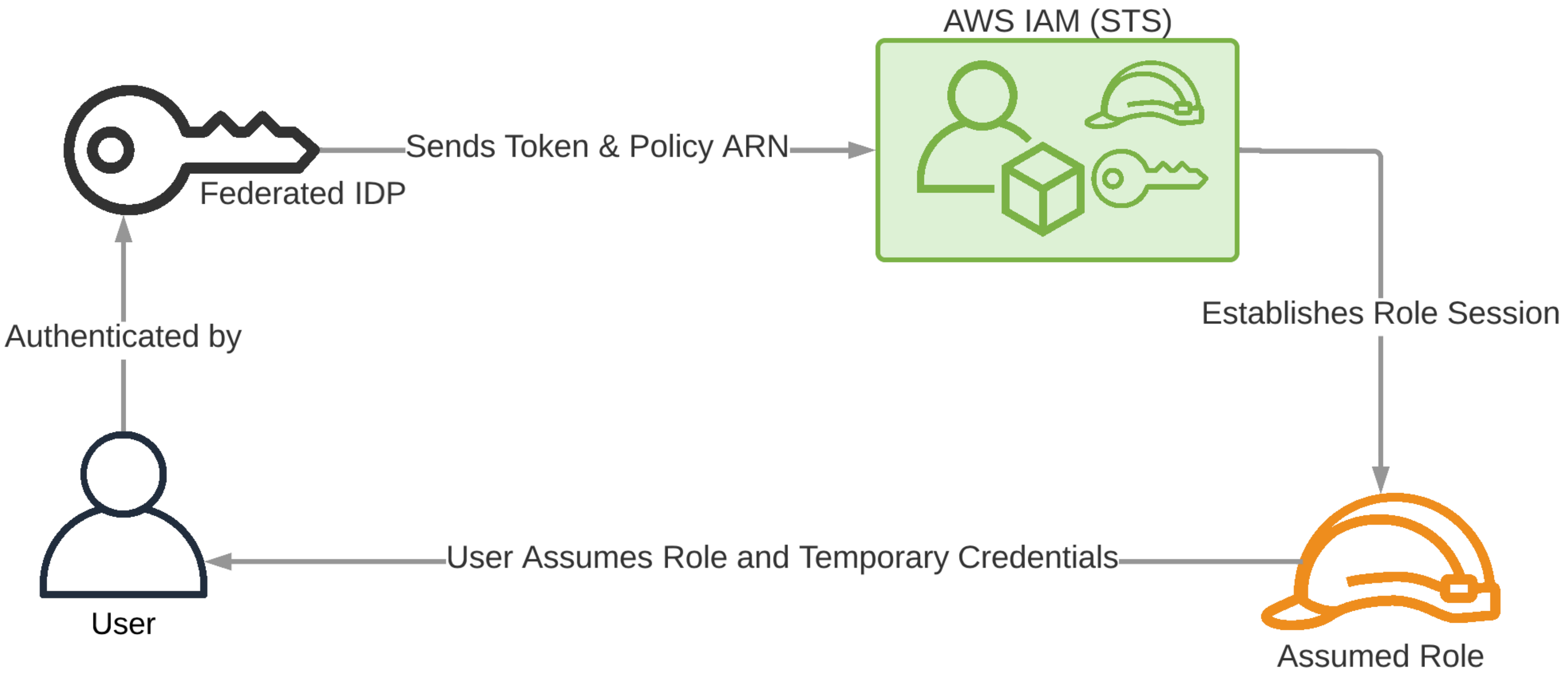
AWS IAM – Authorization Policy Types



```
<?xml version="1.0" encoding="UTF-8"?>
<AccessControlPolicy xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Owner>
    <ID>*** Owner-Canonical-User-ID ***</ID>
    <DisplayName>owner-display-name</DisplayName>
  </Owner>
  <AccessControlList>
    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
               xsi:type="Canonical User">
        <ID>*** Owner-Canonical-User-ID ***</ID>
        <DisplayName>display-name</DisplayName>
      </Grantee>
      <Permission>FULL_CONTROL</Permission>
    </Grant>
  </AccessControlList>
</AccessControlPolicy>
```

Determines the conditions of allowing people outside of your AWS account access to your resources from their own AWS accounts, or from the broader internet.

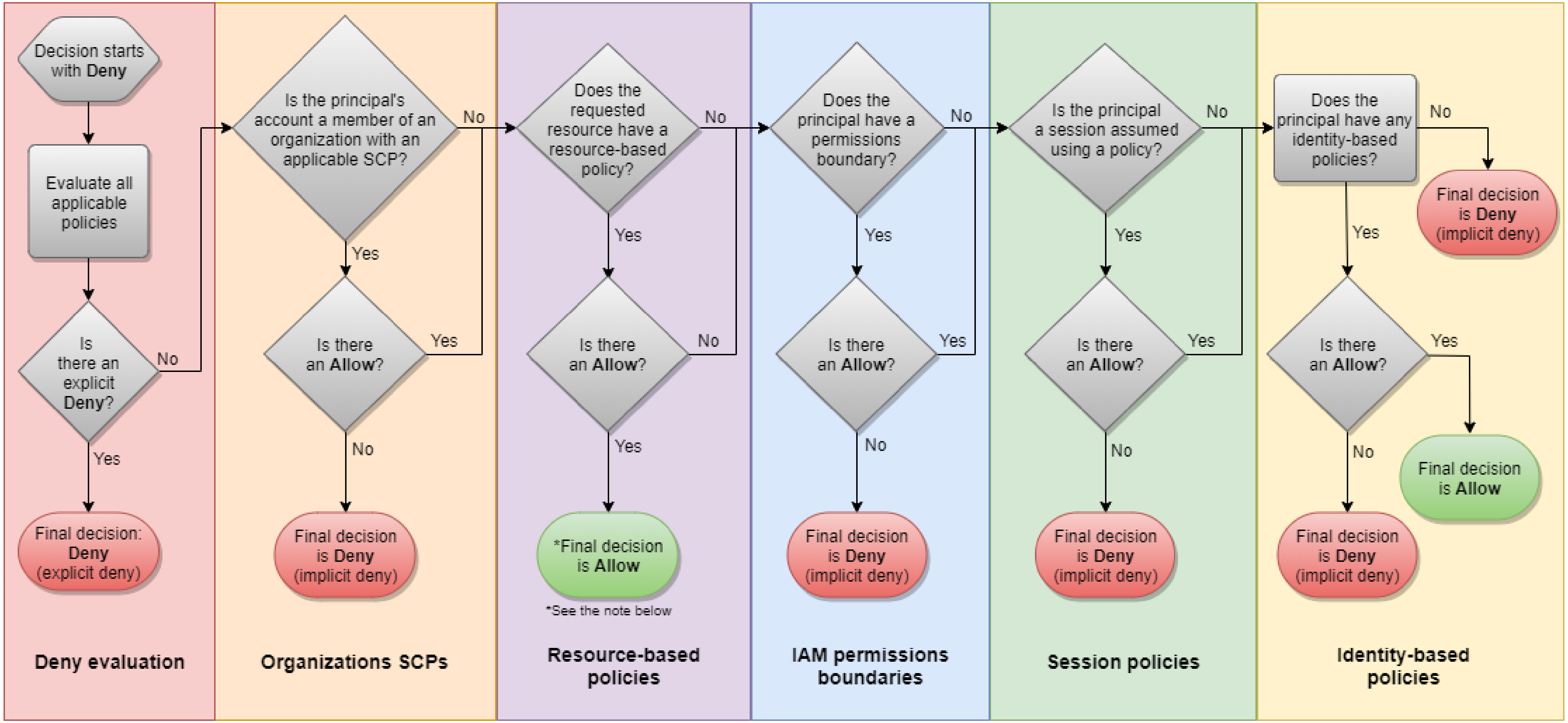
AWS IAM – Authorization Policy Types



SESSION POLICIES

Policies created and applied on the fly during assumption of roles by an entity.

AWS Authorization Policy Evaluation Flow


Decision starts with Deny
Evaluate all applicable policies
Is there an explicit Deny?
No
Yes
Final decision: Deny (explicit deny)
Is the principal's account a member of an organization with an applicable SCP?
No
Yes
Is there an Allow?
Yes
No
Final decision is Deny (implicit deny)
Does the requested resource have a resource-based policy?
No
Yes
Is there an Allow?
No
Yes
*Final decision is Allow
*See the note below
Does the principal have a permissions boundary?
No
Yes
Is there an Allow?
Yes
No
Final decision is Deny (implicit deny)
Is the principal a session assumed using a policy?
No
Yes
Is there an Allow?
Yes
No
Final decision is Deny (implicit deny)
Does the principal have any identity-based policies?
No
Final decision is Deny (implicit deny)
Yes
Is there an Allow?
Yes
Final decision is Allow
No
Final decision is Deny (implicit deny)
Deny evaluation
Organizations SCPs
Resource-based policies
IAM permissions boundaries
Session policies
Identity-based policies

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html

RSA Conference2022

Identity Services So Nice They're Doing 'Em Thrice

(Sort of.)

