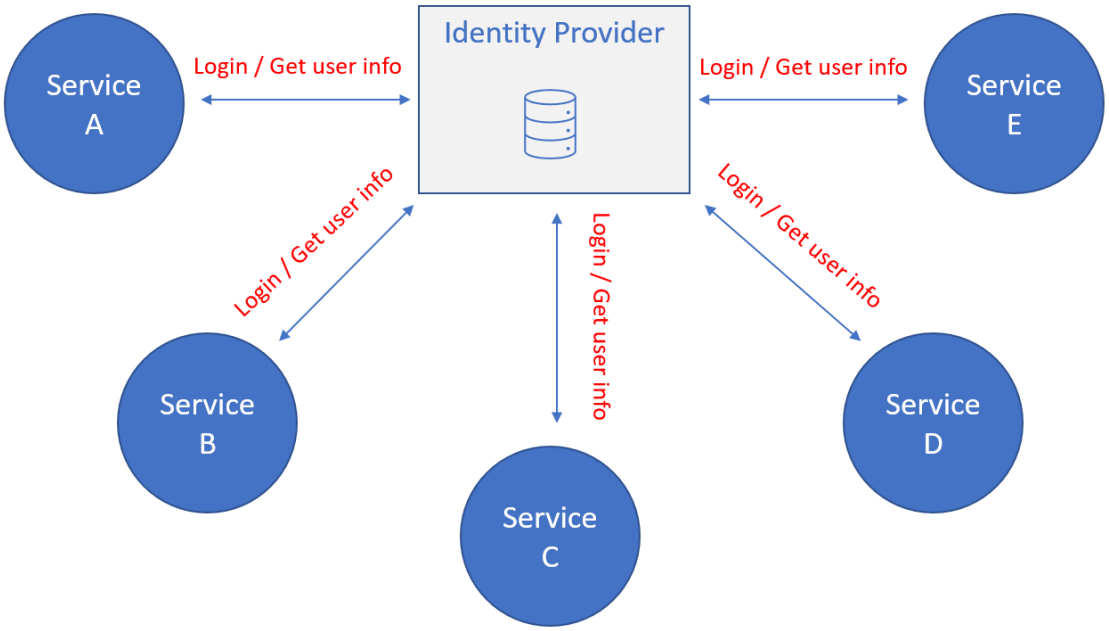
Chapter 1: Walkthrough of Digital Identity in the Enterprise



Individual Registration

*Mandatory

- **GARBAGE/JUNK VALUES IN PROFILE MAY LEAD TO DEACTIVATION**
- **Please use a valid E-Mail ID and mobile number in registration.**

Your user id, password and an activation link will be sent to your registered E-Mail id and mobile verification code will be sent to registered mobile number.

Username * (Max 10 Characters) Check Availability

If you forget your password, we will identify you with this information

Security Question * --Select One--

Your Answer *

First name *

Last name *

Gender * Male Marital Status * Married

Date of birth * 13 Jan Year

Occupation * --Select One--

Email ID *

Mobile * +91

Nationality * -- Select One --

Residential Address

Address *

(optional)

(optional)

City * -- Select One -- (other)

State * -- Select One -- (other)

Pin/Zip *

Country * -- Select One --

Phone *

Copy Residence to office Address Yes No

Other Services

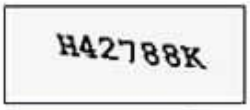
Subscription to Special Offers/Commercial Promotions/Newsletters through email/ SMS

- Information regarding tourism packages & Special offers from IRCTC* Third party offers (Not more than 2 such mails/SMS per month)* Yes No

Third party offers (Not more than 2 such mails per month)* Yes No

Please inform me about Yes No

Enter Verification Code



Enter the text from Image :*

Click here for new Image

Letters are case sensitive.

Submit Reset

Sign up with Facebook

Sign up with Twitter

Sign up with Google

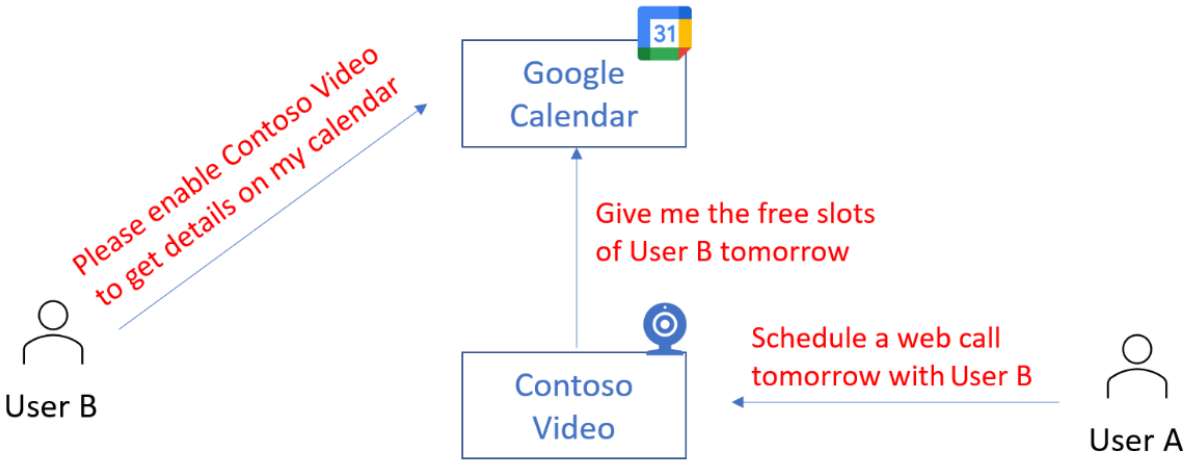
Sign up with Yahoo

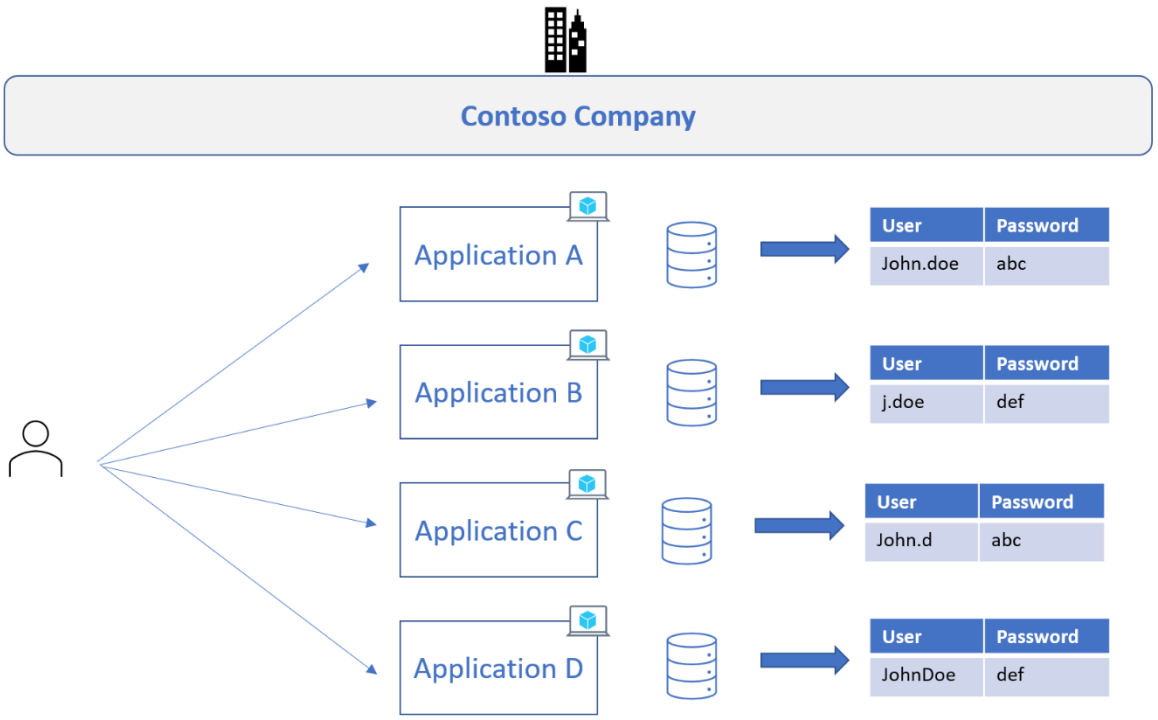
Sign up with LinkedIn

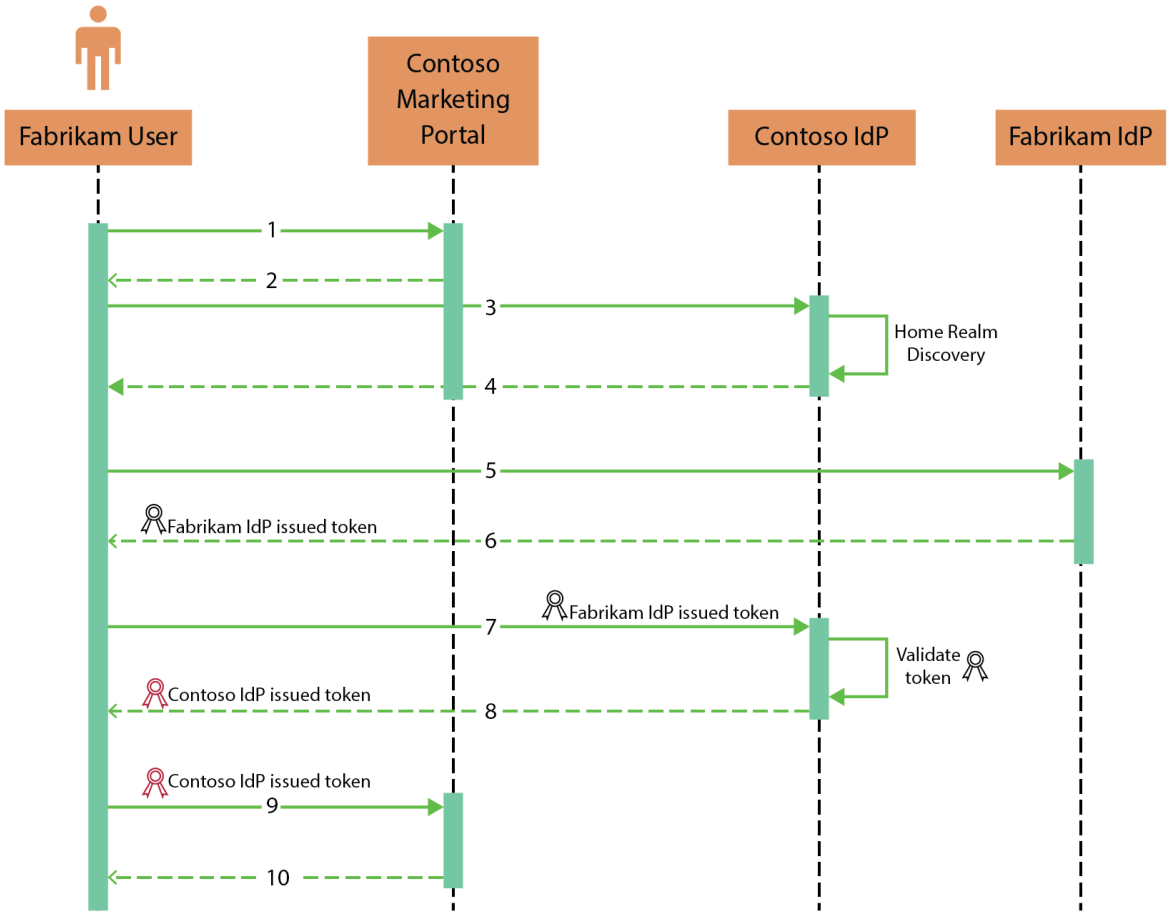
or

Sign up with e-mail

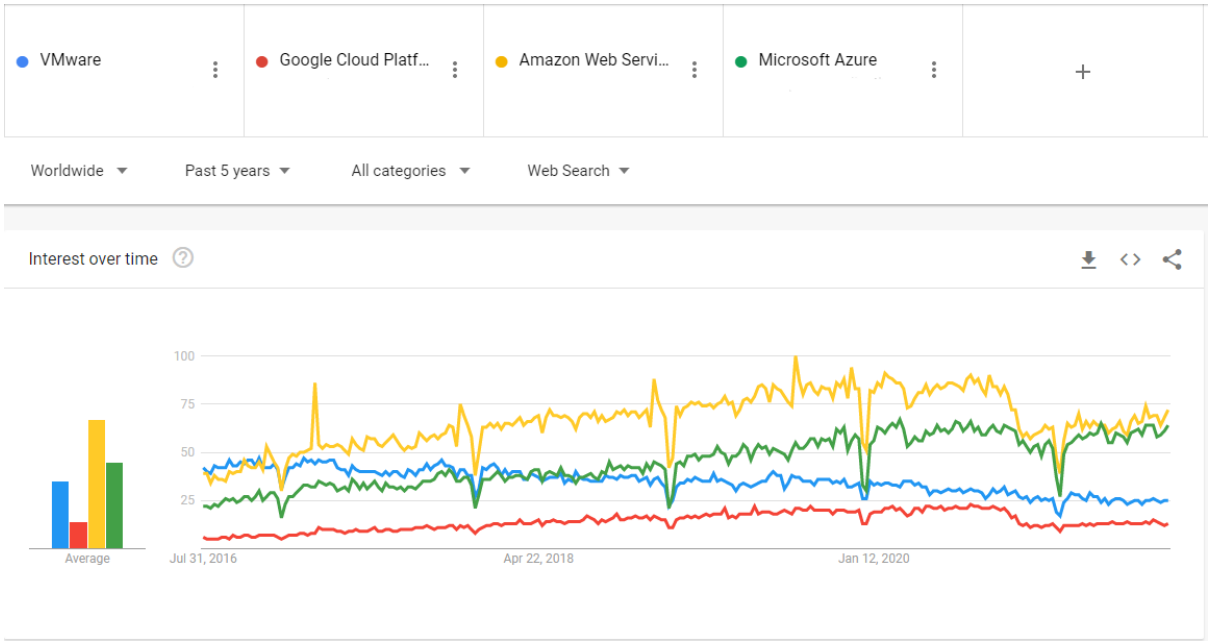
Already a member? Sign in

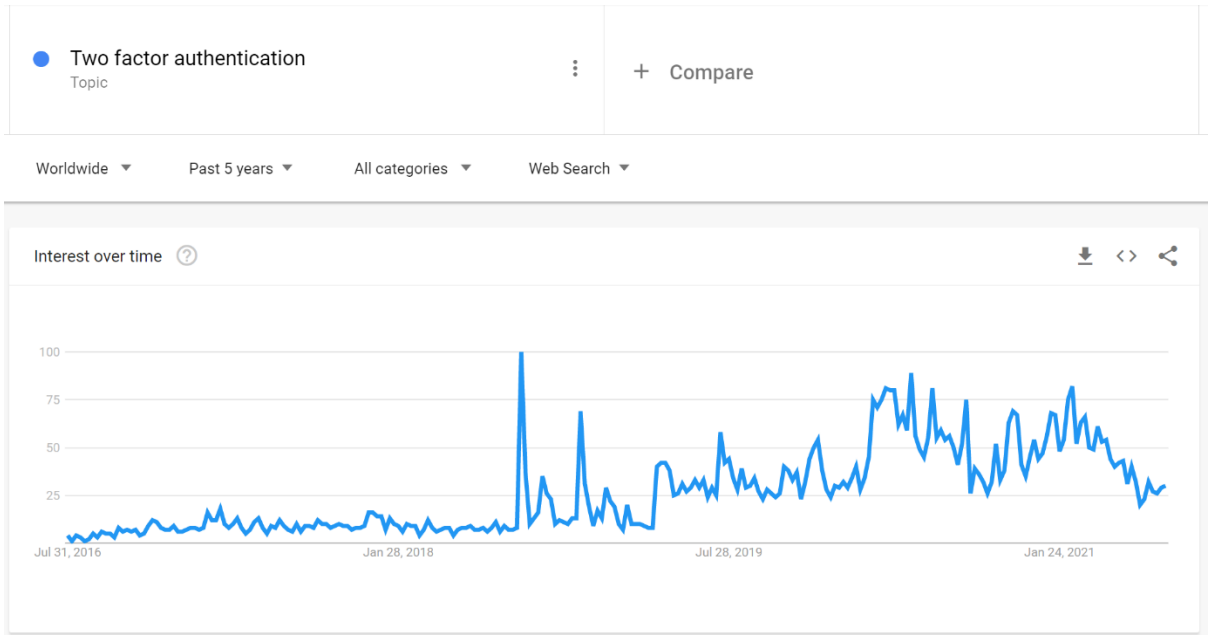


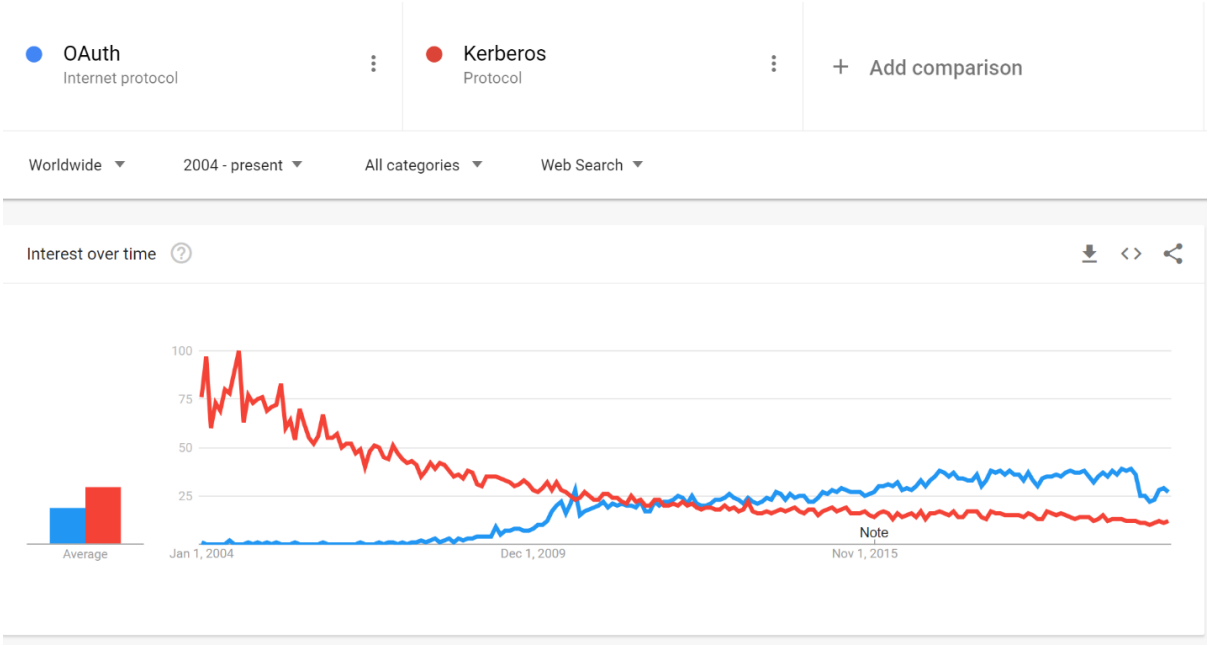

Contoso Company
Application A
Application B
Application C
Application D
User
Password
John.doe
abc
User
Password
j.doe
def
User
Password
John.d
abc
User
Password
JohnDoe
def

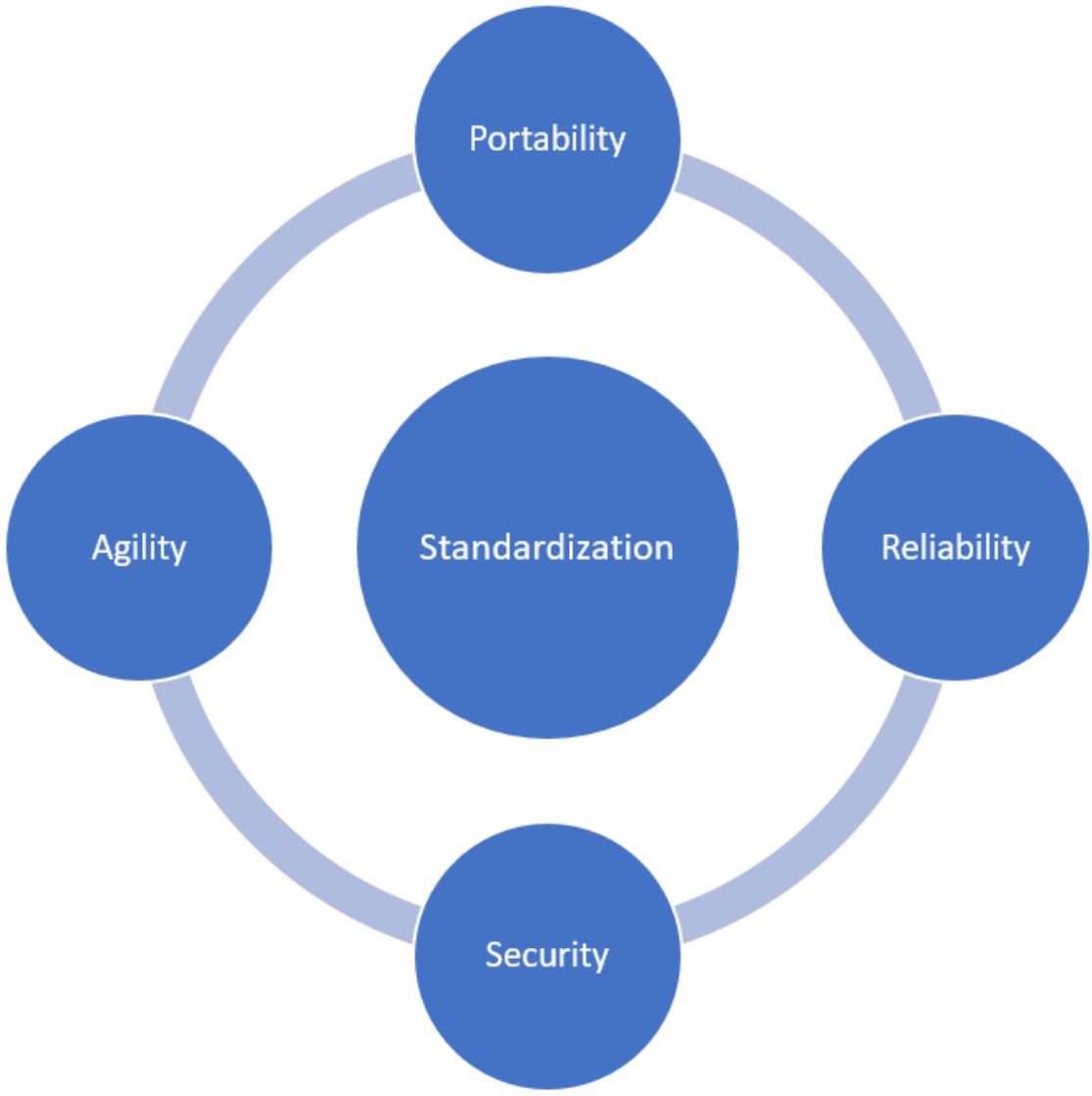

Fabrikam User
Contoso Marketing Portal
Contoso IdP
Fabrikam IdP
1
2
3
Home Realm Discovery
4
5
Fabrikam IdP issued token
6
Fabrikam IdP issued token
7
Validate token
Contoso IdP issued token
8
Contoso IdP issued token
9
10

