

The background features a dark blue gradient with large, overlapping, semi-transparent shapes in shades of purple and magenta. Two thin, light blue lines cross the scene diagonally. The text is positioned on the left side of the image.

AWS re:Invent

DECEMBER 2 - 6, 2024 | LAS VEGAS, NV

SAS307

Supporting federated identity in multi-tenant environments

Toby Buckley

(he/him)

Sr. Partner Solution Architect
AWS SaaS Factory

Dhammika Sriyananda

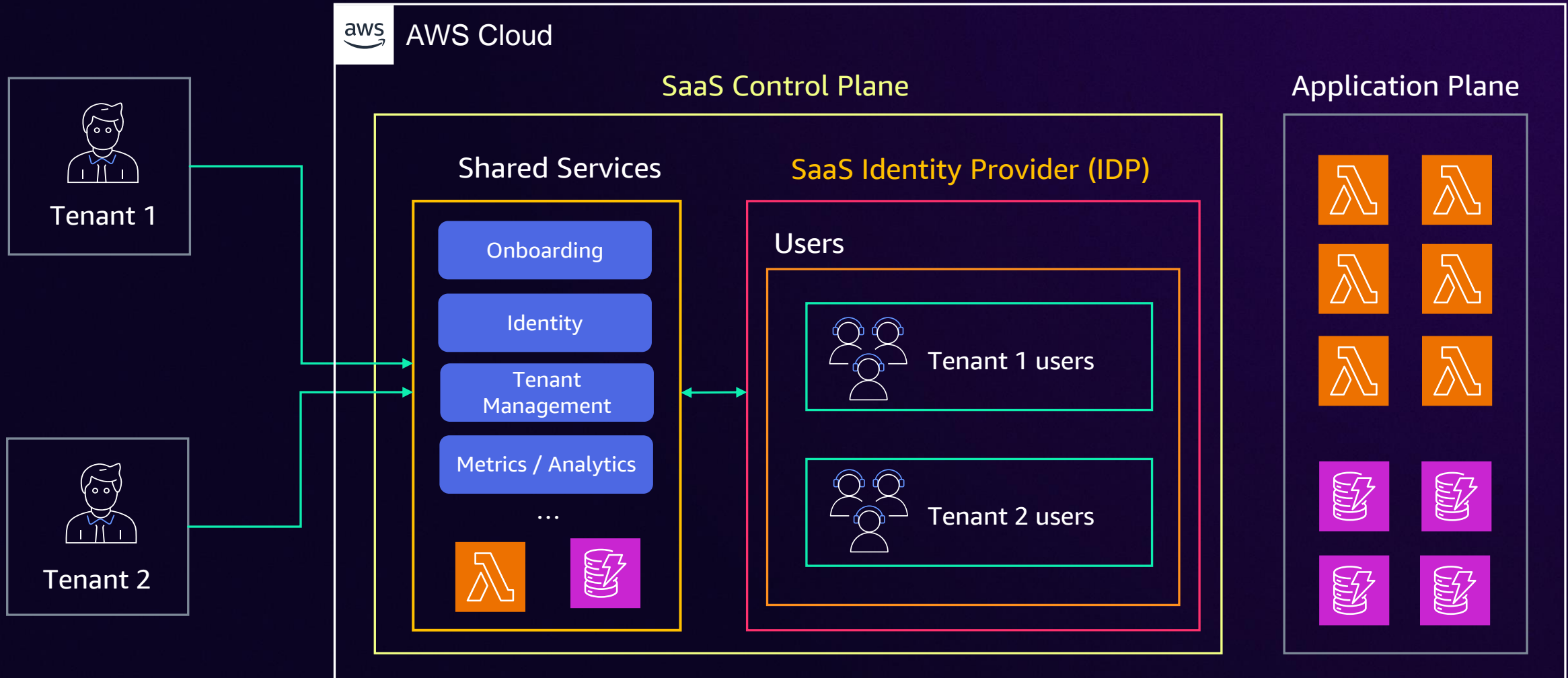
(he/him)

Sr. Partner Solution Architect
AWS SaaS Factory

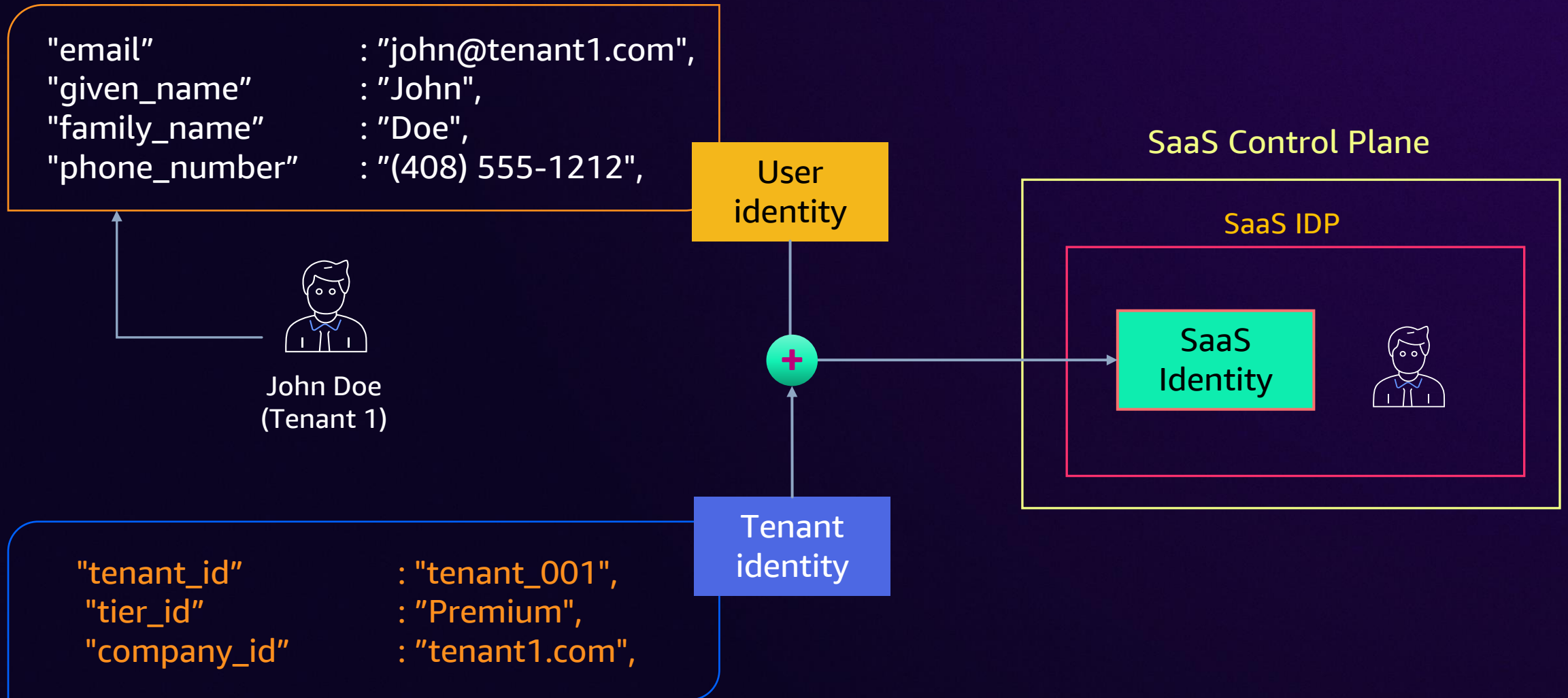


Managing identities in a SaaS

SaaS application



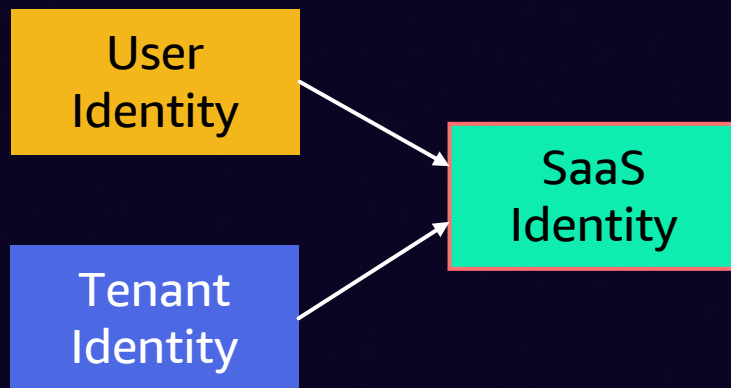
Representing SaaS identity



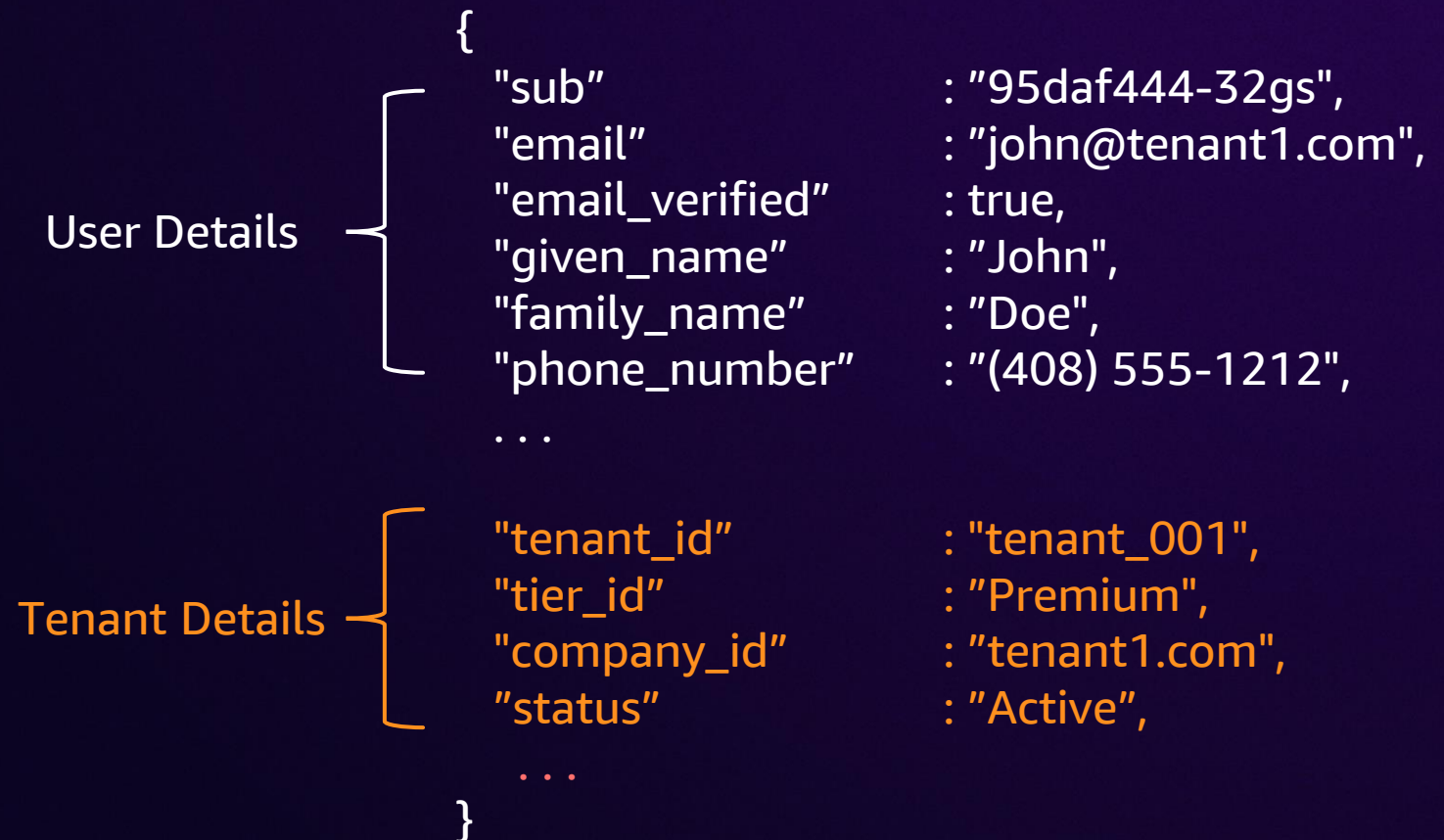
A first-class SaaS token to represent SaaS identity

Identity Tokens

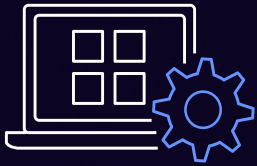
- Fully managed by the SaaS IdP
- Security in-built
- Embedded the SaaS Identity



JSON Web Token (JWT)



User auth flow with Amazon Cognito IDP



SaaS App

SaaS IDP

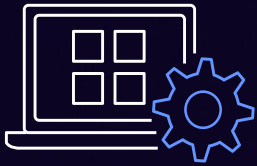


Amazon Cognito



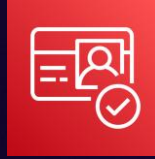
John Doe
(Tenant 1)

User auth flow with Amazon Cognito IDP



SaaS App

SaaS IDP



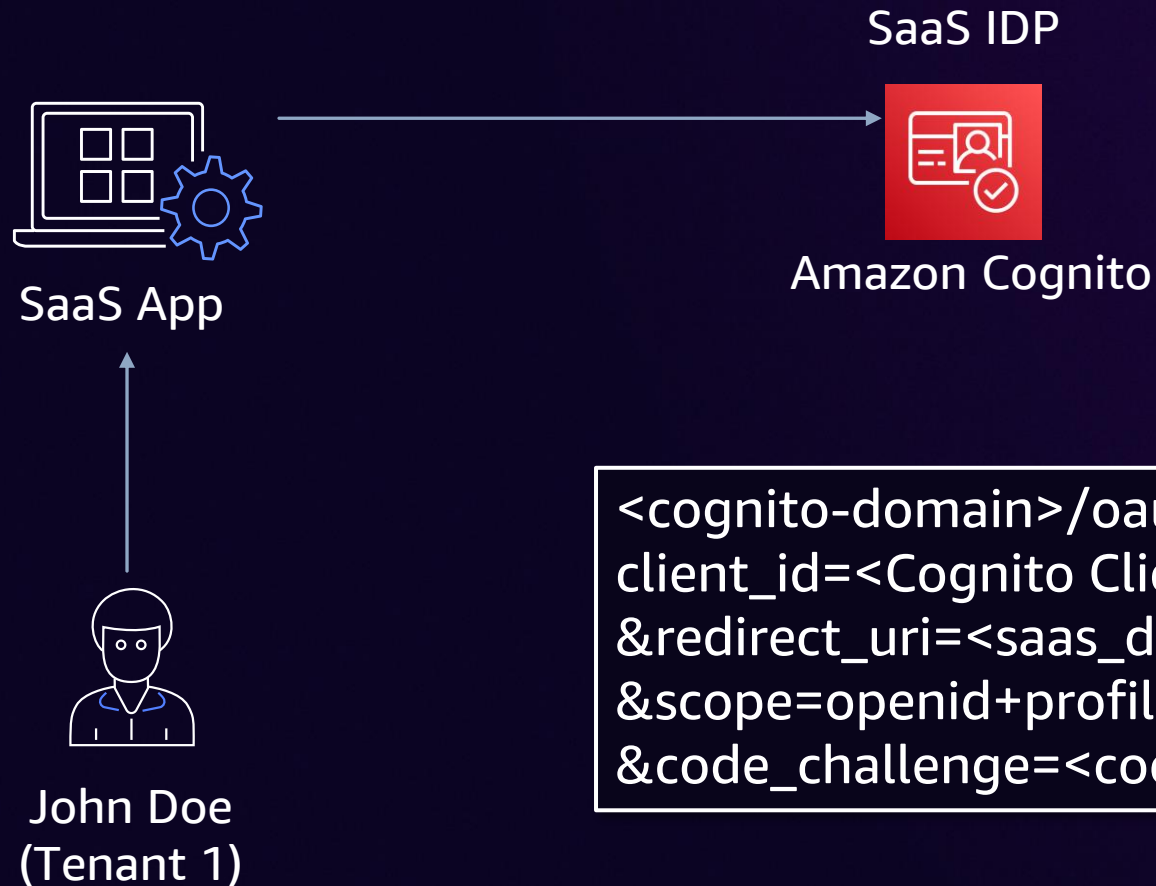
Amazon Cognito



John Doe
(Tenant 1)