AWS IAM

Amazon Cognito

AWS Single Sign-on

Provides user management and controls access to AWS resources

AWS IAM

Provides user management and controls access to AWS resources

Amazon Cognito

Provides user management and ***can*** control access to AWS resources

AWS Single Sign-on

AWS IAM

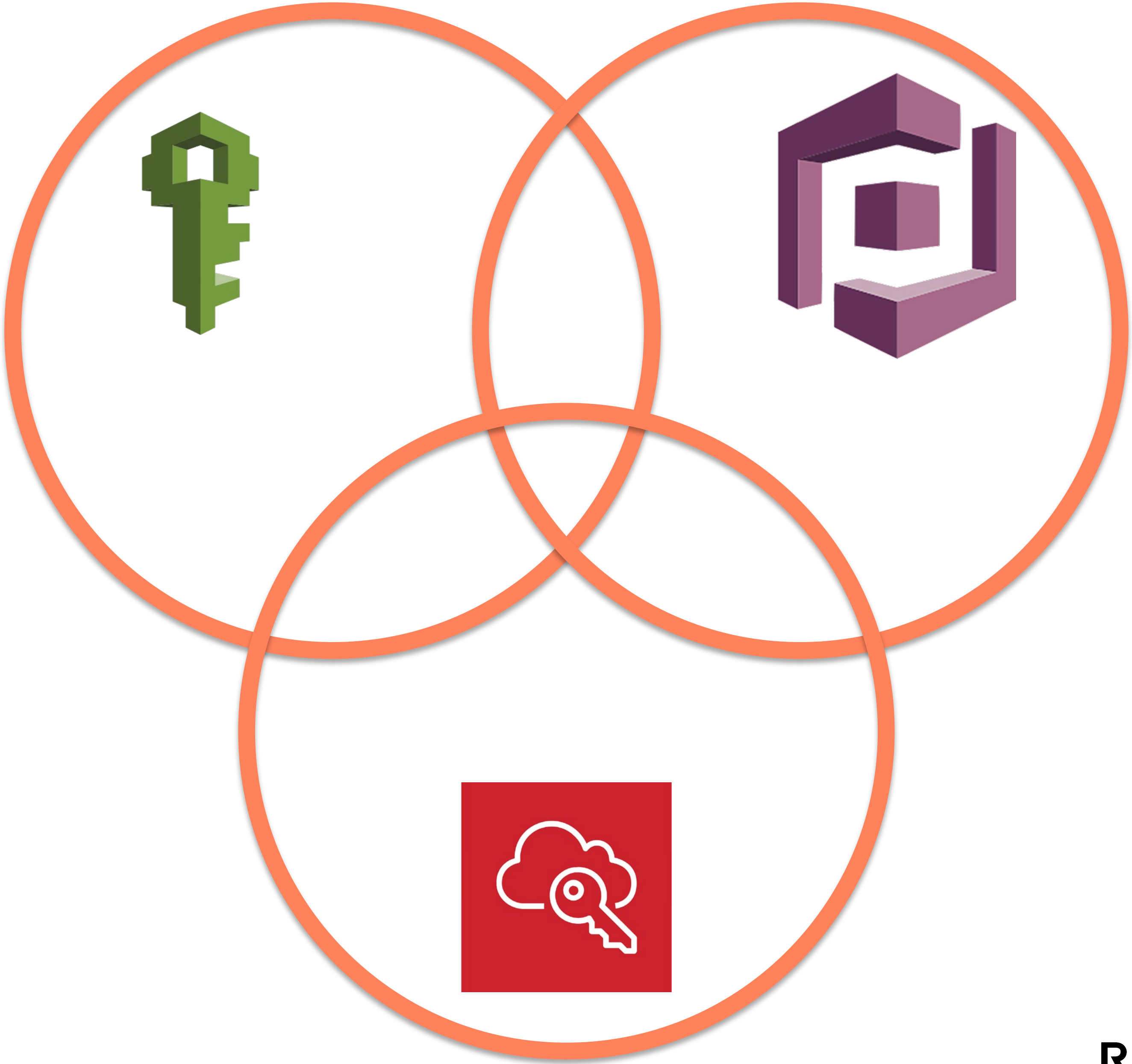
Provides user management and controls access to AWS resources

