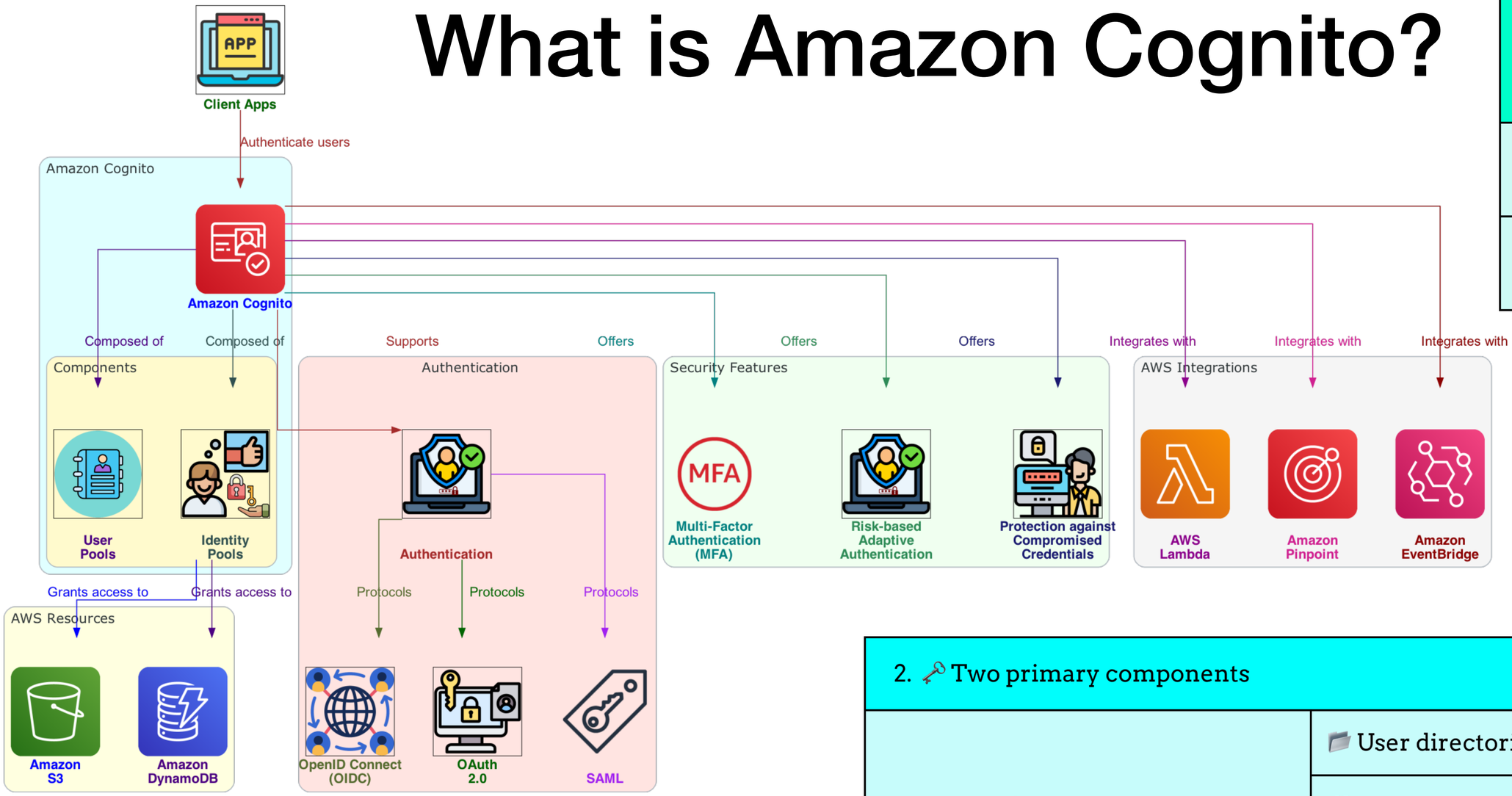
Amazon Cognito

Table of Contents

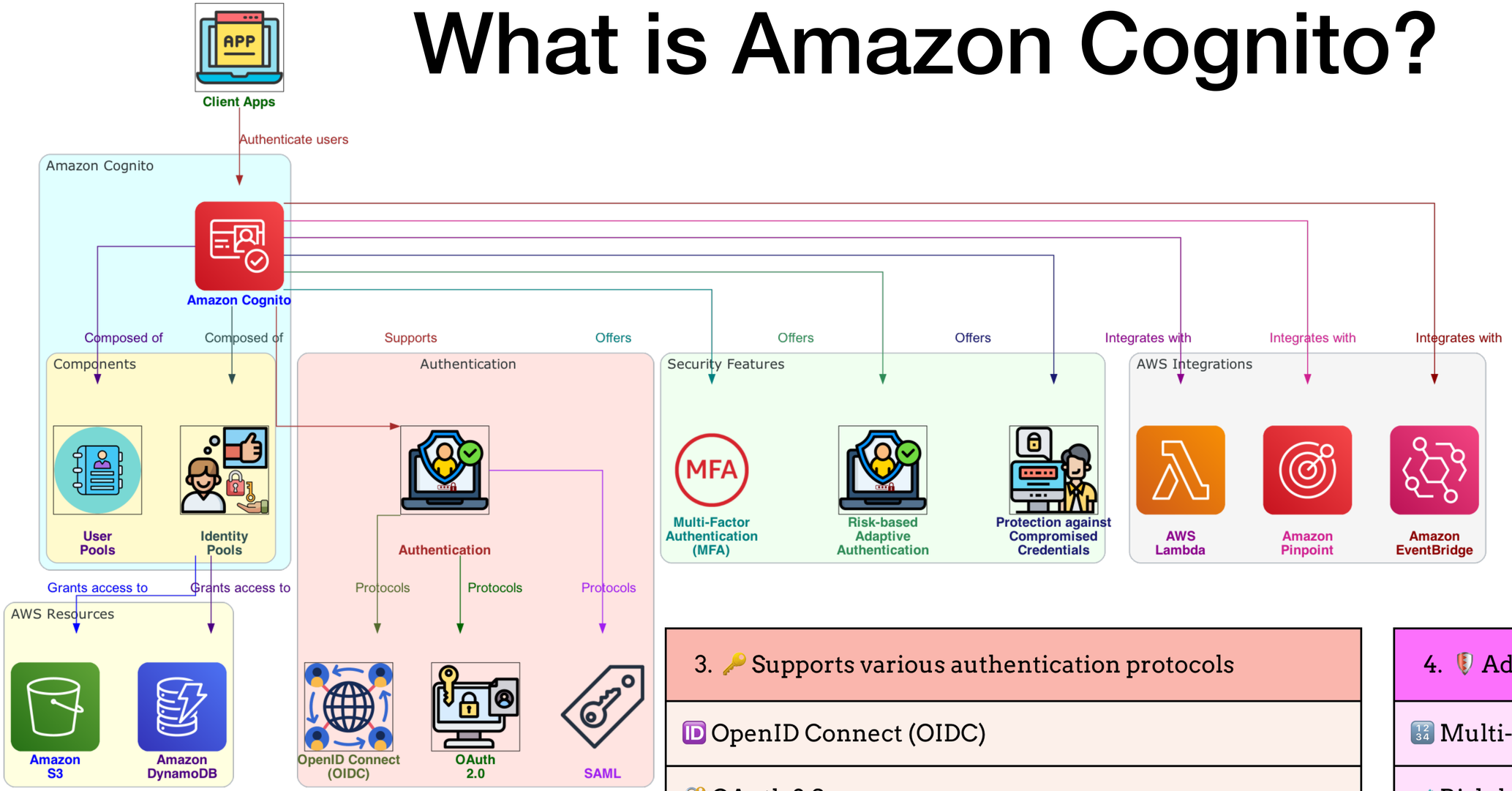
What is Amazon Cognito?