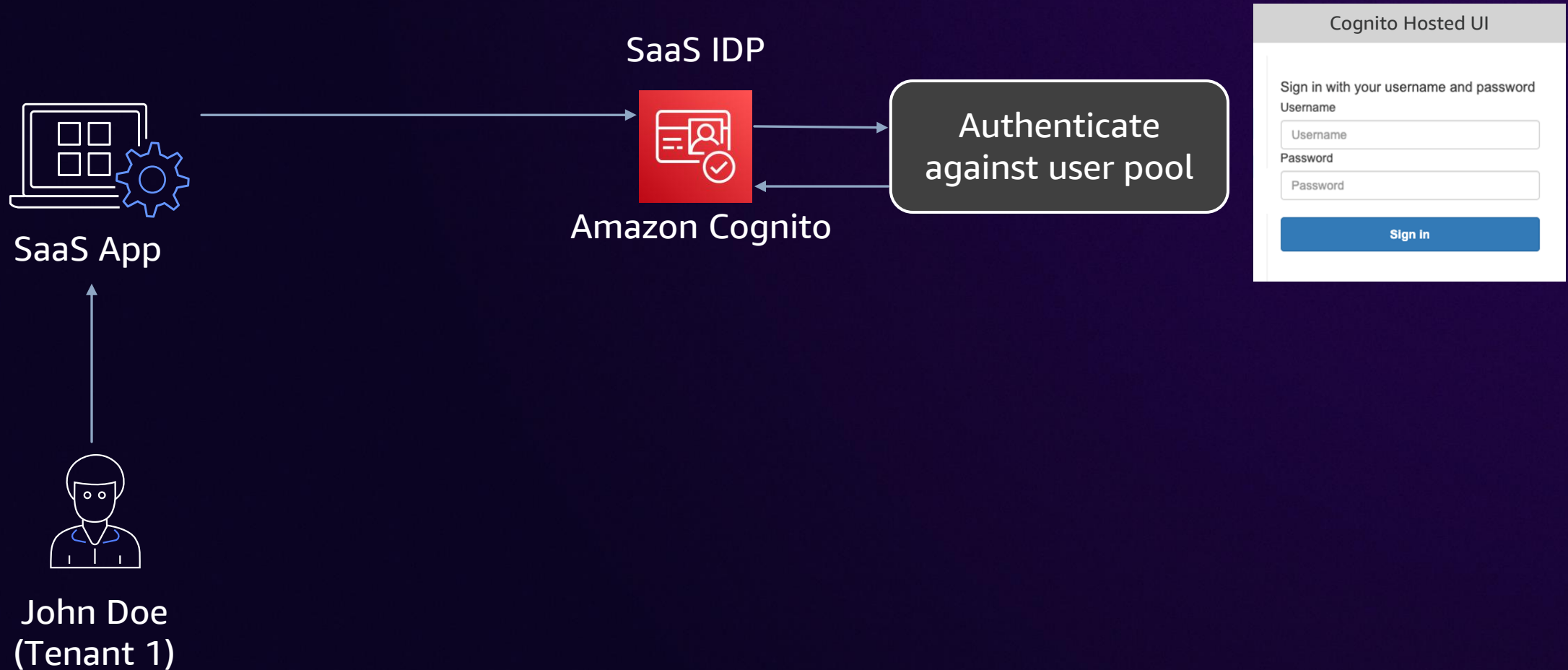


User auth flow with Amazon Cognito IDP

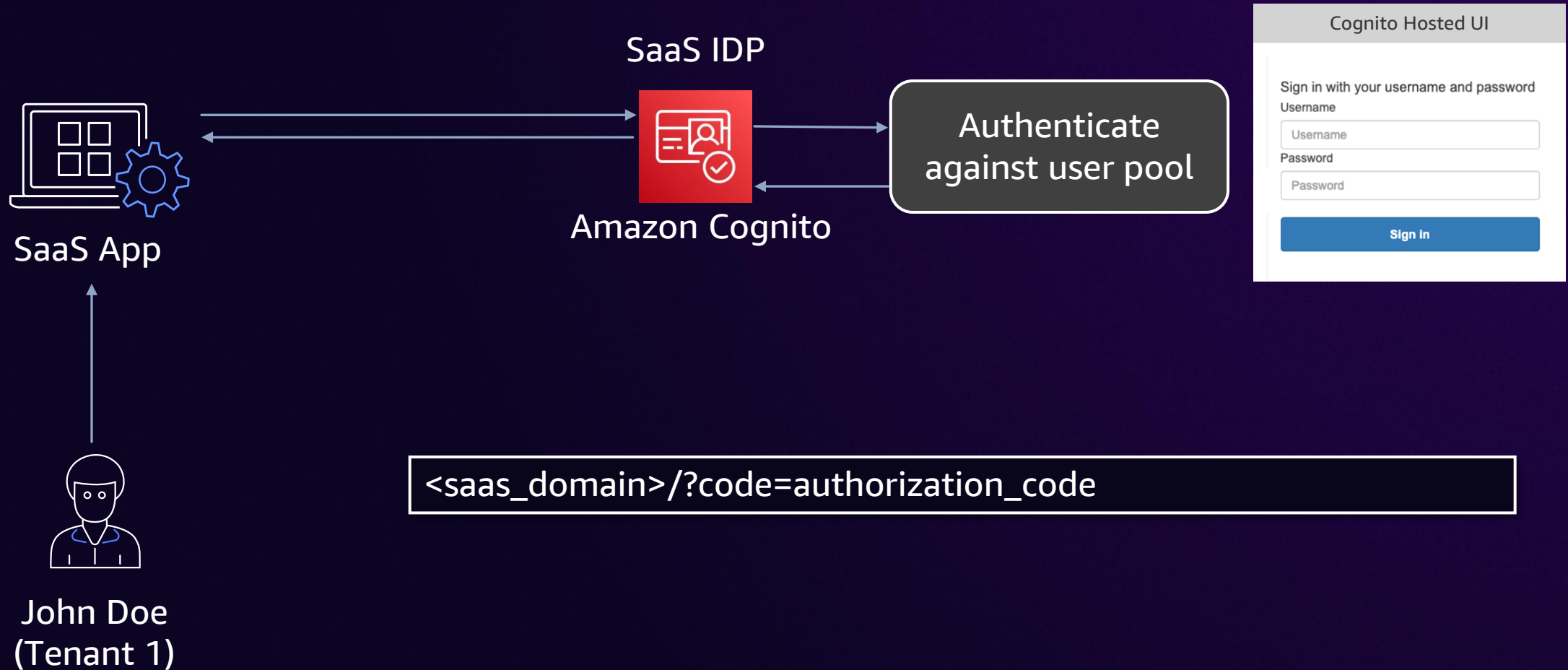


```
<cognito-domain>/oauth2/authorize?  
client_id=<Cognito Client Id>  
&redirect_uri=<saas_domain>  
&scope=openid+profile+email  
&code_challenge=<code challenge>
```


User auth flow with Amazon Cognito IDP



User auth flow with Amazon Cognito IDP



User auth flow with Amazon Cognito IDP



Cognito Hosted UI

Sign in with your username and password

Username

Password

Sign In

SaaS App

SaaS IDP

Amazon Cognito

Authenticate
against user pool



John Doe
(Tenant 1)

```
POST <cognito-domain>/oauth2/token
grant_type=authorization_code
&client_id=<Cognito Client Id>
&code_verifier=<code verifier>
&redirect_uri=<saas_domain>
```

User auth flow with Amazon Cognito IDP



Cognito Hosted UI

Sign in with your username and password

Username

Password

Sign In

John Doe
(Tenant 1)

```
{  
  "id_token": "<id_token>",  
  "access_token": "<access_token>",  
  "refresh_token": "<refresh_token>",  
  "expires_in": 3600,  
  "token_type": "Bearer"  
}
```

User auth flow with Amazon Cognito IDP

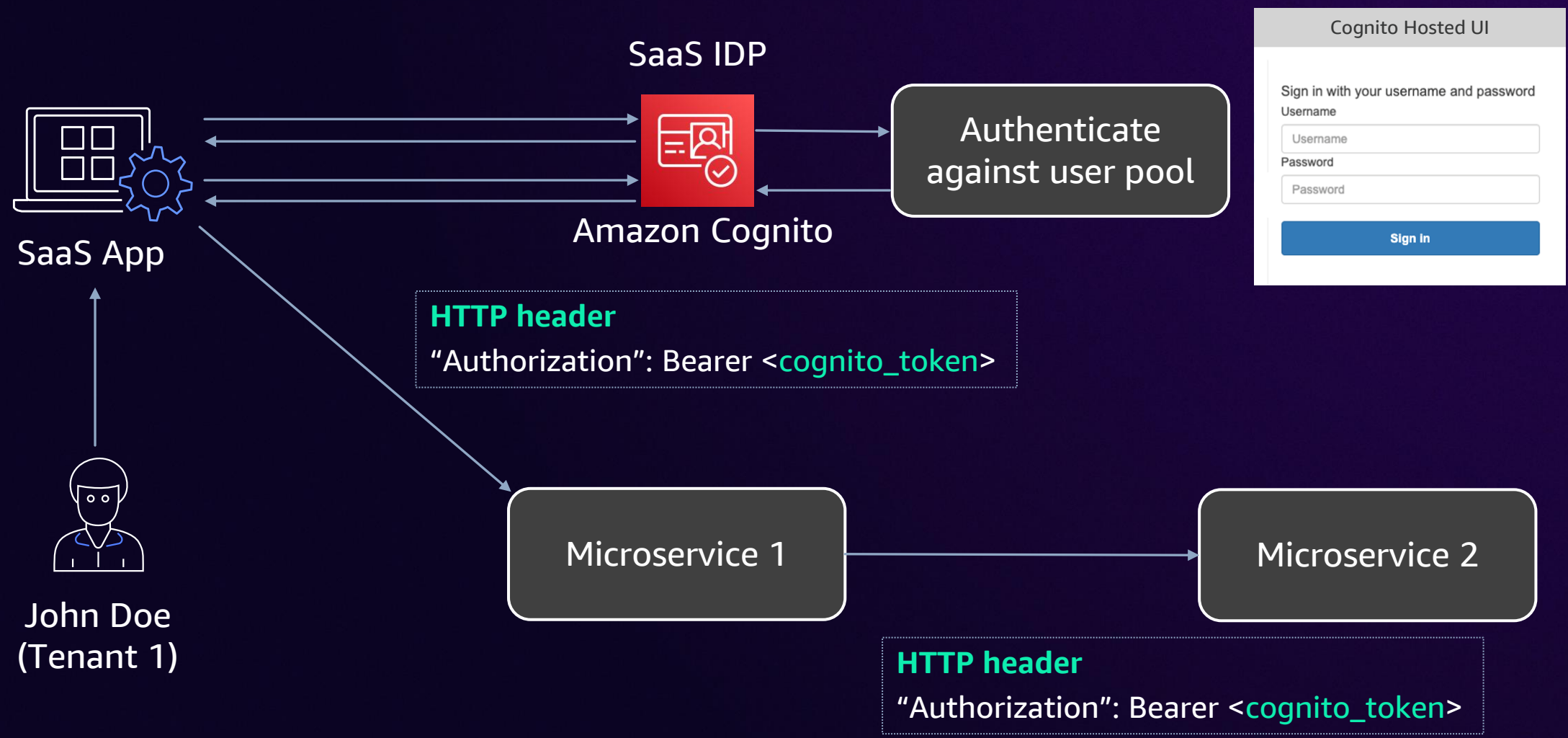


John Doe
(Tenant 1)

Cognito JSON Web Token (JWT)

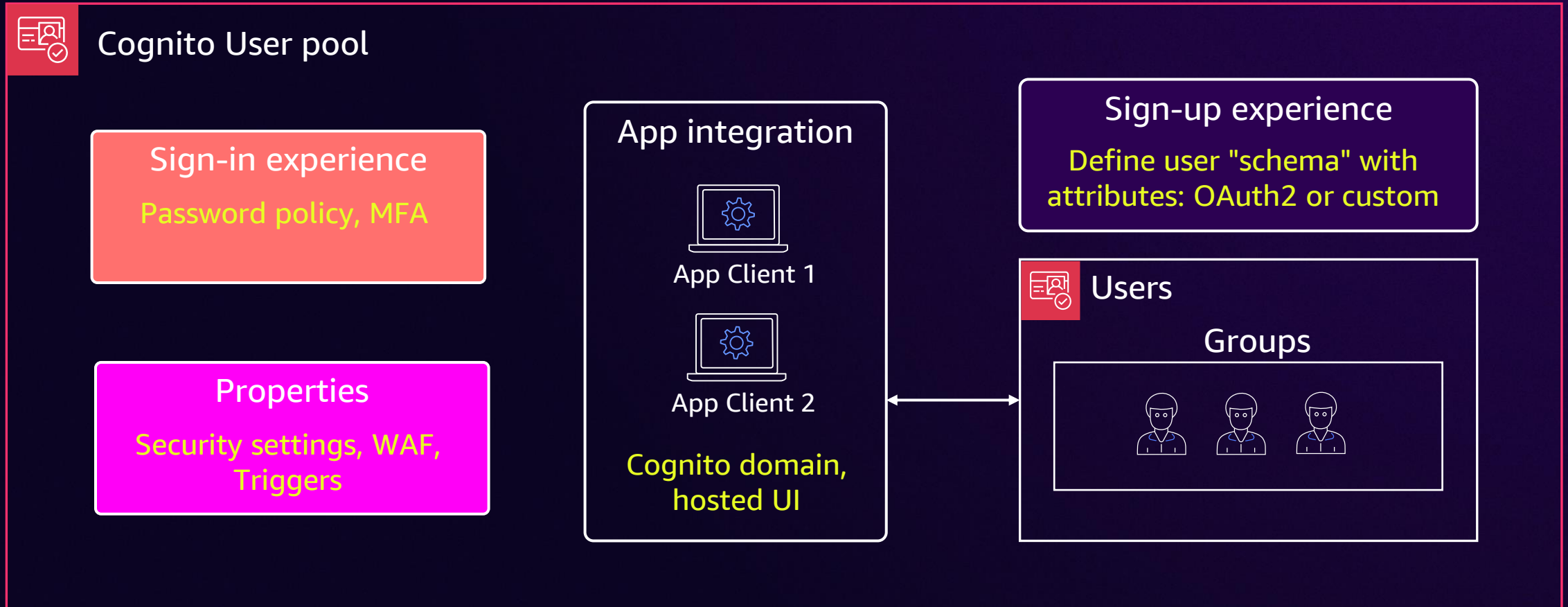
```
{
  "sub" : "95daf444-32gs",
  "email" : "john@tenant1.com",
  "email_verified" : true,
  "given_name" : "John",
  "family_name" : "Doe",
  "phone_number" : "(408) 555-1212",
  "custom:tenant_id" : "tenant_001",
  "custom:tier_id" : "Premium",
  "custom:company_id" : "tenant1.com",
  "custom:status" : "Active",
}
```

User auth flow with Amazon Cognito IDP

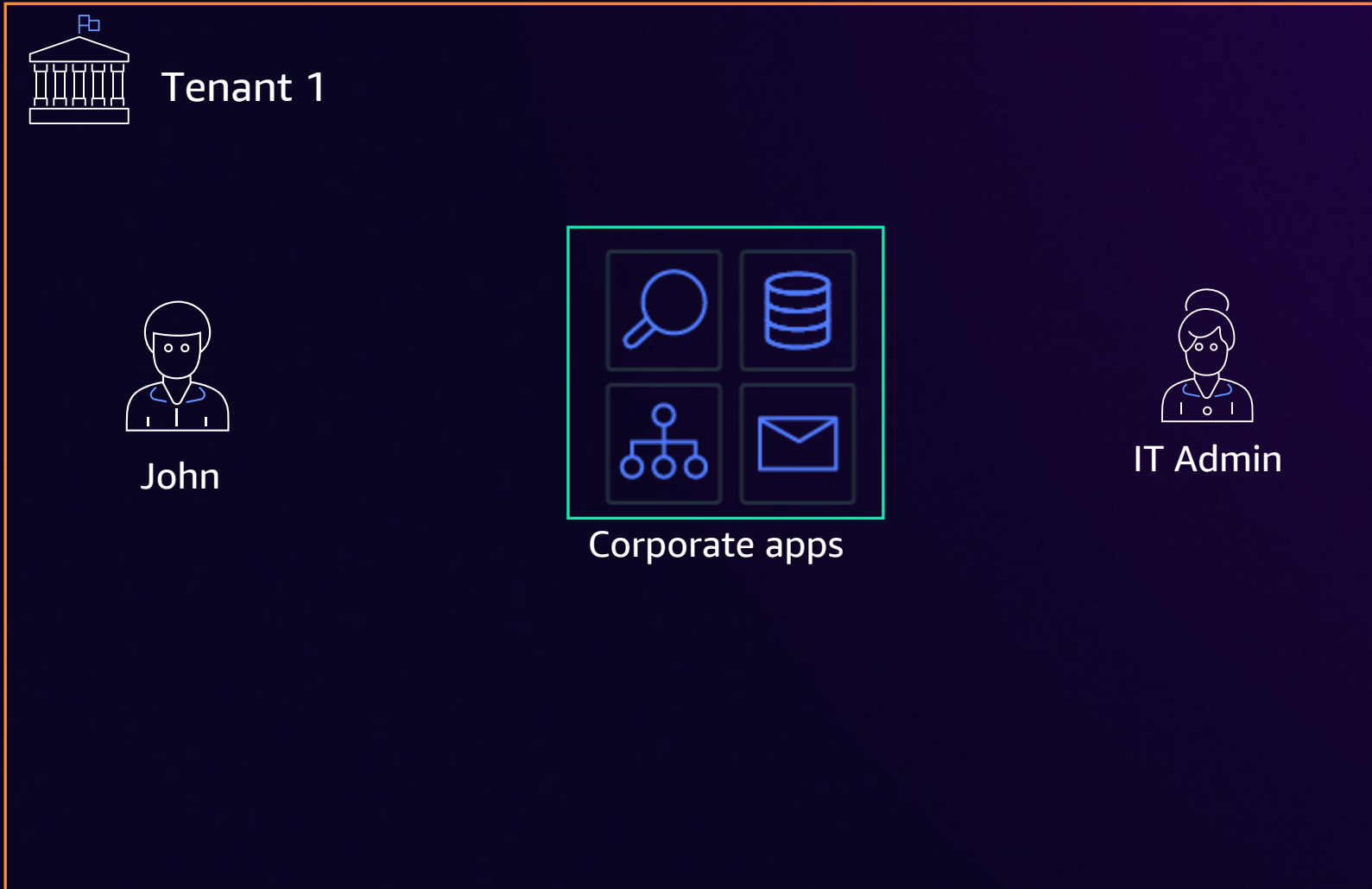


Amazon Cognito as the SaaS IDP

Cognito user pool elements that help to represent SaaS identity



Tenants demand a “single source of identity”