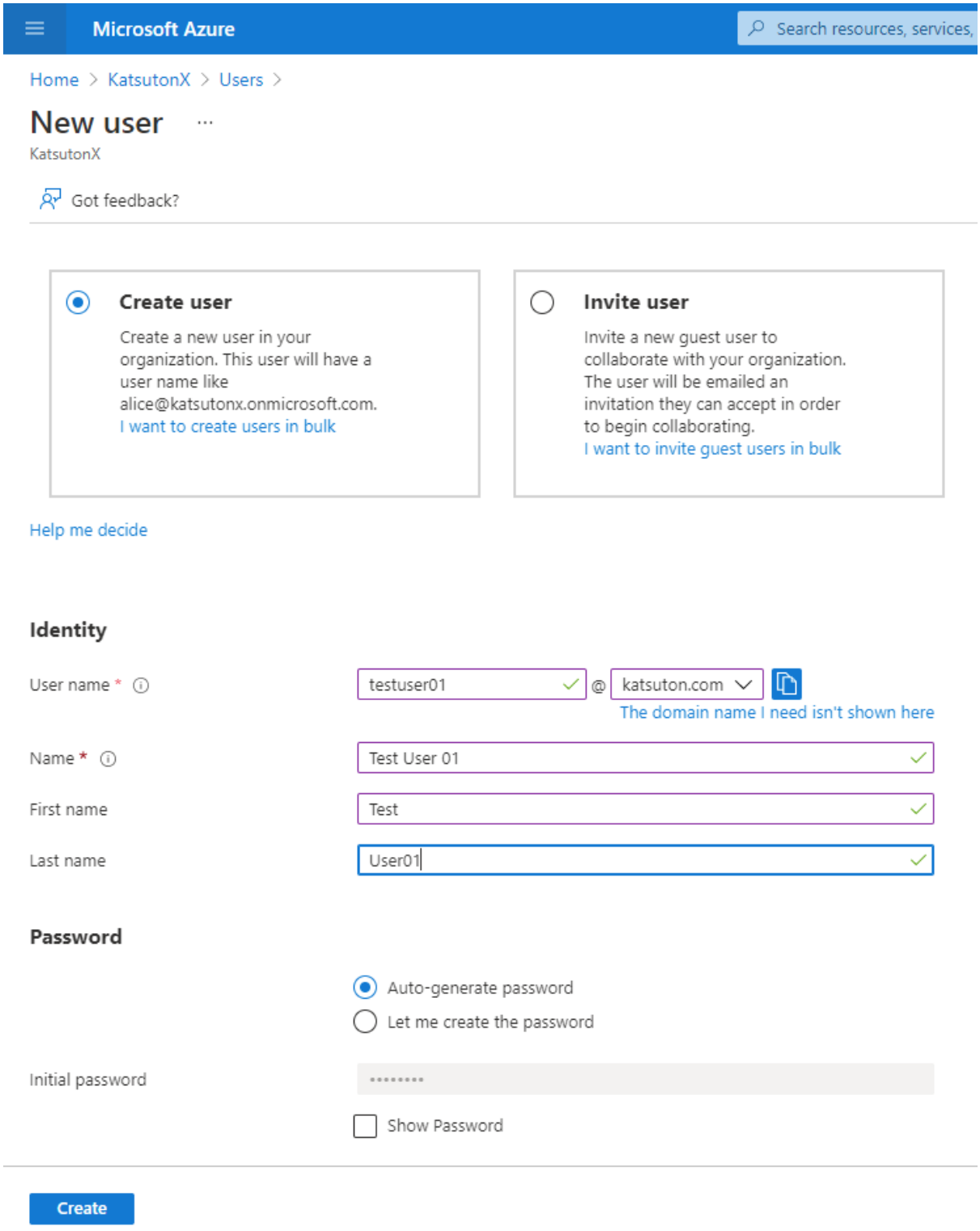
Chapter 2: The Cloud Era and Identity

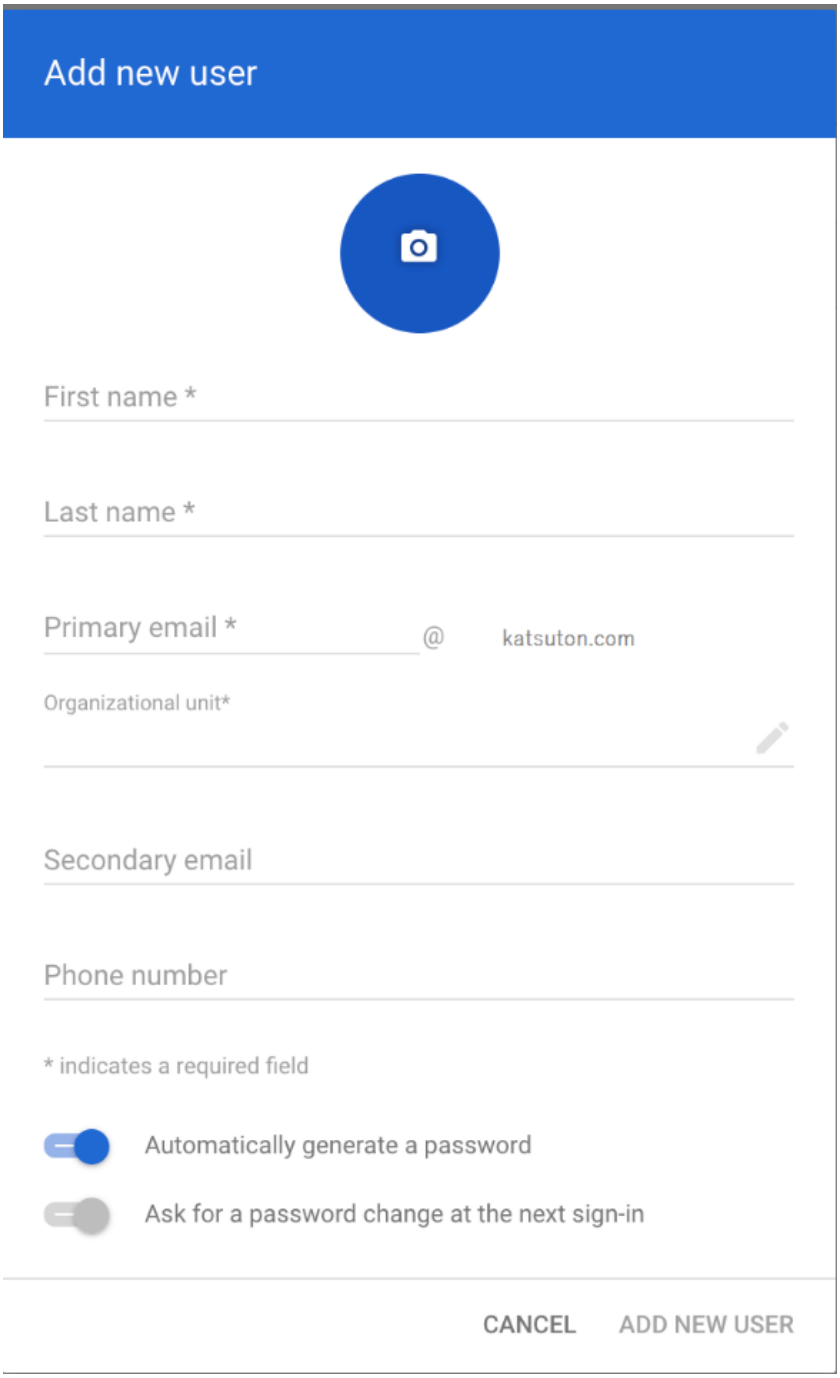




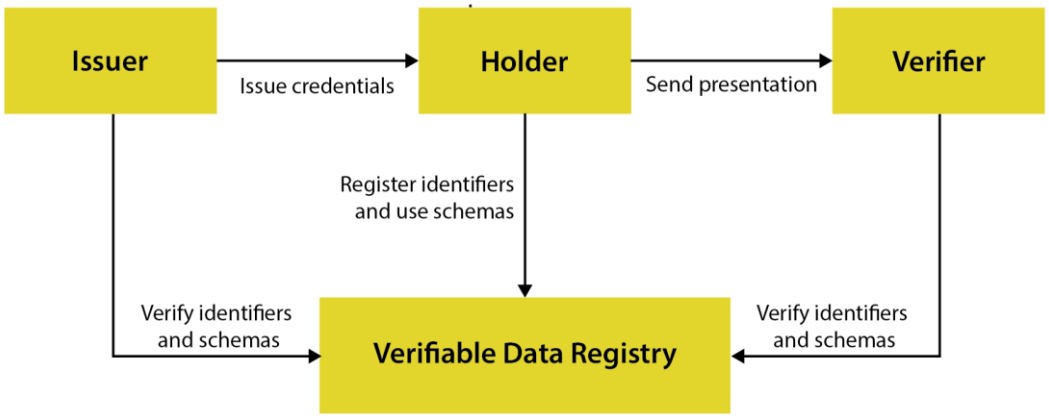

OAuth
Internet protocol
Kerberos
Protocol
Add comparison
Worldwide
2004 - present
All categories
Web Search
Interest over time
100
75
50
25
Note
Average
Jan 1, 2004
Dec 1, 2009
Nov 1, 2015


Portability
Agility
Standardization
Reliability
Security

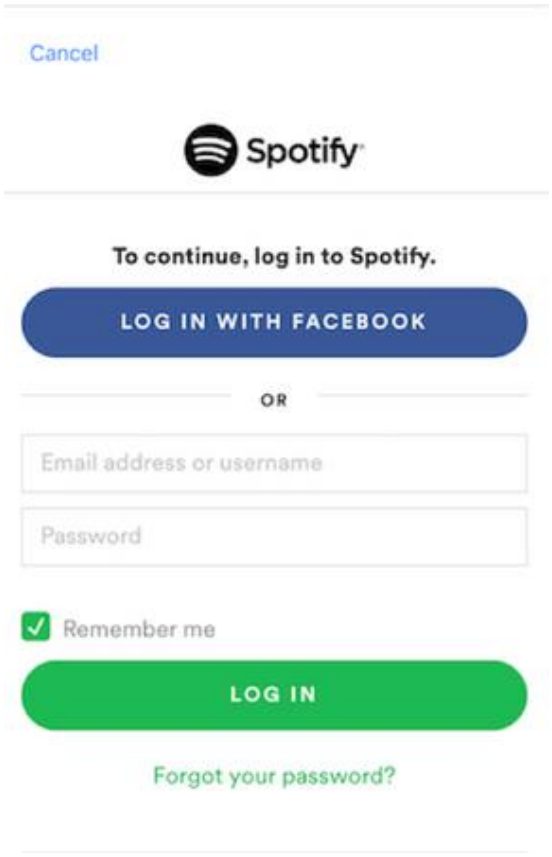

Microsoft Azure
Search resources, services,
Home > KatsutonX > Users >
New user
KatsutonX
Got feedback?
Create user
Create a new user in your organization. This user will have a user name like alice@katsutonx.onmicrosoft.com.
I want to create users in bulk
Invite user
Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.
I want to invite guest users in bulk
Help me decide
Identity
User name *
testuser01
@
katsuton.com
The domain name I need isn't shown here
Name *
Test User 01
First name
Test
Last name
User01
Password
Auto-generate password
Let me create the password
Initial password
Show Password
Create

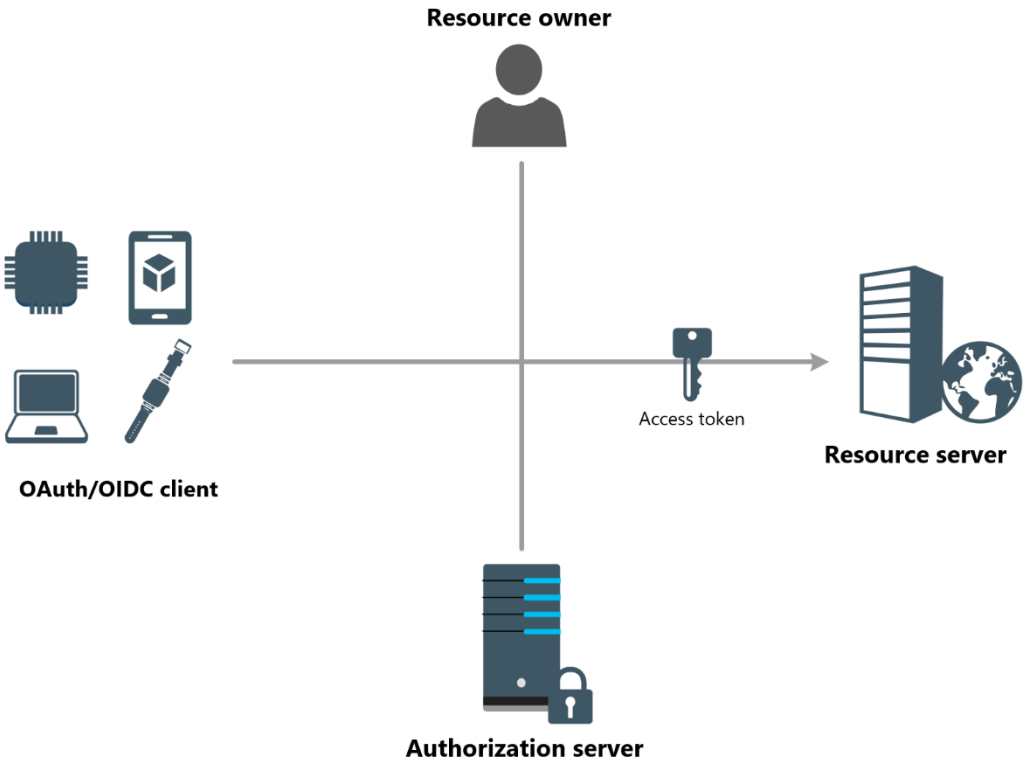

Add new user
First name *
Last name *
Primary email *
@
katsuton.com
Organizational unit*
Secondary email
Phone number
* indicates a required field
Automatically generate a password
Ask for a password change at the next sign-in
CANCEL
ADD NEW USER

Scheme
did:example:123456789abcdefghi
DID Method
DID Method-Specific Identifier


Issuer
Issue credentials
Holder
Send presentation
Verifier
Register identifiers
and use schemas
Verify identifiers
and schemas
Verifiable Data Registry
Verify identifiers
and schemas