1. 🌐 Cloud-based identity and access management service
🧊 Manages user identities, authentication, authorization
🕸️ For web and mobile applications



2. 🗝️ Two primary components	
👥 User pools	🗂️ User directories
	🔐 Sign up, sign in methods
	🧊 Username/password, social media, SAML
🆔 Identity pools	🔑 Grants access to AWS resources, services
	📦 S3, DynamoDB

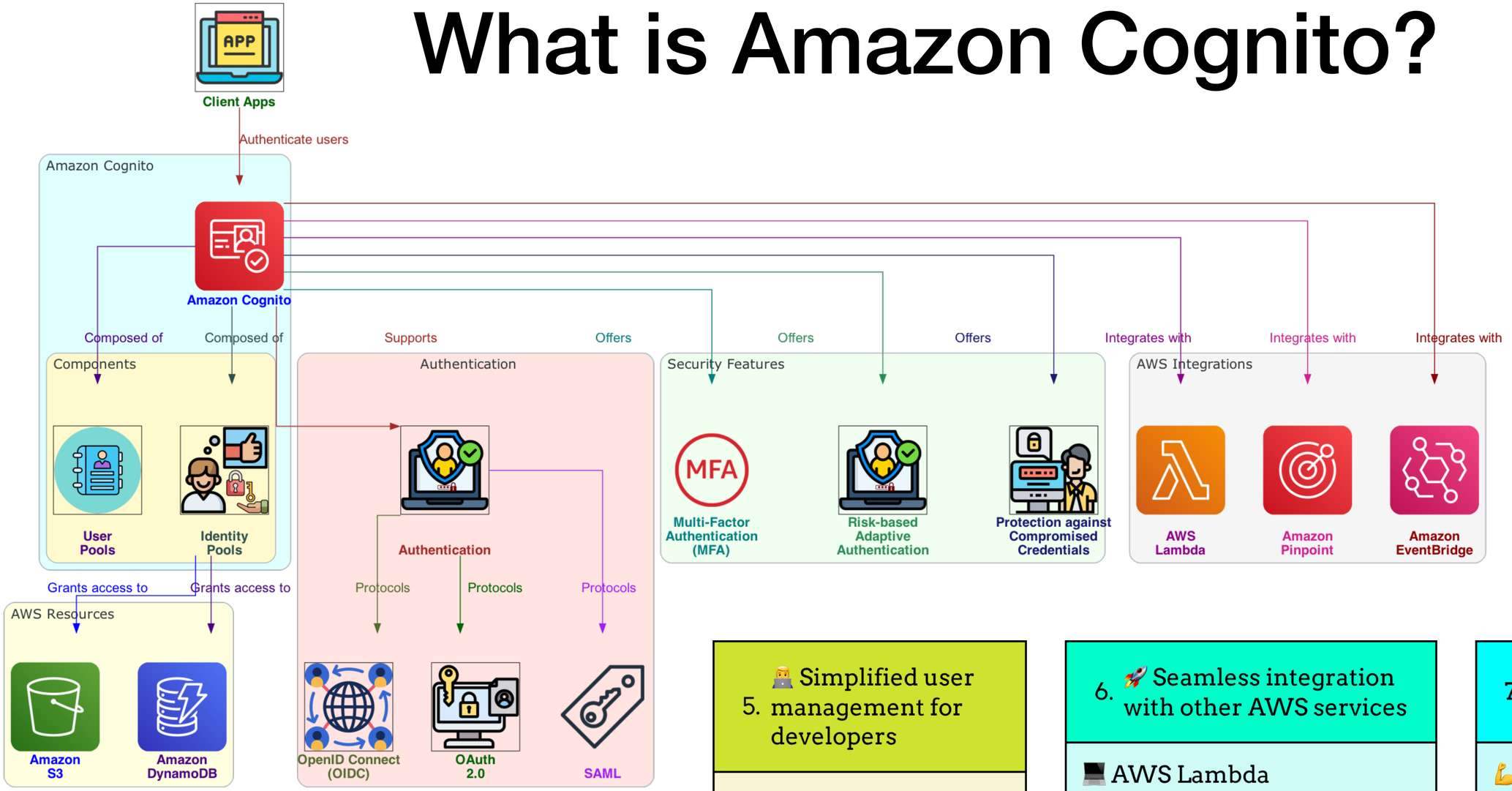
What is Amazon Cognito?