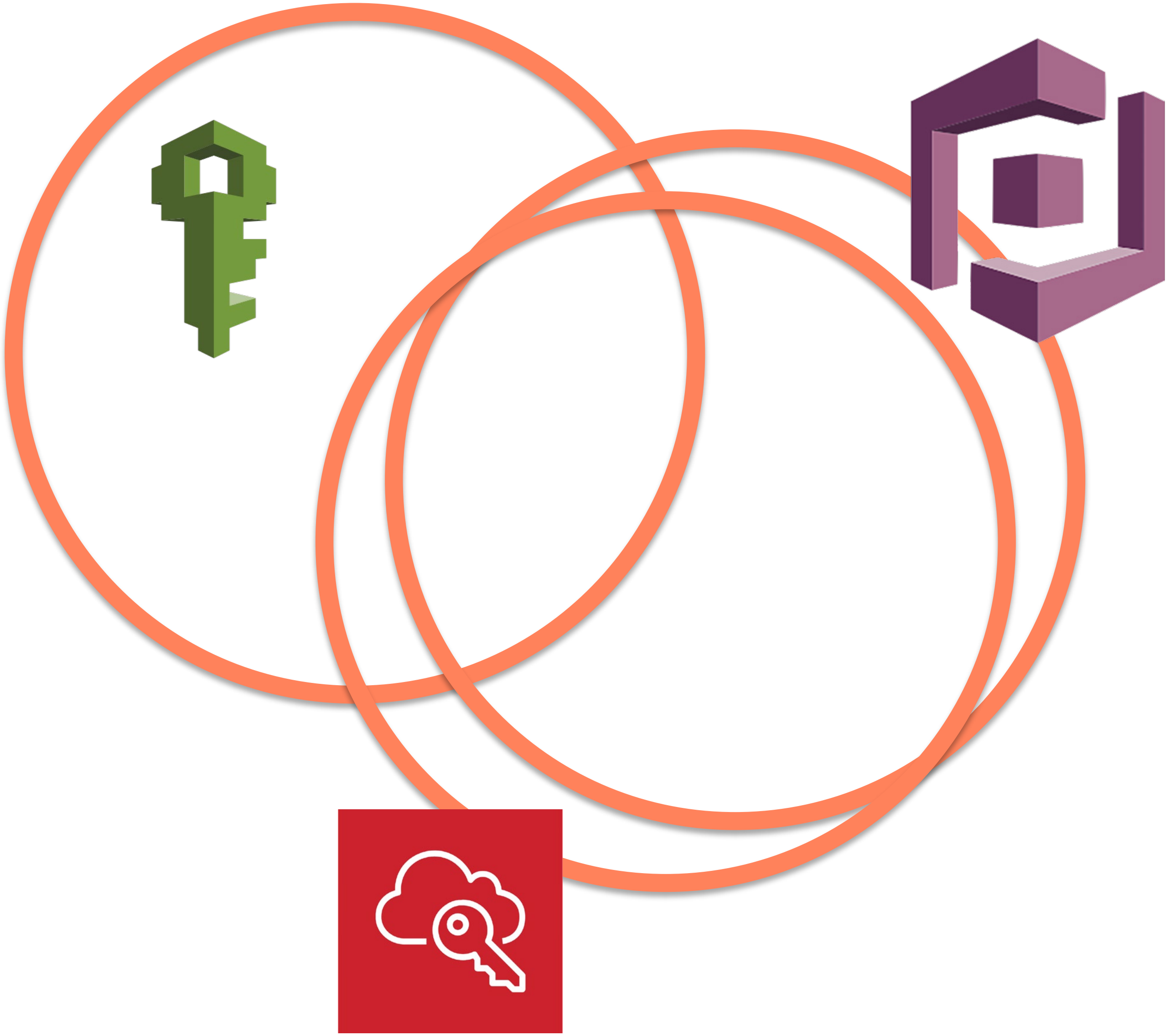
Amazon Cognito

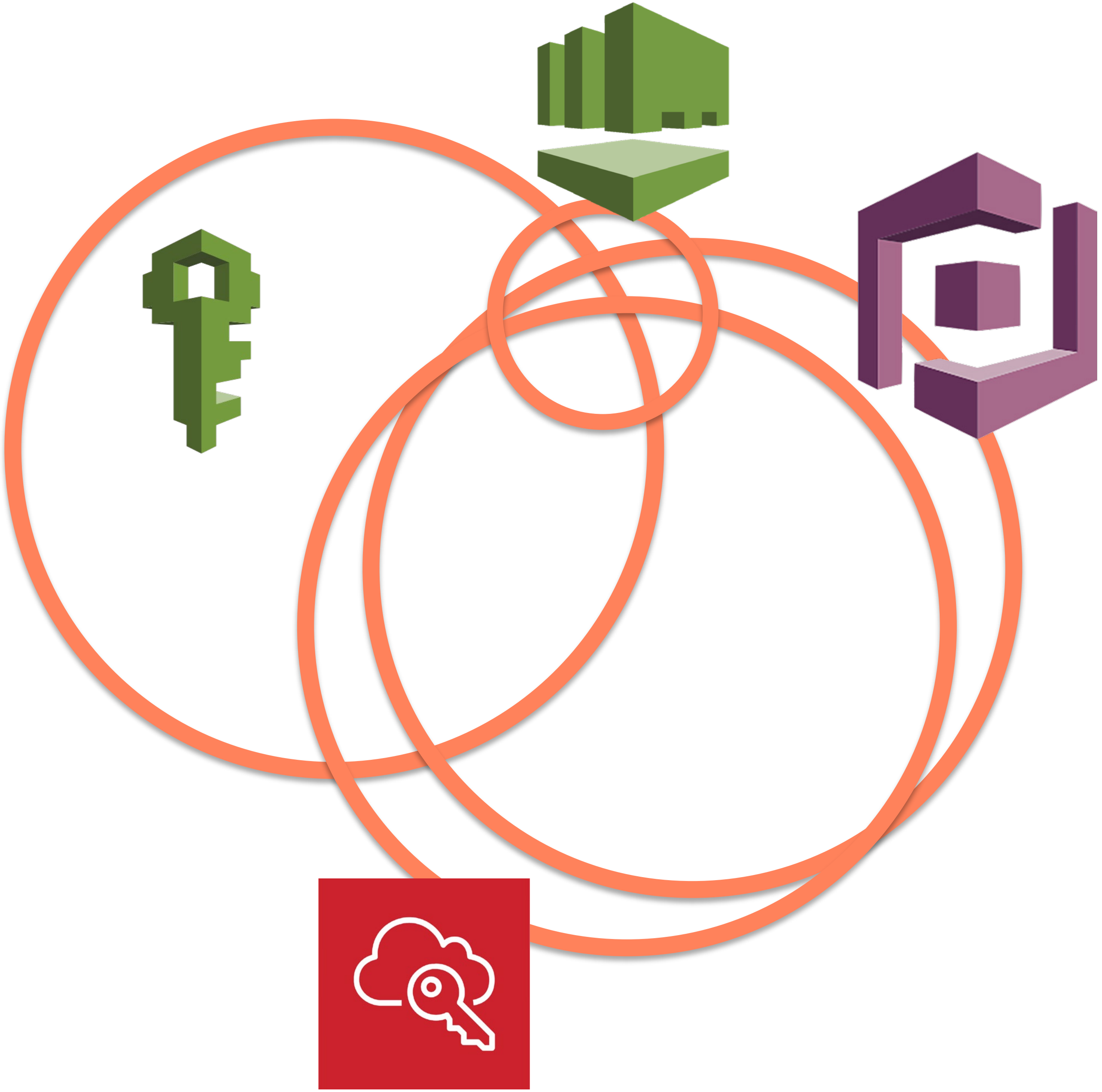
Provides user management and ***can*** control access to AWS resources

AWS Single Sign-on

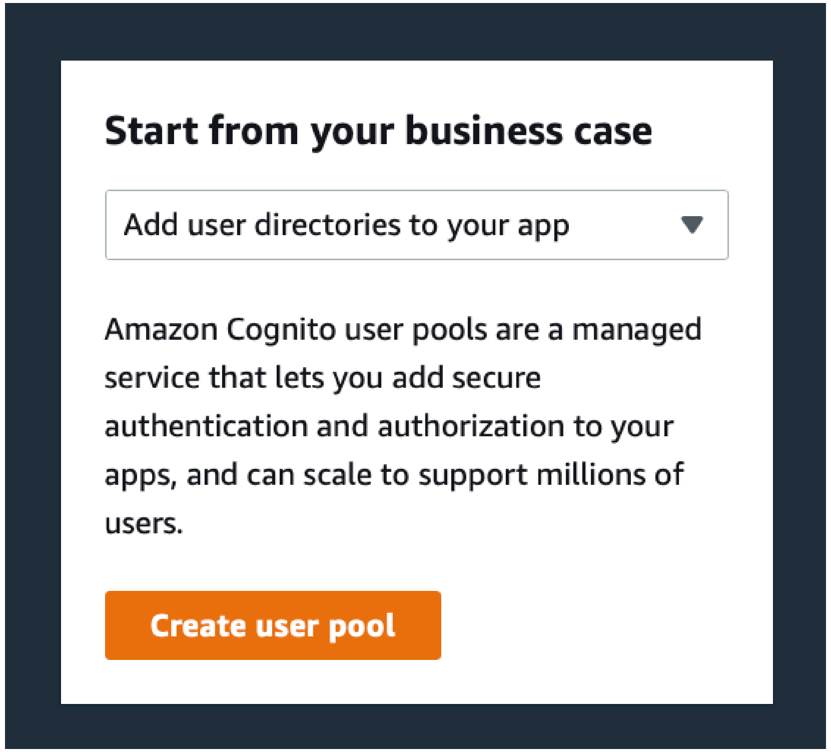
Provides user management and controls access to AWS accounts







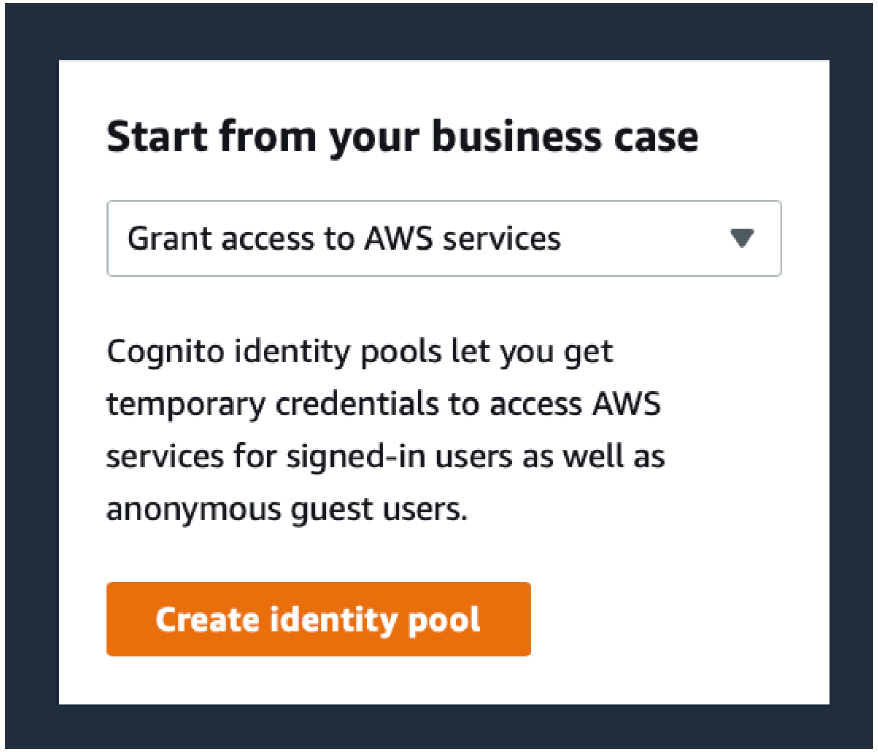
Amazon Cognito



Start from your business case

Add user directories to your app

Amazon Cognito user pools are a managed service that lets you add secure authentication and authorization to your apps, and can scale to support millions of users.

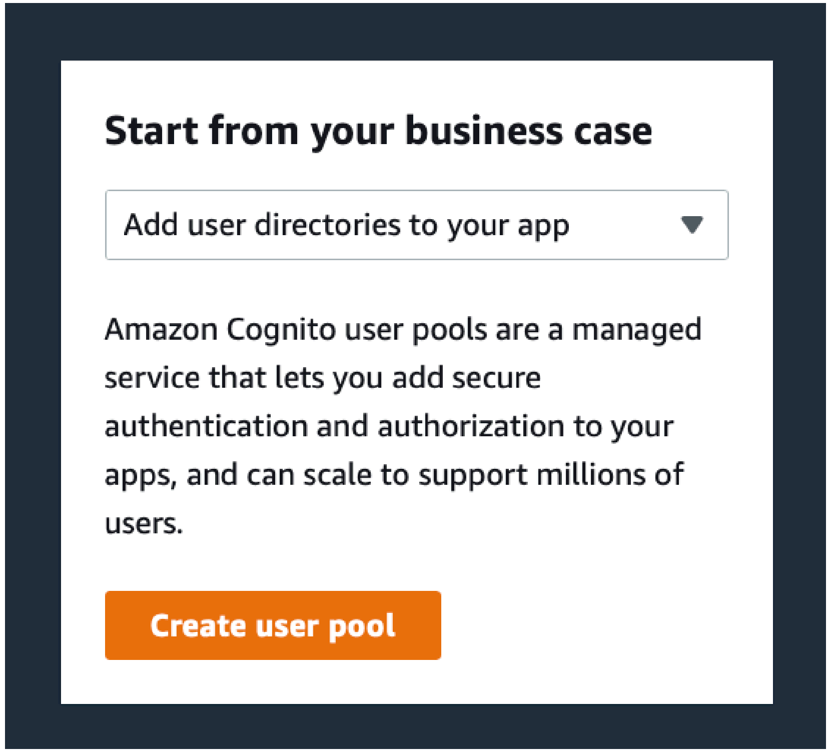


Start from your business case

Grant access to AWS services

Cognito identity pools let you get temporary credentials to access AWS services for signed-in users as well as anonymous guest users.