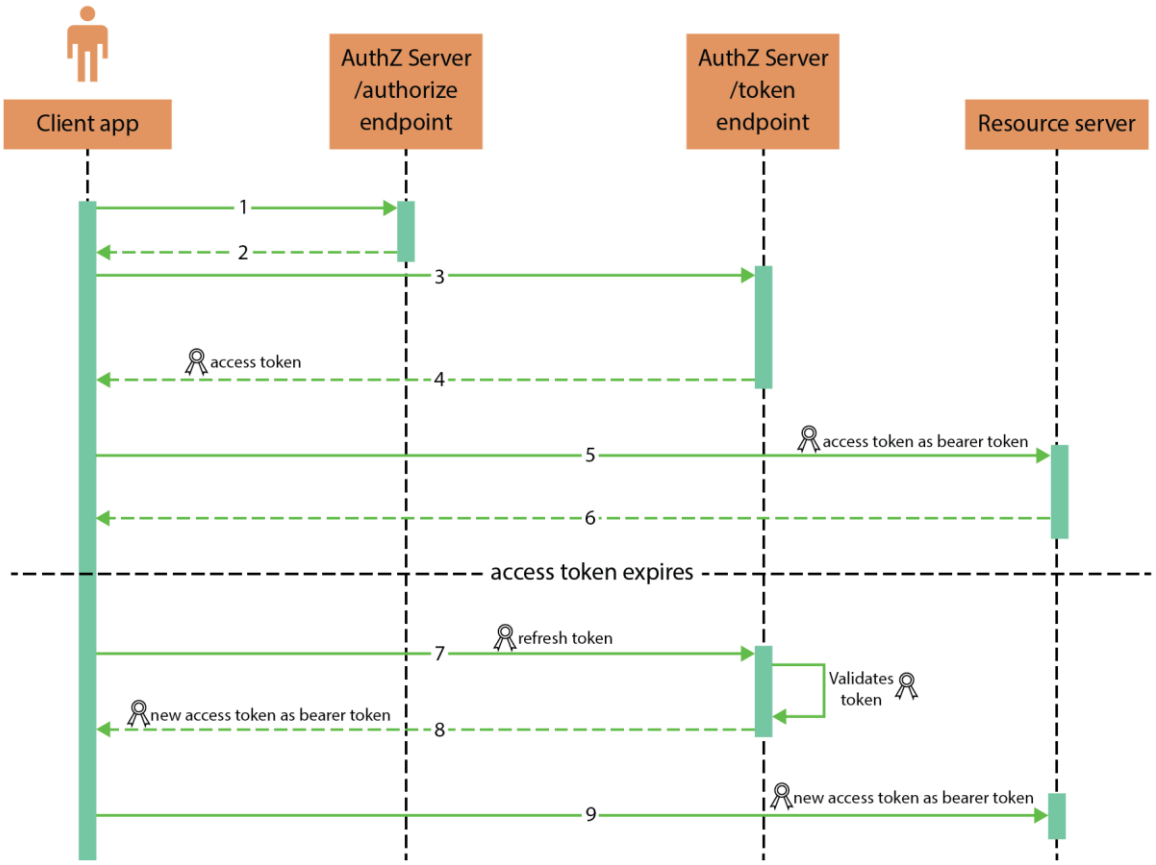
Chapter 3: OAuth 2.0 and OIDC

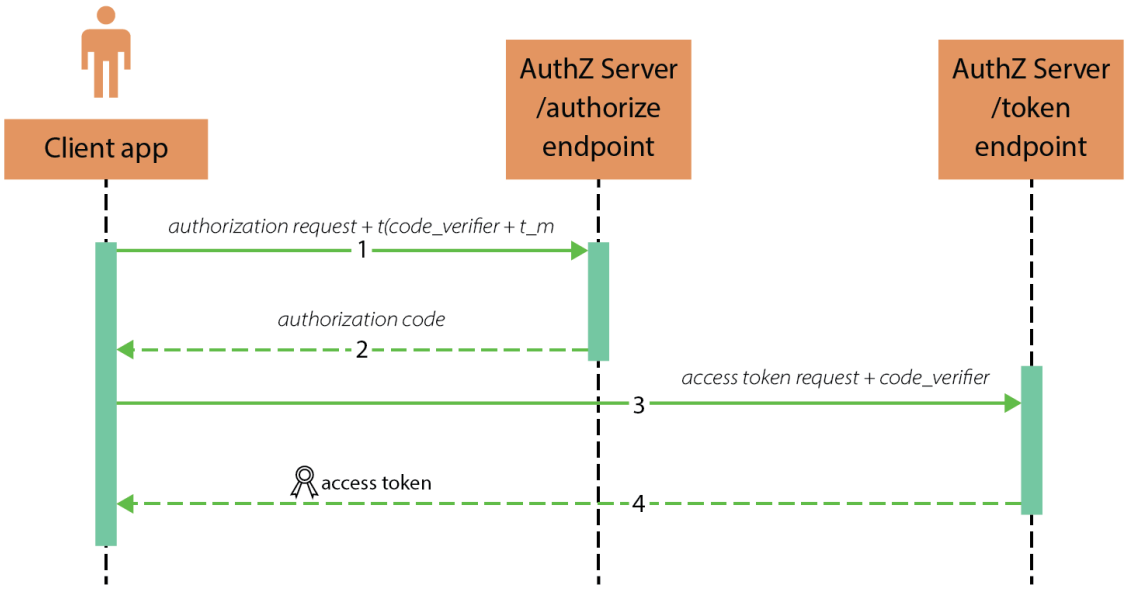


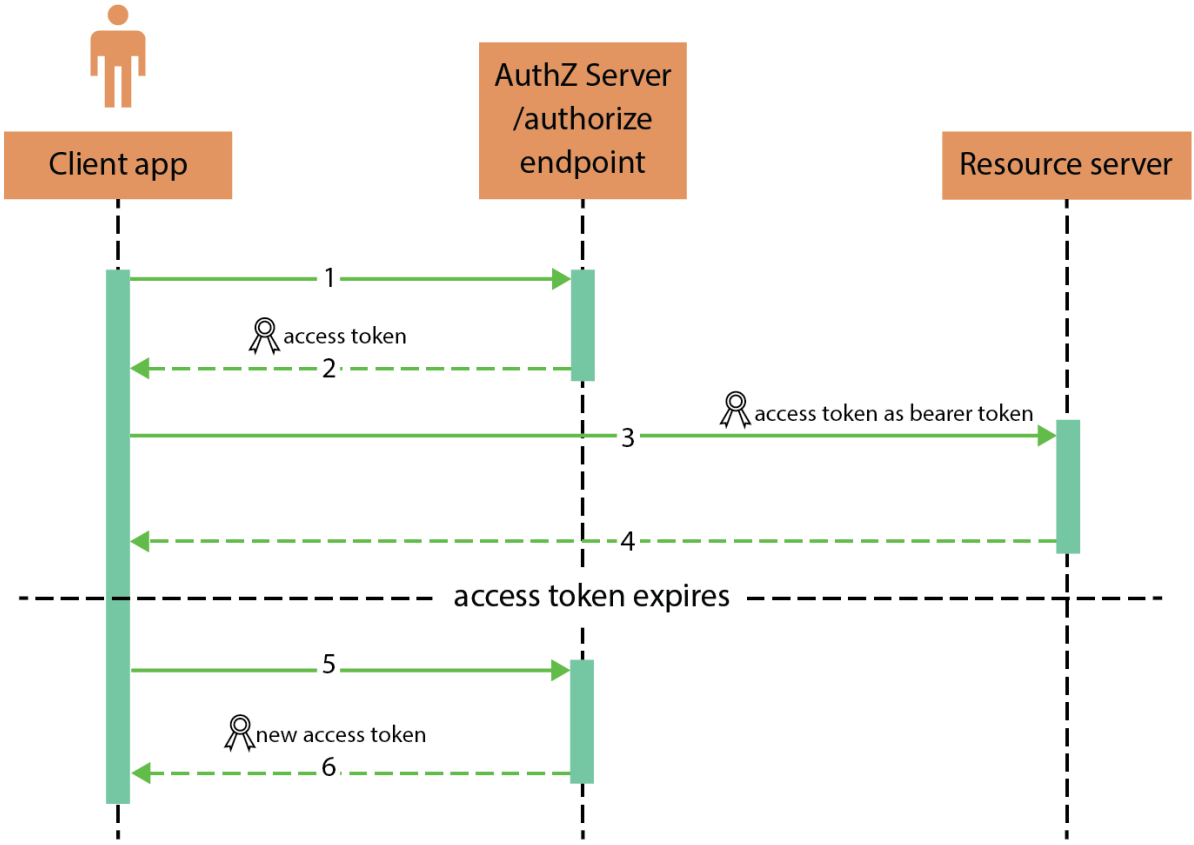


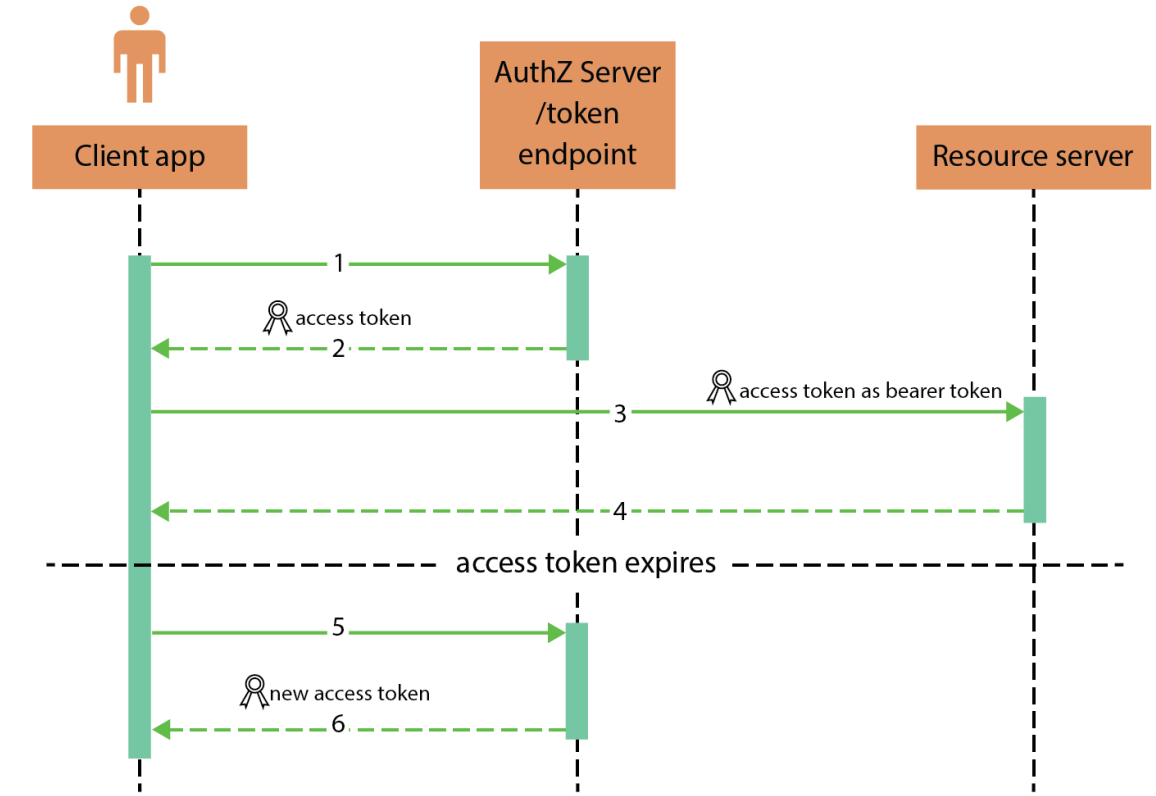
Chapter 4: Authentication Flows

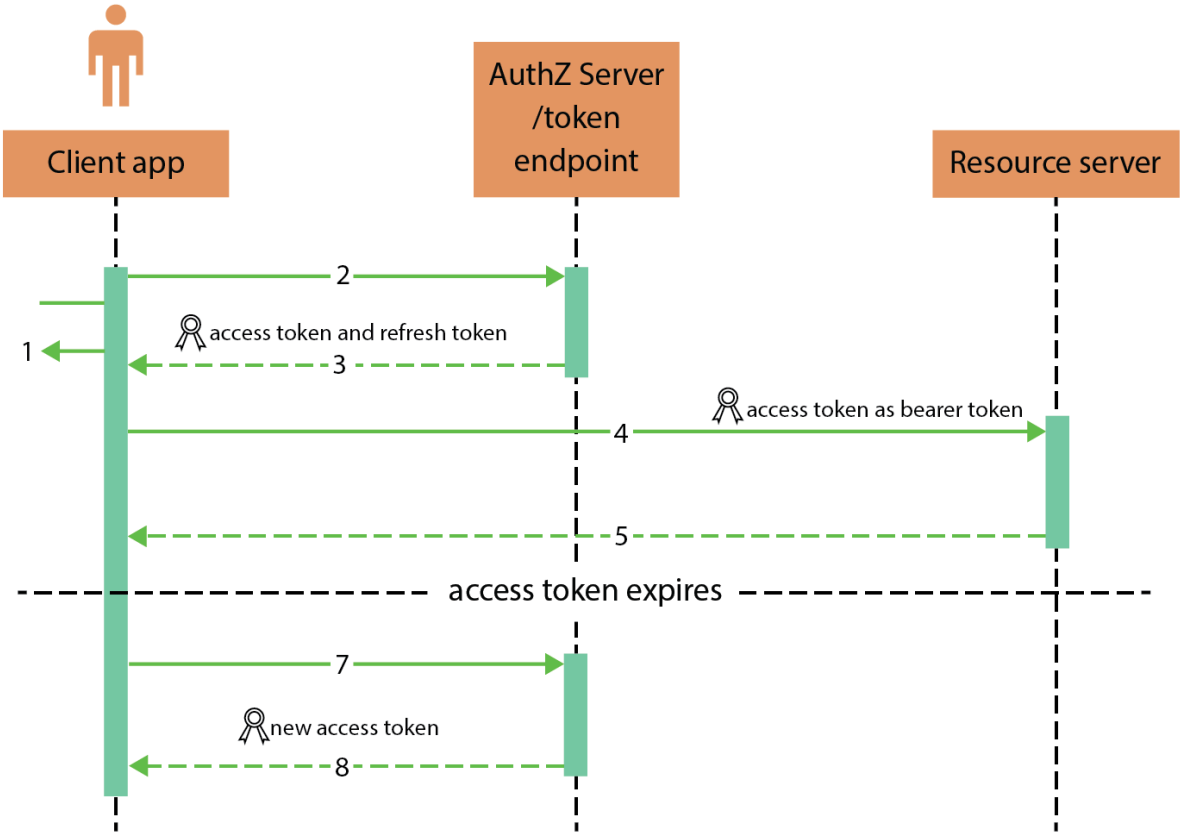
Protocol /Flow	Authorization Code Grant	Implicit	Client Credentials	Resource Owner Password Credentials	On-Behalf-Of	Hybrid
OAuth 2.0	YES	YES	YES	YES	YES	YES
OIDC	YES	YES	NO	NO	NO	YES

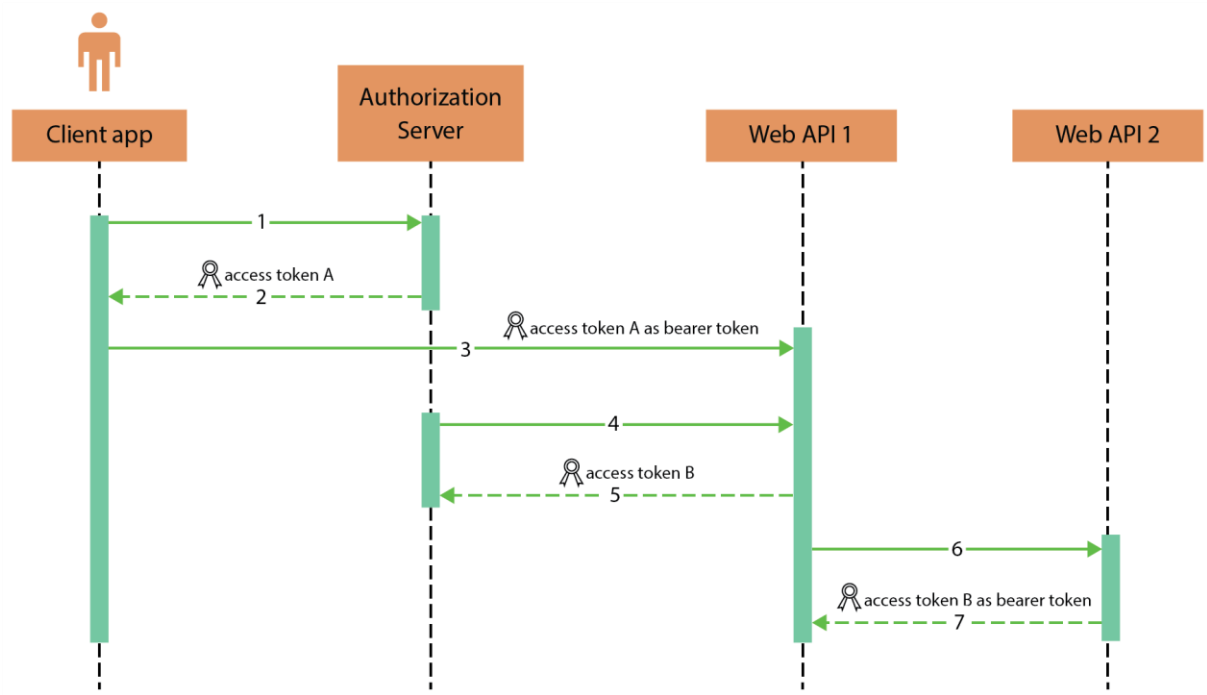



Client app
AuthZ Server /authorize endpoint
AuthZ Server /token endpoint
authorization request + t(code_verifier + t_m
1
authorization code
2
access token request + code_verifier
3
access token
4

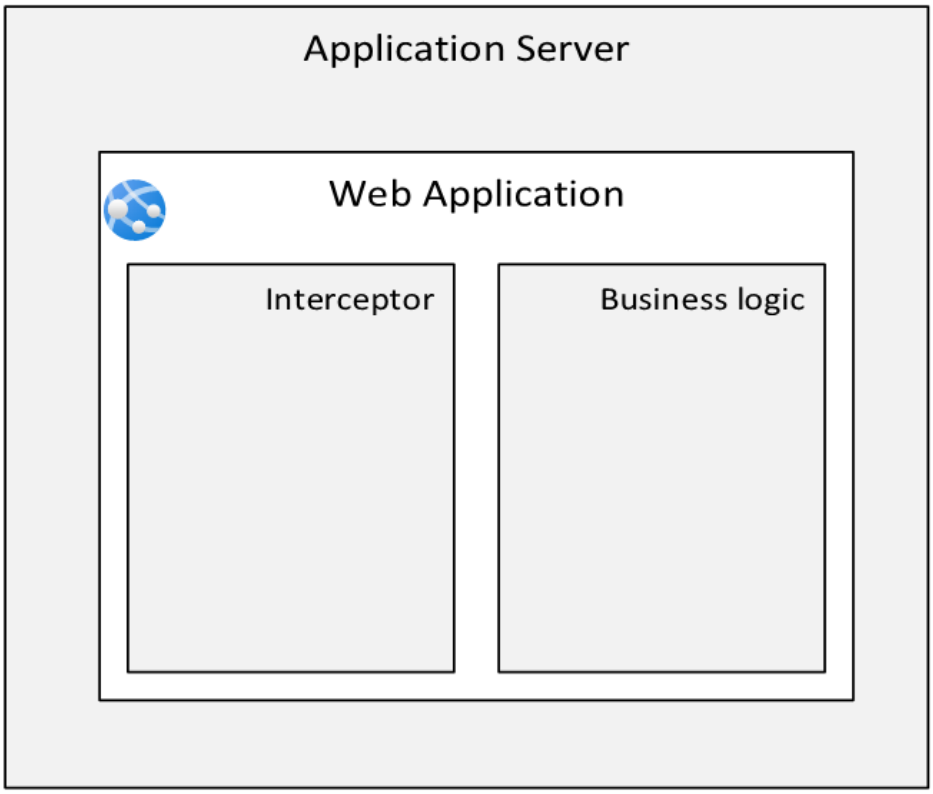

Client app
AuthZ Server /authorize endpoint
Resource server
1
access token
2
access token as bearer token
3
4
access token expires
5
new access token
6

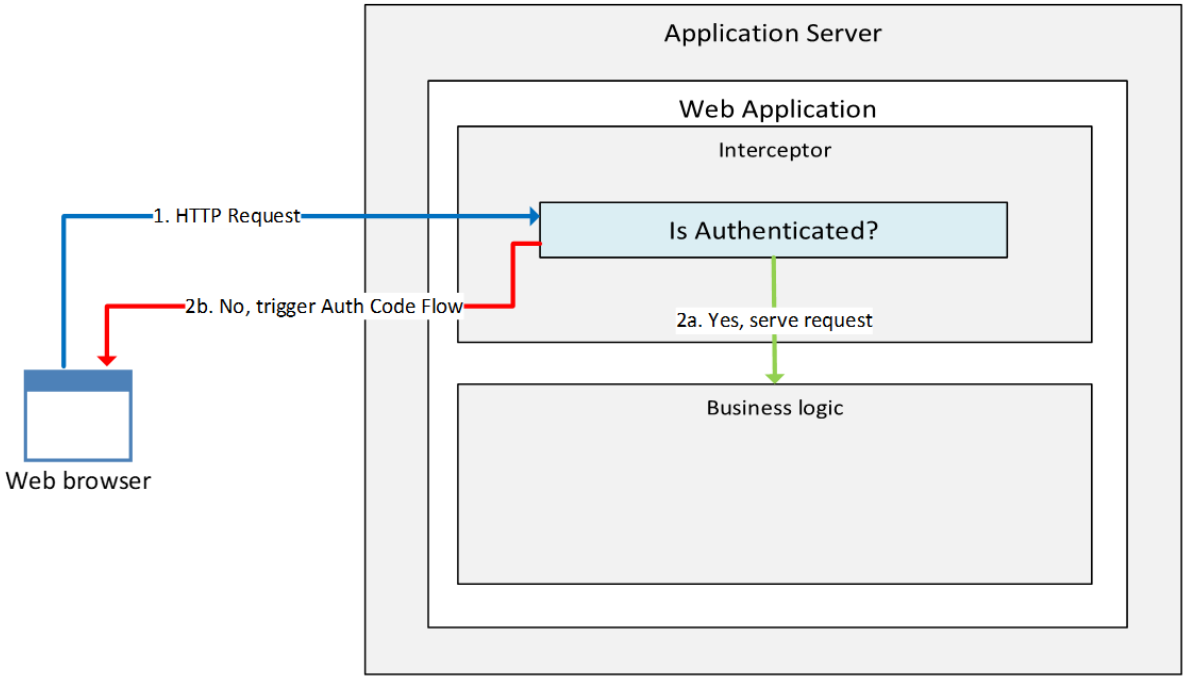

Client app
AuthZ Server /token endpoint
Resource server
1
access token
2
access token as bearer token
3
4
access token expires
5
new access token
6

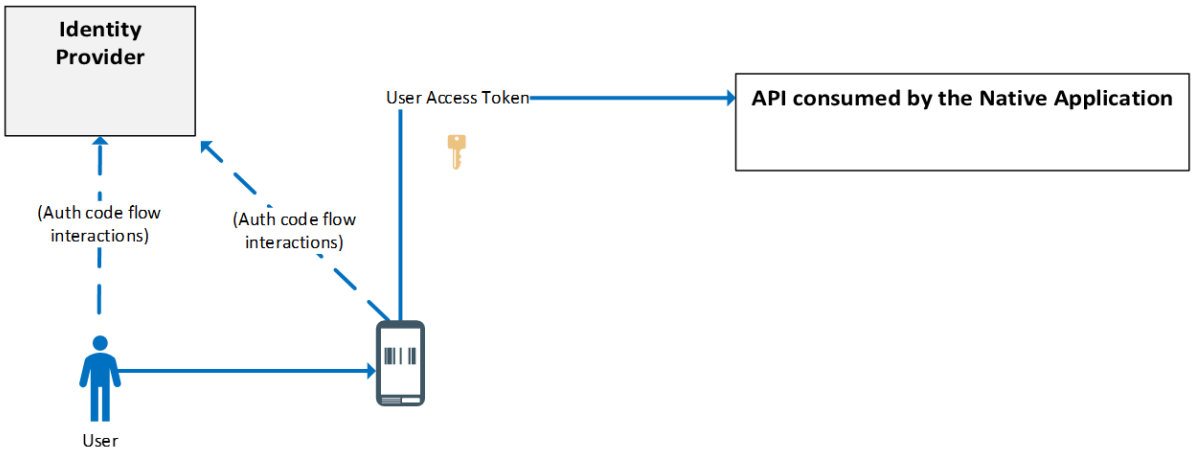

Client app
AuthZ Server /token endpoint
Resource server
2
1
access token and refresh token
3
access token as bearer token
4
5
access token expires
7
new access token
8

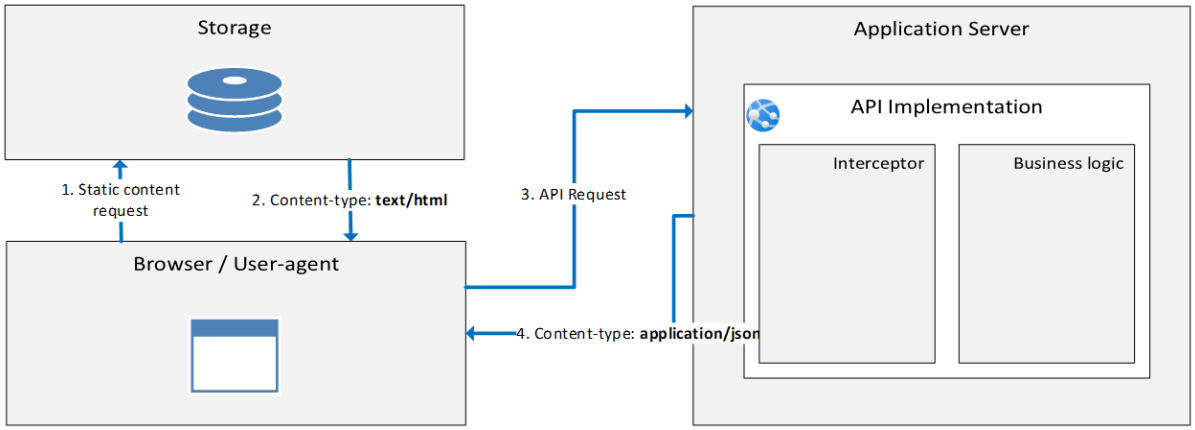

Client app
Authorization Server
Web API 1
Web API 2
1
access token A
2
access token A as bearer token
3
4
access token B
5
6
access token B as bearer token
7

