Manage and secure customer identities with Azure AD B2C

Thomas Naunheim

DNUG Koblenz, 11. Dezember 2019

Agenda

1. Overview of Azure AD B2C
2. Integration of Apps and APIs
3. User flows and policies
4. Branding and Customizing
5. Management and Operations
6. Identity Protection and Security

About Me

Thomas Naunheim

Cloud Engineer
Koblenz, Germany

@Thomas_Live

Thomas@Naunheim.net

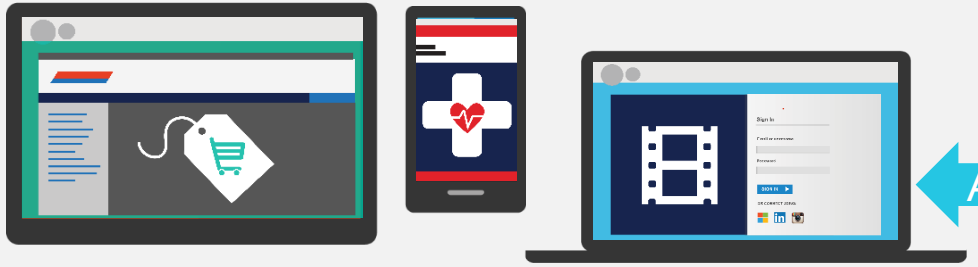
www.cloud-architekt.net

Azure AD B2C
Overview

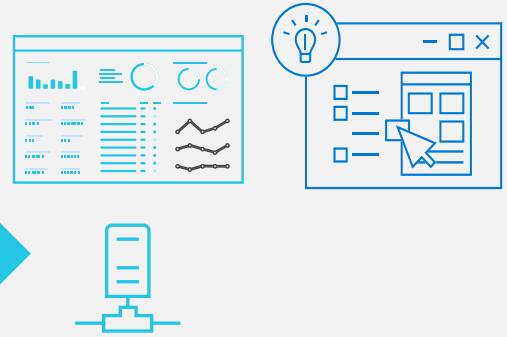
Requirements for
Customer Identity & Access Management (CIAM)

Developer

SSO



API



Bring-Your-Own Identity

Multi-Brand/-Platform Apps

Enterprise-Integration

Source: Microsoft AD B2C GTP

Build-Your-Own (BYO)-Style

- **Security & privacy risks**
  - Storing credentials and PII in application databases
- **Total Cost of Ownership (TCO)**
  - Software licensing, maintenance, and upgrade costs
  - 24x7 operations and support staff
- **QoS challenges**
  - High-availability and disaster recovery infrastructure
  - Scalability (up to millions of consumers)
  - Elastic response to demand spikes
- **Disparate systems**
  - Unified view of the consumer across apps

Source: Microsoft (BRK3179 „Modernize your application's consumer identity management with Azure Active Directory B2C")