3. 🔑 Supports various authentication protocols
🆔 OpenID Connect (OIDC)
🔐 OAuth 2.0
🛡️ Security Assertion Markup Language (SAML)
🌉 Enables seamless integration with identity providers
📱 Ensures compatibility across platforms

4. 🛡️ Advanced security features
🔢 Multi-factor authentication (MFA)
🎯 Risk-based adaptive authentication
🔐 Protection against compromised credentials
🔒 Enhances security of user identities, data

What is Amazon Cognito?

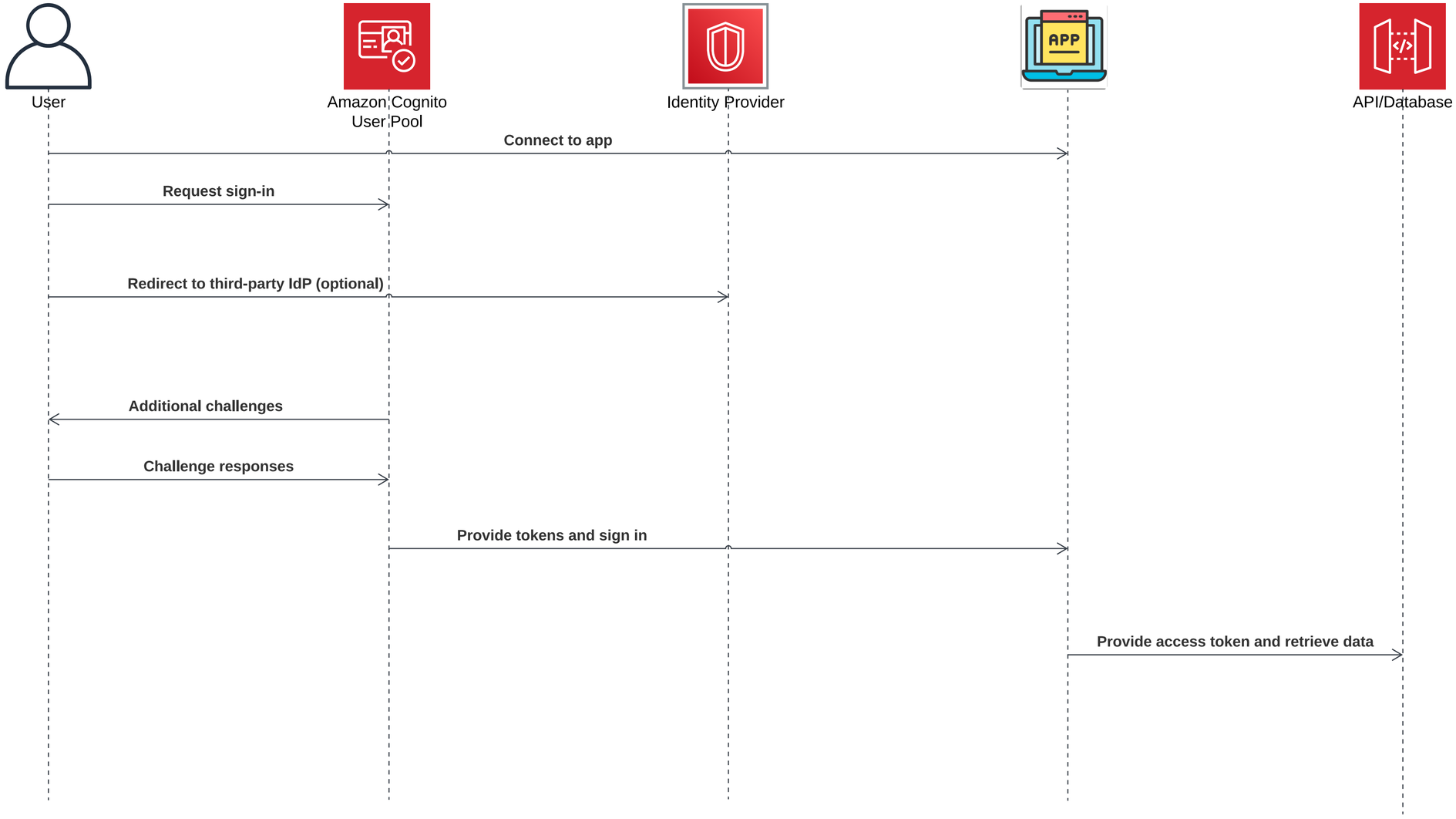


5. 🤷 Simplified user management for developers
🎯 Focus on application development
🚫 Eliminates managing complex identity infrastructure

6. 🚀 Seamless integration with other AWS services
💻 AWS Lambda
📊 Amazon Pinpoint
🧩 Comprehensive solution for app management

7. 📈 Scalable and ideal for complex applications
💪 Robust features
📈 Scales with growing user bases
🔧 Accommodates evolving requirements