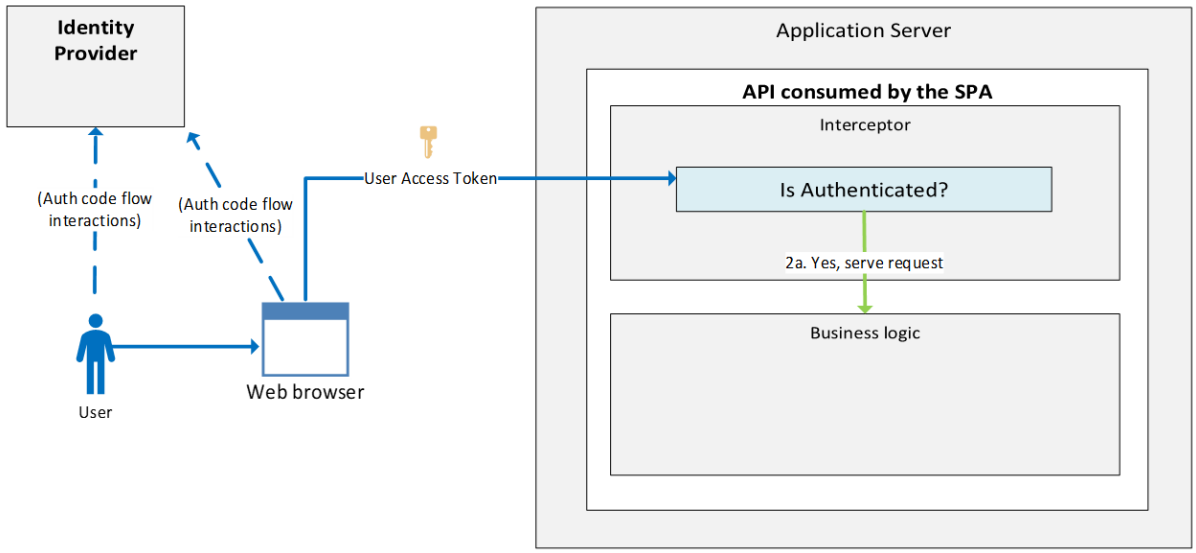
Chapter 5: Exploring Identity Patterns

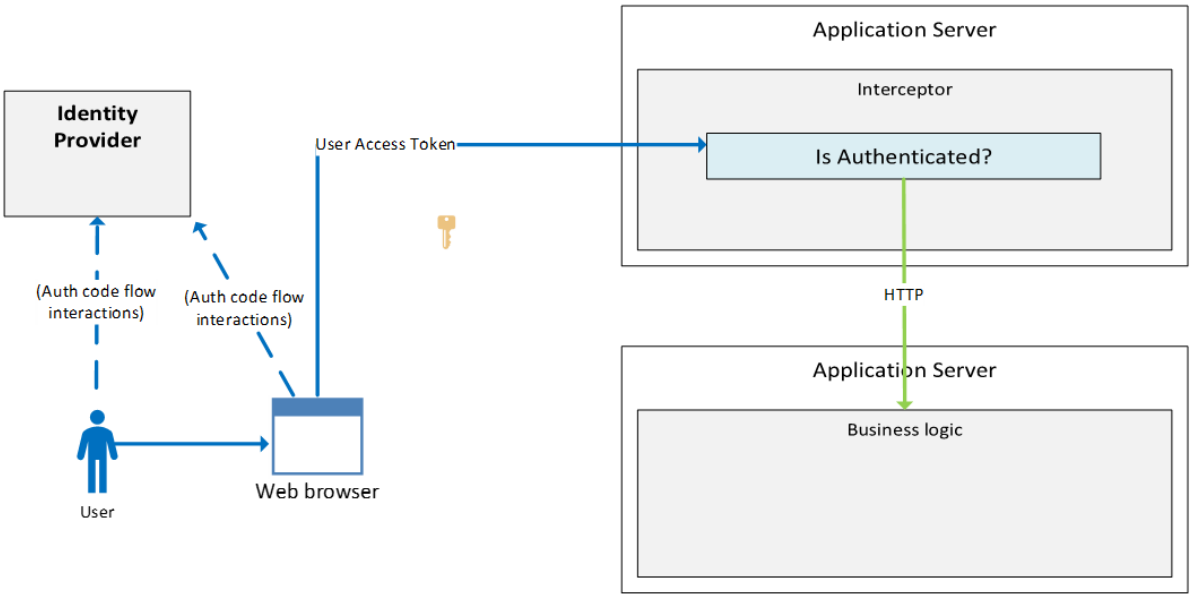


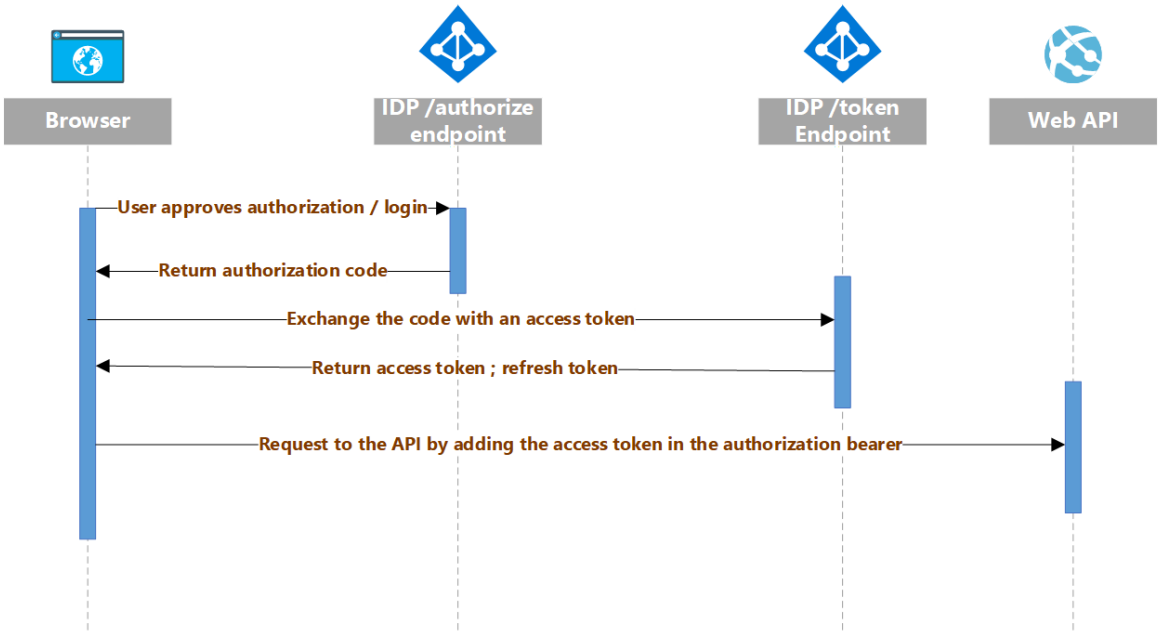


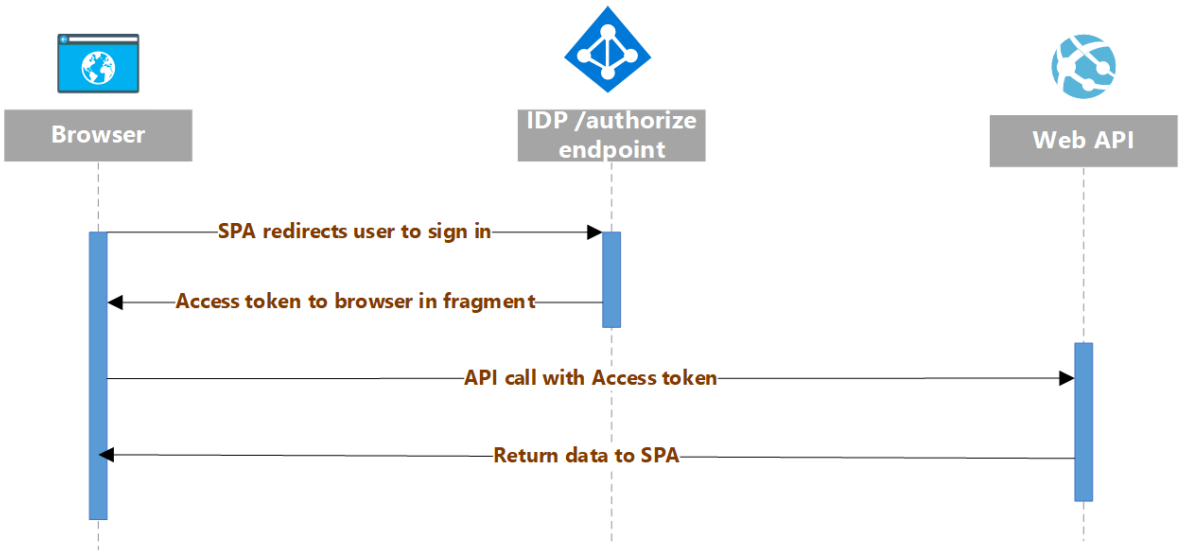

Identity Provider
User Access Token
API consumed by the Native Application
(Auth code flow interactions)
(Auth code flow interactions)
User


Storage
Application Server
API Implementation
Interceptor
Business logic
1. Static content request
2. Content-type: text/html
3. API Request
Browser / User-agent
4. Content-type: application/json

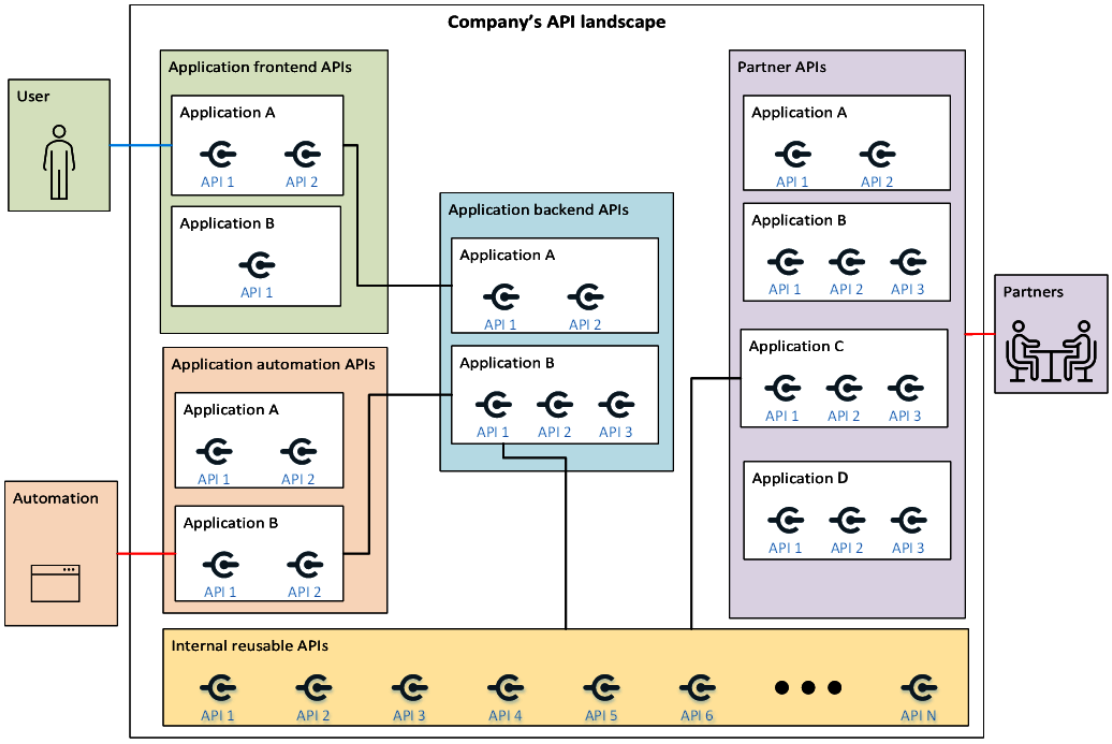

Identity Provider
Application Server
API consumed by the SPA
Interceptor
Is Authenticated?
2a. Yes, serve request
Business logic
User Access Token
(Auth code flow interactions)
(Auth code flow interactions)
User
Web browser

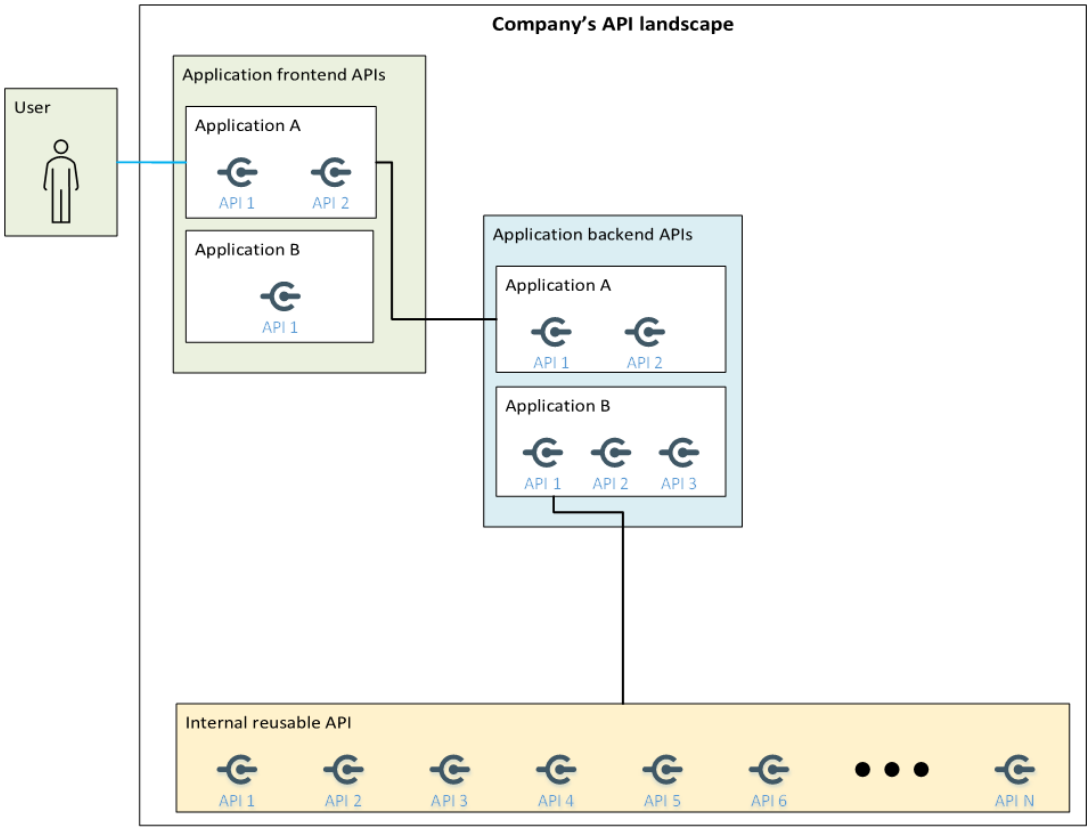

Application Server
Interceptor
Identity Provider
User Access Token
Is Authenticated?
(Auth code flow interactions)
(Auth code flow interactions)
HTTP
Application Server
Business logic
User
Web browser

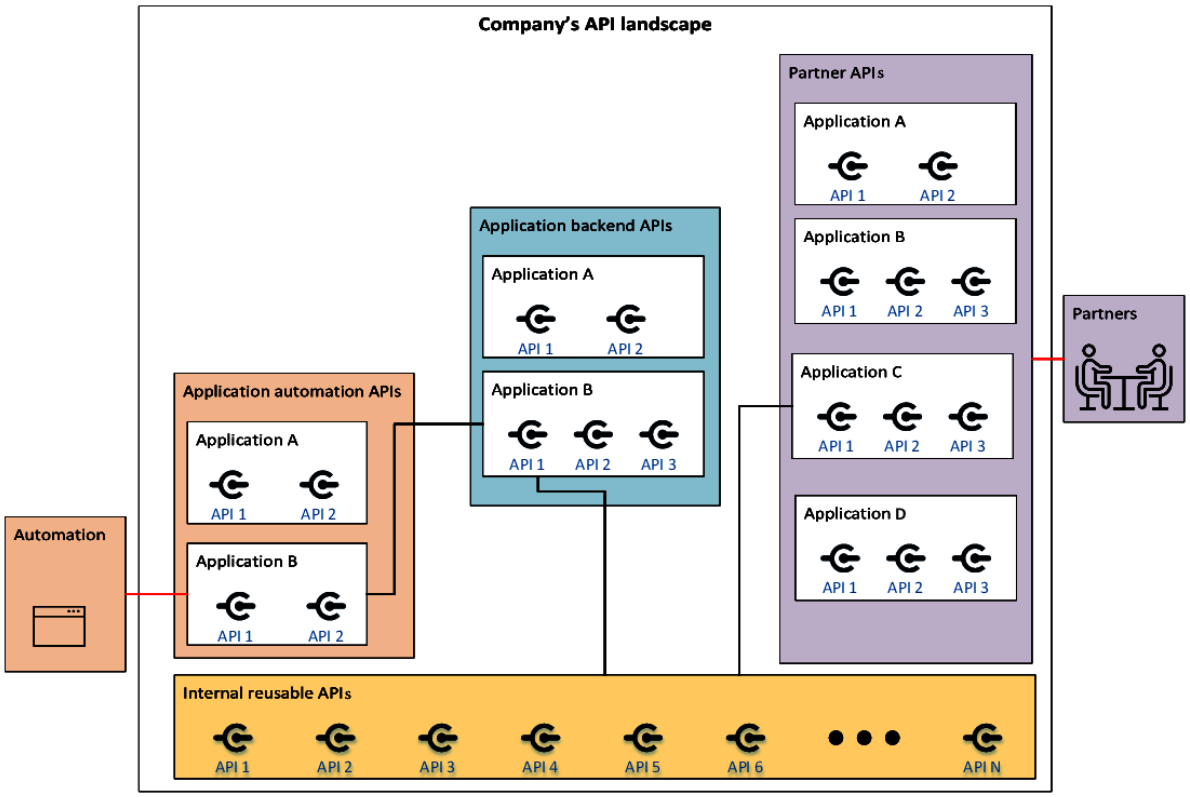

Browser
IDP /authorize endpoint
IDP /token Endpoint
Web API
User approves authorization / login
Return authorization code
Exchange the code with an access token
Return access token ; refresh token
Request to the API by adding the access token in the authorization bearer

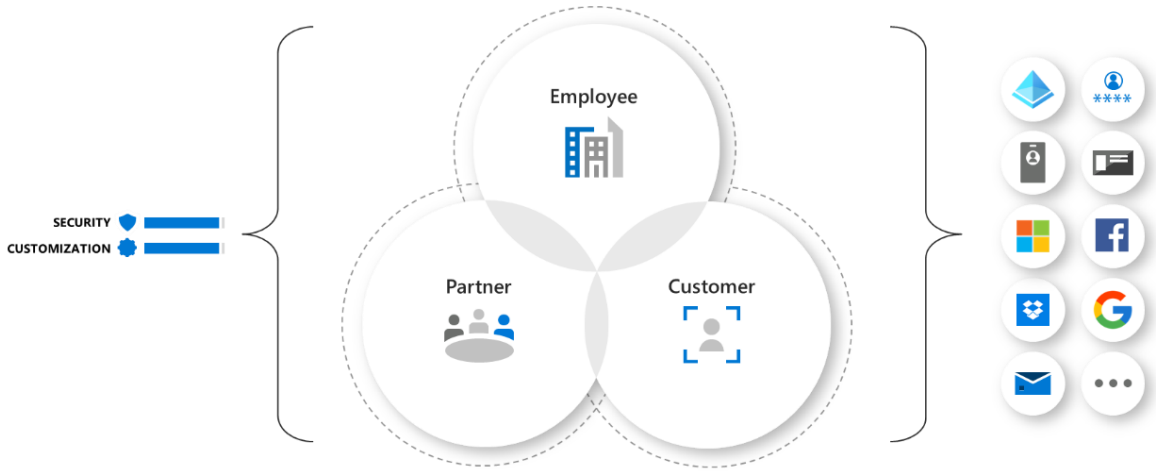

Browser
IDP /authorize endpoint
Web API
SPA redirects user to sign in
Access token to browser in fragment
API call with Access token
Return data to SPA

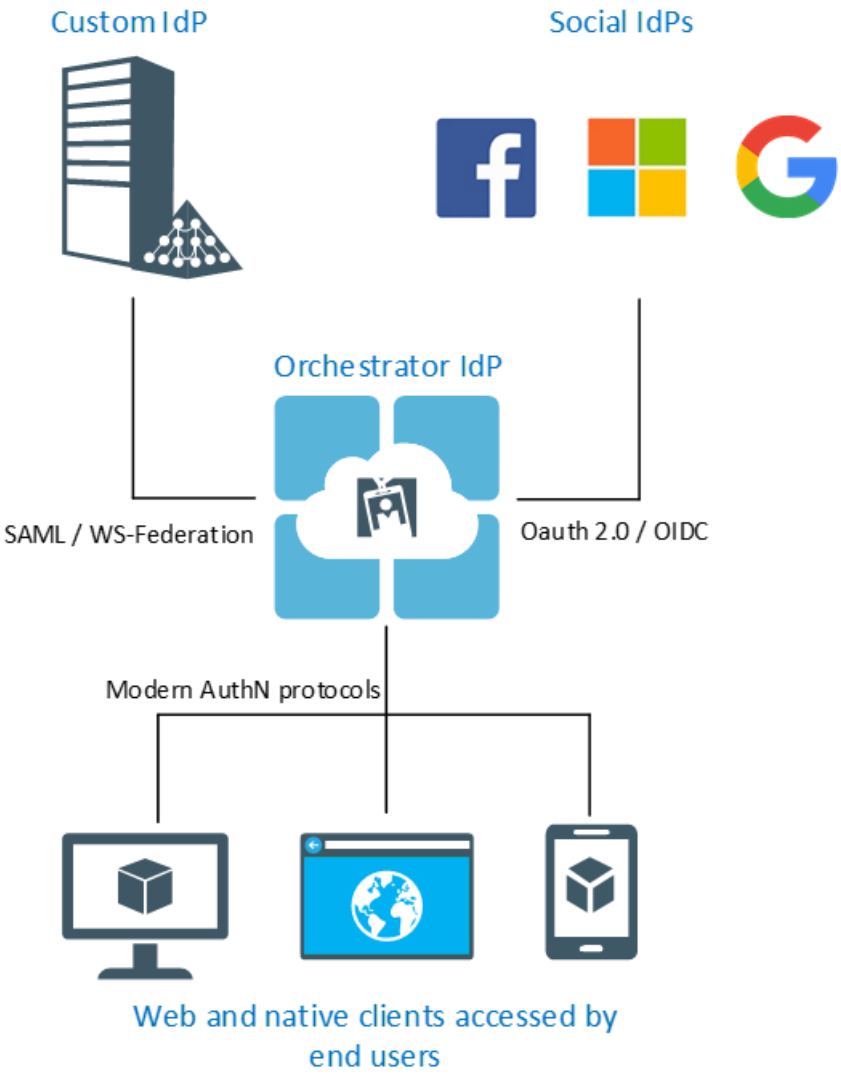
Chapter 6: Trends in API Authentication

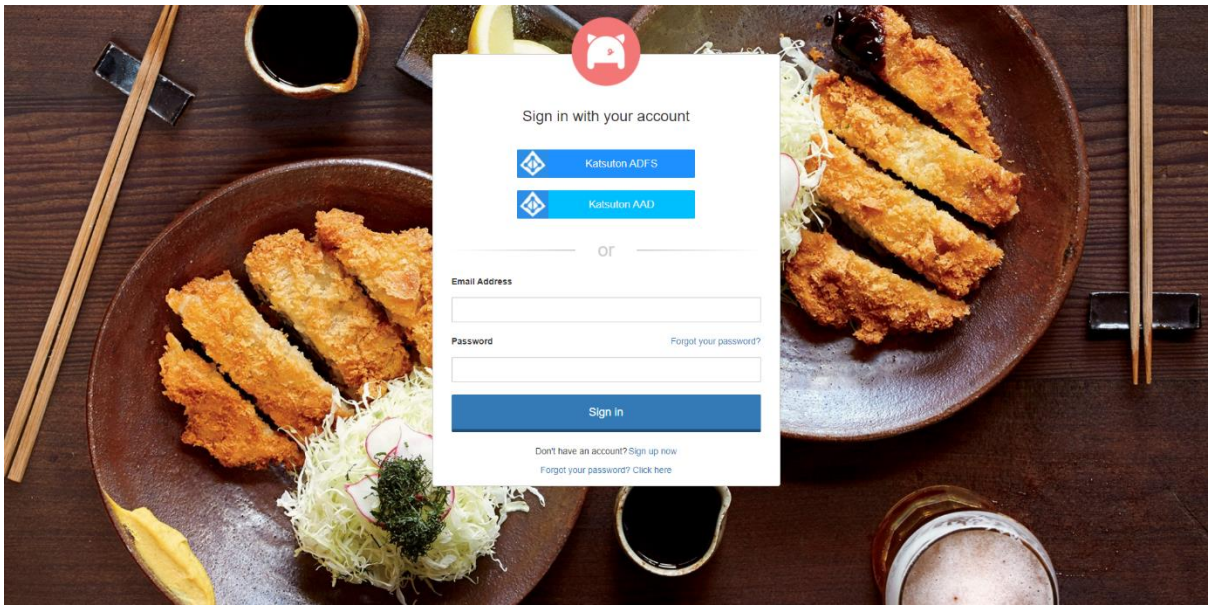


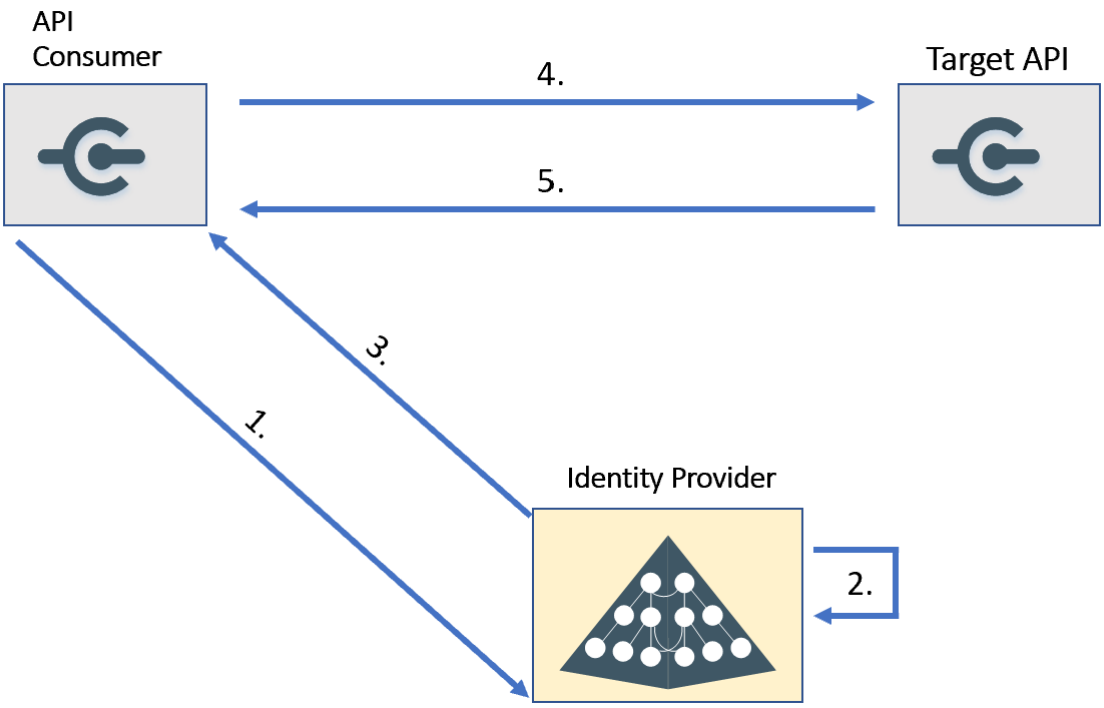


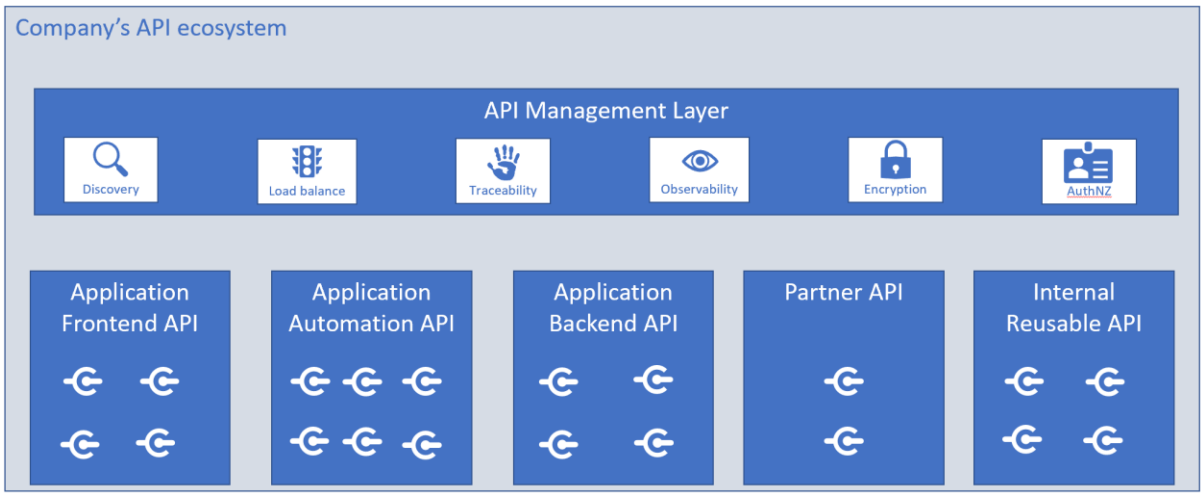

Company's API landscape
Partner APIs
Application A
API 1
API 2
Application B
API 1
API 2
API 3
Application C
API 1
API 2
API 3
Application D
API 1
API 2
API 3
Application backend APIs
Application A
API 1
API 2
Application B
API 1
API 2
API 3
Application automation APIs
Application A
API 1
API 2
Application B
API 1
API 2
Automation
Partners
Internal reusable APIs
API 1
API 2
API 3
API 4
API 5
API 6
API N