Azure AD B2C

Customers

Social IDs, email, or local accounts

Business & Government IDs

Use social accounts

Create custom user attributes

Protect your users with MFA

Customize your pages using HTML and CSS

JavaScript

Business

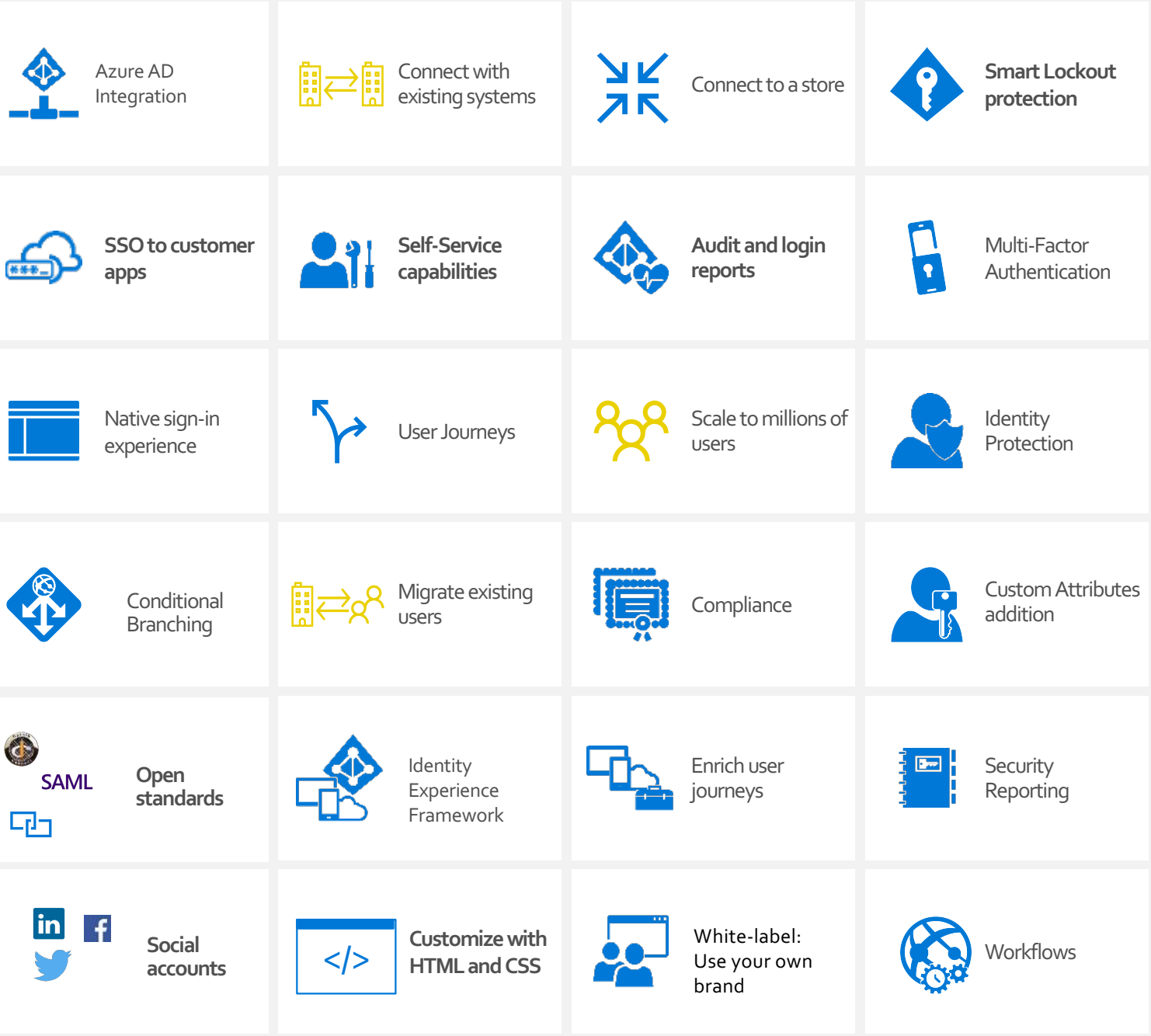
Apps and APIs

Analytics

Integration with other systems

Source: Microsoft (BRK3240 „Secure customer identity and access management using Azure Active Directory B2C “)