User Pools



1. 🔒 Authenticate and authorize users

📱 To your app or API

2. 📂 User directory

🙋‍♂️ Self-service user creation, management, authentication

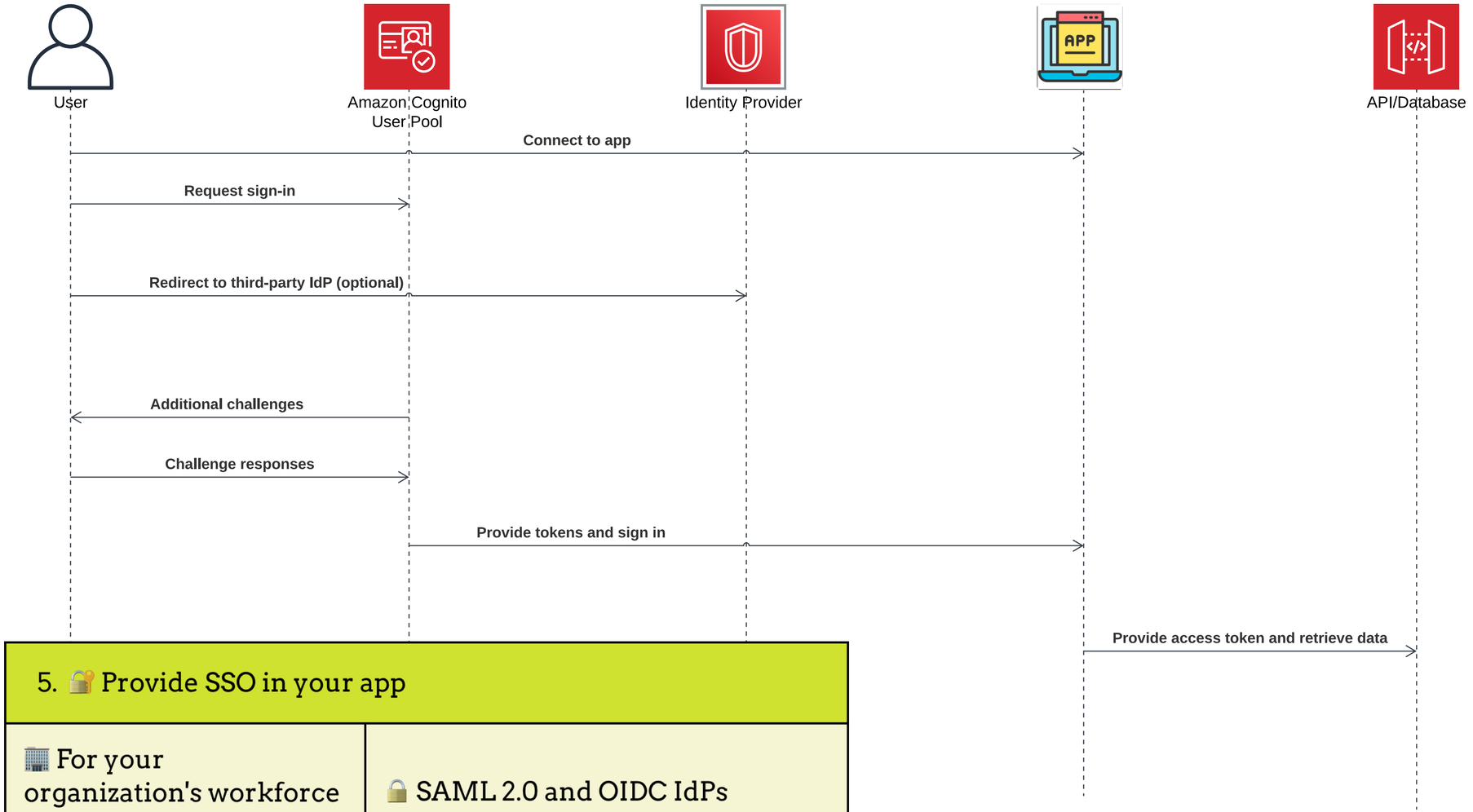
👨‍💼 Administrator-driven user creation, management, authentication

3. 🆔 Can be independent directory and OIDC IdP

4. 🌉 Can be intermediate SP to third-party providers

👥 Workforce and customer identities

User Pools



5. 🔐 Provide SSO in your app

🏢 For your organization's workforce identities	🔒 SAML 2.0 and OIDC IdPs	
👥 For your organization's customer identities	🔑 Public OAuth 2.0 identity stores	🅰️ Amazon
		🔍 Google
		🍎 Apple
		👍 Facebook

6. 🚫 Don't require integration with an identity pool

7. 🎫 Can issue authenticated JWTs directly

- 📱 To an app
- 🌐 To a web server
- 🖥️ To an API

Identity Pools

Amazon Cognito Identity Pool

Identity provider or Amazon Cognito user pool

STS

Authenticate and request token or assertion (optional)

Developer authorization, token or assertion

Request role

Role credentials

1. 🔑 Authorize users to access AWS resources
   - ✅ Authenticated users
   - 👤 Anonymous users
2. 🪪 Issues AWS credentials for your app
   - 🌐 To serve resources to users
3. 🔐 Authenticate users with trusted identity providers
   - 📂 User pool
   - 🛡️ SAML 2.0 service
4. 🎟️ Can optionally issue credentials for guest users

Identity Pools

Amazon Cognito Identity Pool

Identity provider or Amazon Cognito user pool

STS

Authenticate and request token or assertion (optional)

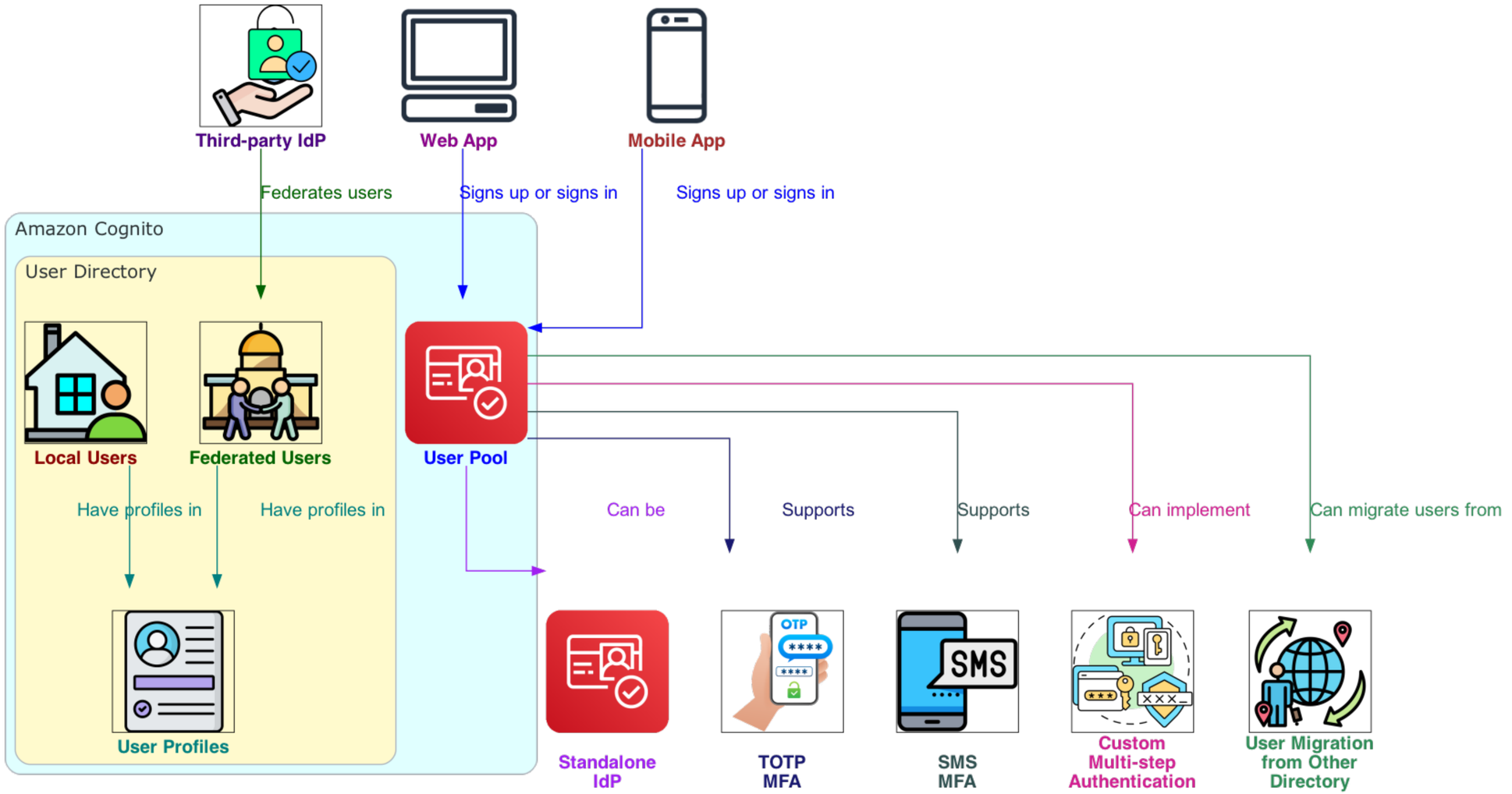
Developer authorization, token or assertion