SaaS Application

Tenant Id	Name
1	Nikki
1	John
1	Jorge

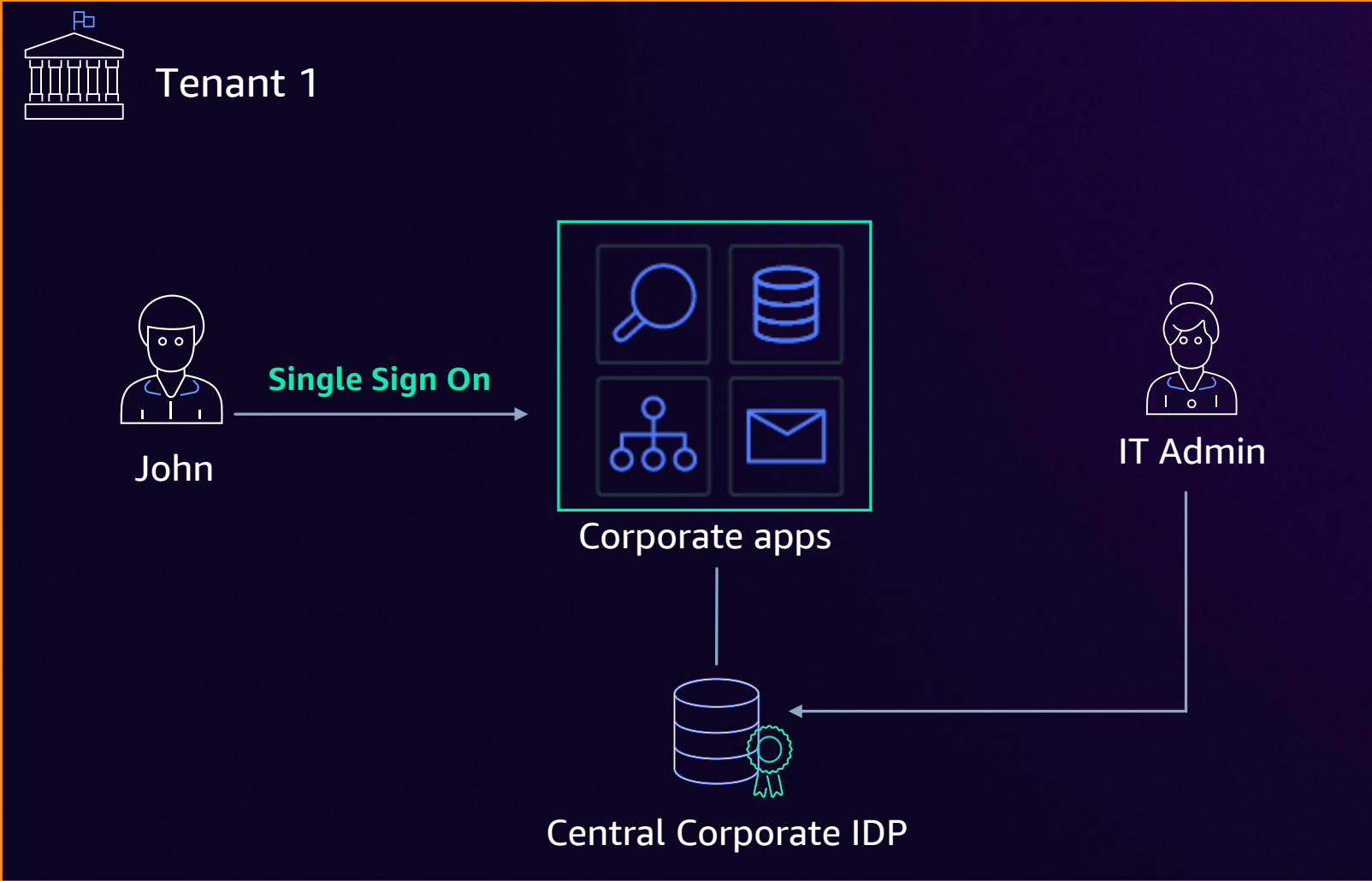
Tenants demand a “single source of identity”



SaaS Application

Tenant Id	Name
1	Nikki
1	John
1	Jorge

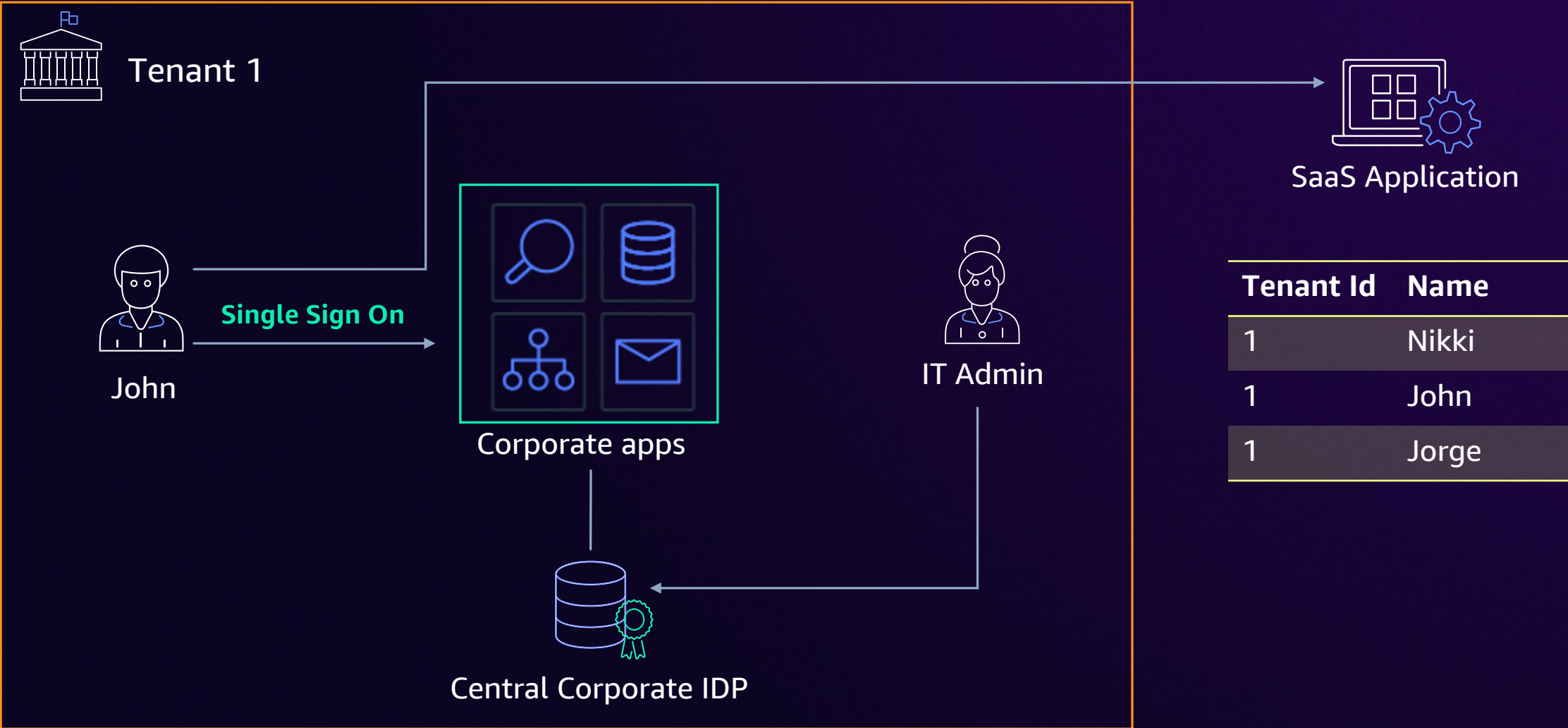
Tenants demand a “single source of identity”



SaaS Application

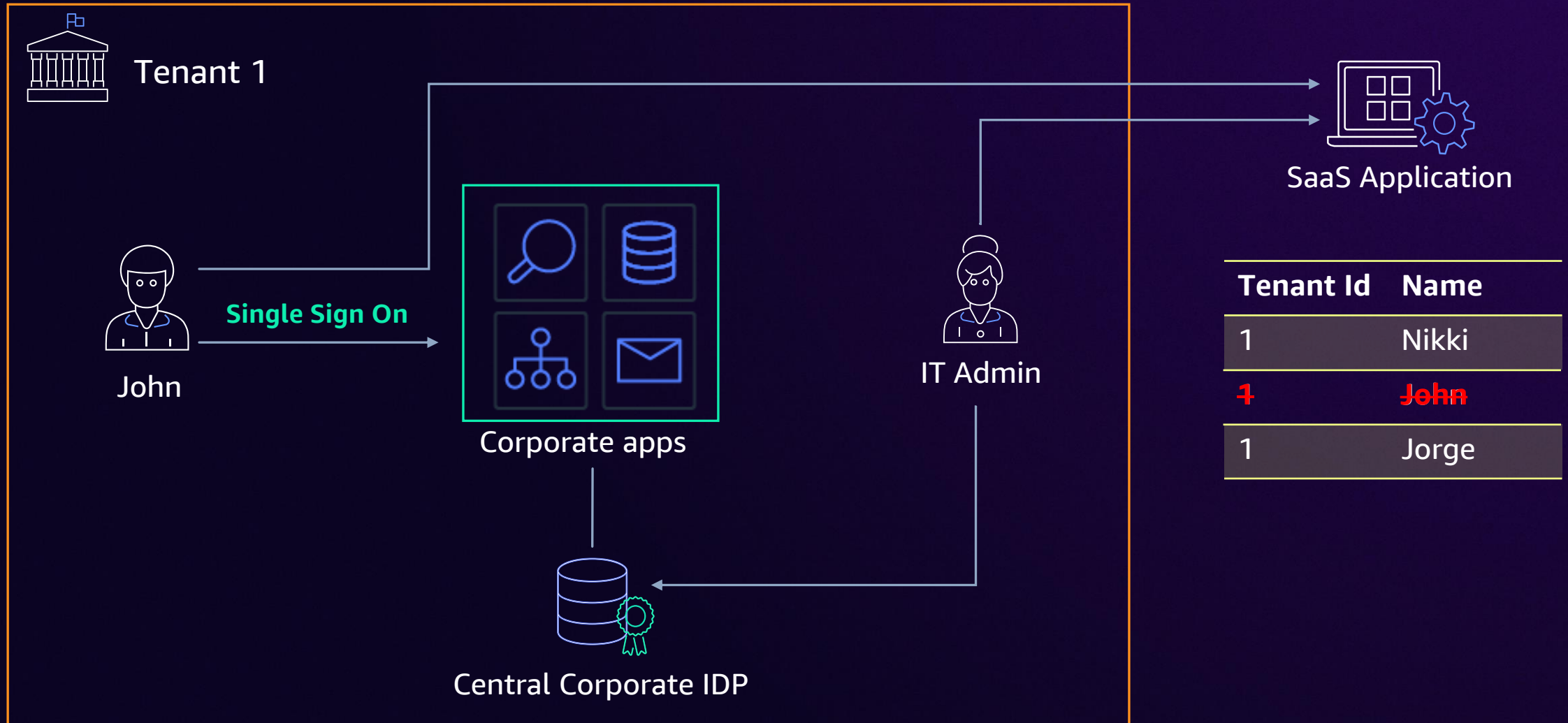
Tenant Id	Name
1	Nikki
1	John
1	Jorge

Tenants demand a "single source of identity"