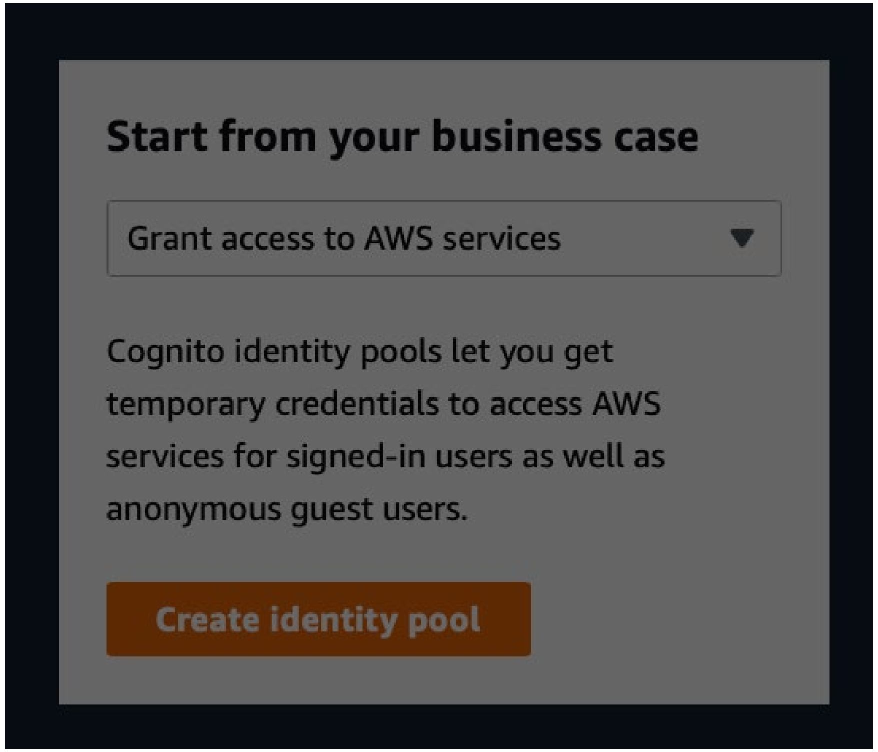
Amazon Cognito



Start from your business case

Add user directories to your app ▼

Amazon Cognito user pools are a managed service that lets you add secure authentication and authorization to your apps, and can scale to support millions of users.

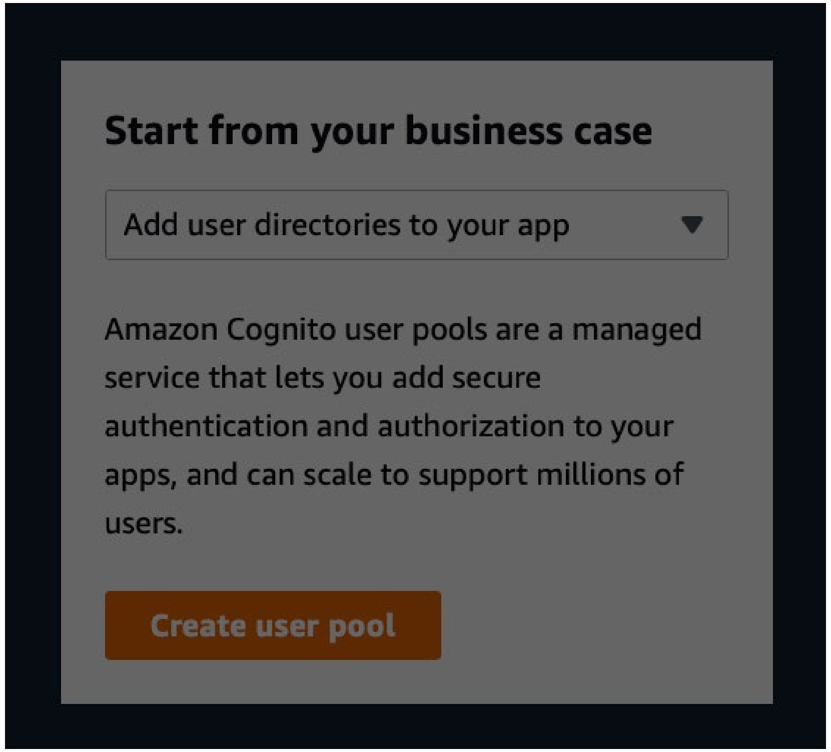


Start from your business case

Grant access to AWS services ▼

Cognito identity pools let you get temporary credentials to access AWS services for signed-in users as well as anonymous guest users.

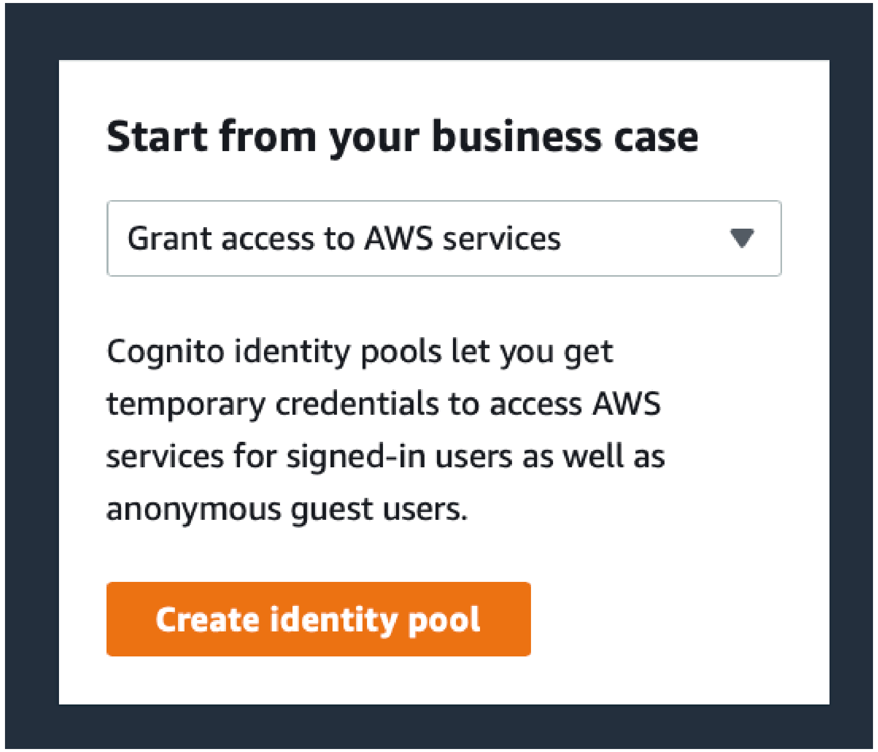
Amazon Cognito



Start from your business case

Add user directories to your app ▼

Amazon Cognito user pools are a managed service that lets you add secure authentication and authorization to your apps, and can scale to support millions of users.