Azure AD B2C
Customer Identity Access Management (CIAM) Features



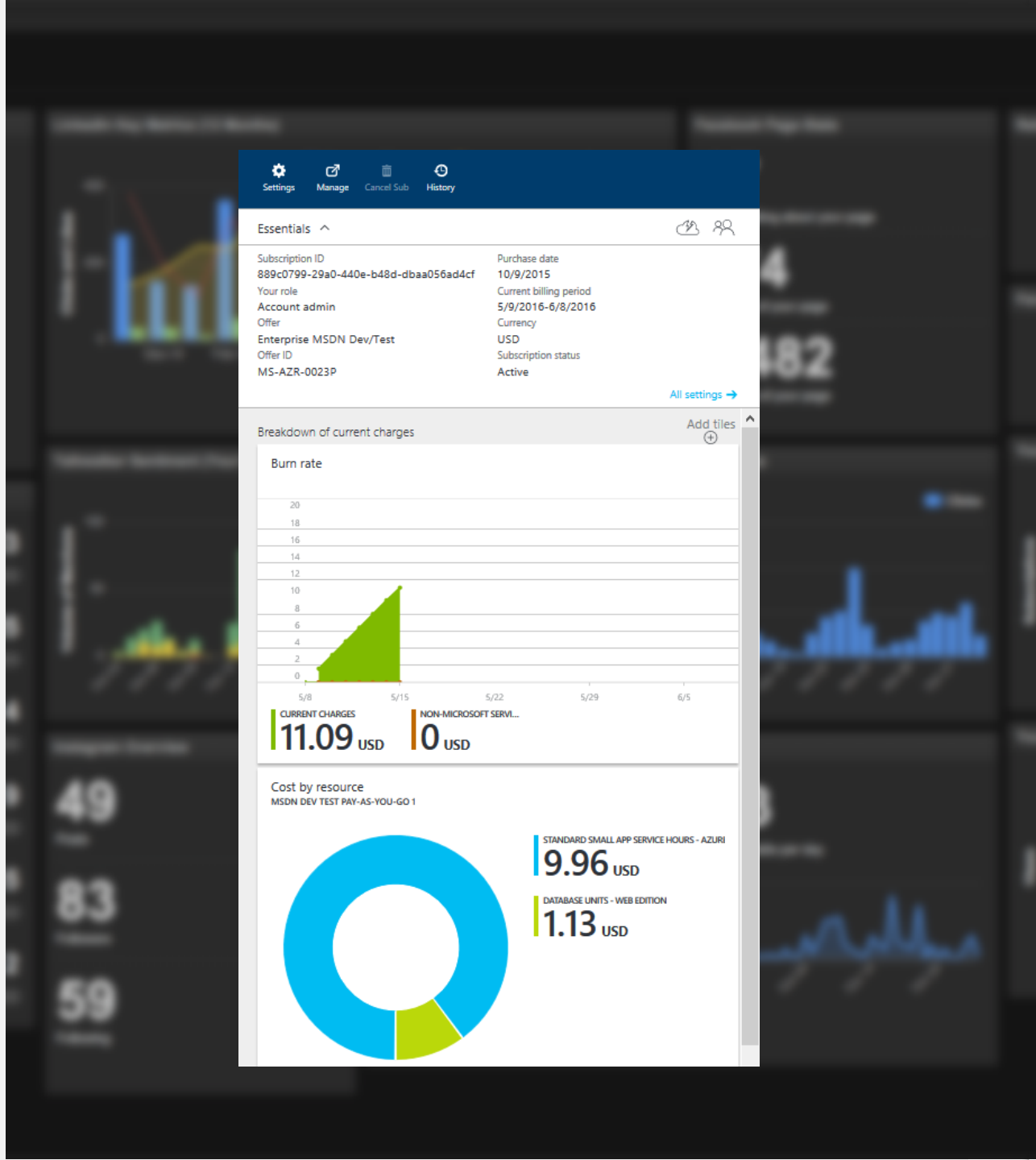
Source: Microsoft (BRK3240 „Secure customer identity and access management using Azure Active Directory B2C ")

Azure AD B2C
Pay-As-You-Grow Pricing Model

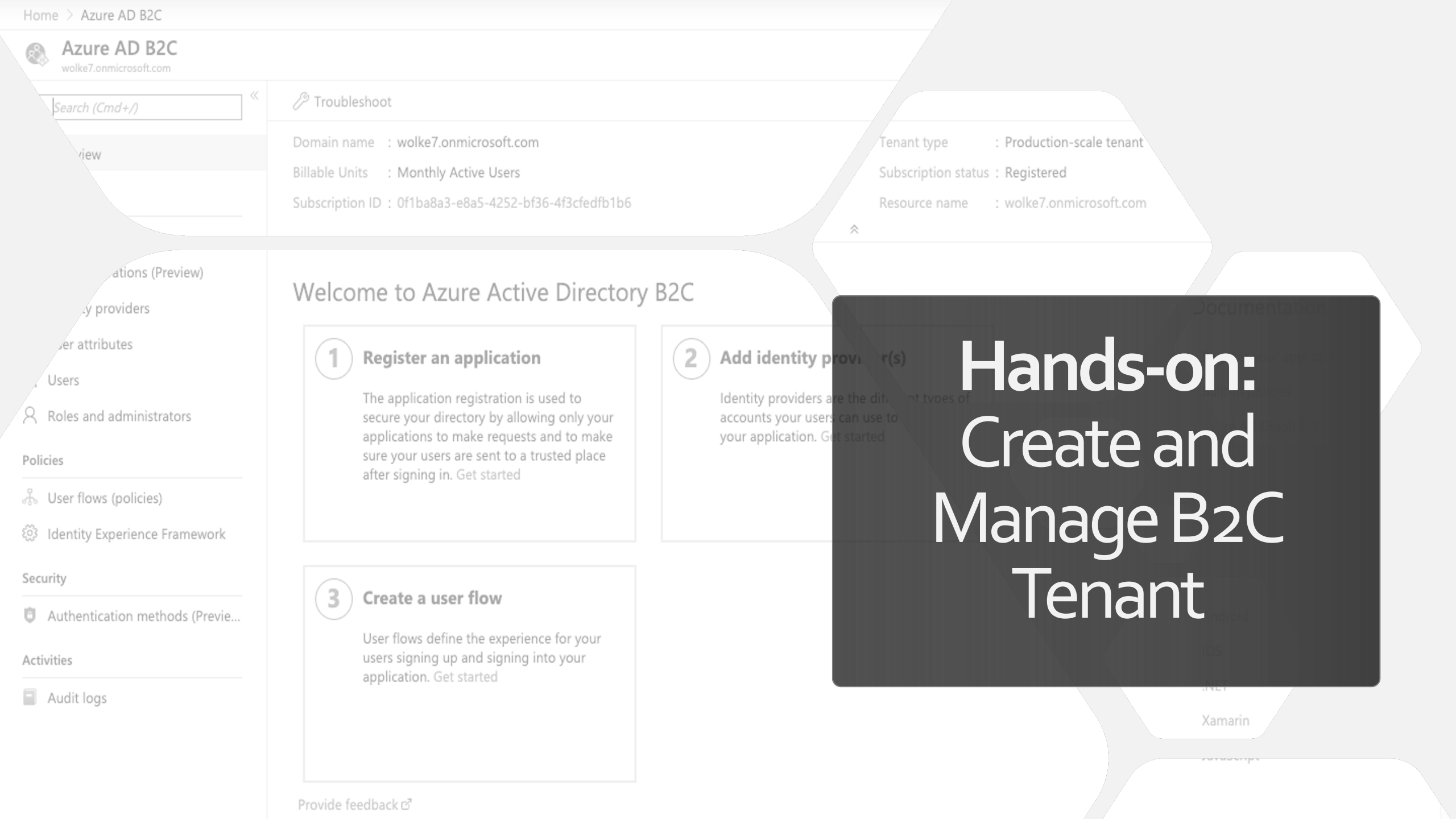
Sample calculation of Montly Active Users (MAUs)