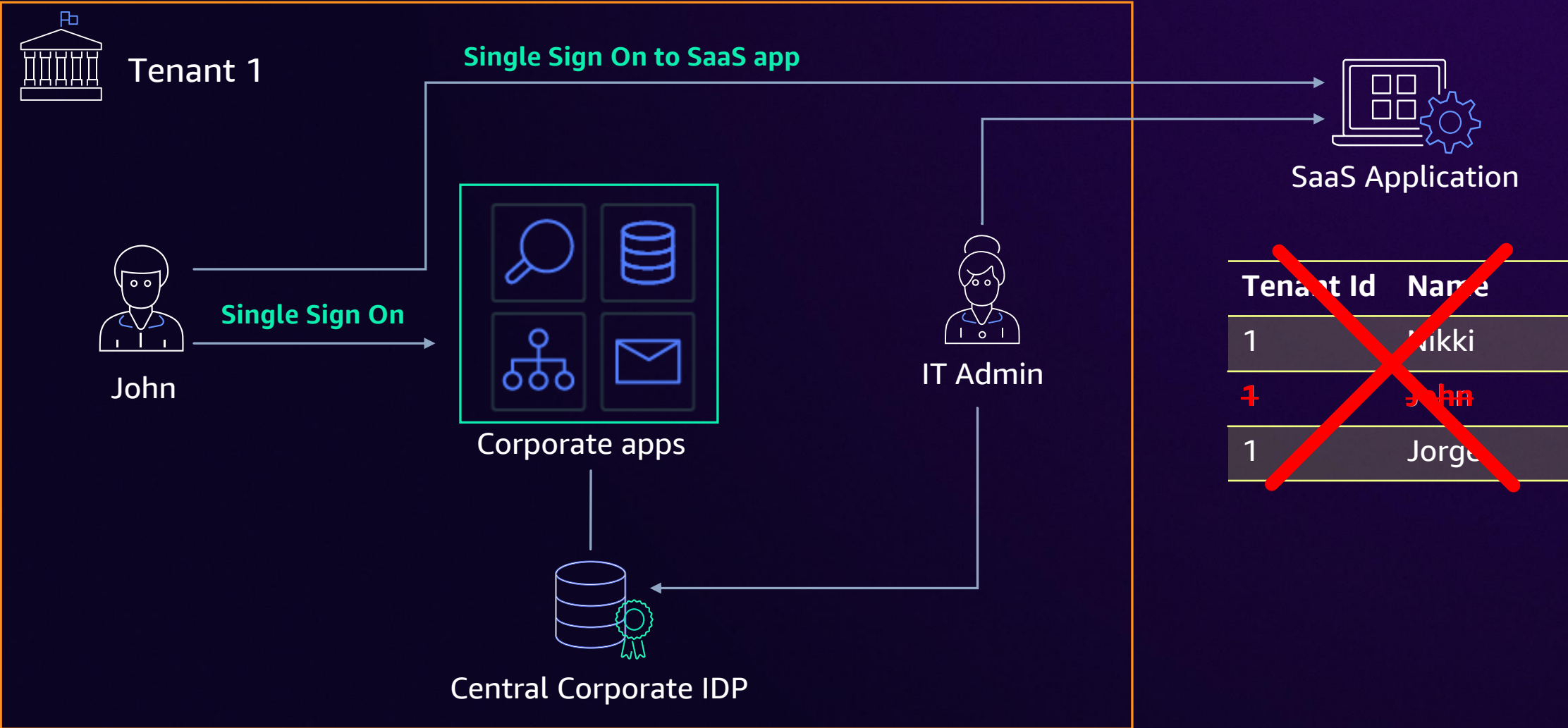


Tenant Id	Name
1	Nikki
1	John
1	Jorge

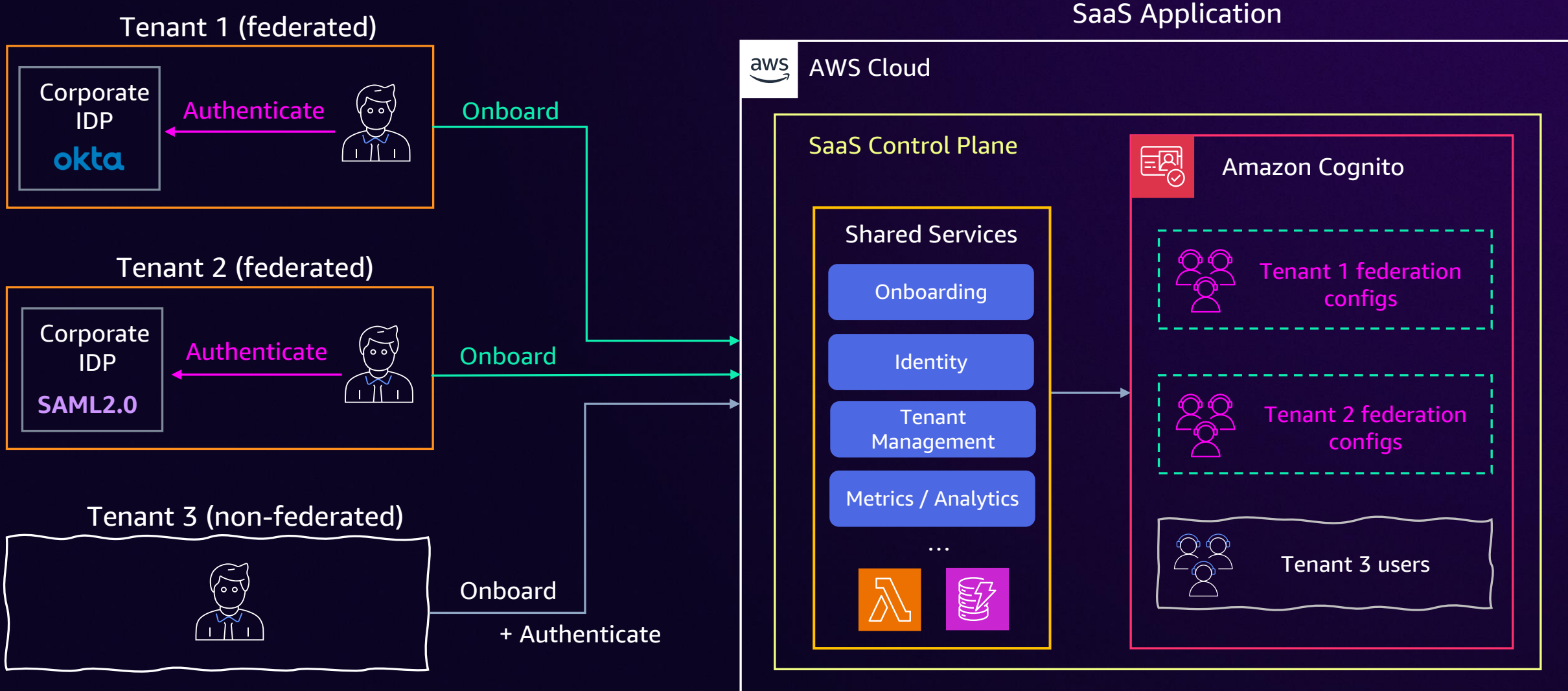
Tenants demand a “single source of identity”



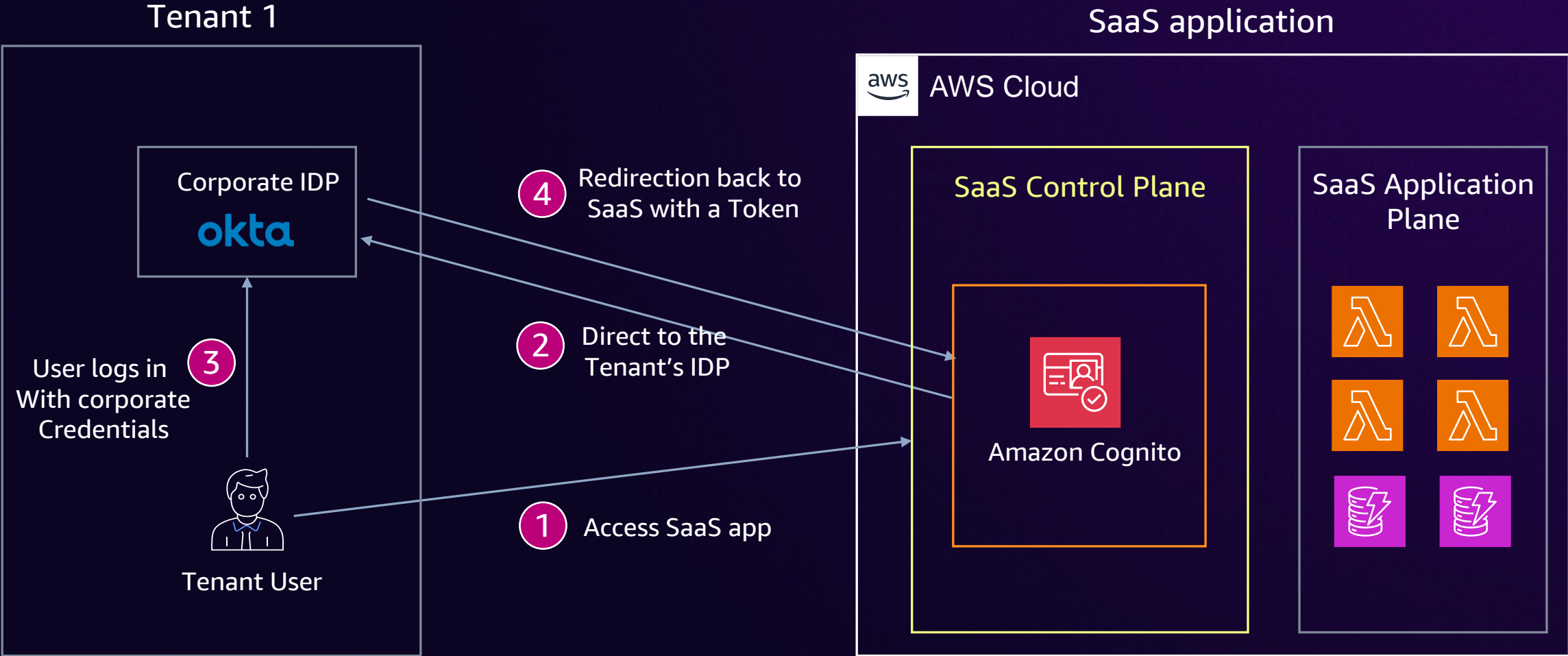
Tenants demand a "single source of identity"



SaaS need federated identity support

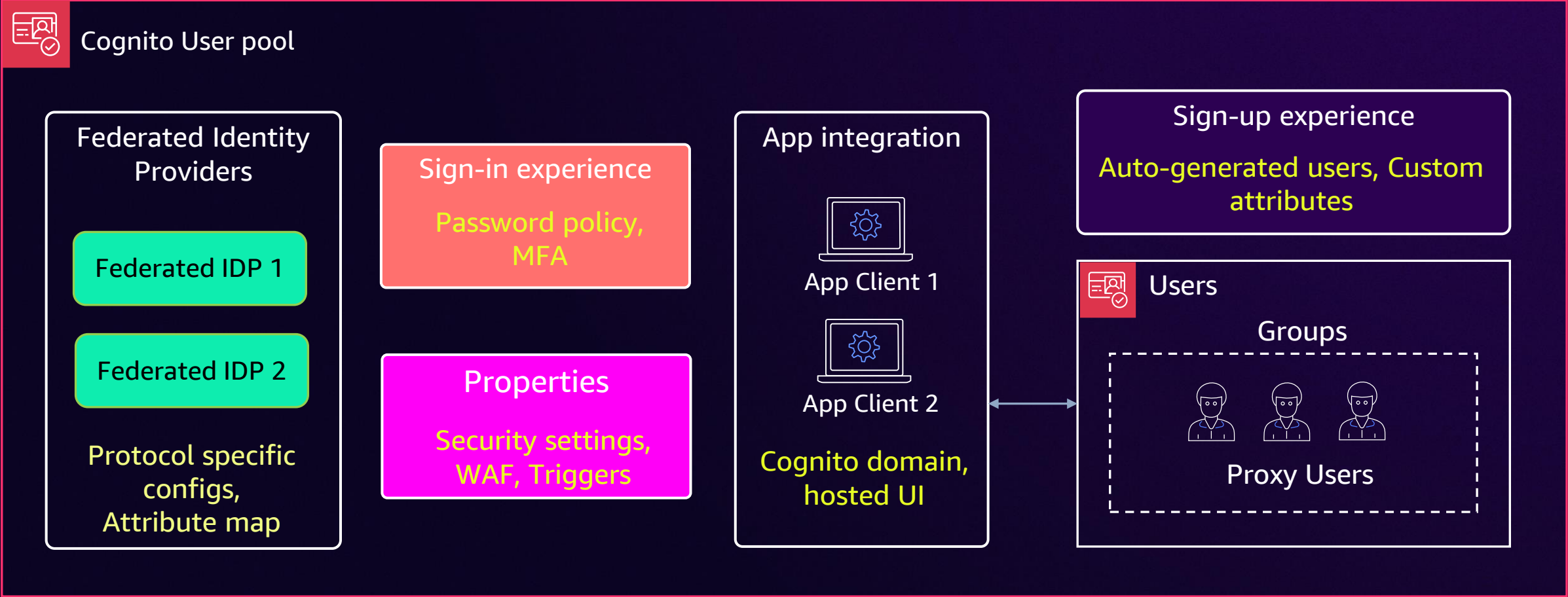


SaaS federated identity flow



Amazon Cognito as federated SaaS IDP

Cognito user pool elements that help to implement federated SaaS Identity



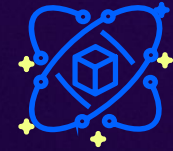
Federated SaaS identity – Challenges



Support both federation
with standard identity flow
in the SaaS



Need a generic way to
support IDP integrations



Still need to support
SaaS Identity = (user + tenant)
identity



Handle compliance, cost and
IDP quotas



Automate workflows for
seamless federated experience

Identity federation protocols



OAuth/OIDC

An identity layer on top of OAuth 2.0. Allows third-party apps to verify user identities



SAML 2.0

Simplifies the user authentication using XML based communication



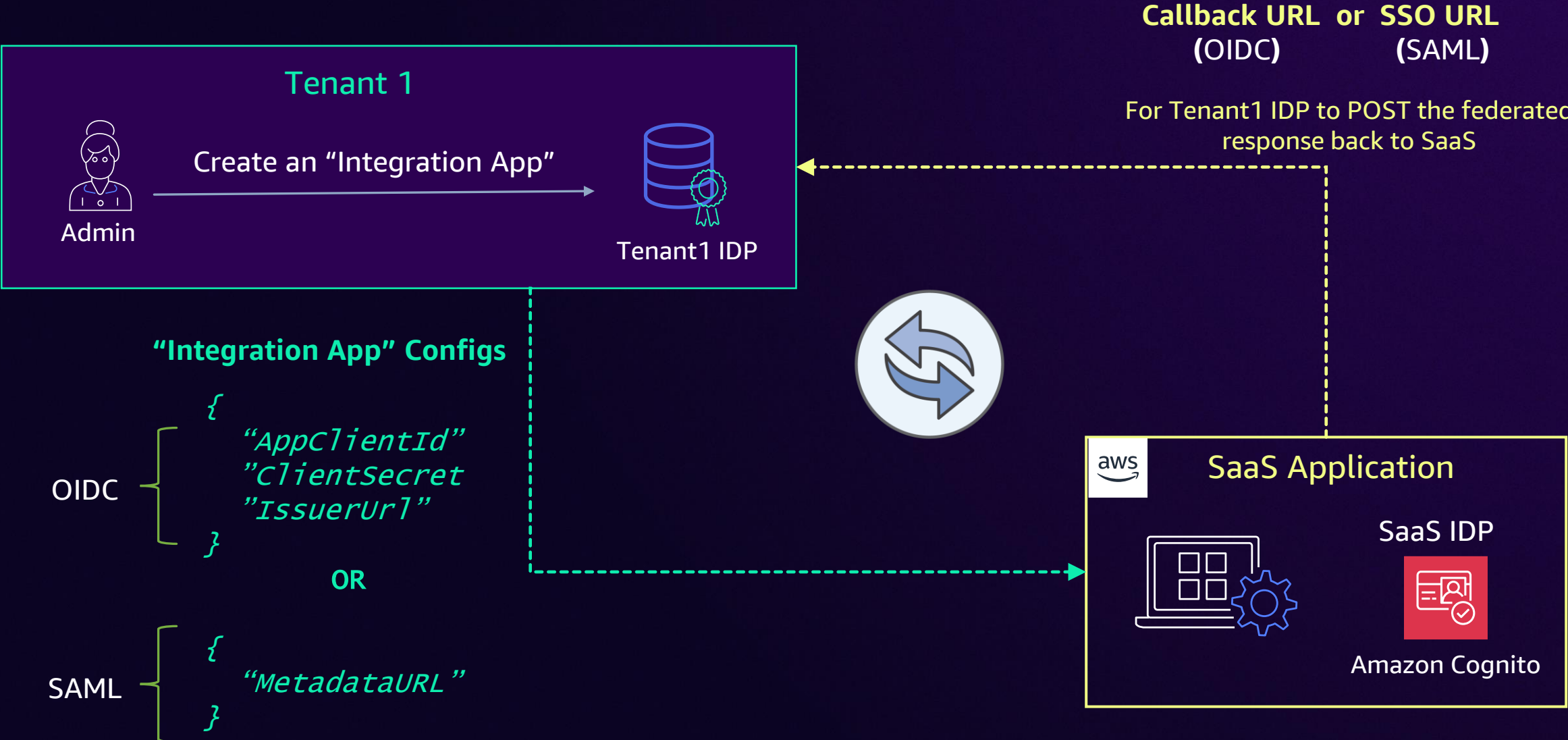
Social Providers

Sign-in through social identity providers such as Google, Amazon, Apple

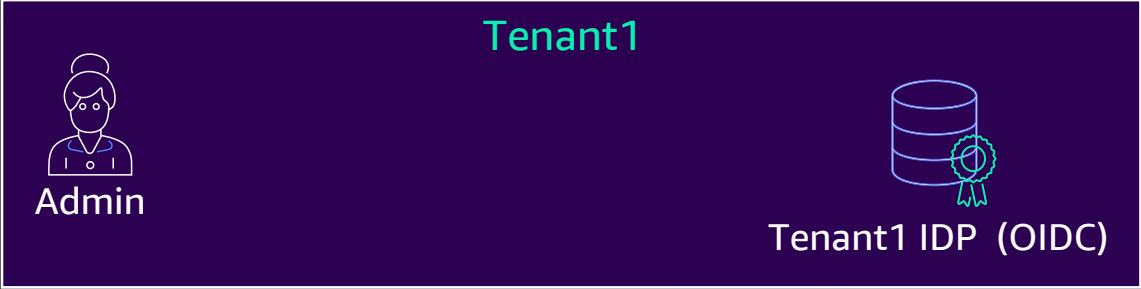
Tenant onboarding with federated identity setup