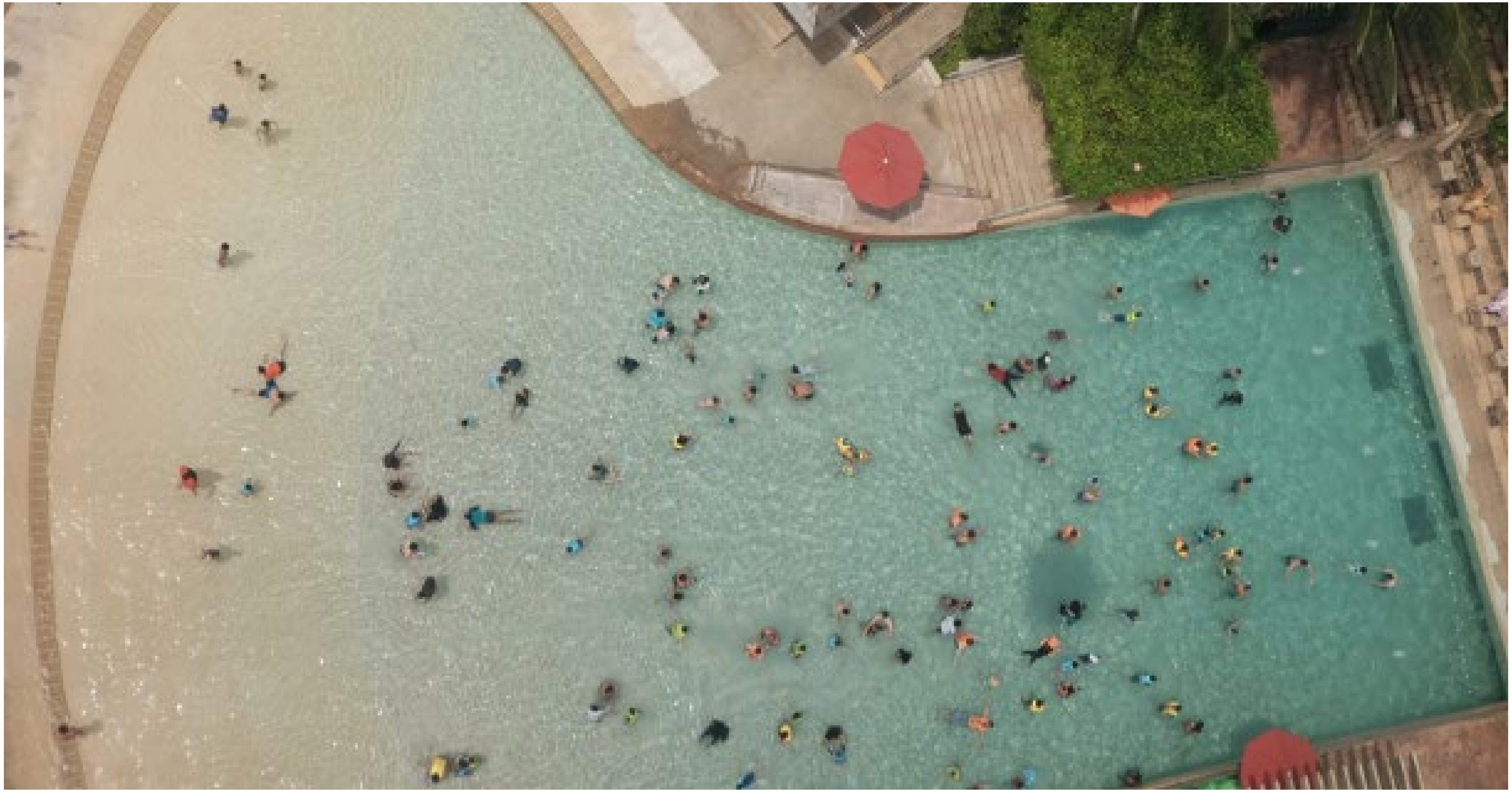


Start from your business case

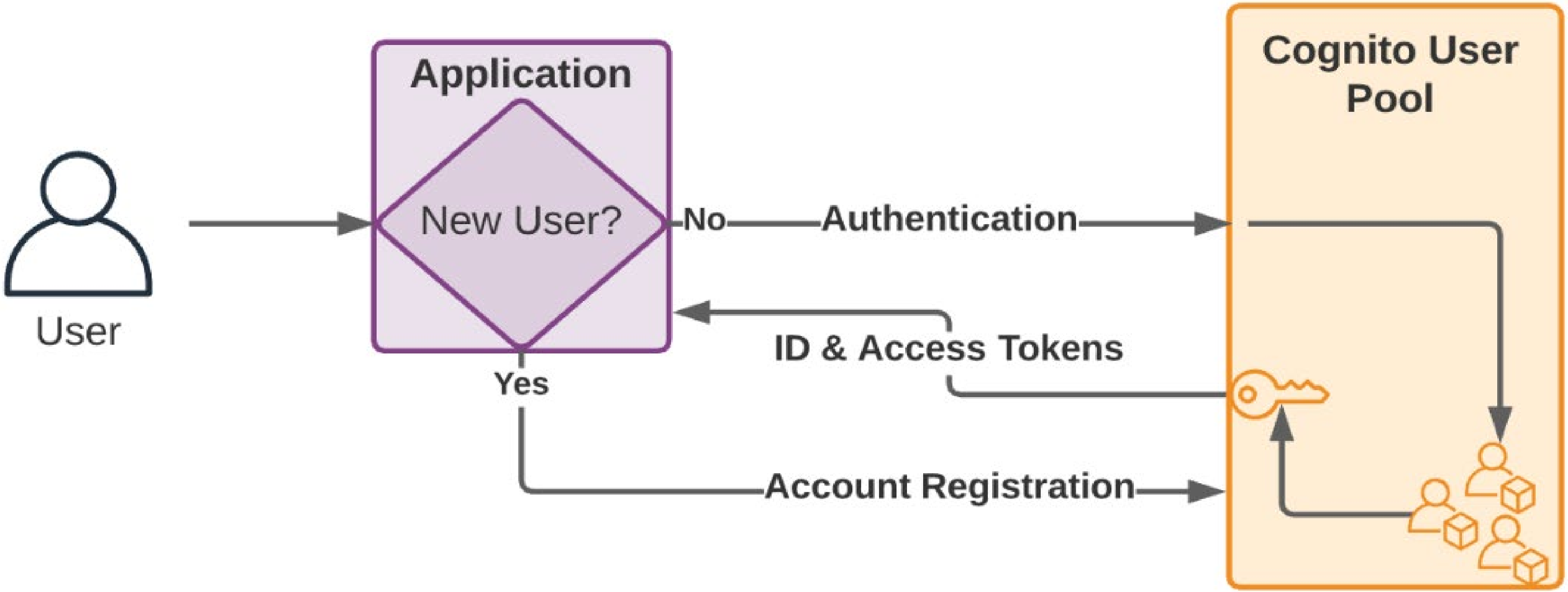
Grant access to AWS services ▼

Cognito identity pools let you get temporary credentials to access AWS services for signed-in users as well as anonymous guest users.