(50,000 MAUs x 0 EUR (Free tier))
+ (50,000 MAUs x 0,00464 EUR)

= 232 EUR



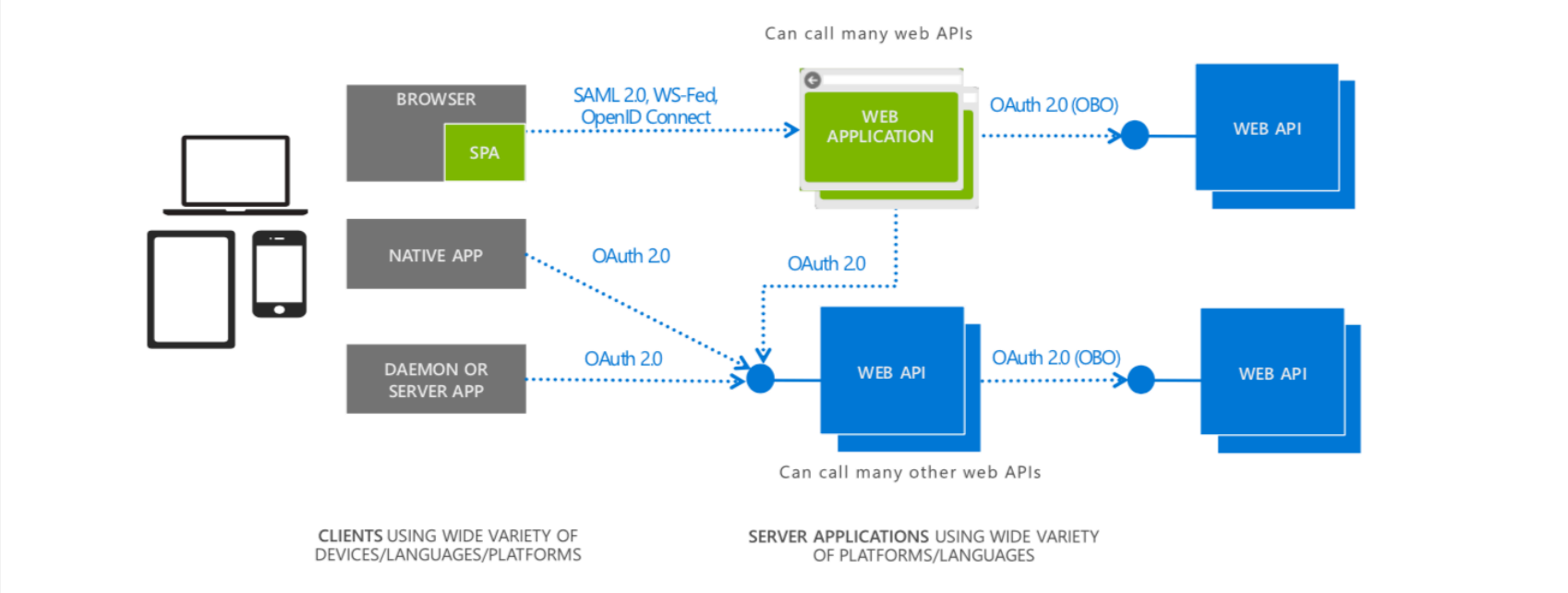
Source: Microsoft (BRK3240 „Secure customer identity and access management using Azure Active Directory B2C “)