Tenant onboarding challenge



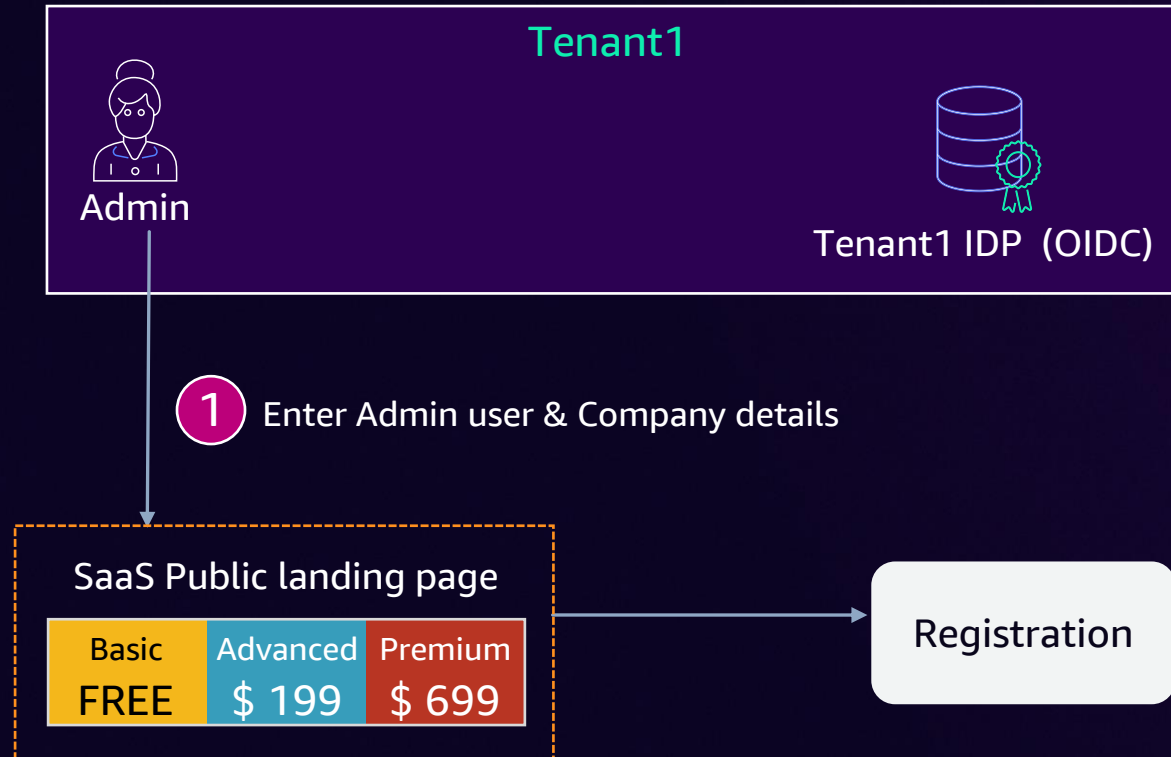
Flow 1 : Federated tenant onboarding



SaaS Public landing page

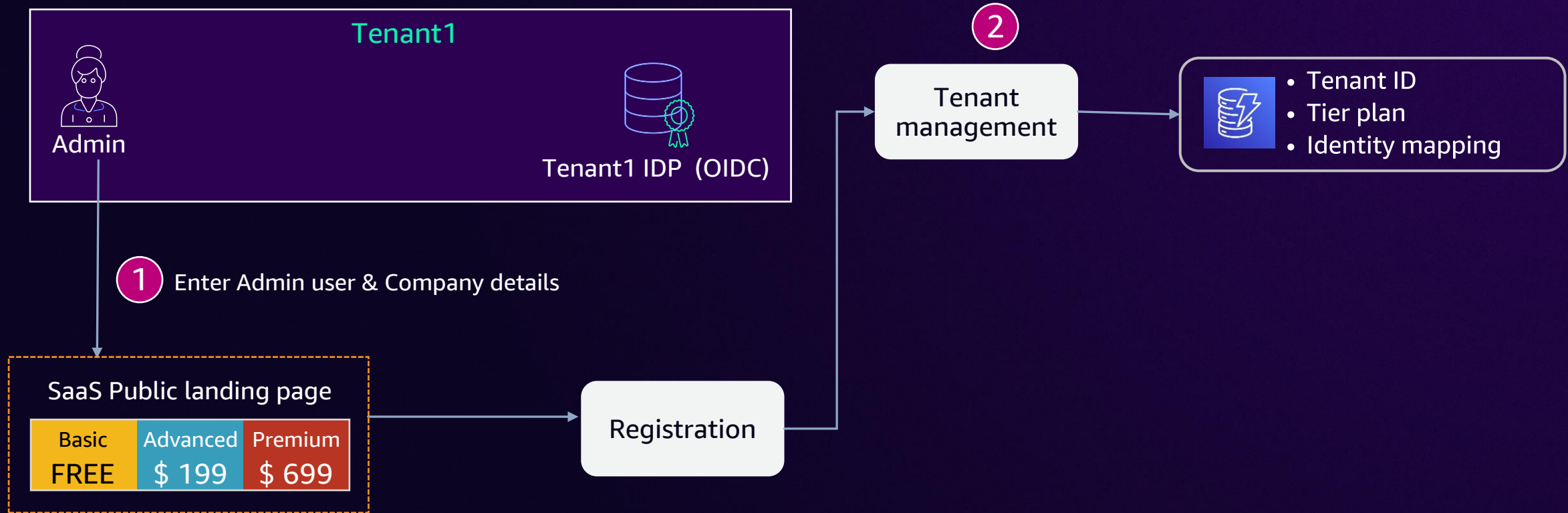
Basic	Advanced	Premium
FREE	\$ 199	\$ 699

Flow 1 : Federated tenant onboarding

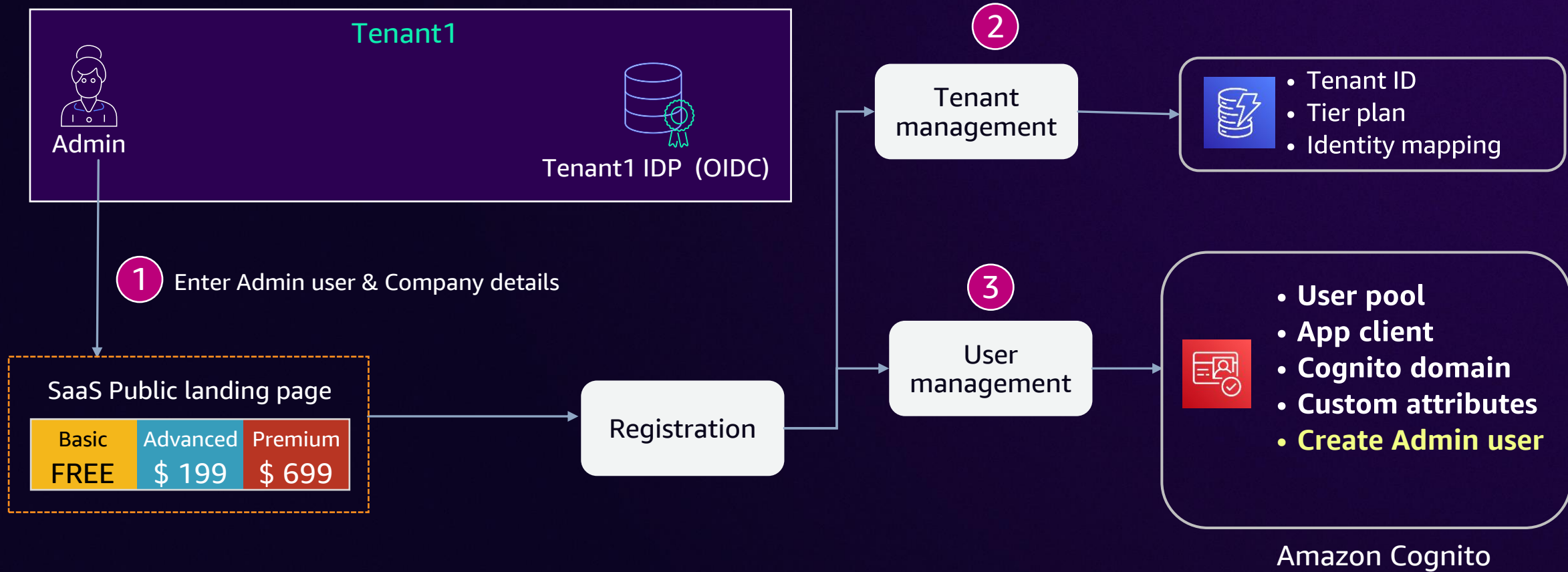


```
{  
  "adminName": "Jane Doe",  
  "adminEmail": "jane@tenant1.com",  
  "tier": "Premium",  
  "companyName": "Tenant1",  
  "companyURL": "https://tenant1.com"  
}
```