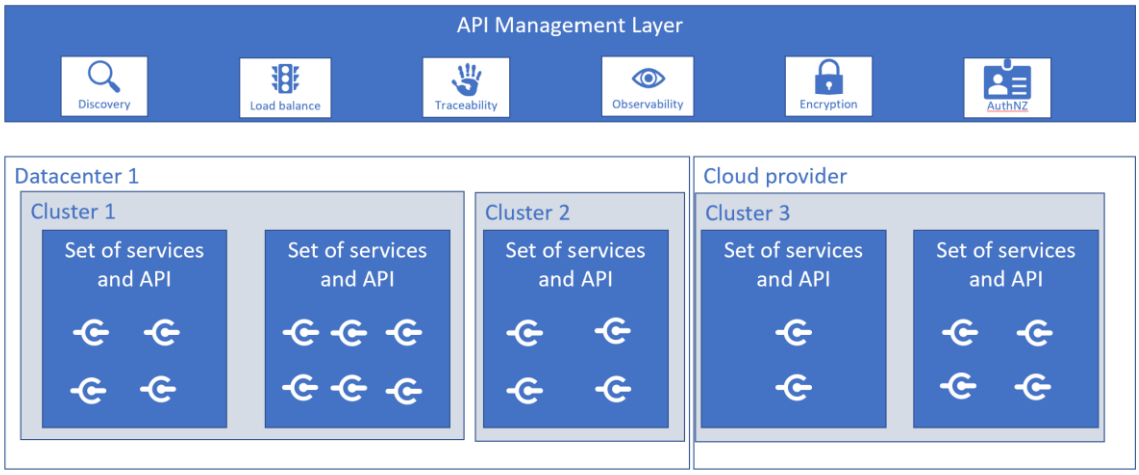

SECURITY
CUSTOMIZATION
Employee
Partner
Customer

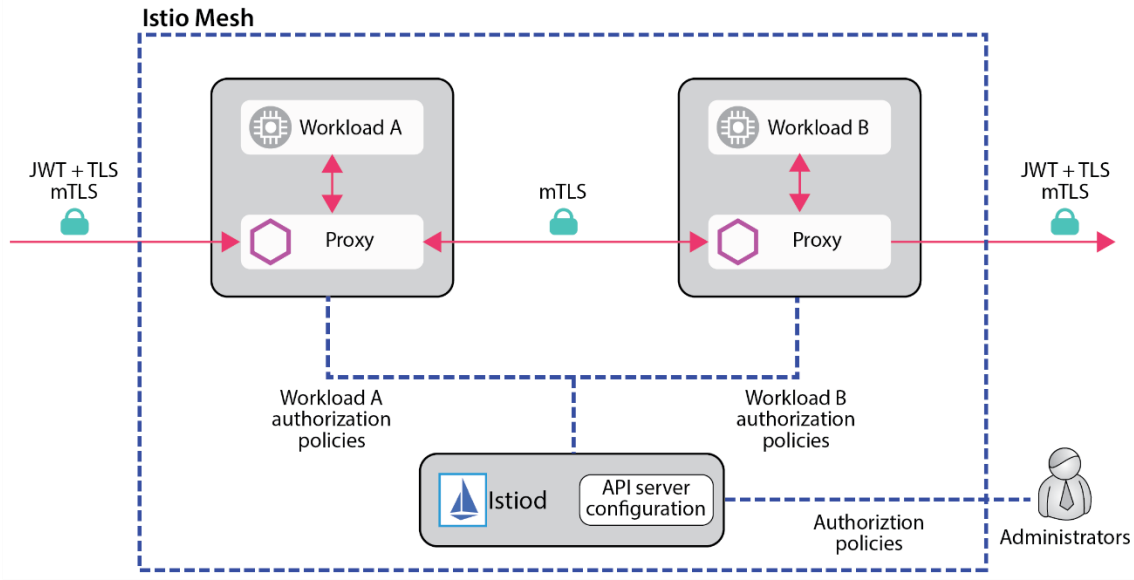

Custom IdP
Social IdPs
Orchestrator IdP
SAML / WS-Federation
Oauth 2.0 / OIDC
Modern AuthN protocols
Web and native clients accessed by end users

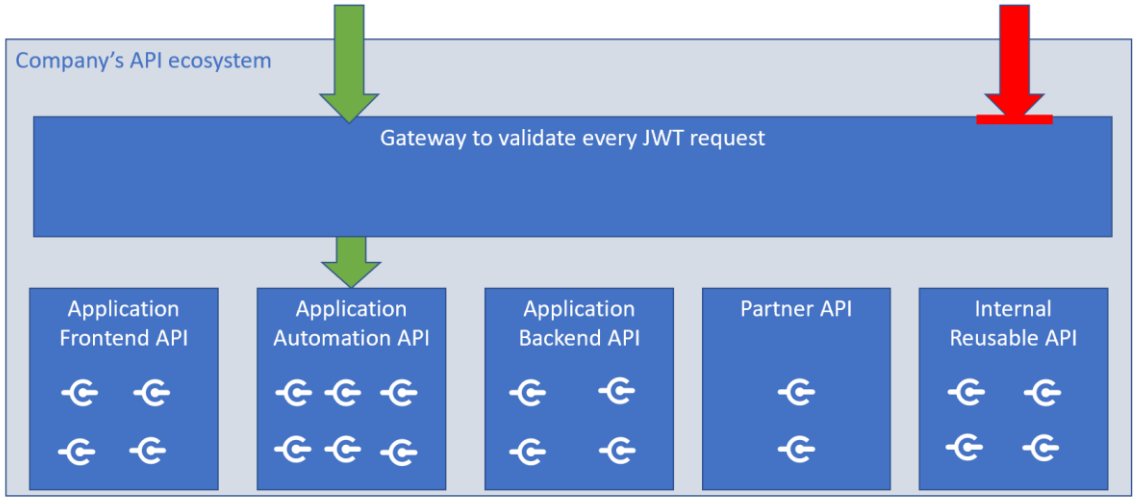

Sign in with your account
Katsuton ADFS
Katsuton AAD
or
Email Address
Password
Forgot your password?
Sign in
Don't have an account? Sign up now
Forgot your password? Click here


API
Consumer
Target API
4.
5.
3.
1.
Identity Provider
2.

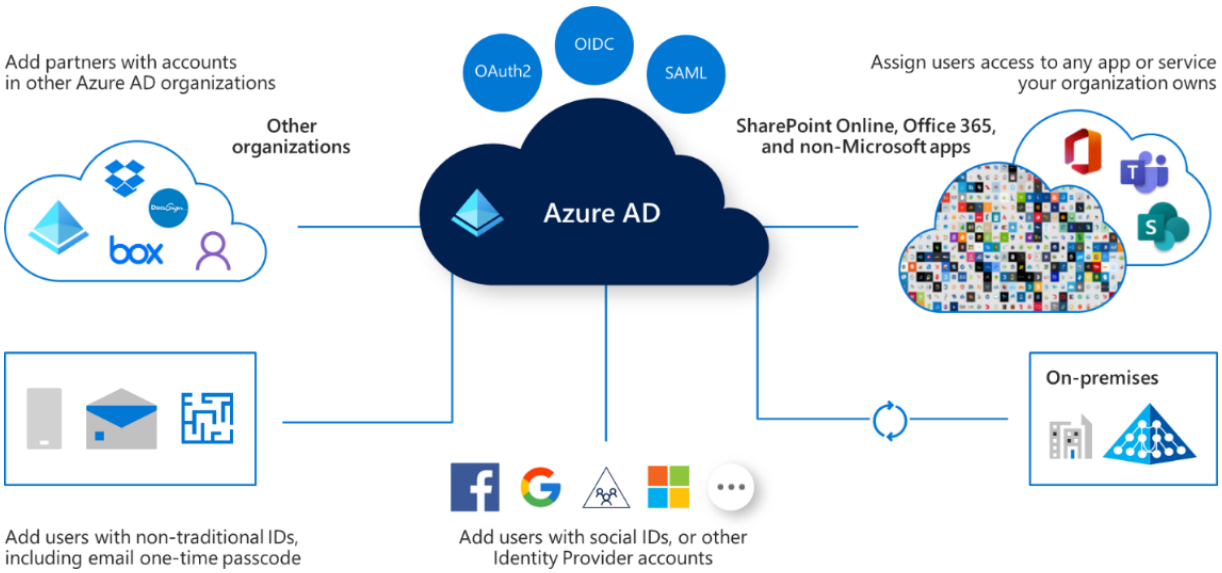

Company's API ecosystem
API Management Layer
Discovery
Load balance
Traceability
Observability
Encryption
AuthNZ
Application Frontend API
Application Automation API
Application Backend API
Partner API
Internal Reusable API

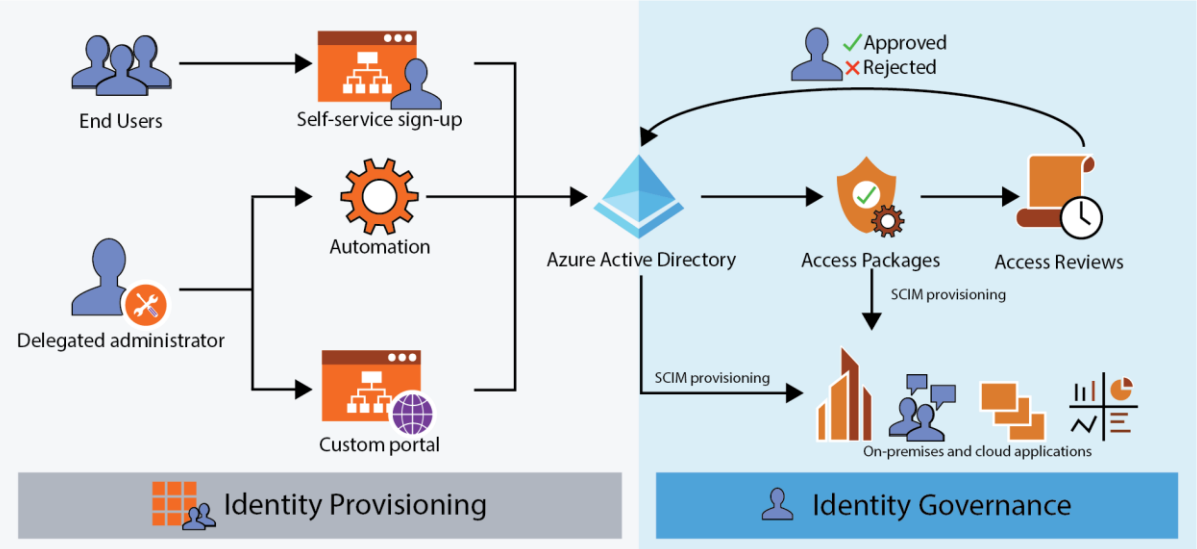

API Management Layer
Discovery
Load balance
Traceability
Observability
Encryption
AuthNZ
Datacenter 1
Cluster 1
Set of services and API
Set of services and API
Cluster 2
Set of services and API
Cloud provider
Cluster 3
Set of services and API
Set of services and API

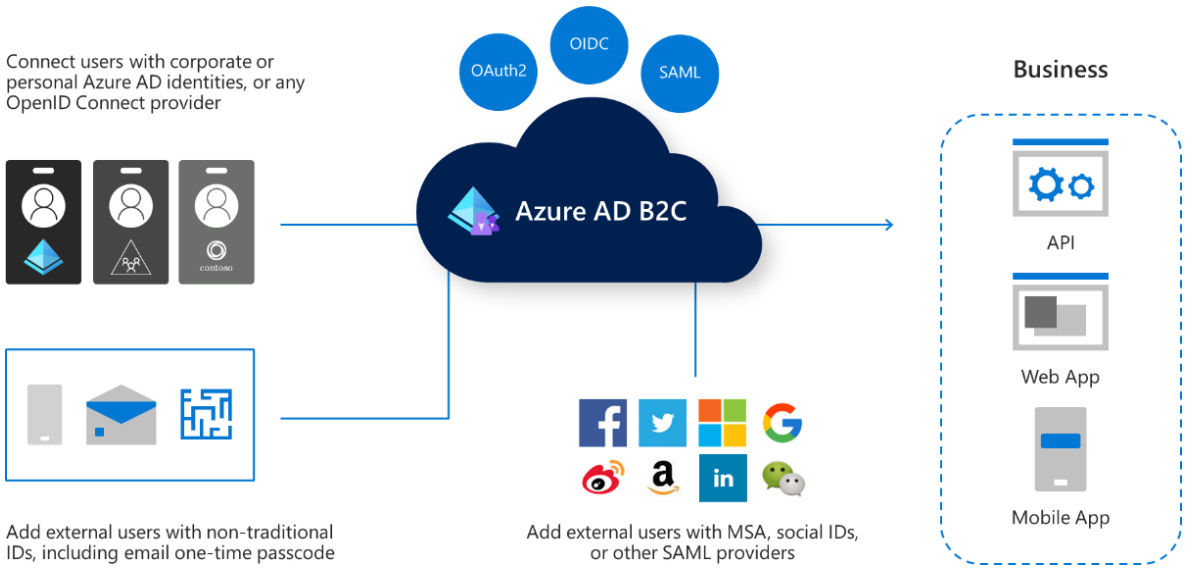

Istio Mesh
Workload A
Proxy
Workload B
Proxy
JWT + TLS
mTLS
mTLS
JWT + TLS
mTLS
Workload A authorization policies
Workload B authorization policies
Istiod
API server configuration
Authoriztion policies
Administrators

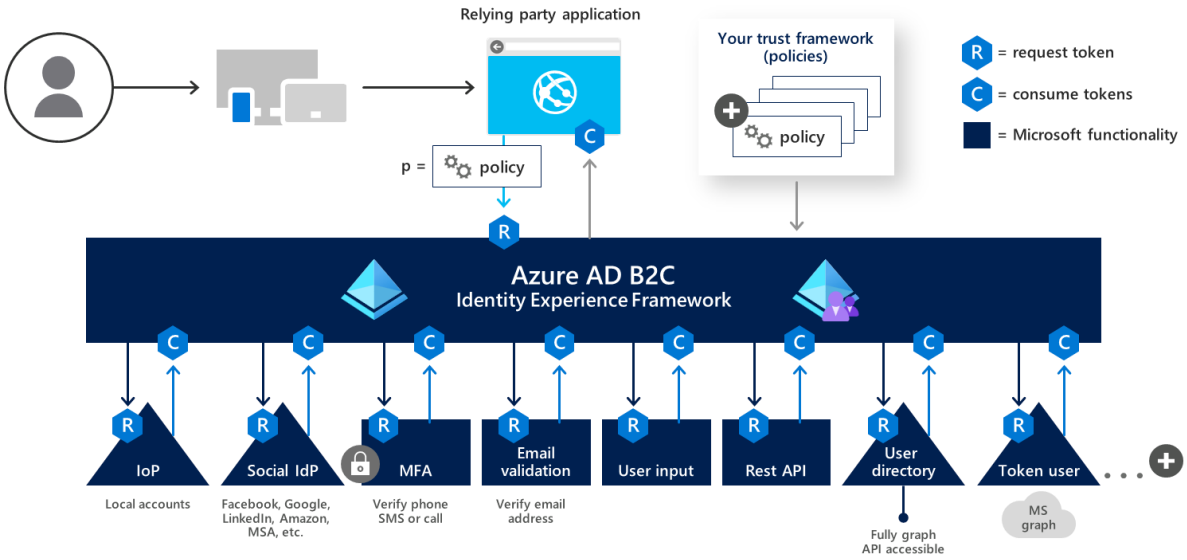

Company's API ecosystem
Gateway to validate every JWT request
Application Frontend API
Application Automation API
Application Backend API
Partner API
Internal Reusable API

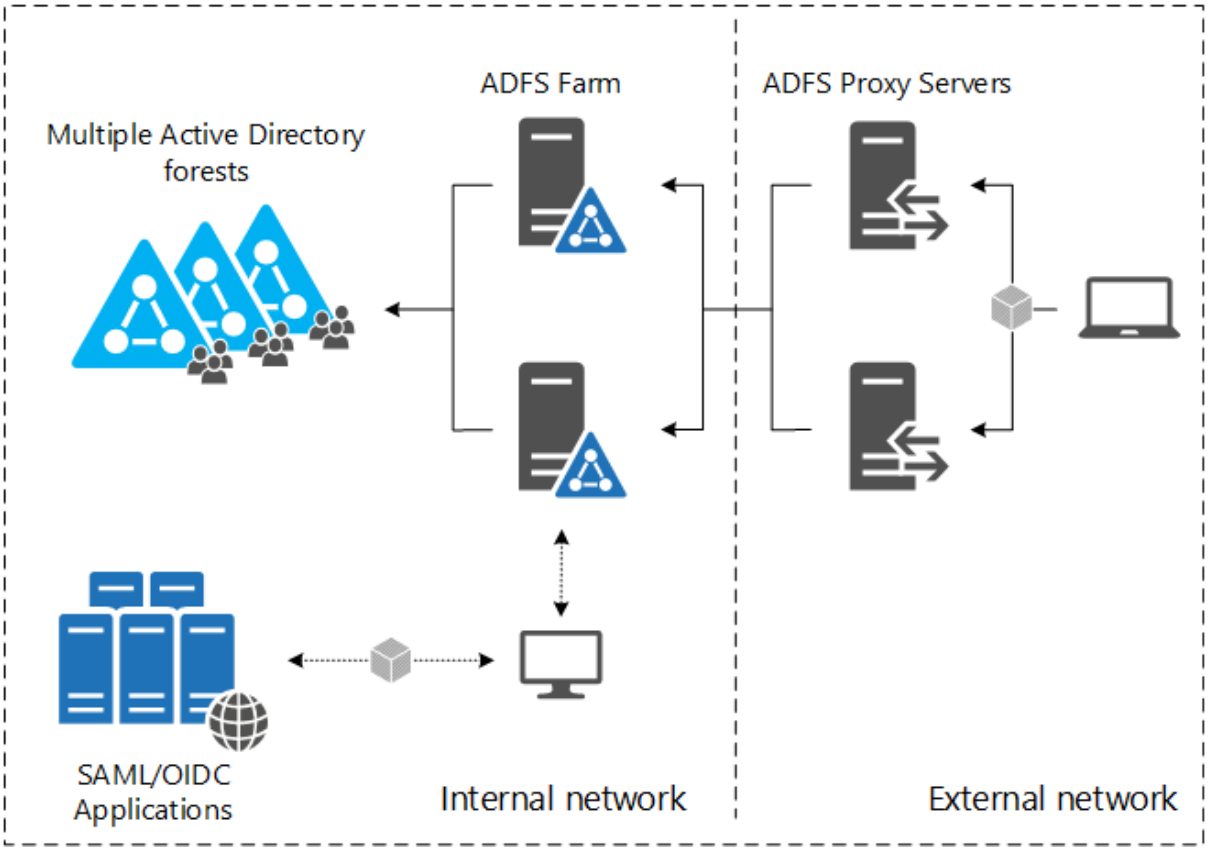
Chapter 7: Identity Providers in the Real World



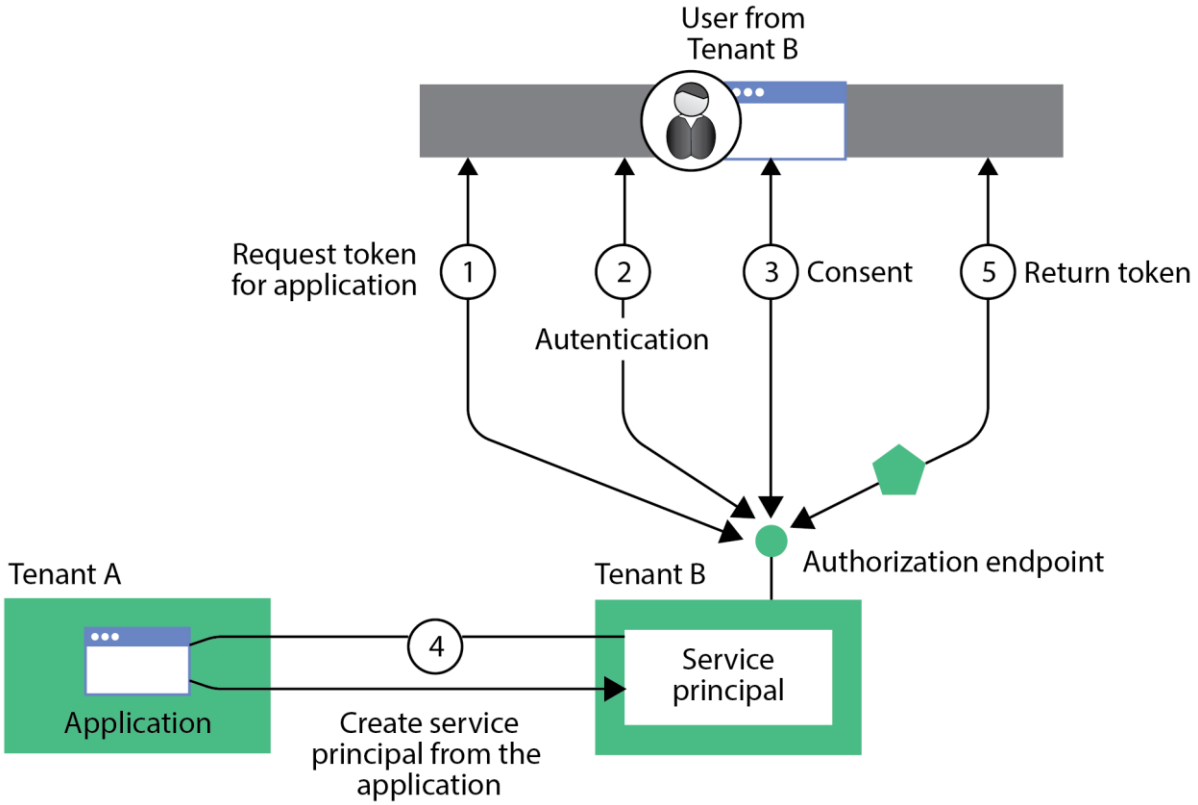

End Users
Self-service sign-up
Automation
Delegated administrator
Custom portal
Azure Active Directory
Approved
Rejected
Access Packages
Access Reviews
SCIM provisioning
SCIM provisioning
On-premises and cloud applications
Identity Provisioning
Identity Governance