Request role

Role credentials

5. 🚦 Manage users' authorization to access AWS resources
   - 🎭 Role-based access control
   - 🩹 Attribute-based access control
6. 🚫 Don't require integration with a user pool
7. 🤝 Can accept authenticated claims directly
   - 👔 From workforce identity providers
   - 👥 From consumer identity providers

User Pools Detailed



1. 📁 User directory for web and mobile apps

🖥️ Users sign in through Amazon Cognito

2. 🔑 Supports local and federated user sign-in

👤 Local users (Amazon Cognito)

🌐 Federated users (third-party IdP)

3. 👤 User profiles for local and federated users

📁 Stored in Amazon Cognito user pool

4. 🔧 Manage user profiles

🖥️ AWS Management Console

💻 AWS SDK

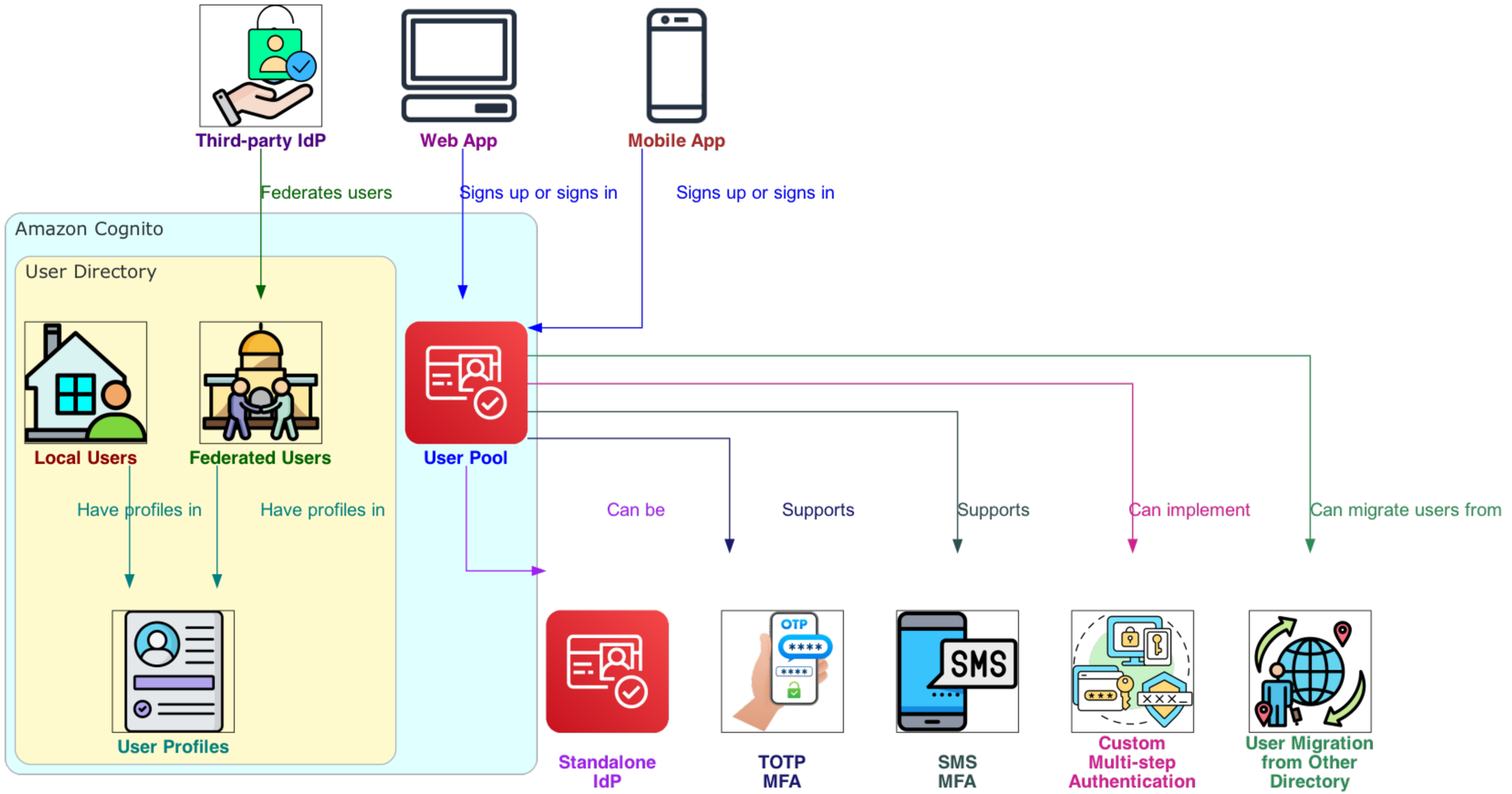
⌨️ AWS CLI

5. 🌐 Accepts tokens from third-party IdPs

6. 🎫 Issues JWTs to your app

📝 Contains user attributes

User Pools Detailed



8. 🚀 Customize authentication, authorization, and user management