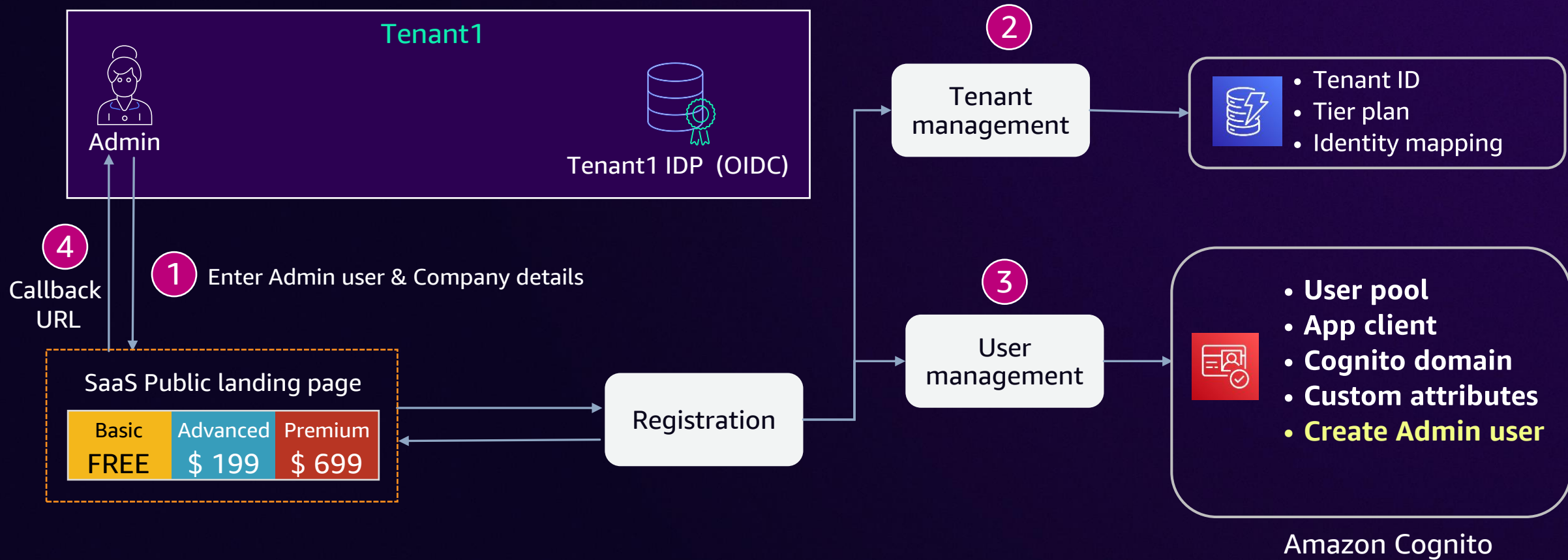
Flow 1 : Federated tenant onboarding



Flow 1 : Federated tenant onboarding

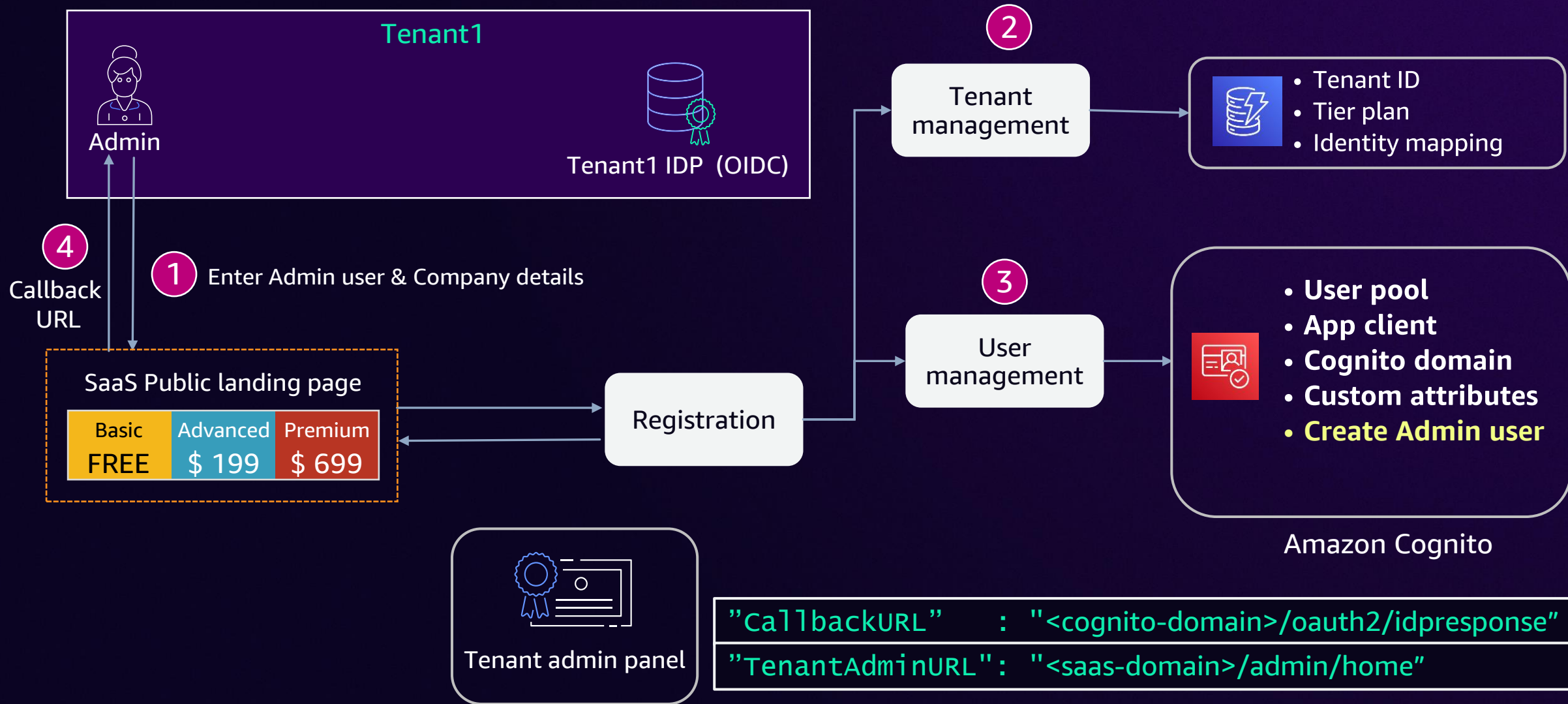


Flow 1 : Federated tenant onboarding

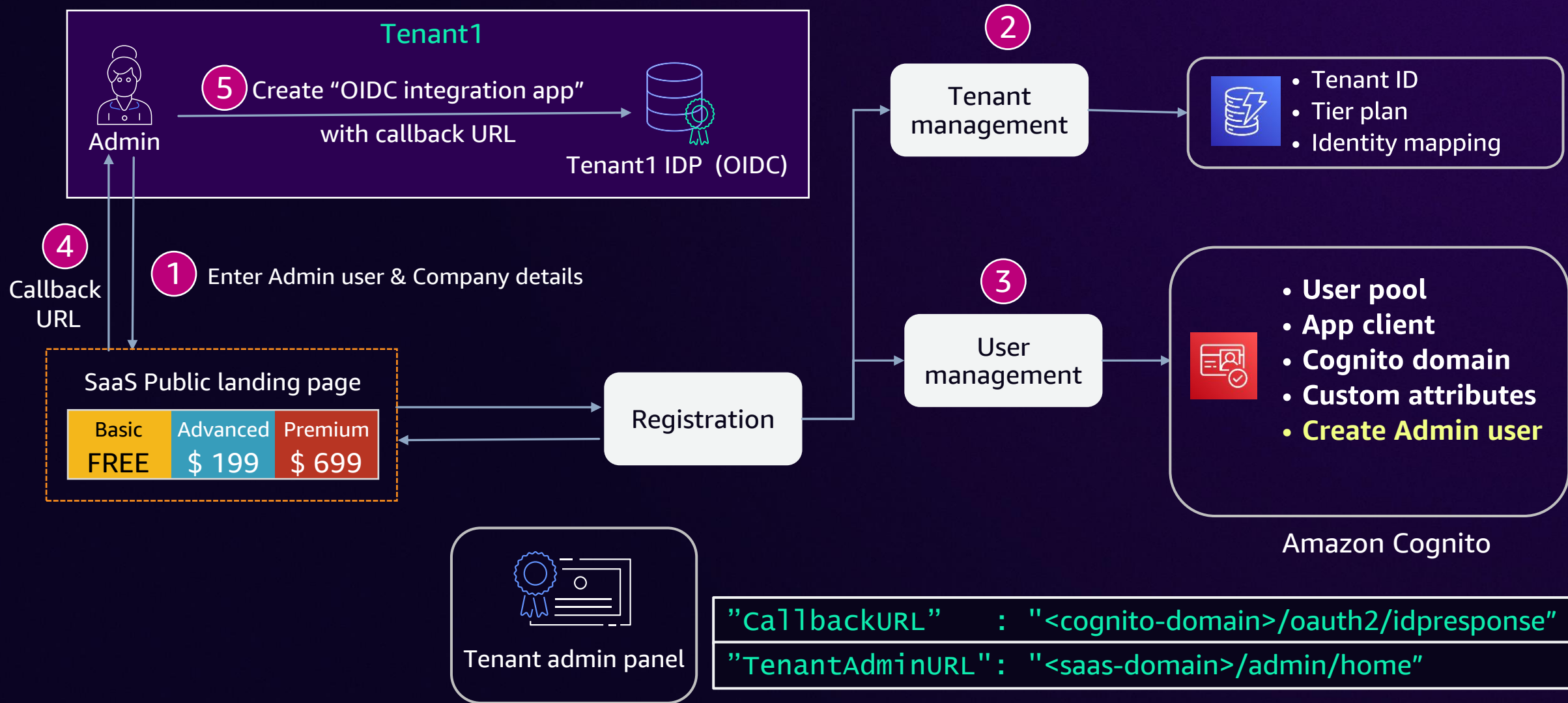


`"callbackURL"` : `"<cognito-domain>/oauth2/idpresponse"`

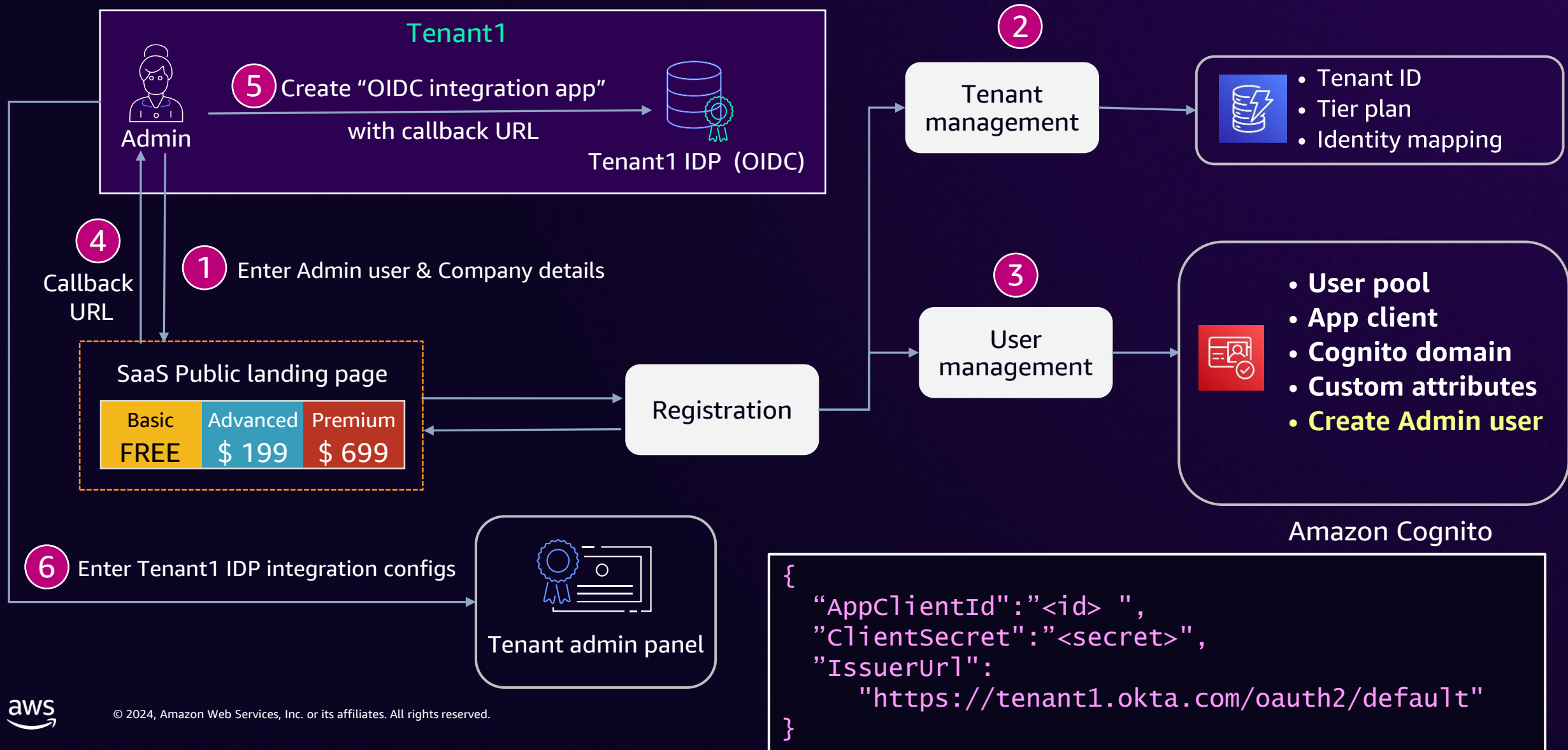
Flow 1 : Federated tenant onboarding



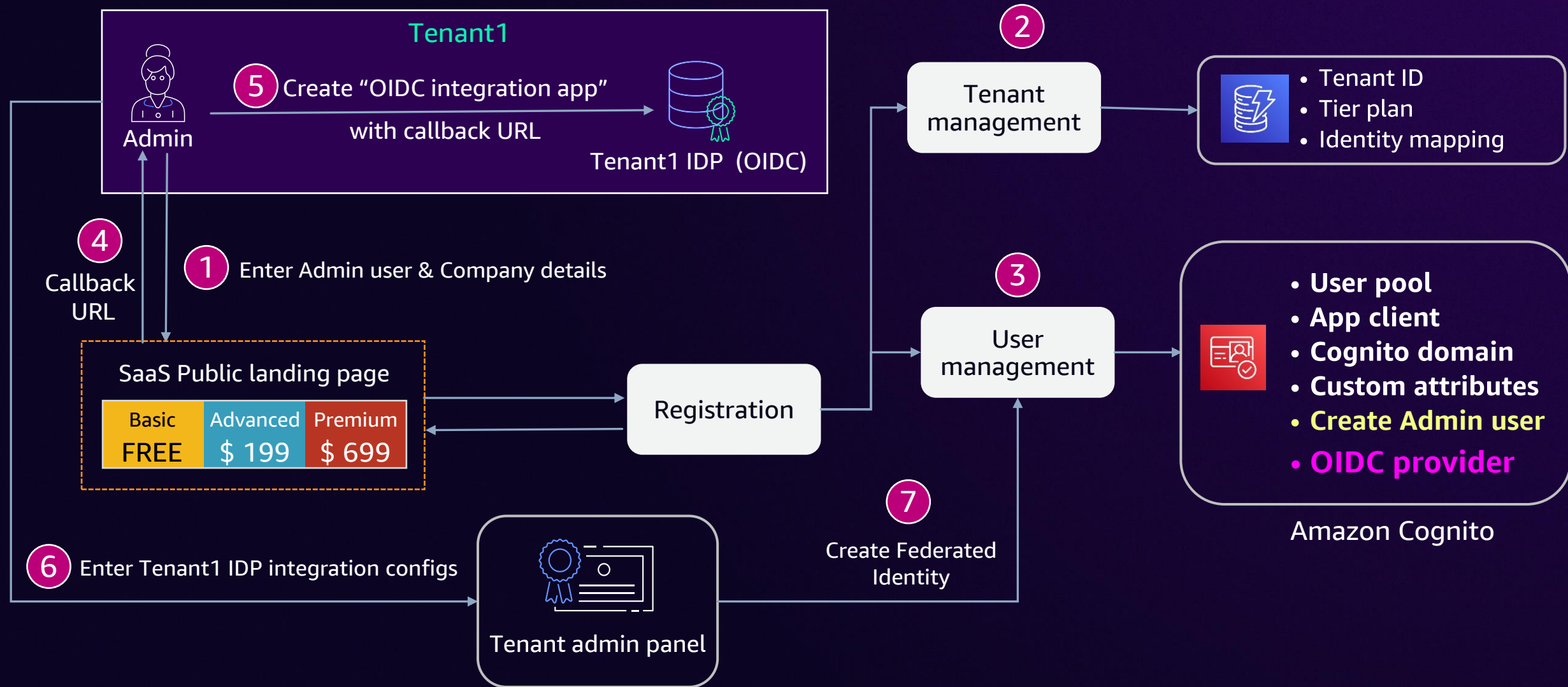
Flow 1 : Federated tenant onboarding



Flow 1 : Federated tenant onboarding



Flow 1 : Federated tenant onboarding



Amazon Cognito – OIDC provider

Identity provider information

Provider type

OIDC

Provider name

oktaoidc

Client ID

7asdna6az86hbOsdNHGIDD5d7

Client secret

assdg87YNKSJ7T_30W1j0vOYslsgweggsoc8bngoAiasdfdsg
Nyww2Refnl-_qa

Identifiers

-

Attribute request method

GET

Issuer

<https://anycompany.okta.com/oauth2/default>

Authorization endpoint

-

Flow 2 : Federated tenant onboarding

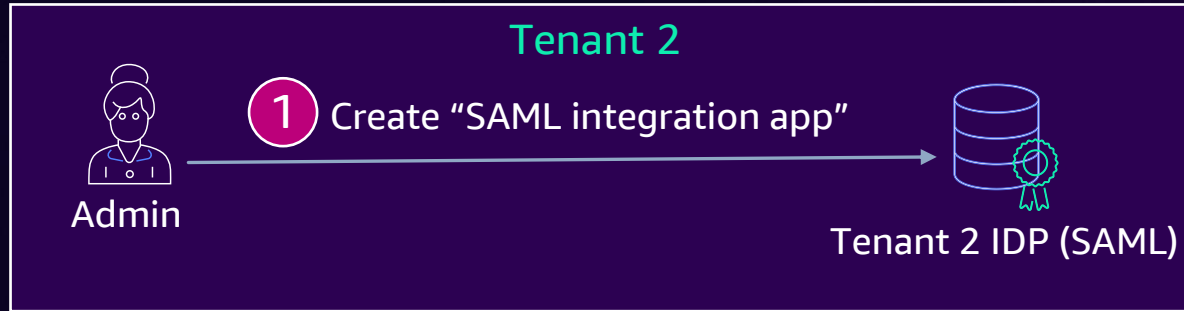


SaaS Public landing page

Basic	Advanced	Premium
FREE	\$ 199	\$ 699



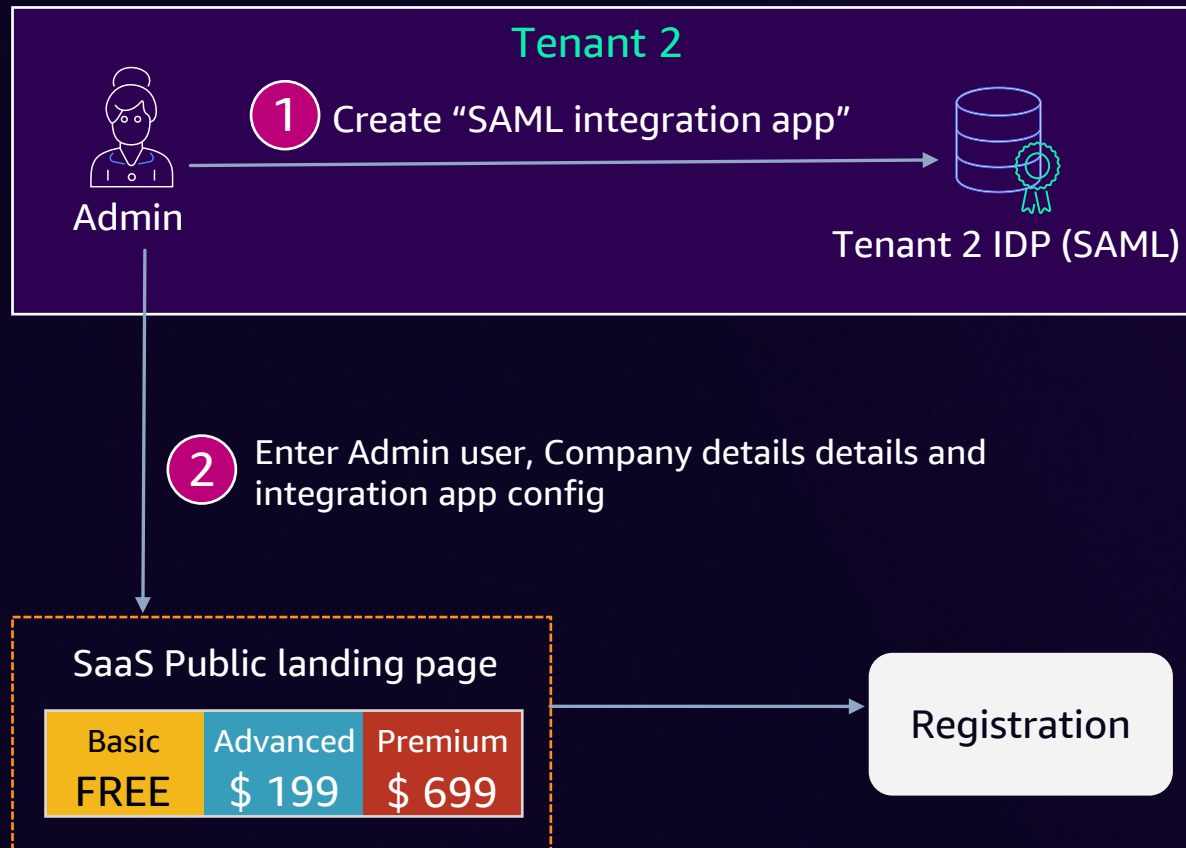
Flow 2 : Federated tenant onboarding



SaaS Public landing page

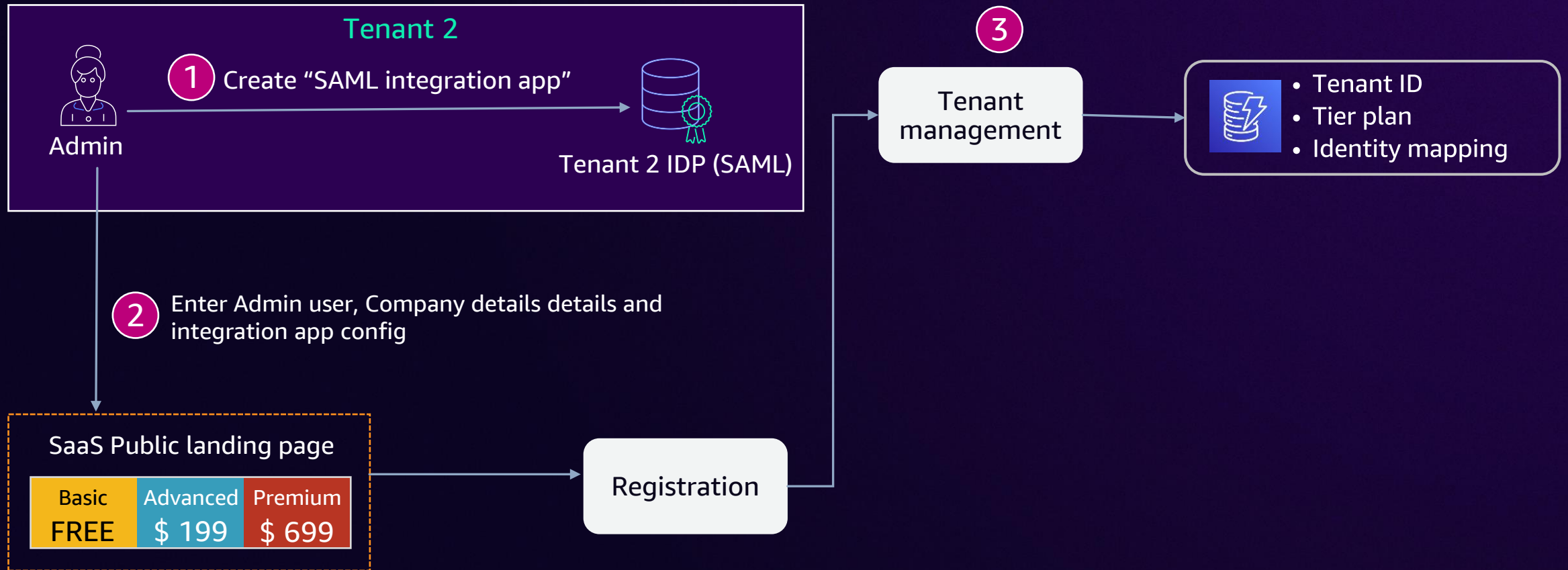
Basic	Advanced	Premium
FREE	\$ 199	\$ 699

Flow 2 : Federated tenant onboarding

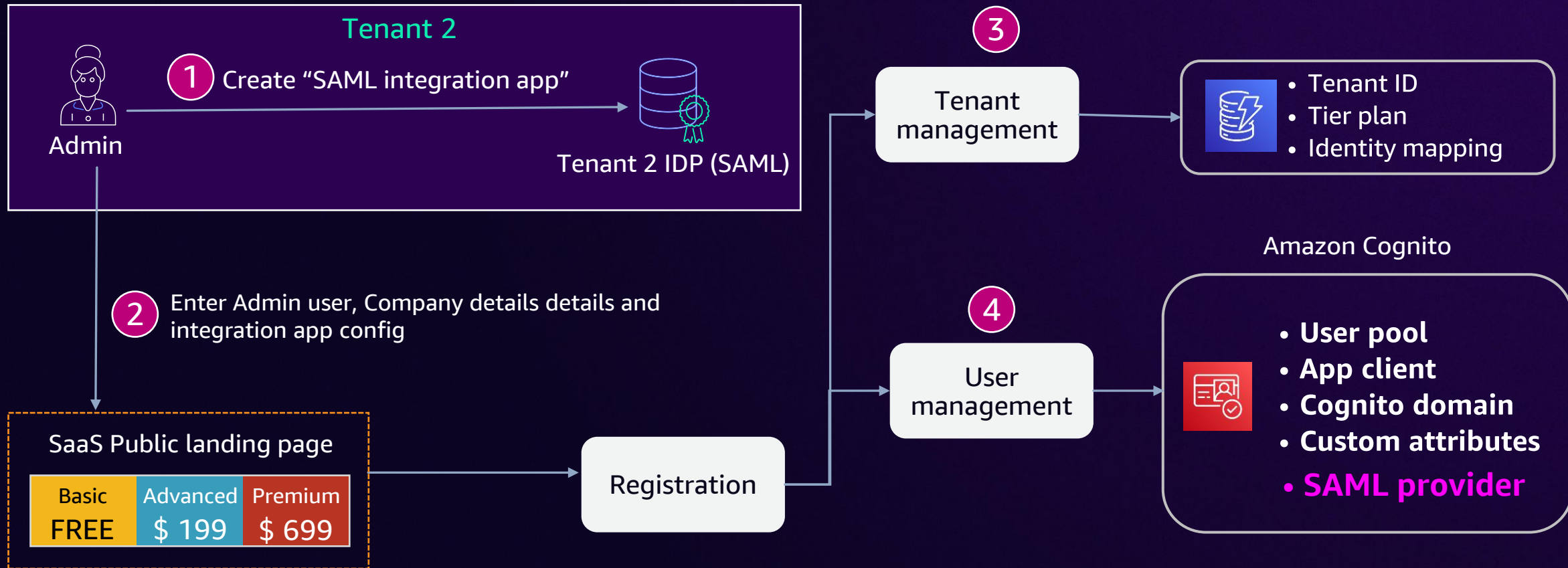


```
{  
  "adminName": " Jane Doe ",  
  "adminEmail": "jane@tenant2.com",  
  "tier": "Premium",  
  "companyName": "Tenant2",  
  "companyURL": " https://tenant2.com"  
  "MetadataURL":  
    "https://tenant2.okta.com/  
    <id>/sso/saml/metadata"  
}
```