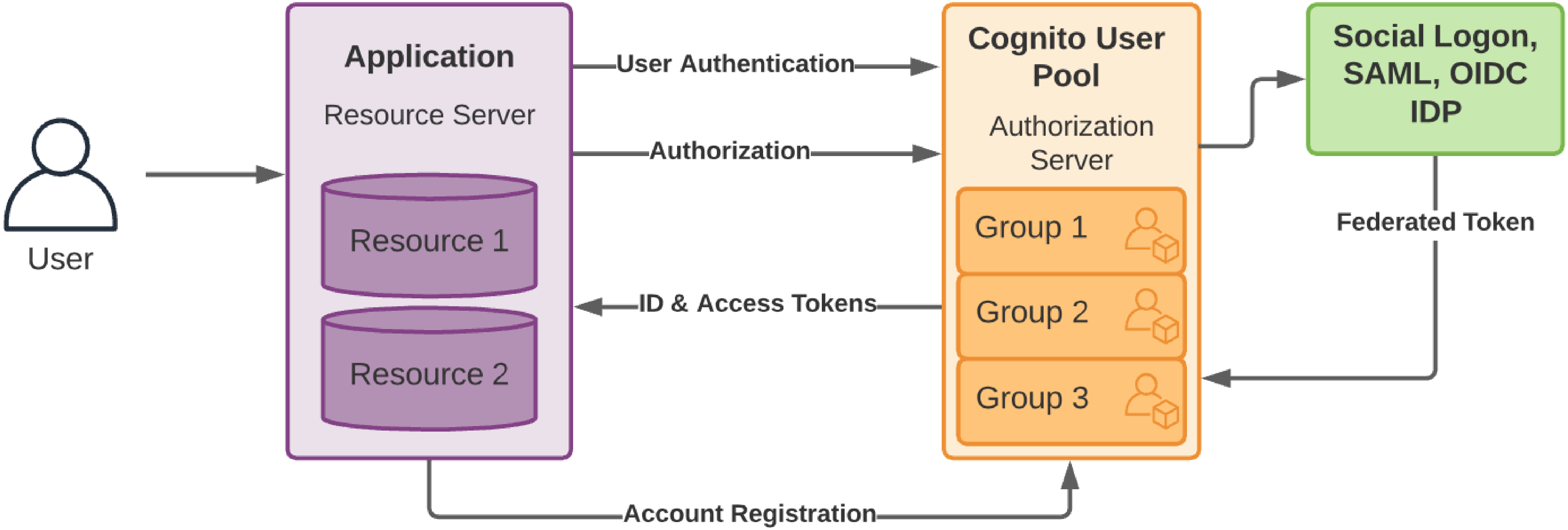
Cognito User Pools



Cognito User Pools

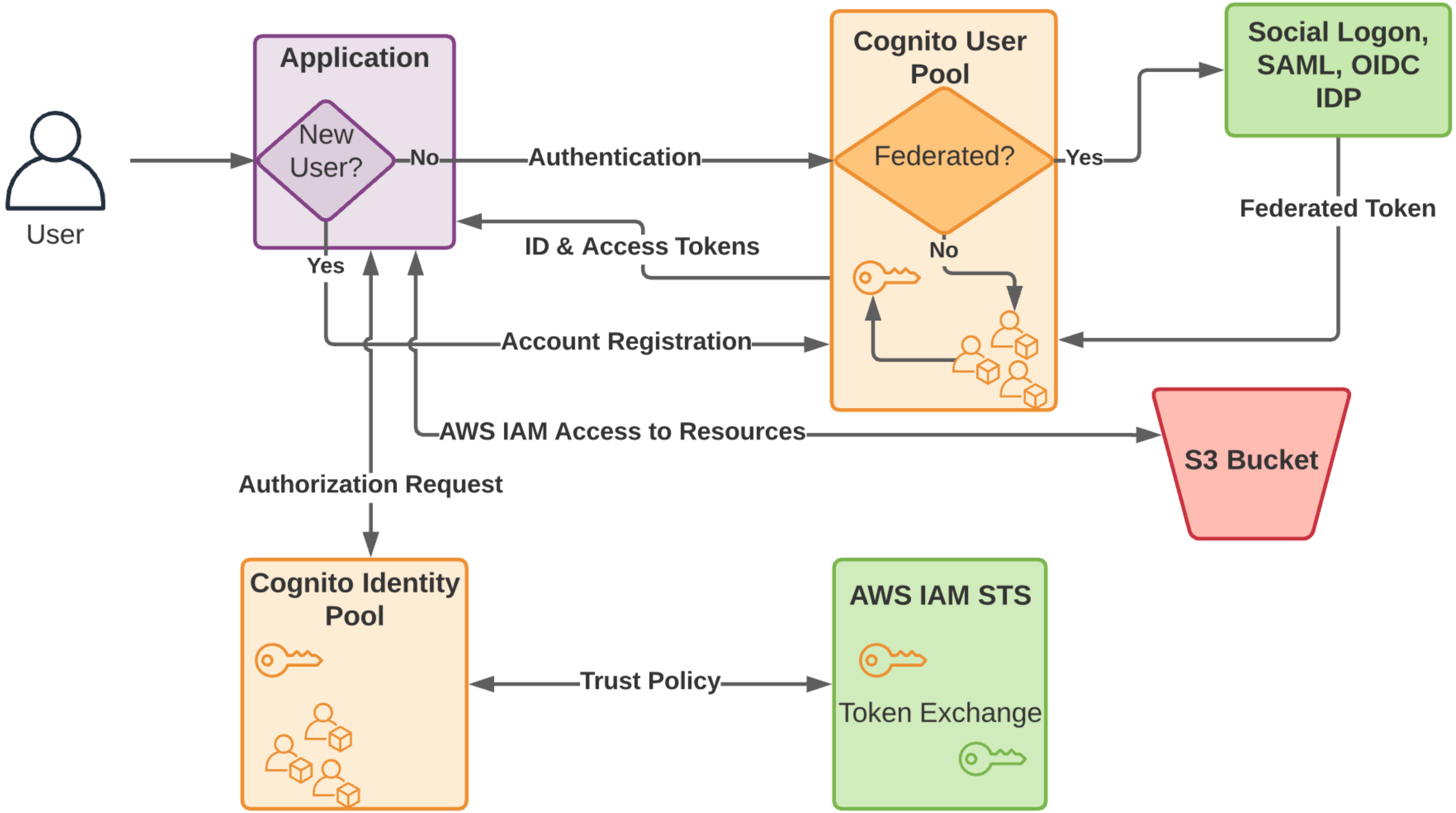


Cognito User Pools

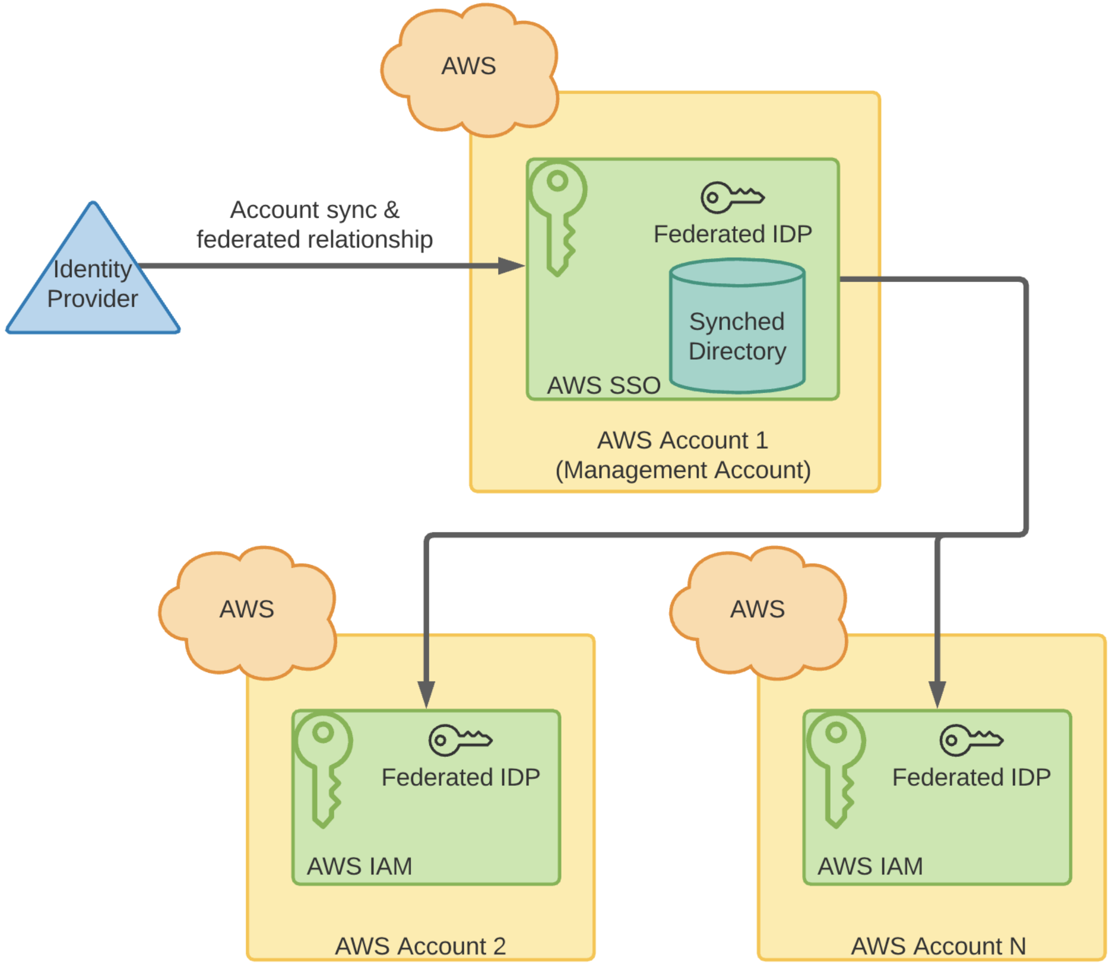


Cognito Identity Pools

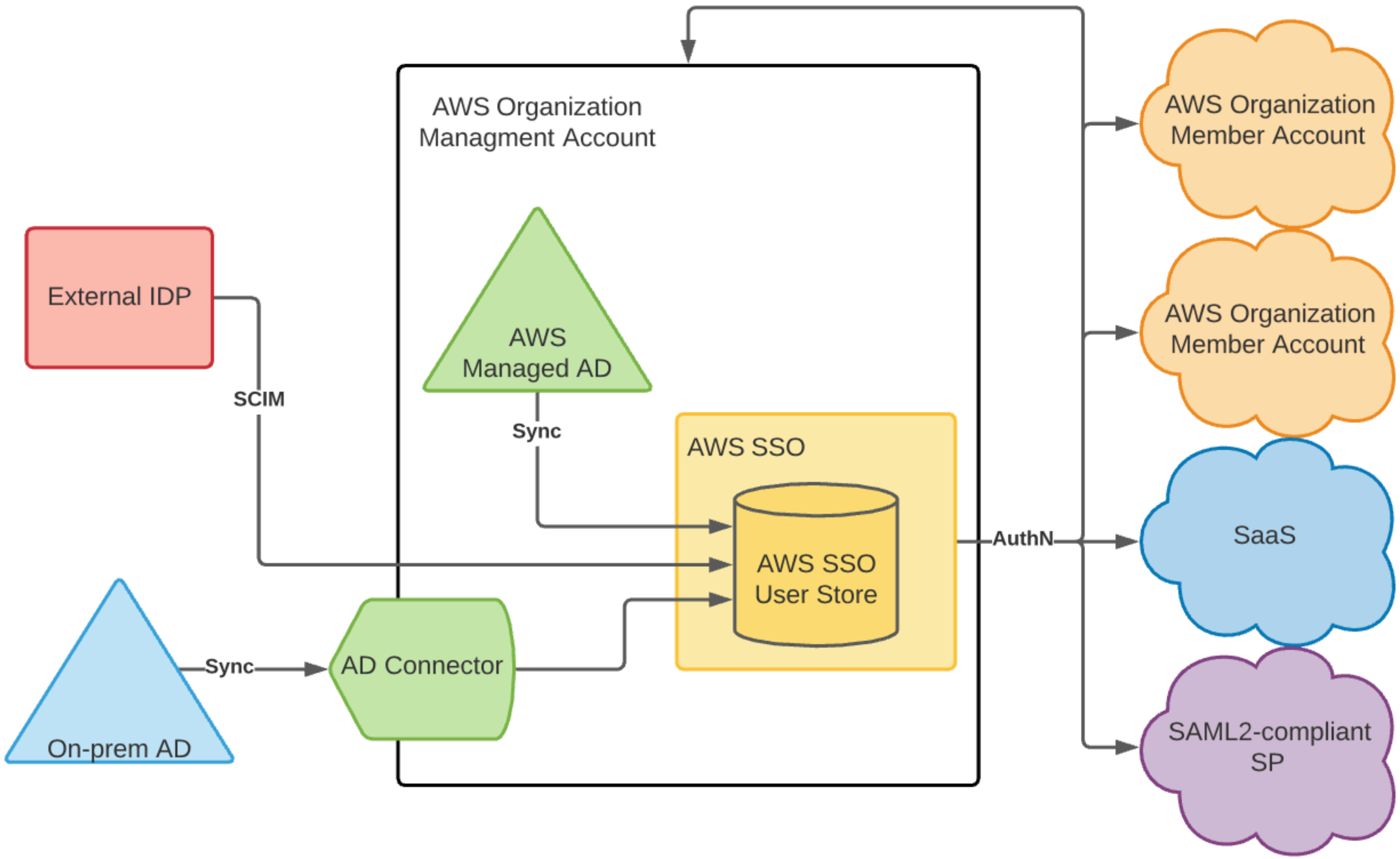
Cognito Identity Pools



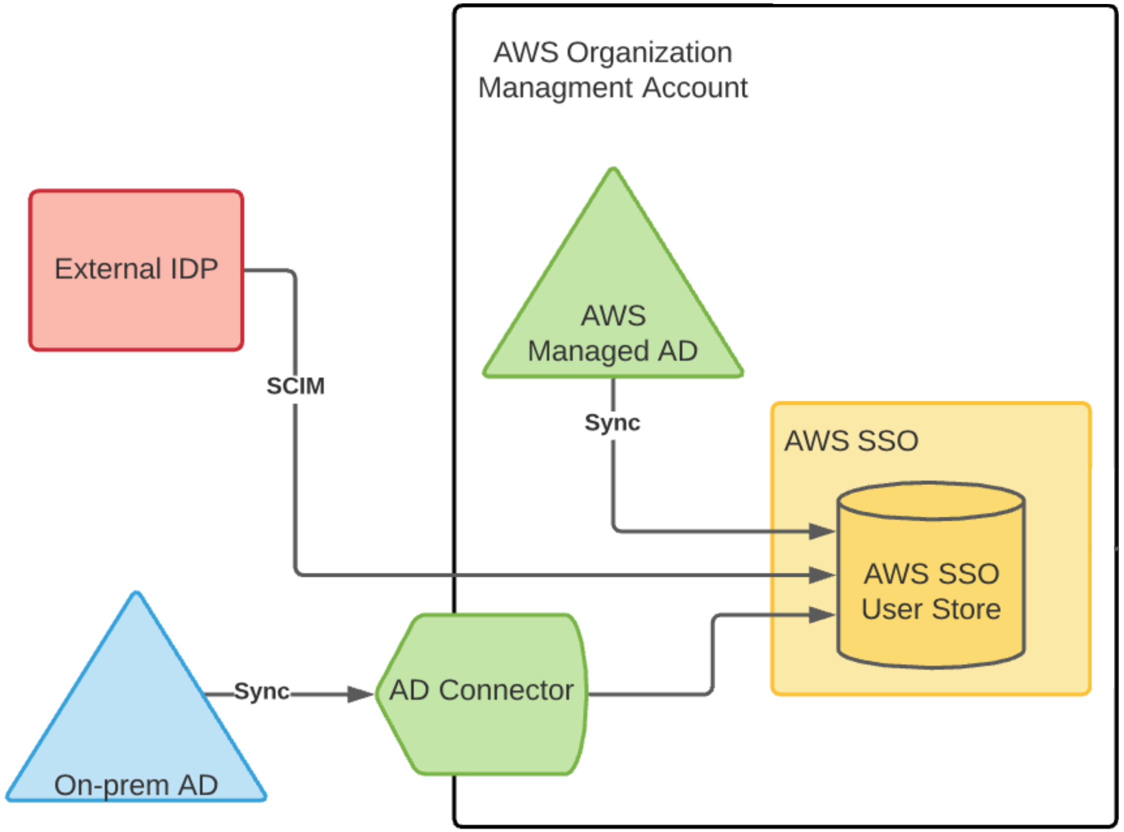
AWS Single Sign-on



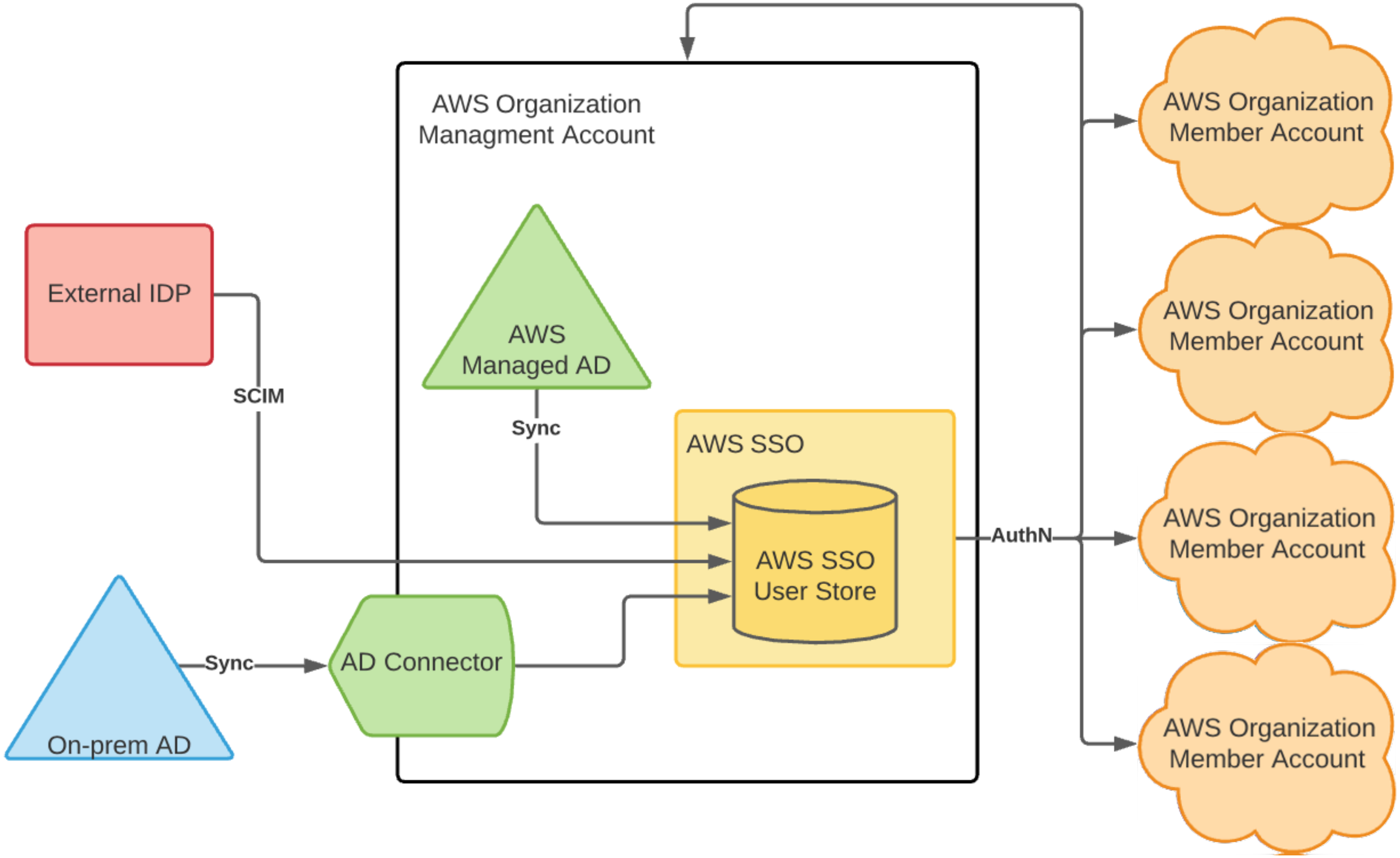
Available Identity Flows in AWS IAM



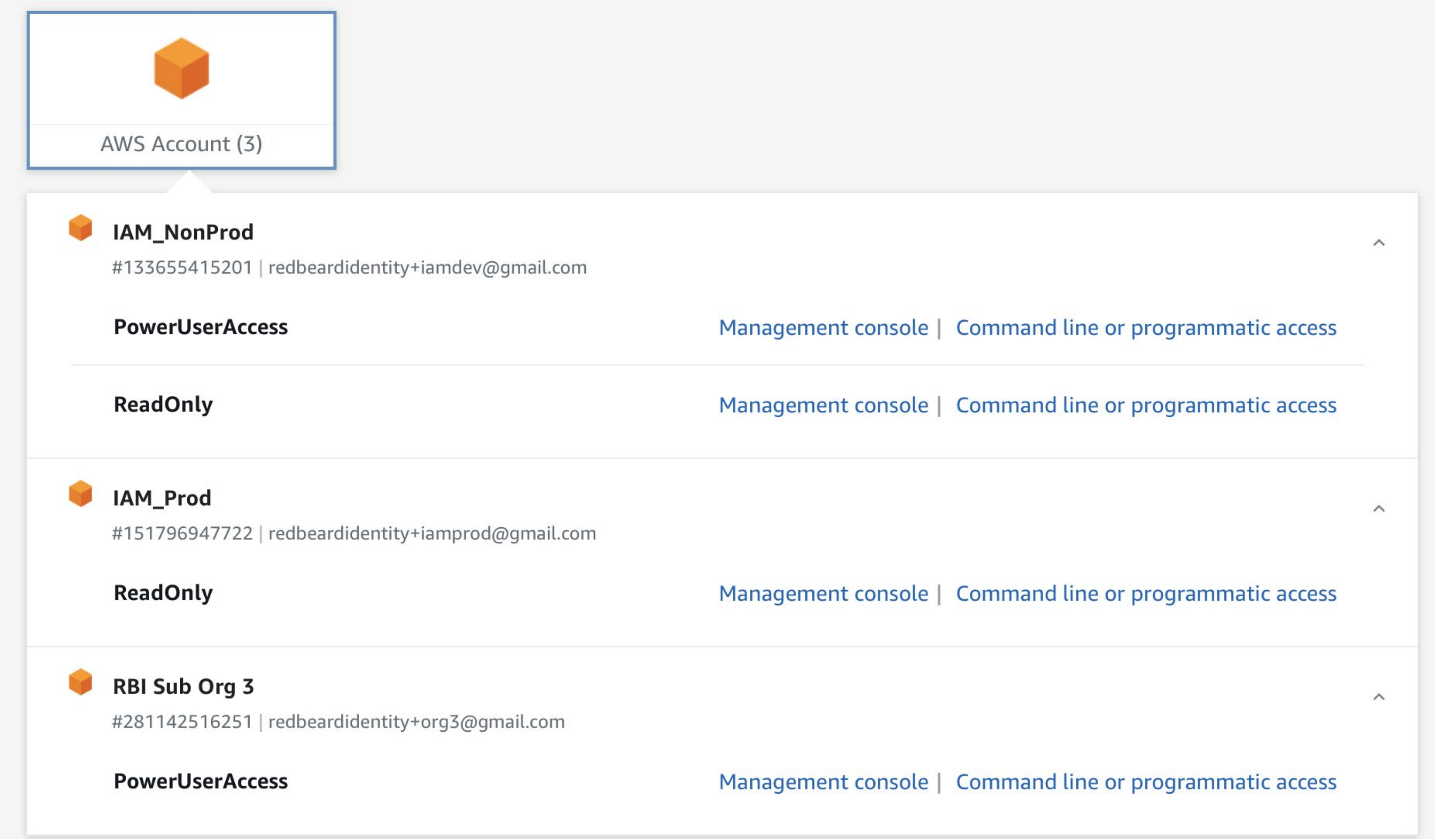
Available Identity Flows in AWS IAM



Available Identity Flows in AWS IAM



Permission Sets (Assumable Roles)



AWS Account (3)

IAM_NonProd
#133655415201 | redbeardidentity+iamdev@gmail.com

PowerUserAccess Management console | Command line or programmatic access

ReadOnly Management console | Command line or programmatic access

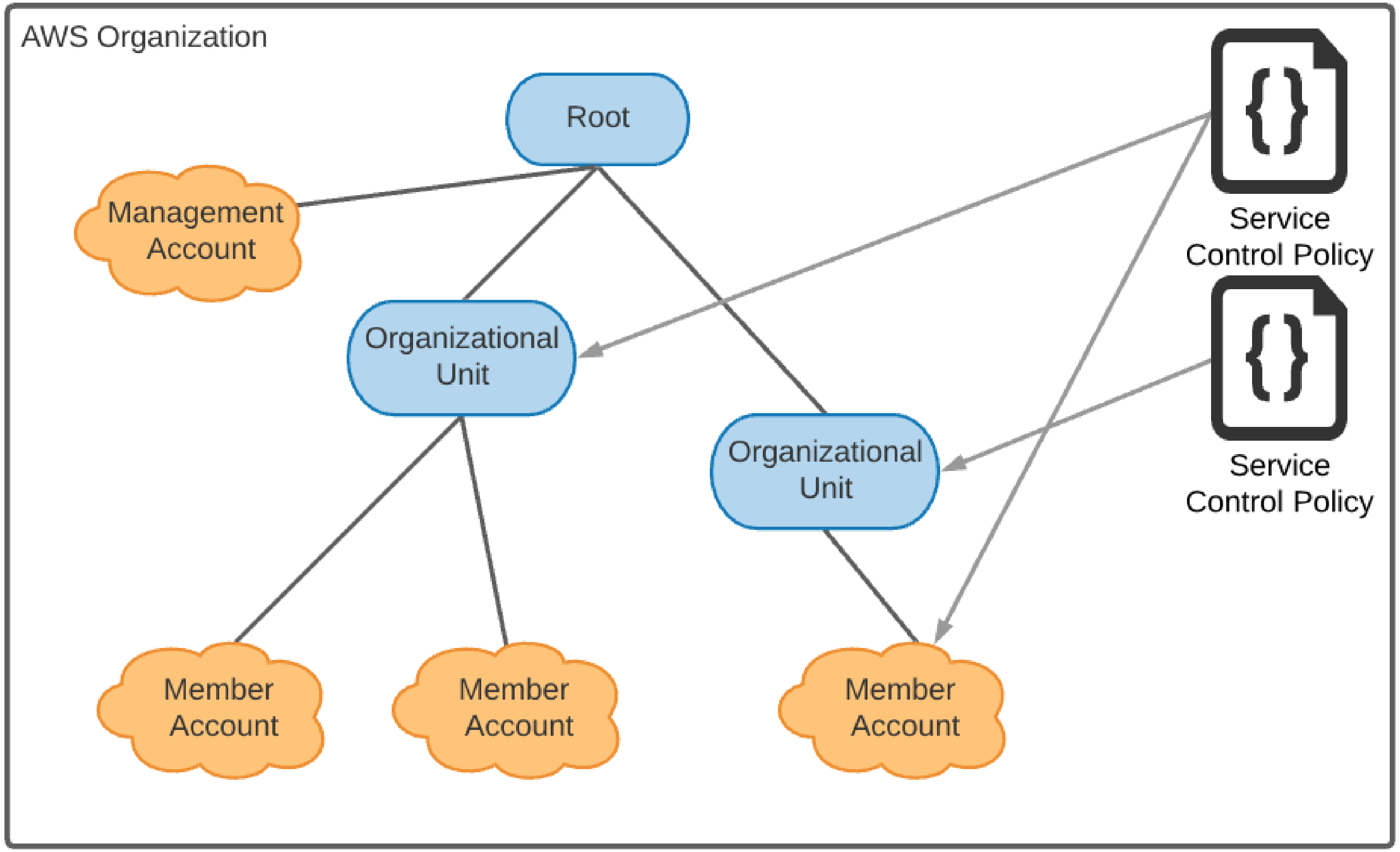
IAM_Prod
#151796947722 | redbeardidentity+iamprod@gmail.com

ReadOnly Management console | Command line or programmatic access

RBI Sub Org 3
#281142516251 | redbeardidentity+org3@gmail.com

PowerUserAccess Management console | Command line or programmatic access