🌐 Implement your own web front-end

🔧 Calls Amazon Cognito user pools API

9. 🔢 Set up MFA

⏰ TOTP

📱 SMS

10. 🛡️ Secure against malicious user accounts

11. 🔀 Create custom multi-step authentication flows

🔒 Enhance security

👥 Improve user experience

12. 🔍 Migrate users from other directories

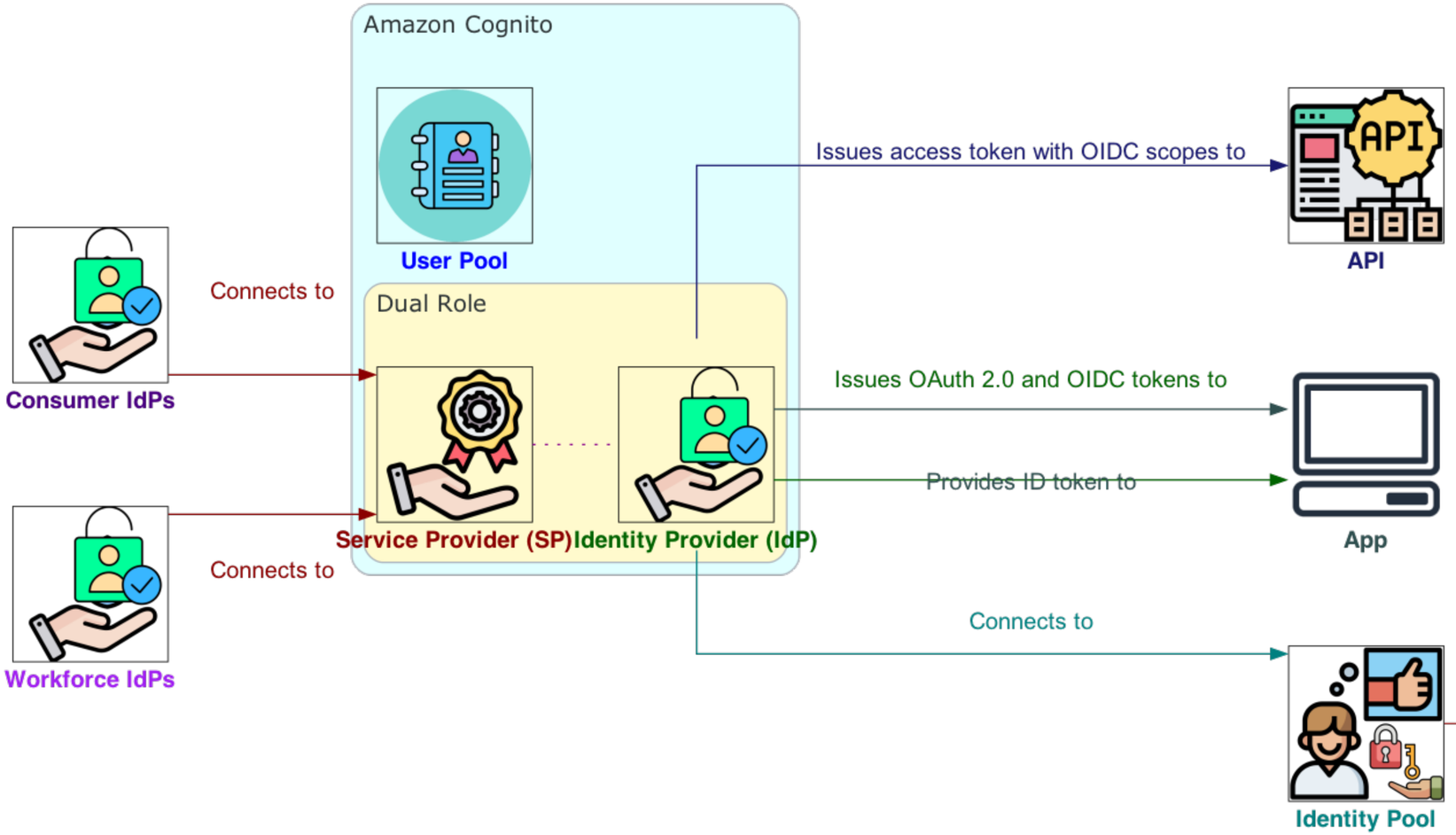
7. 🔐 Can be a standalone IdP

🔑 Uses OIDC standard

🎟️ Generates JWTs for authentication and authorization

User Pool Dual Role(SP and IdP)

1. 🌉 Connects to IdPs	2. 🔐 Acts as Identity Provider (IdP) to your app	5. 🔐 Retrieves AWS credentials
🏢 Acts as Service Provider (SP)		🆔 From Amazon Cognito identity pool



3. 🔗 Connects to	
👥 Consumer IdPs	👍 Facebook
	🔍 Google
🏢 Workforce IdPs	🔐 Okta
	🔄 Active Directory Federation Services (ADFS)

4. 🪪 Issues OAuth 2.0 and OIDC tokens	
🆔 ID token	👤 Authenticates user
	📝 Provides user profile information
🔑 Access token	🖥️ Authorizes API calls
	🔍 Uses OIDC scopes