Flow 2 : Federated tenant onboarding

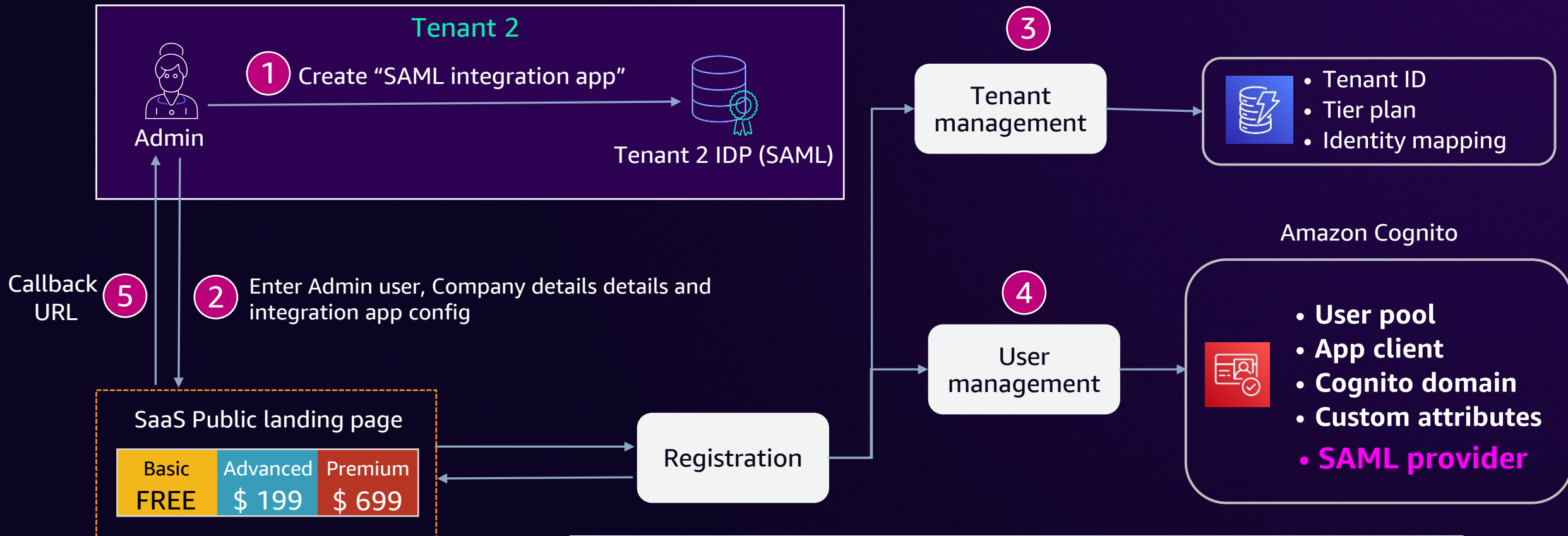


Flow 2 : Federated tenant onboarding



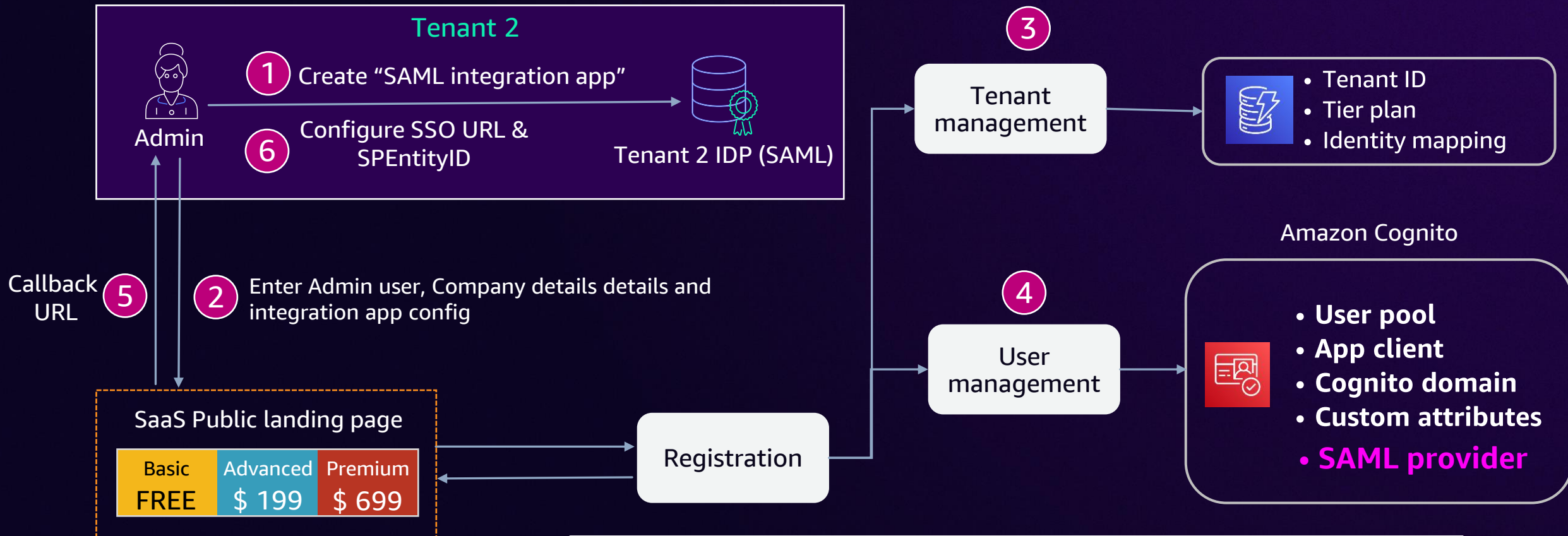
```
{  
  "MetadataURL":  
    "https://tenant2.okta.com/<id>/sso/saml/metadata"  
}
```

Flow 2 : Federated tenant onboarding



```
{  
  "SSOURL" : "<cognito-domain>/saml2/idpresponse",  
  "SPentityID": "urn:amazon:cognito:sp:<UserPoolId>"  
}
```

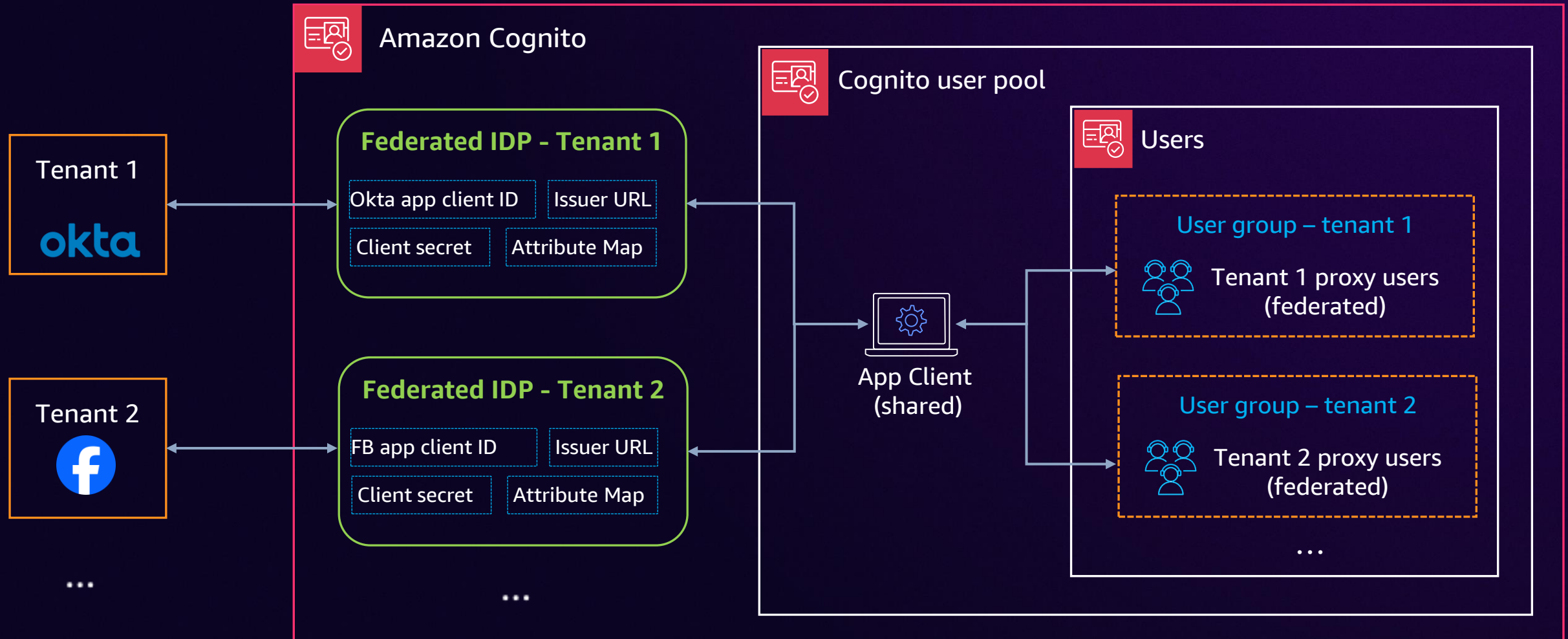
Flow 2 : Federated tenant onboarding



```
{  
  "SSOURL" : "<cognito-domain>/saml2/idpresponse",  
  "SPEntityID": "urn:amazon:cognito:sp:<UserPoolId>"  
}
```

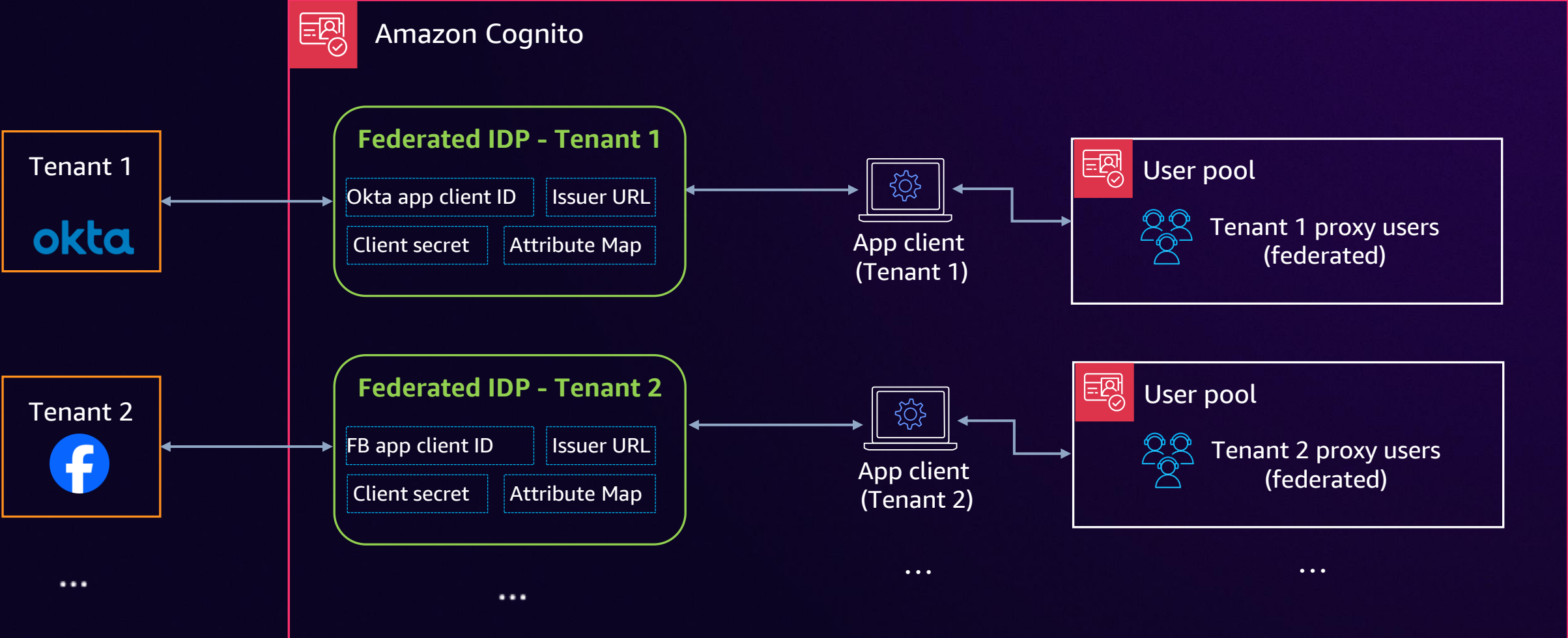
Cognito design – Pool model

Each tenant will have dedicated federated identity provider and shared App client with a shared user pool

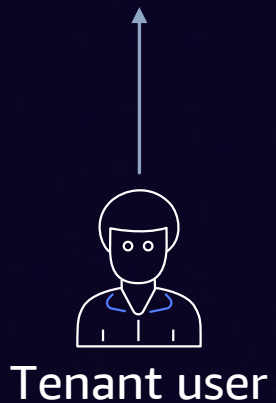
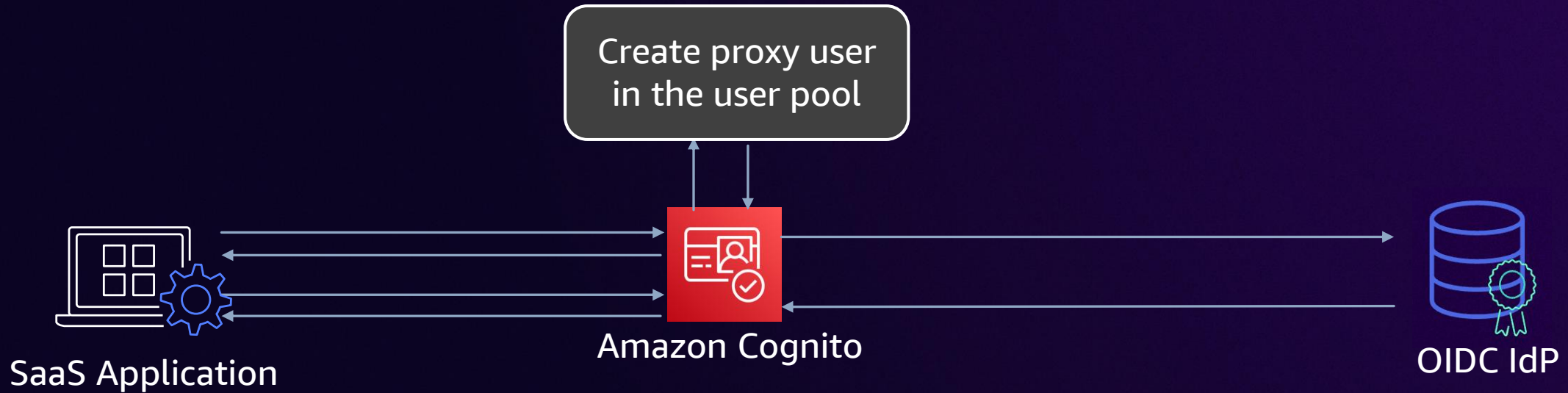


Cognito design – Silo model

Each tenant will have dedicated federated identity provider and dedicated user pool (and so an app client)