AWS Organizations



RSA®Conference2022

Recap for Enterprise Practitioners

	User Management	Credential Management	Federation	AWS Resource AuthZ	AWS-deployed App AuthN	App AuthN	App AuthZ
IAM	**Yes** (IaaS)	**Yes**, Password (IaaS) **Yes**, MFA (IaaS)	**Yes** (Inbound, IaaS)	**Yes**	**No**	**No**	**No**
Cognito	**Yes** (PaaS)	**Yes**, Password (PaaS) **Yes**, MFA (PaaS)	**Yes** (OP/RP, User Pools) **Yes** (Inbound, Identity Pools)	**Yes** (Identity Pools AWS STS for resource access)	**Yes**	**Yes** (User Pools)	**Conditionally Yes** (Identity Pools w/ deep AWS integration)
SSO	**Yes** (IaaS w/ AWS IAM) Yes (PaaS)	**Yes**, Password (IaaS) Yes, MFA (IaaS)	**Yes** (Workforce) Yes (AWS accounts)	**Yes** (through AWS IAM)	**Yes** (through AWS IAM)	**Yes** (Workforce)	**Yes** (Workforce)
Directory Service	**Yes**	**Yes**, Password (AD as AWS IAM/AWS SSO User Store)	No	**Conditionally Yes** (If used as AWS SSO user store)	**Yes** (AD workloads, AWS SSO user store)	**Yes** (AD workloads, AWS SSO user store)	**Yes** (AD workloads, AWS SSO user store)

Things to Remember & Next Steps

- AWS IAM will always ultimately control access to AWS resources
- Use AWS SSO to simplify the authorization constructs of AWS IAM and bridge the platform-centric mindset with a use case-driven mindset
- AWS SSO and AWS Organizations make administrative LCM and access to AWS accounts much easier
- Refine authorization when using AWS SSO & AWS Organization via additional policies in AWS IAM

Things to Remember & Next Steps, cont.

- Amazon Cognito provides identity services for applications. It is good for enterprise-developed applications, *assuming you connect the User Pool to your enterprise IDP*
- Cognito Identity Pools plus AWS STS allows Cognito identities to access AWS resources like any other AWS IAM principal. This is good for app teams w/ deep AWS integration
- AWS Directory Service is useful for organizations that us AD as their user store. AWS Directory Service can populate AWS IAM directly, but it’s easier to use it as AWS SSO’s user store

Questions?

Jon Lehtinen
jon.lehtinen@okta.com
jlehtinen@idpro.org
@jonlehtinen