Features of Amazon Cognito User Pools

1. 🆔 **OIDC IdP**: 🎟️ Issue ID tokens to authenticate users
2. 🔑 **Authorization server**: 🔐 Issue access tokens to authorize user access to APIs
3. 🔄 **SAML 2.0 SP**: 🔁 Transform SAML assertions into ID and access tokens
4. 🔗 **OIDC SP**: 🔁 Transform OIDC tokens into ID and access tokens
5. 🌐 **OAuth 2.0 SP**: 🔁 Transform ID tokens from Apple, Facebook, Amazon, or Google, 🎟️ Into your own ID and access tokens
6. 🖥️ **Authentication frontend service**: 📝 Sign up users, 👤 Manage users, 🔑 Authenticate users with hosted UI
7. 🖥️ **API support for your own UI**: 📝 Create users, 👤 Manage users, 🔑 Authenticate users through API requests, 🛠️ Using supported AWS SDKs
8. 🔢 **MFA**: 📱 Use SMS messages, ⏰ Use TOTPs, 📱 Use user's device as additional authentication factor
9. 🔒 **Security monitoring & response**: 🛡️ Secure against malicious activity, 🔑 Secure against insecure passwords
10. 🔀 **Customize authentication flows**: 🔧 Build your own authentication mechanism, ➕ Add custom steps to existing flows
11. 👥 **Groups**: 📂 Create logical groupings of users, 🔑 Create hierarchy of IAM role claims, 🎟️ When passing tokens to identity pools
12. 🎟️ **Customize ID tokens**: ➕ Add new claims, 🔧 Modify claims, ➖ Suppress claims
13. 👤 **Customize user attributes**: 📝 Assign values to user attributes, ➕ Add your own custom attributes

Identity Pools Detailed

1. 📂 Collection of unique identifiers (identities)

👤 For users or guests

2. 🪪 Assigns temporary AWS credentials

🔑 To identities

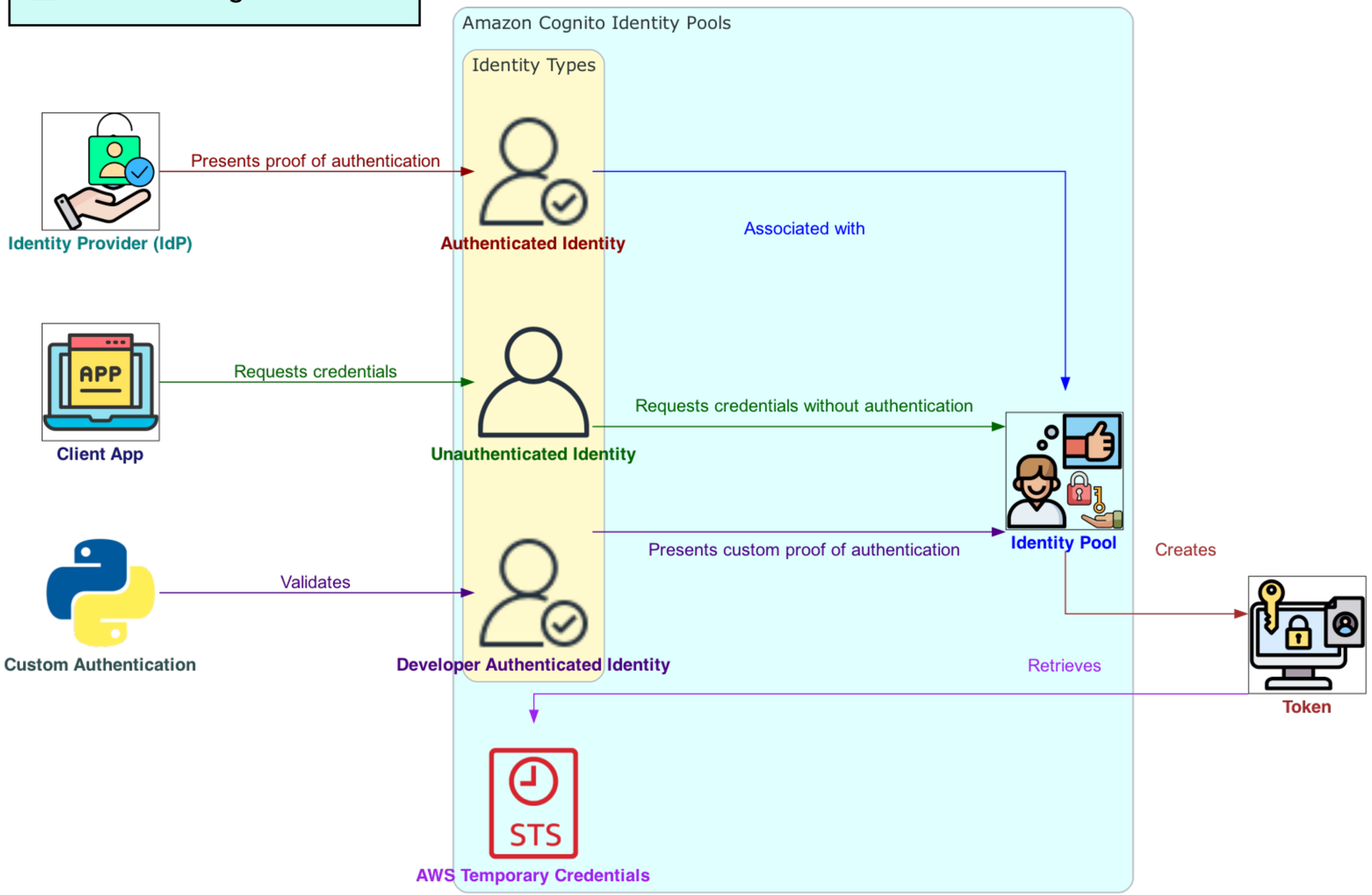
3. 🔐 Associates user with identity

🔓 Upon proof of authentication

🔑 From SAML 2.0, OIDC, or OAuth 2.0 IdP

4. 🔑 Token retrieves temporary session credentials

🔐 From AWS STS



5. 🌐 Supports various identity types

✅ Authenticated identities

❌ Unauthenticated identities

👨‍💻 Developer-authenticated identities

7. 📱 Grants temporary AWS credentials

👤 To app users who request them

❌ With unauthenticated identities

🔧 Based on custom schema with developer-authenticated identities

6. 🛠️ Configurable to authorize AWS access

🚫 Without IdP authentication

🔒 Identity Pools: 2 Access Control Types 🔑

1. 🎭 Role-based access control (RBAC)