Federated tenant user login – OIDC



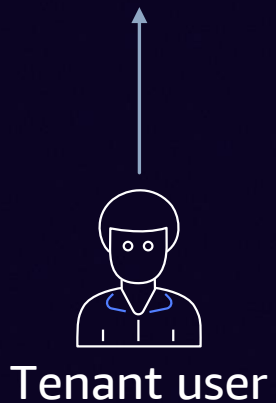
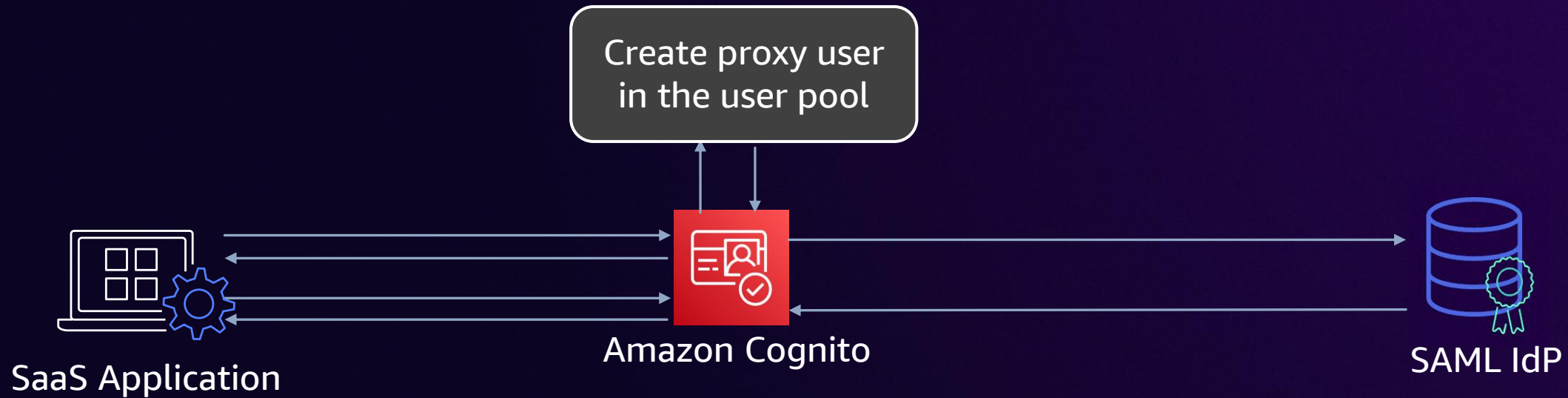
```
https://<cognito-domain>/oauth2/idpresponse?code=<code>
```

```
?client_id=<client_id>  
&redirect_uri=<redirect_uri>  
&scope=openid+profile+email  
&response_type=code  
&state=<state>
```

```
{  
  "access_token": "<access_token>",  
  "refresh_token": "<refresh_token>",  
  "expires_in": 3600,  
  "token_type": "Bearer"  
}
```

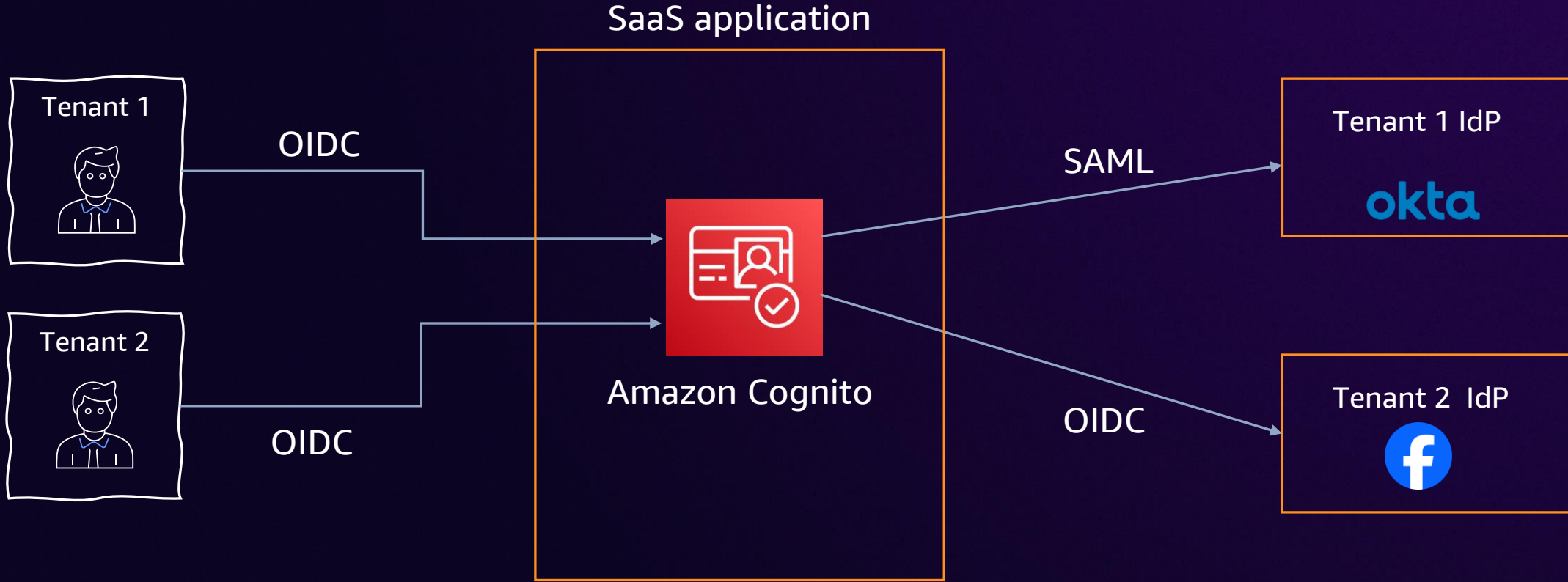
```
&code_challenge_method=S256
```


Tenant user login – Federated SAML flow



```
<cognito-domain>/oauth2/authorize?client_id=<Cognito Client Id>
&redirect_uri=<SaaS App URL>
&response_type=code
&scope=openid profile email
&code_challenge=<code challenge>
&code_challenge_method=S256
```

Cognito as a federation hub



Federated proxy users

Users (2) [Info](#)

View, edit, and create users in your user pool. Users that are enabled and confirmed can sign in to your user pool.



Delete user

Create user

Property: User name

< 1 >

	User name	Email address	Email verified	Confirmation status	Status
<input type="radio"/>	OktaOIDC_00u9zk52xj8pF0VeT5d7	bob@anycompany.com	No	External provider	✓ Enabled
<input type="radio"/>	OktaOIDC_00u9zk68vjaBuTqtT5d7	sally@anycompany.com	No	External provider	✓ Enabled

Groups (4) [Info](#)

Configure groups and add users. Groups can be used to add permissions to the access token for multiple users.

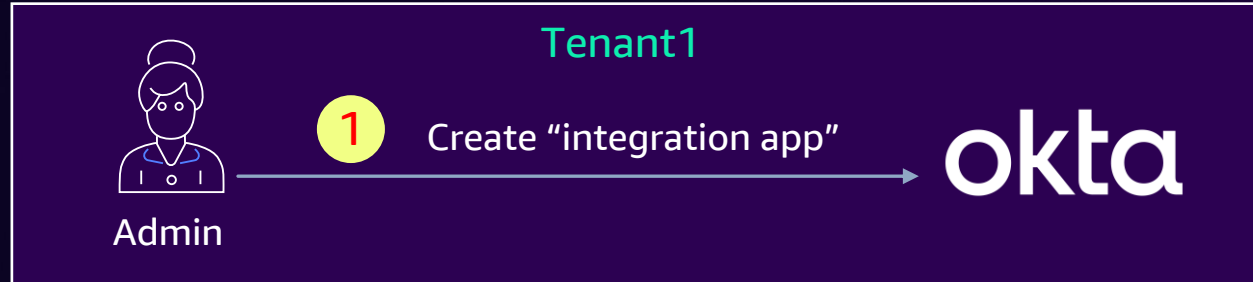
Delete

Create group

< 1 >

	Group name	Description	Precedence	Created time
<input type="radio"/>	us-west-2_fjbUmaKSz_OktaOIDC	Autogenerated group for users who sign in using OktaOIDC	-	2 years ago
<input type="radio"/>	us-west-2_fjbUmaKSz_OktaSAML	Autogenerated group for users who sign in using OktaSAML	-	4 weeks ago

Attribute mapping – Tenant IDP



Maps user attributes from tenant IDP to standard OIDC attributes for handshaking

The screenshot shows the Okta configuration interface for attribute mapping. On the left, the "Okta User User Profile" is selected, with the user "user" chosen. On the right, the "Cognito-Test User Profile" is selected, with the user "appuser" chosen. A note states "Username is set by Cognito-Test · Override with mapping". Three attribute mappings are shown, each with a green arrow pointing from the Okta attribute to the Cognito-Test attribute:

Okta Attribute	Cognito-Test Attribute	Target Type
user.firstName	given_name	string
user.lastName	family_name	string
user.email	email	string

Cognito attribute mappings – OIDC

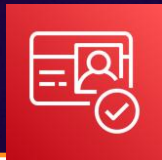
Maps attributes from OIDC ID Token to the Cognito user profile attributes

User pool attribute	OpenID Connect attribute	
name	name	Remove
given_name	given_name	Remove
family_name	family_name	Remove
email	email	
username	sub	Remove
Add another attribute		

Cognito attribute mappings – SAML

okta

Name	Name Format	Value
<code>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</code>	Basic	user.email
<code>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name</code>	Basic	user.firstName
<code>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname</code>	Basic	user.lastName



User pool attribute	SAML attribute
email	<code>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</code>
family_name	<code>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname</code>
name	<code>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name</code>

Cognito Lambda triggers

User Pool Flow	Operation	Description
Custom Authentication Flow	Define Auth Challenge	Determines the next challenge in a custom auth flow
	Create Auth Challenge	Creates a challenge in a custom auth flow
	Verify Auth Challenge Response	Determines if a response is correct in a custom auth flow
Authentication Events	Pre authentication Lambda trigger	Custom validation to accept or deny the sign-in request
	Post authentication Lambda trigger	Logs events for custom analytics
	Pre token generation Lambda trigger	Augments or suppresses token claims
Sign-Up	Pre sign-up Lambda trigger	Performs custom validation that accepts or denies the sign-up request
	Post confirmation Lambda trigger	Adds custom welcome messages or event logging for custom analytics
	Migrate user Lambda trigger	Migrates a user from an existing user directory to user pools
Messages	Custom message Lambda trigger	Performs advanced customization and localization of messages
Token Creation	Pre token generation Lambda trigger	Adds or removes attributes in Id tokens
Email and SMS third-party providers	Custom sender Lambda triggers	Uses a third-party provider to send SMS and email messages



Adding the tenant context and custom attributes



Inside the Lambda trigger

```
1  export const handler = async (<
2  |  event: PostConfirmationTriggerEvent,
3  |  context: Context
4  >): Promise<any> => {
5  |  const email = event.request.userAttributes.email;
6  |  const tenantId = await DynamoDB.fetchTenantId(email);
7  |  const client = new CognitoIdentityProviderClient({ region: process.env.AWS_REGION });
8  |  const input = {
9  |  |  UserPoolId: event.userPoolId,
10 |  |  Username: event.userName,
11 |  |  UserAttributes: [
12 |  |  |  {
13 |  |  |  |  Name: 'custom:tenant-id',
14 |  |  |  |  Value: tenantId,
15 |  |  |  |  },
16 |  |  |  ],
17 |  |  };
18 |  const command = new AdminUpdateUserAttributesCommand(input);
19 |  await client.send(command);
20 |  return event;
21 |  };
```



Company identifier	Tenant ID
saascompany.com	AB4CD5034208
anycompany.com	06EC0C83E010

User sign-in – Default behavior

Sign in with your corporate ID

SaaSCompany-SAML

AnyCompany-OIDC

or

Sign in with your username and password

Username

Username

Password

Password

Sign In

Identity providers [Info](#)

Select the identity providers that will be available to this app client.

Select identity providers

- AnyCompany-OIDC X
- Cognito user pool X
Users can sign in to Cognito using an email, phone number, or username.
- SaaSCompany-SAML X



Dynamically select the correct provider



Configure your client

Identity provider: SaaSCompany-SAML [Info](#) [Delete](#)

Identity provider information [View signing certificate](#) [View encryption certificate](#) [Edit](#)

Provider type SAML	Identifiers saascompany.com	Created time October 22, 2024 at 08:32 PDT
Provider name SaaSCompany-SAML	Sign out flow Disabled	Last updated time October 22, 2024 at 11:23 PDT
IdP-initiated SAML sign-in Require SP-initiated SAML assertions	SAML signing and encryption -	

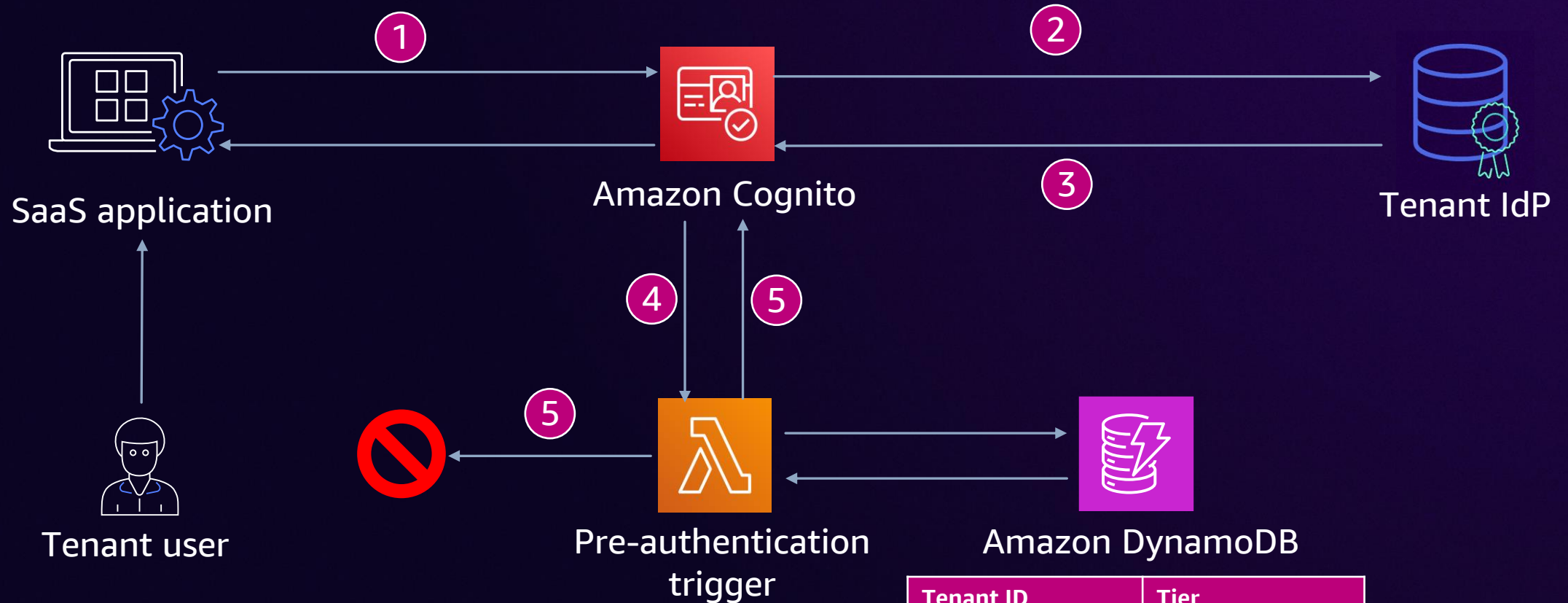
```
https://<cognito-domain>/oauth2/authorize
?client_id=<Cognito Client Id>
&redirect_uri=<SaaS App URL>
&response_type=code
&code_challenge=<code challenge>
&code_challenge_method=S256
&idp_identifier=saascompany.com
&identity_provider=SaaSCompany-SAML
&login_hint=joe@saascompany.com
```

The image shows an Okta 'Sign In' page. At the top is the Okta logo. Below it is the text 'Sign In'. There are two buttons for 'Sign in with your corporate identity': 'SaaSCompany' and 'AnyCompany'. The 'SaaSCompany' button is highlighted with an orange arrow pointing to the 'Username' field. The 'Username' field contains 'joe@saascompany.com'. Below it is the 'Password' field. There is a 'Remember me' checkbox and a blue 'Sign In' button. At the bottom, there is a link for 'Need help signing in?' and a QR code on the right side.

Special considerations



Handling entitlements



Federated considerations with Cognito

- A deeper understanding of OAuth 2.0/OIDC is helpful for understanding Cognito's mental model
- Quotas (both resource and rate) are in effect
- Price goes up a bit
 - SAML/OIDC federation MAU cost is more than user pool/social
- Cognito identity pools are NOT at play here



Quotas



Pricing

Summary

- Federation has more moving parts, but is automatable
- Cognito is a federation hub
- Lambda triggers for customization
- Reconcile user differences with mapping
- Automatically pick federated IdP when pooled
- Unify federated and unfederated in a single onboarding process

Thank you!

Toby Buckley

tobuck@amazon.com

Dhammika Sriyananda

sriyana@amazon.com



Please complete the session survey in the mobile app