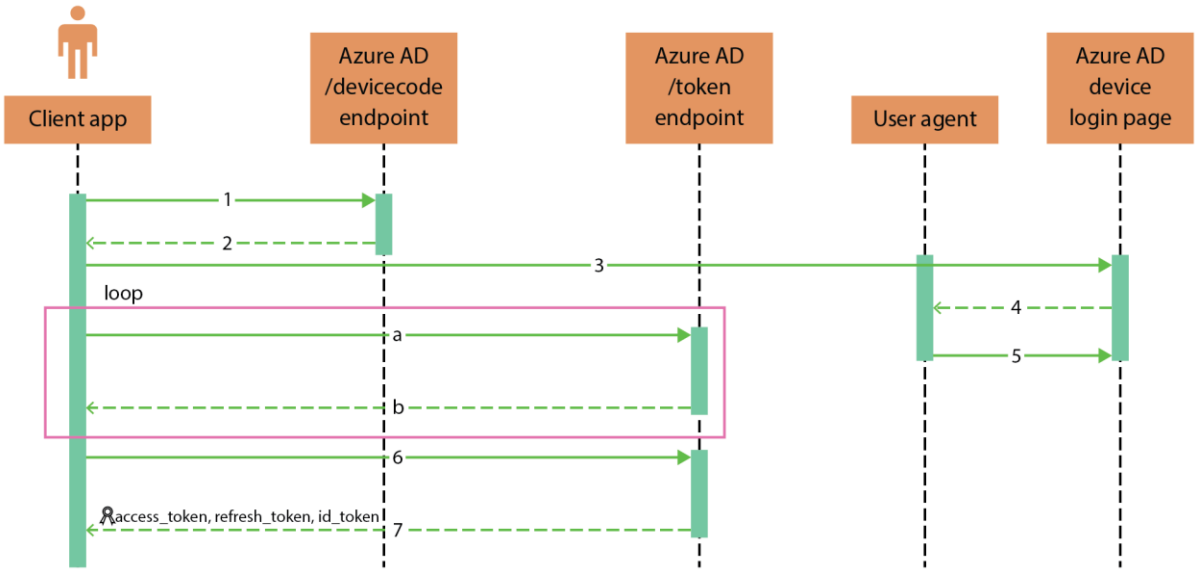

Connect users with corporate or personal Azure AD identities, or any OpenID Connect provider
OAuth2
OIDC
SAML
Azure AD B2C
Business
API
Web App
Mobile App
Add external users with non-traditional IDs, including email one-time passcode
Add external users with MSA, social IDs, or other SAML providers

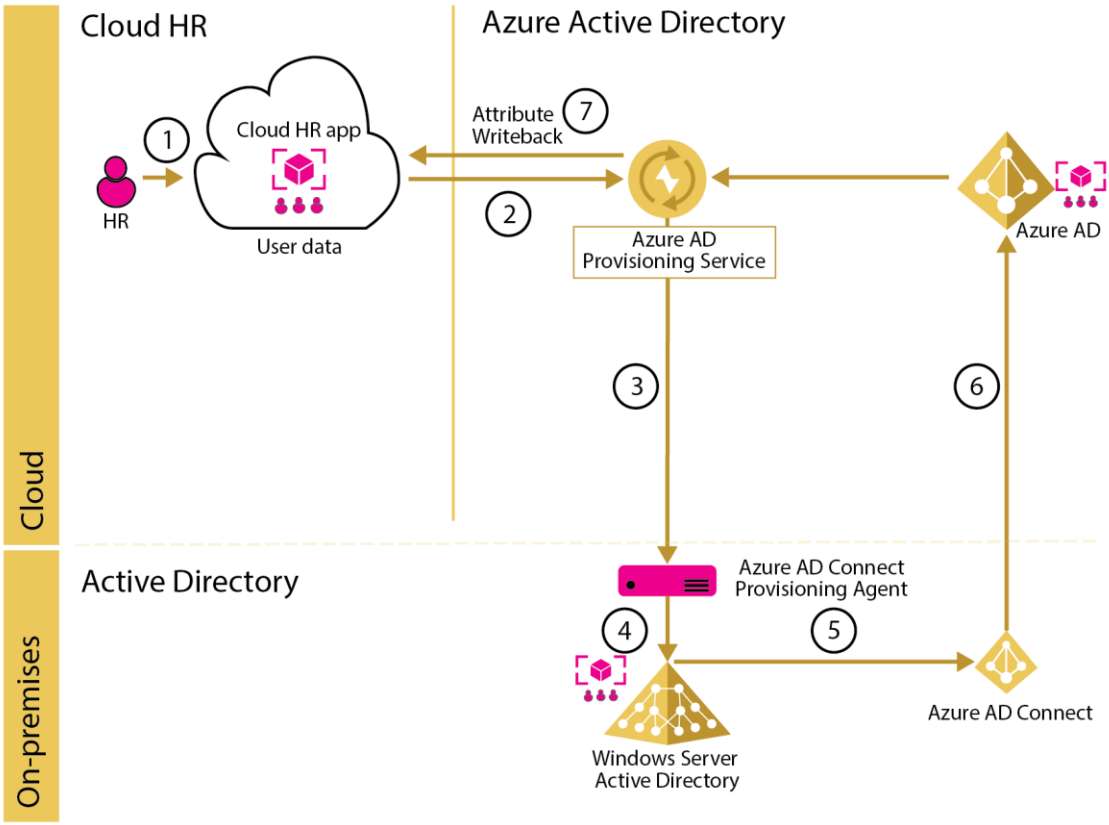

Relying party application
Your trust framework (policies)
policy
p =
policy
= request token
= consume tokens
= Microsoft functionality
Azure AD B2C
Identity Experience Framework
IoP
Local accounts
Social IdP
Facebook, Google, LinkedIn, Amazon, MSA, etc.
MFA
Verify phone SMS or call
Email validation
Verify email address
User input
Rest API
User directory
Fully graph API accessible
Token user
MS graph

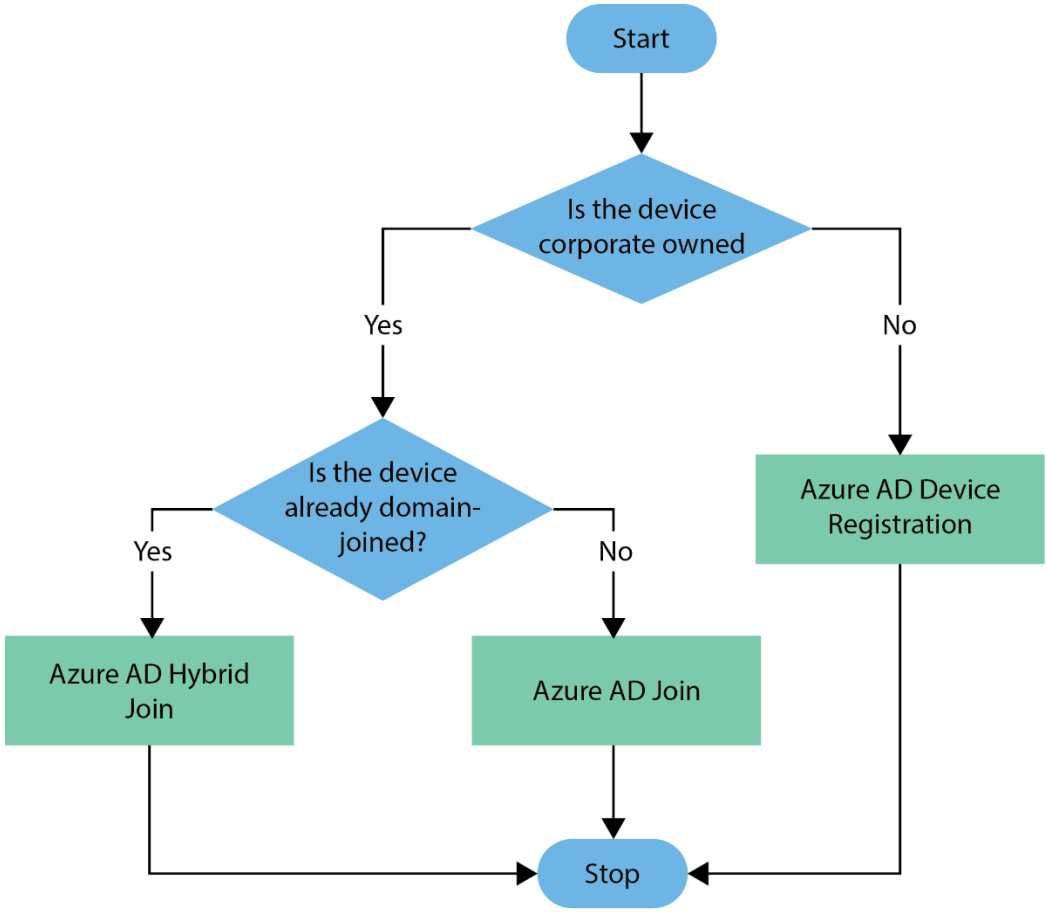

ADFS Farm
ADFS Proxy Servers
Multiple Active Directory forests
SAML/OIDC Applications
Internal network
External network

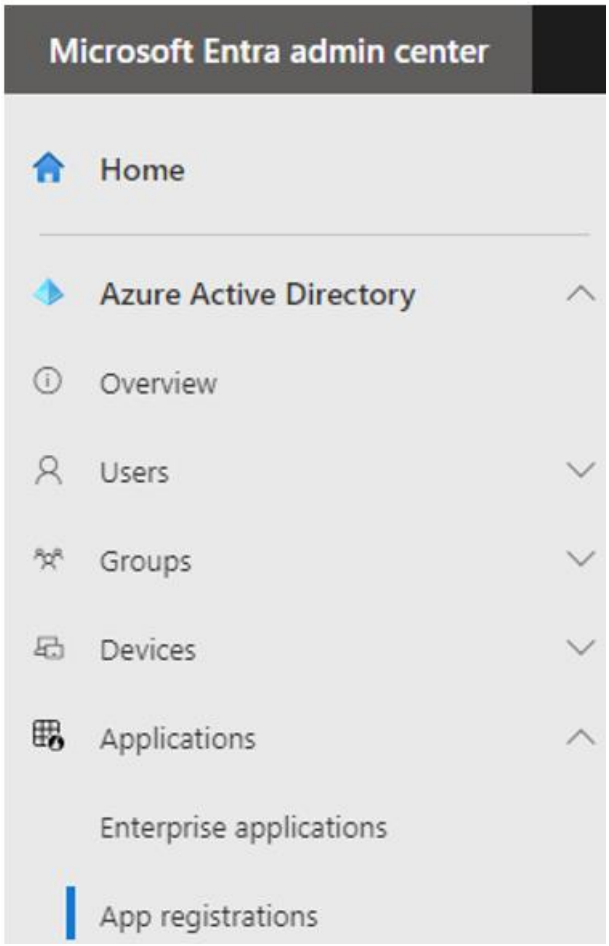
Chapter 8: Real-World Identity Provider – A Zoom-In on Azure Active Directory

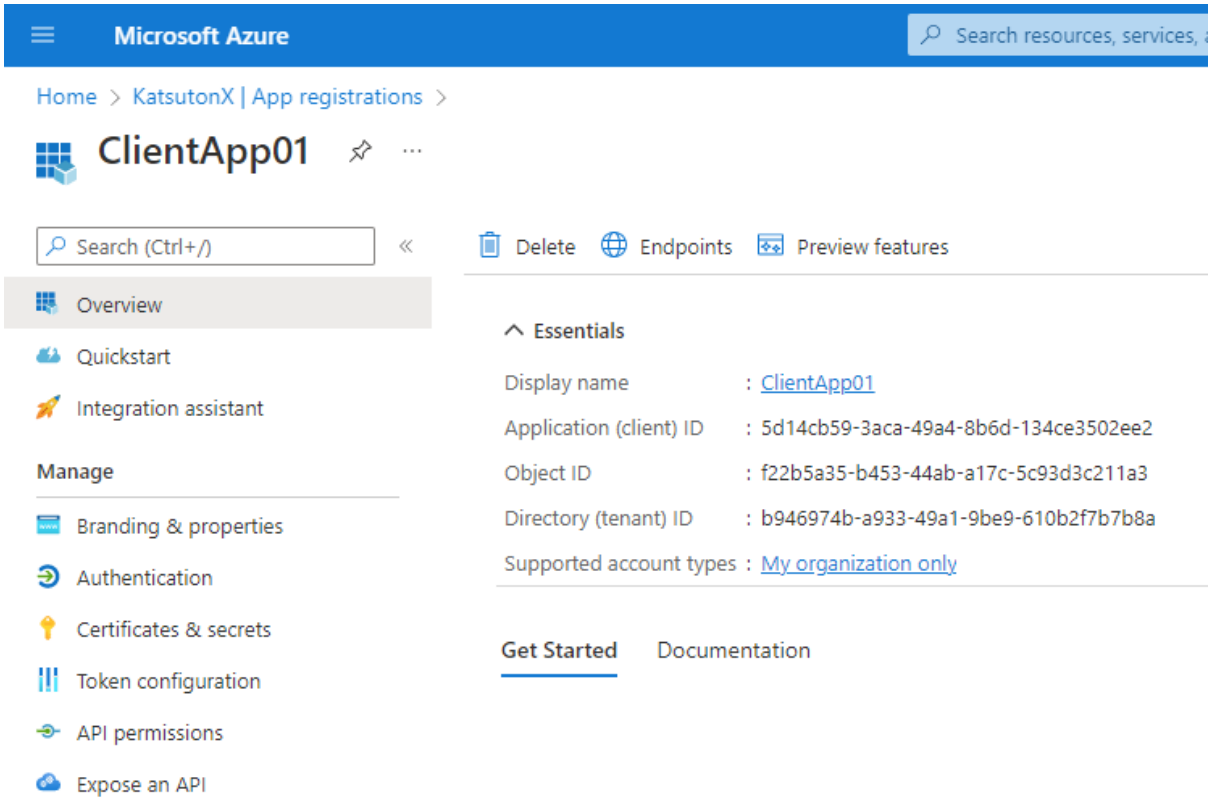


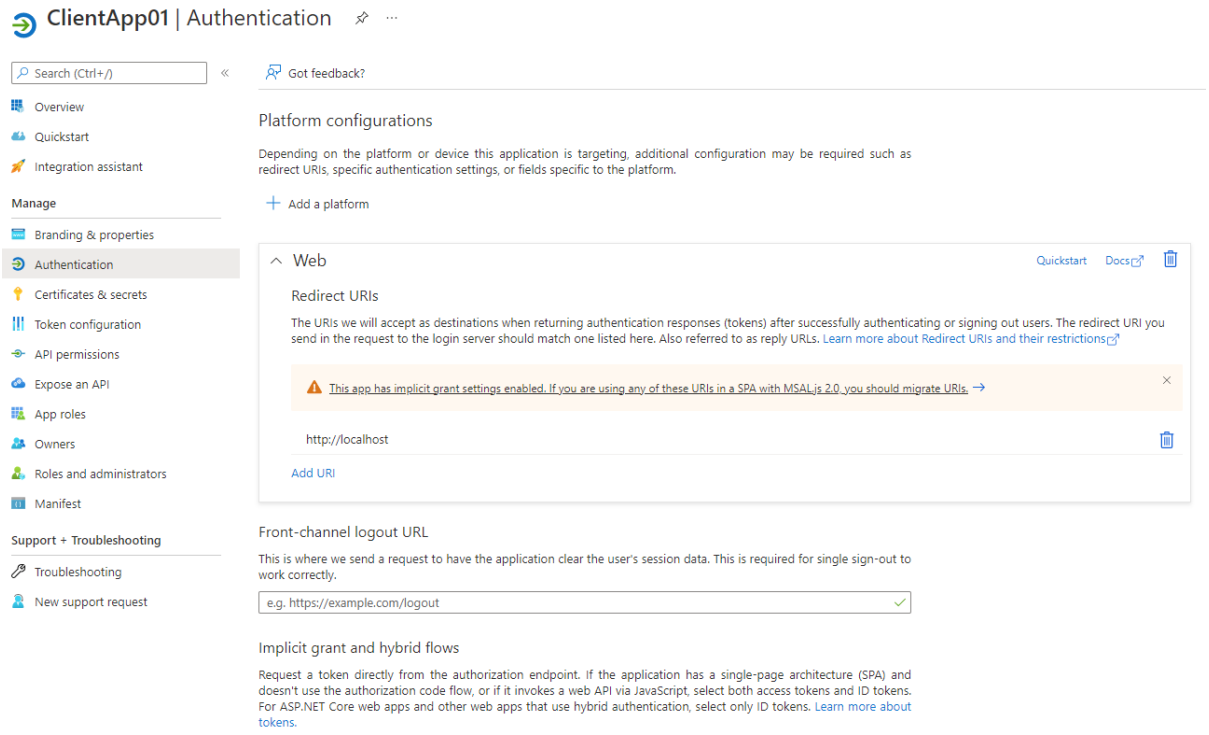



Cloud HR
Azure Active Directory
Cloud
On-premises
Cloud HR app
User data
HR
Attribute Writeback
Azure AD Provisioning Service
Azure AD
Active Directory
Azure AD Connect Provisioning Agent
Azure AD Connect
Windows Server Active Directory
1
2
3
4
5
6
7


Start
Is the device corporate owned
Yes
No
Is the device already domain-joined?
Yes
No
Azure AD Device Registration
Azure AD Hybrid Join
Azure AD Join
Stop


Microsoft Entra admin center
Home
Azure Active Directory
Overview
Users
Groups
Devices
Applications
Enterprise applications
App registrations


Microsoft Azure
Search resources, services,
Home > KatsutonX | App registrations >
ClientApp01
Search (Ctrl+/)
Overview
Quickstart
Integration assistant
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
Delete
Endpoints
Preview features
Essentials
Display name : ClientApp01
Application (client) ID : 5d14cb59-3aca-49a4-8b6d-134ce3502ee2
Object ID : f22b5a35-b453-44ab-a17c-5c93d3c211a3
Directory (tenant) ID : b946974b-a933-49a1-9be9-610b2f7b7b8a
Supported account types : My organization only
Get Started
Documentation



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

New client secret

Description	Expires	Value	Secret ID
main	12/30/2022	xDJ******************	ccdc4bf8-8fb0-4e8c-bc9e-07cb529bde7f

Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. Learn more

Add optional claim Add groups claim

Claim	Description	Token type
email	The addressable email for this user, if the user has one	ID
email	The addressable email for this user, if the user has one	Access
family_name	Provides the last name, surname, or family name of the user as defined in the user object	ID
given_name	Provides the first or "given" name of the user, as set on the user object	ID

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

+ Add a permission ✓ Grant admin consent for KatsutonX

API / Permissions name	Type	Description	Admin consent requ...	Status	
Microsoft Graph (3)					•••
email	Delegated	View users' email address	No	Granted for KatsutonX	•••
profile	Delegated	View users' basic profile	No	Granted for KatsutonX	•••
User.Read	Delegated	Sign in and read user profile	No	Granted for KatsutonX	•••
ServerApp01 (2)					•••
Read	Delegated	Read app data	No	Granted for KatsutonX	•••
Write	Delegated	Write app data	Yes	Granted for KatsutonX	•••

To view and manage permissions and user consent, try Enterprise applications.

Application ID URI api://ceff2f83-b273-470c-8d05-23d04d877528

Scopes defined by this API

Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.

Adding a scope here creates only delegated permissions. If you are looking to create application-only scopes, use 'App roles' and define app roles assignable to application type. Go to App roles.

+ Add a scope

Scopes	Who can consent	Admin consent display ...	User consent display na...	State
api://ceff2f83-b273-470c-8d05-23d04d877528/Write	Admins only	Write app data		Enabled
api://ceff2f83-b273-470c-8d05-23d04d877528/Read	Admins and users	Read app data		Enabled

Authorized client applications

Authorizing a client application indicates that this API trusts the application and users should not be asked to consent when the client calls this API.

+ Add a client application

Client Id	Scopes
No client applications have been authorized	

Endpoints

OAuth 2.0 authorization endpoint (v2)
https://login.microsoftonline.com/b946974b-a933-49a1-9be9-610b2f7b7b8a/oauth2/v2.0/authorize

OAuth 2.0 token endpoint (v2)
https://login.microsoftonline.com/b946974b-a933-49a1-9be9-610b2f7b7b8a/oauth2/v2.0/token

OAuth 2.0 authorization endpoint (v1)
https://login.microsoftonline.com/b946974b-a933-49a1-9be9-610b2f7b7b8a/oauth2/authorize

OAuth 2.0 token endpoint (v1)
https://login.microsoftonline.com/b946974b-a933-49a1-9be9-610b2f7b7b8a/oauth2/token

OpenID Connect metadata document
https://login.microsoftonline.com/b946974b-a933-49a1-9be9-610b2f7b7b8a/v2.0/.well-known/openid-configuration

Microsoft Graph API endpoint
https://graph.microsoft.com

Federation metadata document
https://login.microsoftonline.com/b946974b-a933-49a1-9be9-610b2f7b7b8a/federationmetadata/2007-06/federationmetadata.xml

WS-Federation sign-on endpoint
https://login.microsoftonline.com/b946974b-a933-49a1-9be9-610b2f7b7b8a/wsfed

SAML-P sign-on endpoint
https://login.microsoftonline.com/b946974b-a933-49a1-9be9-610b2f7b7b8a/saml2

SAML-P sign-out endpoint
https://login.microsoftonline.com/b946974b-a933-49a1-9be9-610b2f7b7b8a/saml2

Permissions

Applications can be granted permissions to your organization and its data by three methods: an admin consents to the application for all users, a user grants consent to the application, or an admin integrating an to the application. Learn more.