🔑 Integrates with IAM policies

6. 🔍 ABAC: Identity pool reads user attributes

🗺️ Maps to principal tags

👤 In user's temporary session

2. 🏷️ Attributes for access control (ABAC)

🪄 Maps user attributes to principal tags

⏳ In temporary sessions

3. 🤝 Can be used together or individually

🎭 RBAC

🏷️ ABAC

4. 🚦 RBAC: Amazon Cognito chooses IAM role

📜 Based on user claims

5. 📝 IAM policies applied to each role

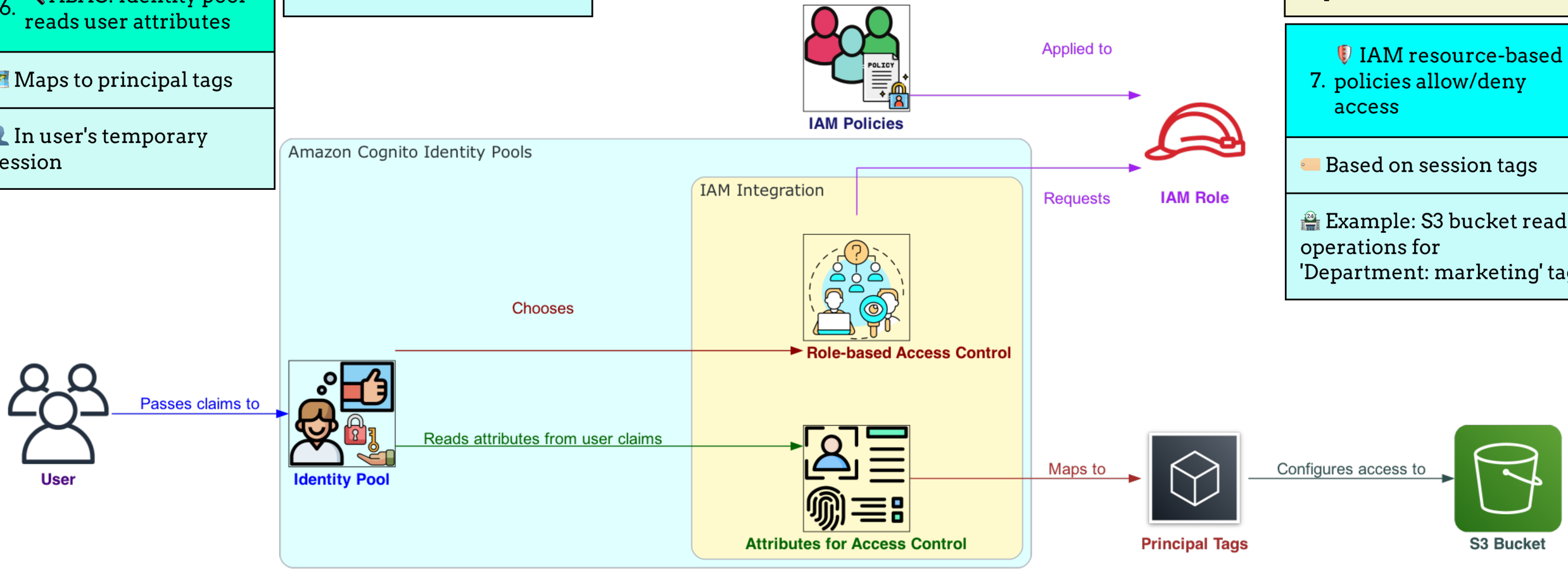
🎨 For customization

🏬 Example: Marketing department access needs

7. 🛡️ IAM resource-based policies allow/deny access

🏷️ Based on session tags

🏪 Example: S3 bucket read operations for 'Department: marketing' tag



Features of Amazon Cognito Identity Pools

1. 🔄 **Amazon Cognito user pool SP**: 🆔 Exchange ID token for web identity credentials, 🔐 From AWS STS
2. 🔒 **SAML 2.0 SP**: 🔄 Exchange SAML assertions for web identity credentials, 🔐 From AWS STS
3. 🔑 **OIDC SP**: 🔄 Exchange OIDC tokens for web identity credentials, 🔐 From AWS STS
4. 🔗 **OAuth 2.0 SP**: 🔄 Exchange OAuth tokens for web identity credentials, 🔐 From AWS STS, 🏢 Supported providers: Amazon, Facebook, Google, Apple, Twitter
5. 🛠️ **Custom SP**: 🔐 With AWS credentials, 🔄 Exchange claims in any format for web identity credentials, 🔐 From AWS STS
6. 🤷‍♂️ **Unauthenticated access**: 🎟️ Issue limited-access web identity credentials, 🔐 From AWS STS, 🚫 Without authentication
7. 🎭 **Role-based access control**: 🔑 Choose IAM role for authenticated user, 📜 Based on user claims, ⚙️ Configure roles to be assumed only in identity pool context
8. 🏷️ **Attribute-based access control**: 🔄 Convert claims into principal tags, ⏳ For AWS STS temporary session, 🔒 Use IAM policies to filter resource access based on principal tags

Feature Comparison between User Pools and Identity Pools

S.No.	Feature	User Pools	Identity Pools
1	OIDC IdP	Yes	No
2	API authorization server	Yes	No
3	IAM web identity authorization server	No	Yes
4	SAML 2.0 SP & OIDC IdP	Yes	No
5	OIDC SP & OIDC IdP	Yes	No
6	OAuth 2.0 SP & OIDC IdP	Yes	No
7	SAML 2.0 SP & credentials broker	No	Yes
8	OIDC SP & credentials broker	No	Yes
9	OAuth 2.0 SP & credentials broker	No	Yes
10	Amazon Cognito user pool SP & credentials broker	No	Yes
11	Custom SP & credentials broker	No	Yes
12	Authentication frontend service	Yes	No
13	API support for your own authentication UI	Yes	No
14	MFA	Yes	No
15	Security monitoring & response	Yes	No
16	Customize authentication flows	Yes	No
17	Groups	Yes	No
18	Customize ID tokens	Yes	No
19	AWS WAF web ACLs	Yes	No
20	Customize user attributes	Yes	No
21	Unauthenticated access	No	Yes
22	Role-based access control	No	Yes
23	Attribute-based access control	No	Yes

Thanks for Watching