To request additional permissions for this application, use the application registration.

As an administrator you can grant consent on behalf of all users in this tenant, ensuring that end users will not be required to consent when using the application. Click the button below to grant admin consent.

Grant admin consent for KatsutonX

Admin consent | User consent

Search permissions

API Name	Claim value	Permission	Type
Microsoft Graph			
Microsoft Graph	email	View users' email address	Delegated
Microsoft Graph	profile	View users' basic profile	Delegated
Microsoft Graph	User.Read	Sign in and read user profile	Delegated
ServerApp01			
ServerApp01	Write	Write app data	Delegated
ServerApp01	Read	Read app data	Delegated

New ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Enable MFA for Engineers

Assignments

Users or workload identities

Specific users included

Cloud apps or actions

All cloud apps

Conditions

0 conditions selected

Access controls

Grant

1 control selected

Session

0 controls selected

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. Learn more

What does this policy apply to?

Users and groups

Include Exclude

- None
- All users
- Select users and groups
  - All guest and external users
  - Directory roles
  - Users and groups

Select

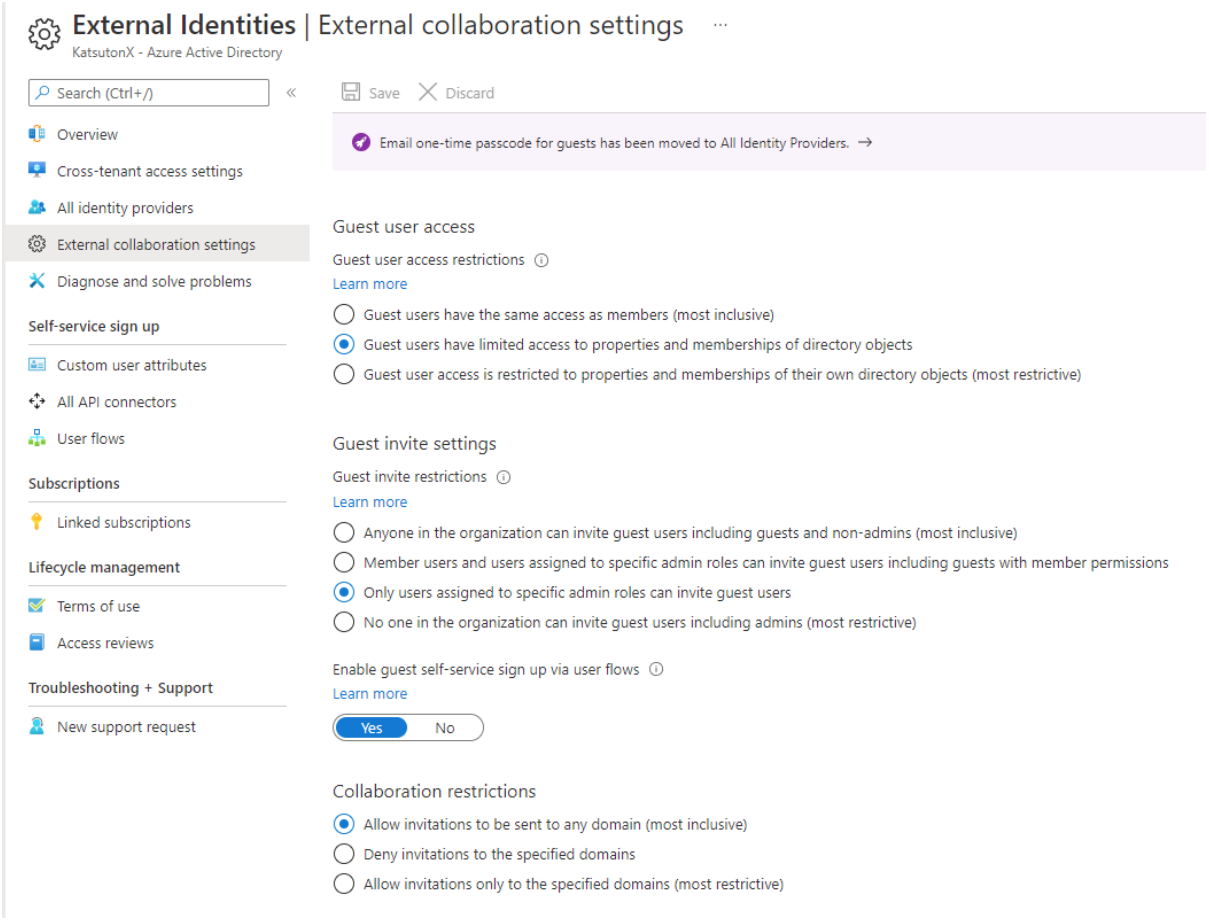
1 group

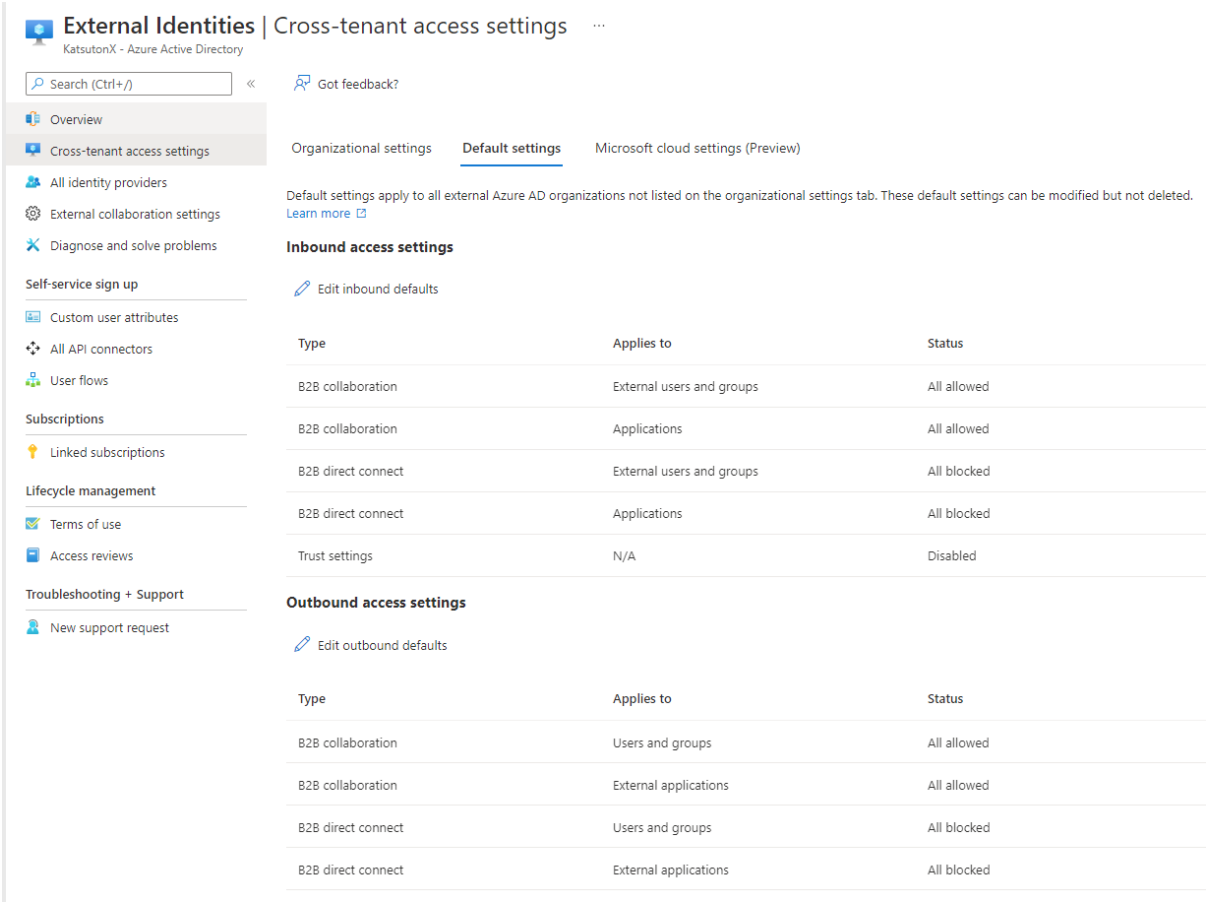
EN Engineers ...

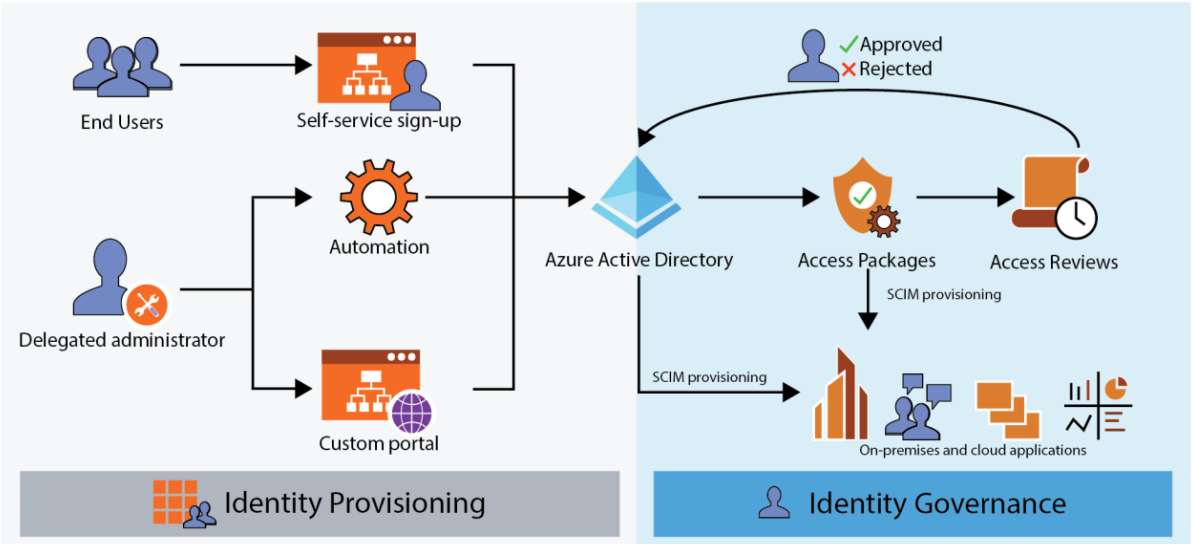
Enable policy

Report-only On Off

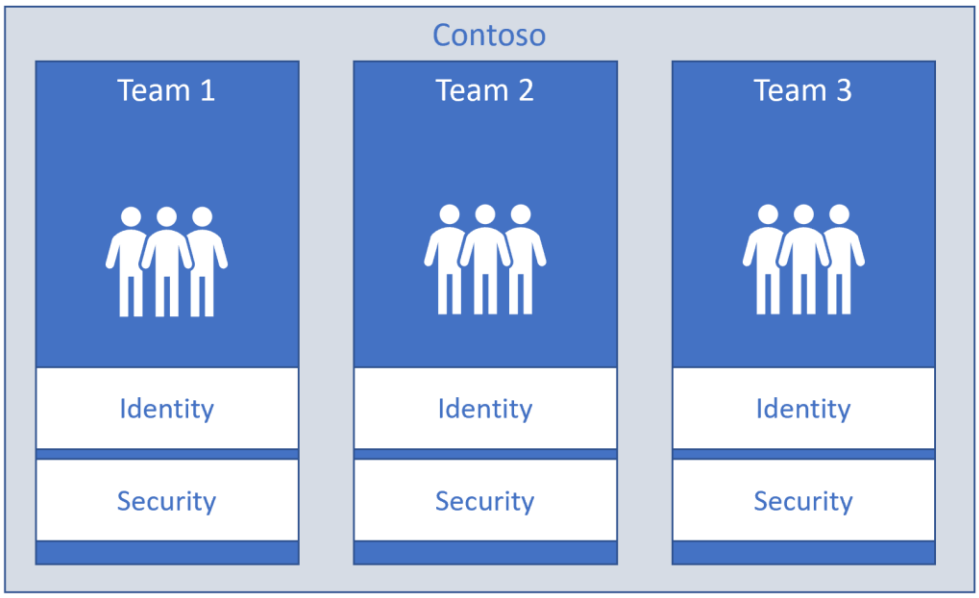
Create

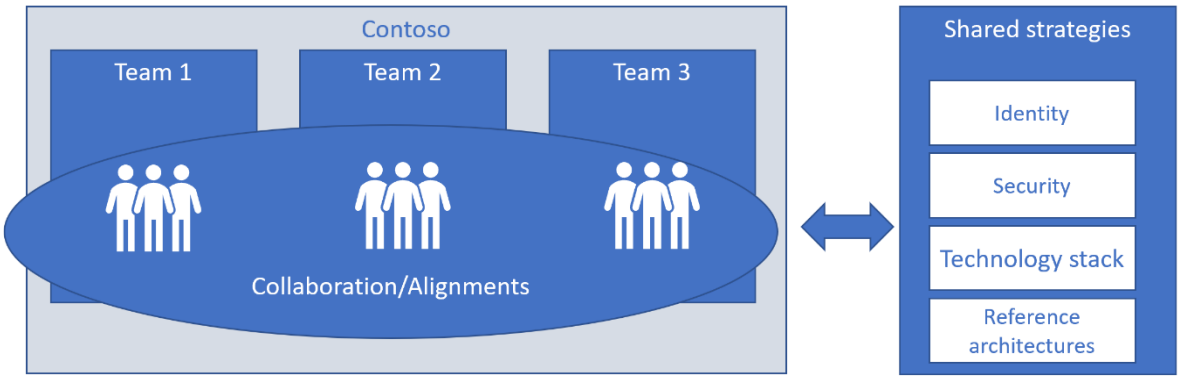

External Identities | External collaboration settings
KatsutonX - Azure Active Directory
Search (Ctrl+/)
Overview
Cross-tenant access settings
All identity providers
External collaboration settings
Diagnose and solve problems
Self-service sign up
Custom user attributes
All API connectors
User flows
Subscriptions
Linked subscriptions
Lifecycle management
Terms of use
Access reviews
Troubleshooting + Support
New support request
Save
Discard
Email one-time passcode for guests has been moved to All Identity Providers.
Guest user access
Guest user access restrictions
Learn more
Guest users have the same access as members (most inclusive)
Guest users have limited access to properties and memberships of directory objects
Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)
Guest invite settings
Guest invite restrictions
Learn more
Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
Member users and users assigned to specific admin roles can invite guest users including guests with member permissions
Only users assigned to specific admin roles can invite guest users
No one in the organization can invite guest users including admins (most restrictive)
Enable guest self-service sign up via user flows
Learn more
Yes
No
Collaboration restrictions
Allow invitations to be sent to any domain (most inclusive)
Deny invitations to the specified domains
Allow invitations only to the specified domains (most restrictive)

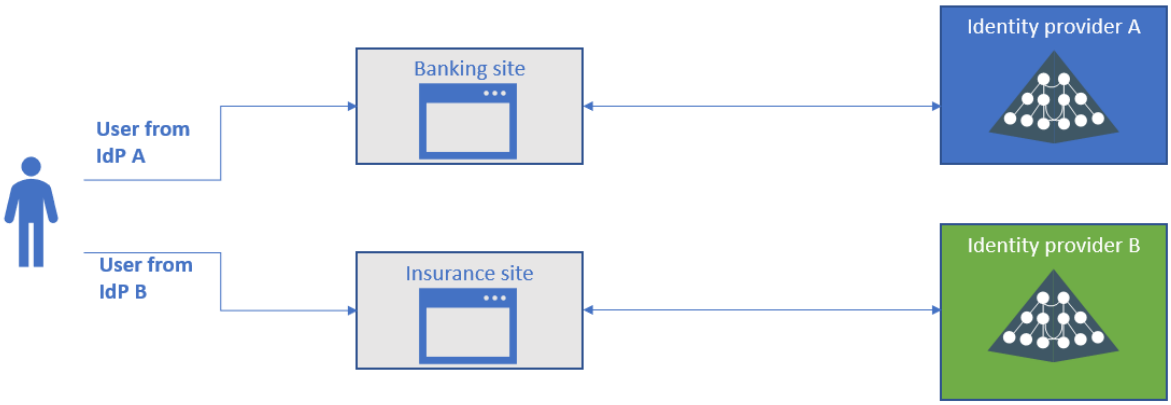

External Identities | Cross-tenant access settings
KatsutonX - Azure Active Directory
Search (Ctrl+/)
Got feedback?
Overview
Cross-tenant access settings
All identity providers
External collaboration settings
Diagnose and solve problems
Self-service sign up
Custom user attributes
All API connectors
User flows
Subscriptions
Linked subscriptions
Lifecycle management
Terms of use
Access reviews
Troubleshooting + Support
New support request
Organizational settings
Default settings
Microsoft cloud settings (Preview)
Default settings apply to all external Azure AD organizations not listed on the organizational settings tab. These default settings can be modified but not deleted.
Learn more
Inbound access settings
Edit inbound defaults
Type
Applies to
Status
B2B collaboration
External users and groups
All allowed
B2B collaboration
Applications
All allowed
B2B direct connect
External users and groups
All blocked
B2B direct connect
Applications
All blocked
Trust settings
N/A
Disabled
Outbound access settings
Edit outbound defaults
Type
Applies to
Status
B2B collaboration
Users and groups
All allowed
B2B collaboration
External applications
All allowed
B2B direct connect
Users and groups
All blocked
B2B direct connect
External applications
All blocked

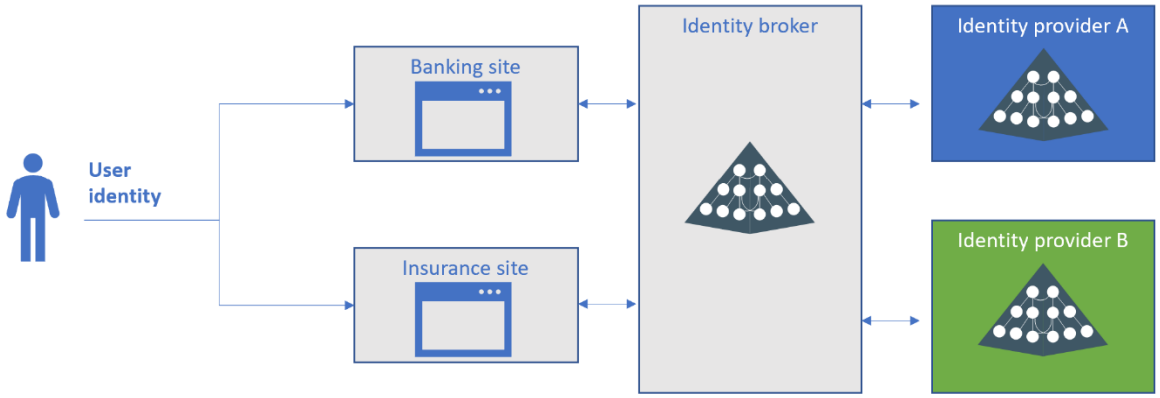

End Users
Self-service sign-up
Automation
Delegated administrator
Custom portal
Approved
Rejected
Azure Active Directory
Access Packages
Access Reviews
SCIM provisioning
SCIM provisioning
On-premises and cloud applications
Identity Provisioning
Identity Governance

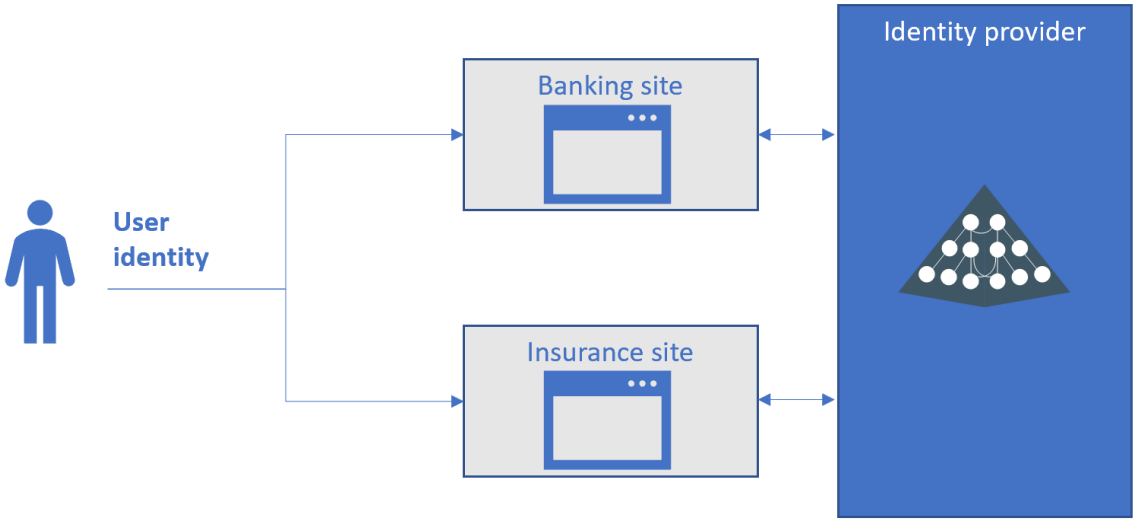
Chapter 9: Exploring Real-World Scenarios

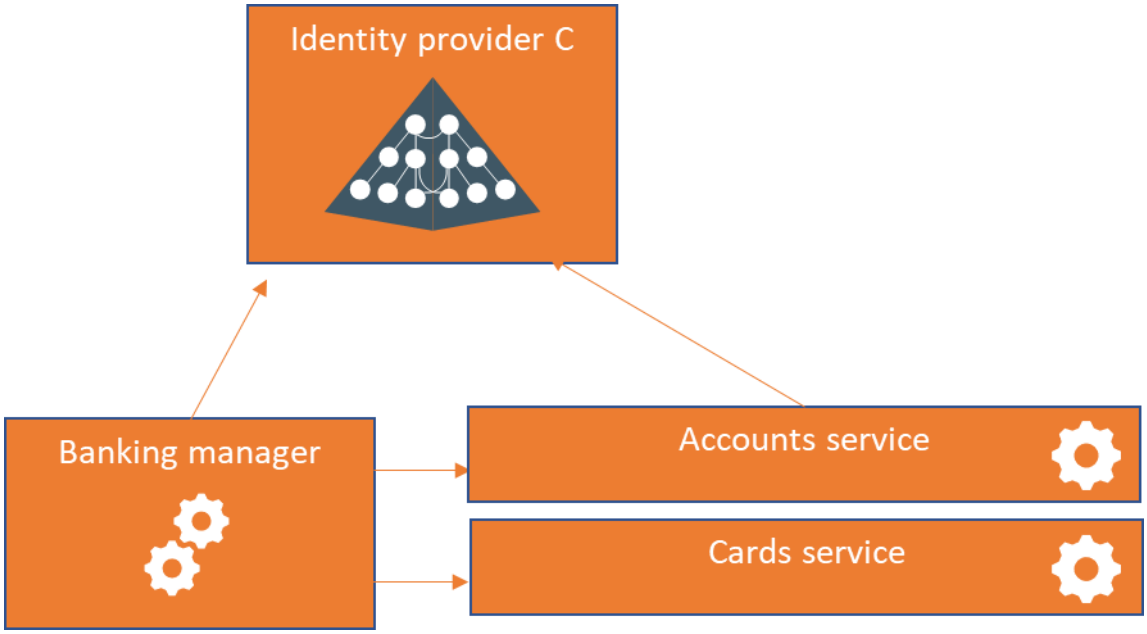


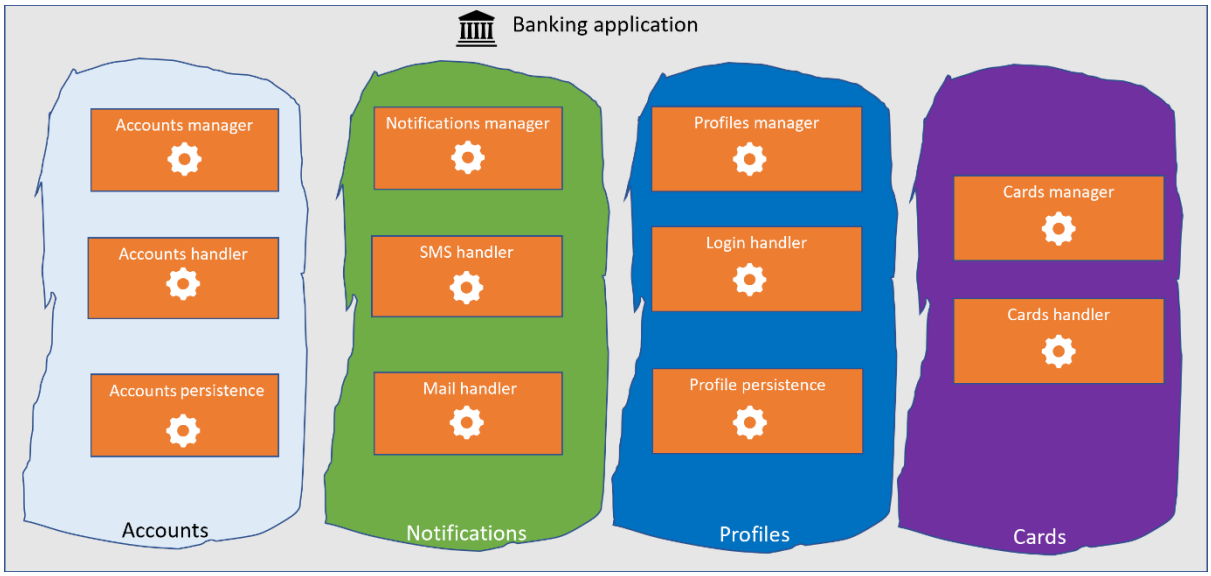


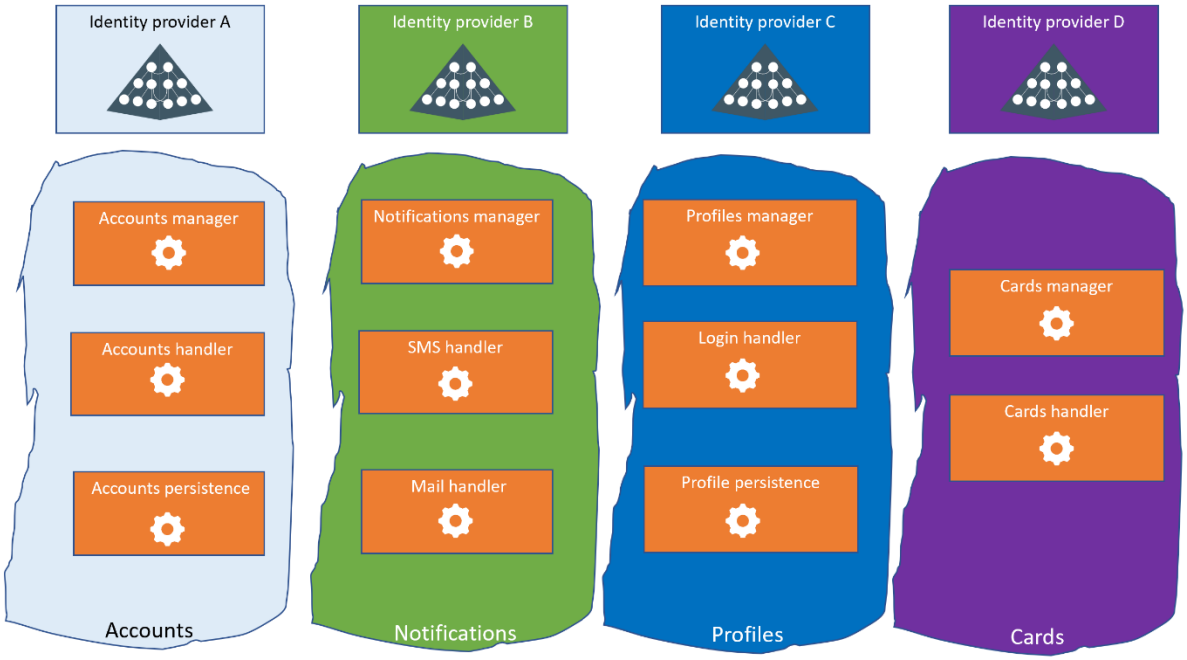


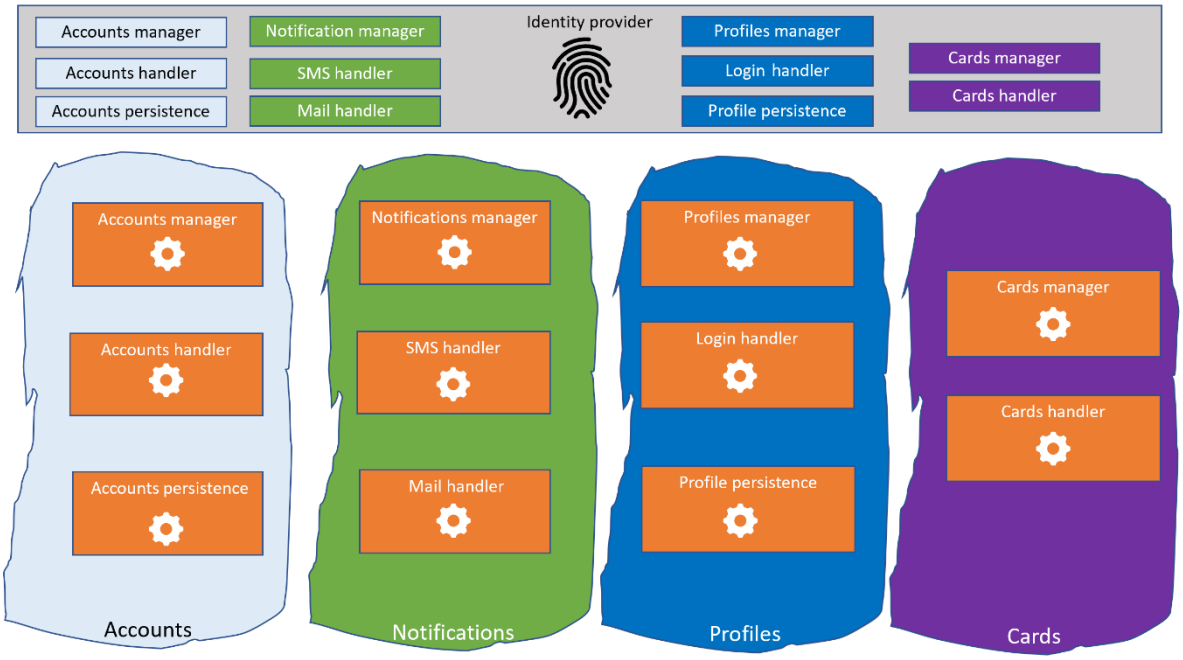

User identity
Banking site
Insurance site
Identity broker
Identity provider A
Identity provider B

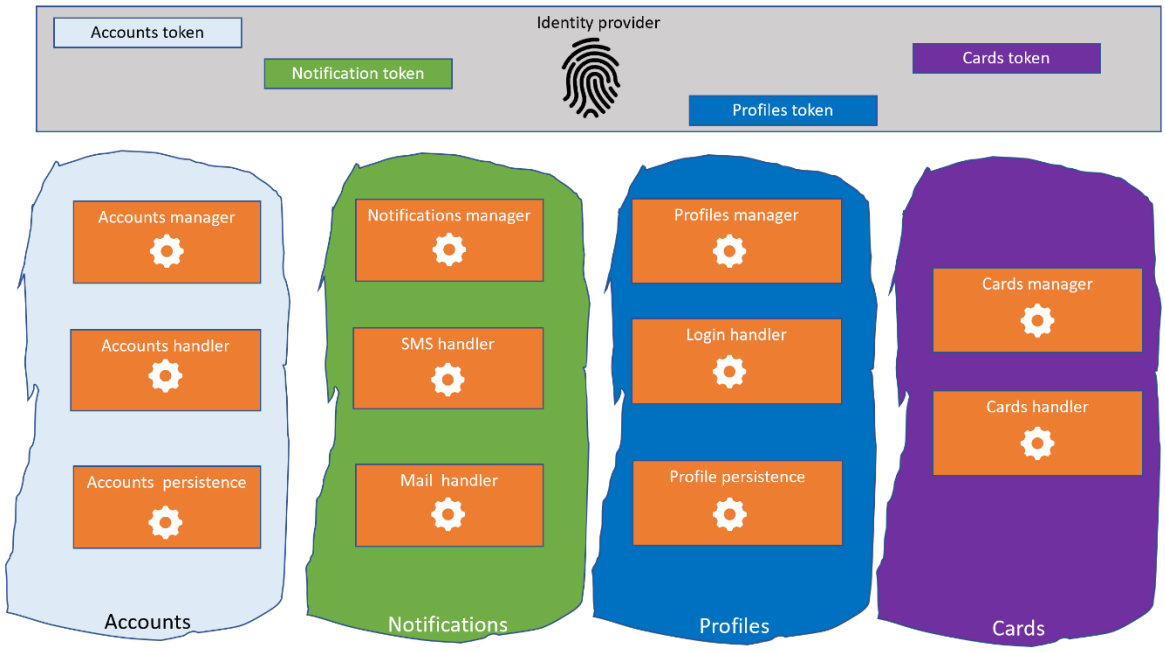

User identity
Banking site
Insurance site
Identity provider

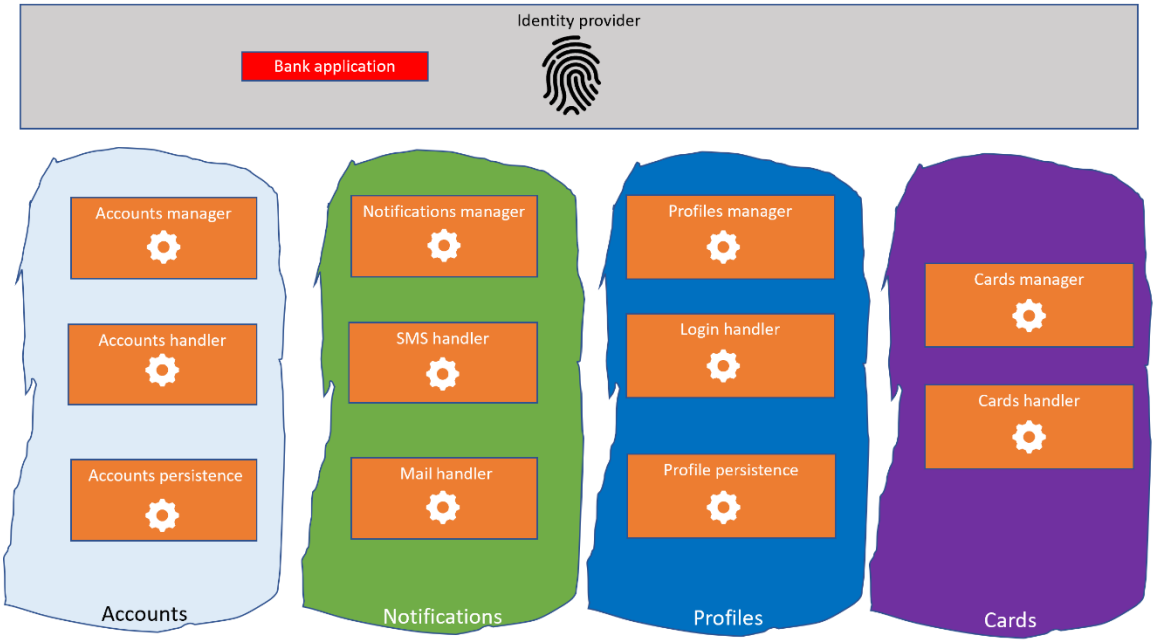

Identity provider C
Banking manager
Accounts service
Cards service

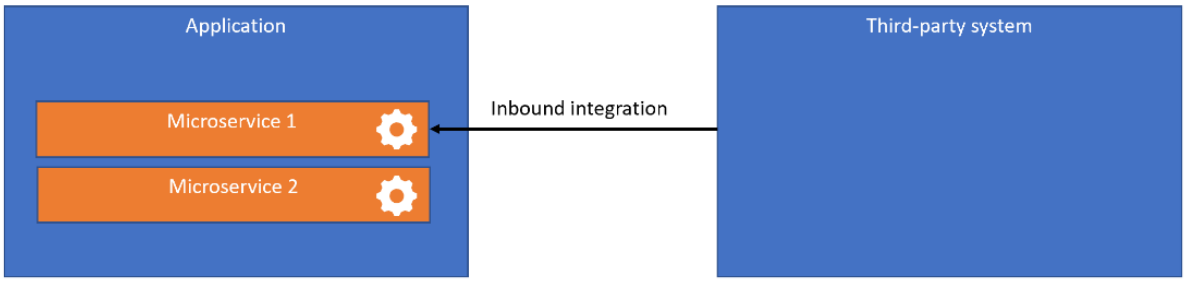

Banking application
Accounts manager
Accounts handler
Accounts persistence
Accounts
Notifications manager
SMS handler
Mail handler
Notifications
Profiles manager
Login handler
Profile persistence
Profiles
Cards manager
Cards handler
Cards

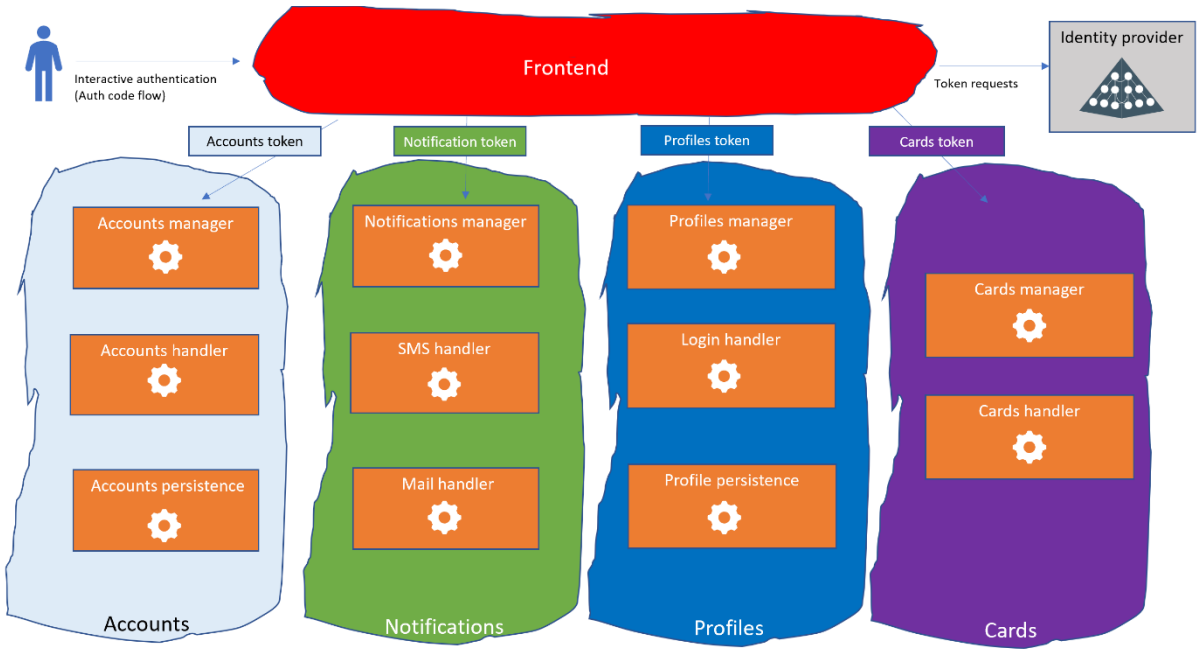

Identity provider A
Identity provider B
Identity provider C
Identity provider D
Accounts manager
Accounts handler
Accounts persistence
Accounts
Notifications manager
SMS handler
Mail handler
Notifications
Profiles manager
Login handler
Profile persistence
Profiles
Cards manager
Cards handler
Cards

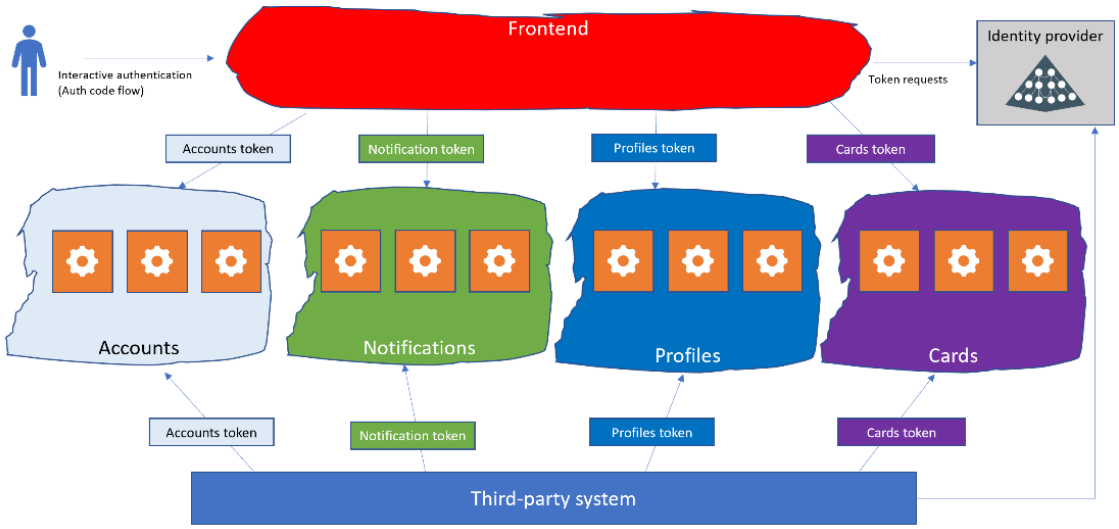

Accounts manager
Accounts handler
Accounts persistence
Notification manager
SMS handler
Mail handler
Identity provider
Profiles manager
Login handler
Profile persistence
Cards manager
Cards handler
Accounts manager
Accounts handler
Accounts persistence
Accounts
Notifications manager
SMS handler
Mail handler
Notifications
Profiles manager
Login handler
Profile persistence
Profiles
Cards manager
Cards handler
Cards

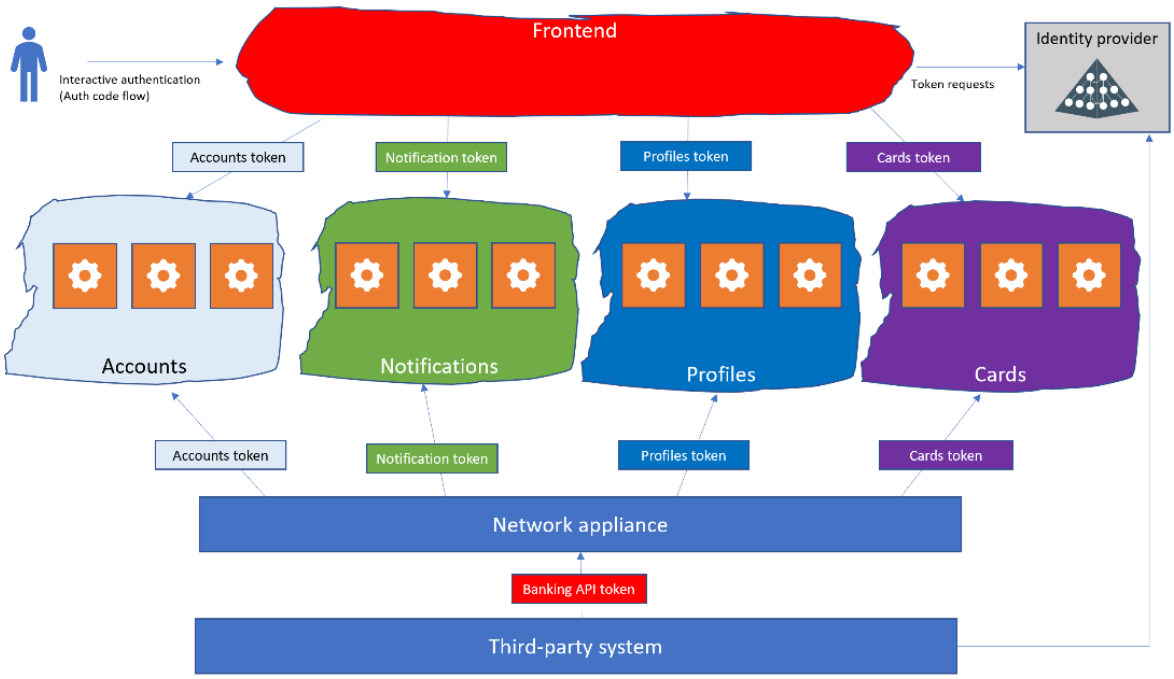

Accounts token
Notification token
Identity provider
Profiles token
Cards token
Accounts manager
Accounts handler
Accounts persistence
Accounts
Notifications manager
SMS handler
Mail handler
Notifications
Profiles manager
Login handler
Profile persistence
Profiles
Cards manager
Cards handler
Cards


Identity provider
Bank application
Accounts manager
Accounts handler
Accounts persistence
Accounts
Notifications manager
SMS handler
Mail handler
Notifications
Profiles manager
Login handler
Profile persistence
Profiles
Cards manager
Cards handler
Cards


Application
Microservice 1
Microservice 2
Inbound integration
Third-party system


Interactive authentication
(Auth code flow)
Frontend
Token requests
Identity provider
Accounts token
Notification token
Profiles token
Cards token
Accounts manager
Accounts handler
Accounts persistence
Accounts
Notifications manager
SMS handler
Mail handler
Notifications
Profiles manager
Login handler
Profile persistence
Profiles
Cards manager
Cards handler
Cards


Interactive authentication
(Auth code flow)
Frontend
Token requests
Identity provider
Accounts token
Notification token
Profiles token
Cards token
Accounts
Notifications
Profiles
Cards
Accounts token
Notification token
Profiles token
Cards token
Third-party system


Frontend
Identity provider
Interactive authentication
(Auth code flow)
Token requests
Accounts token
Notification token
Profiles token
Cards token
Accounts
Notifications
Profiles
Cards
Accounts token
Notification token
Profiles token
Cards token
Network appliance
Banking API token
Third-party system