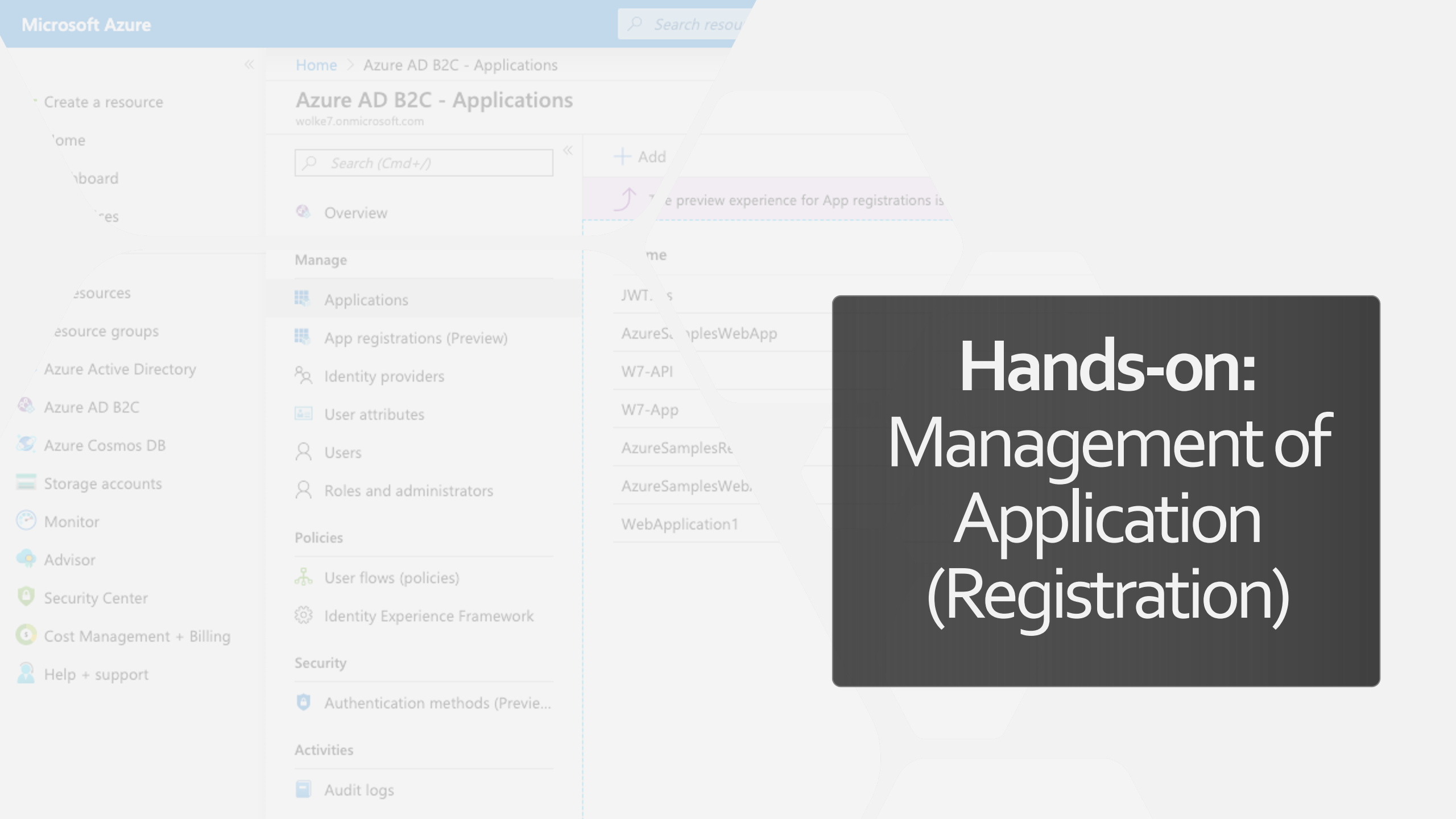
Hands-on: Create and Manage B2C Tenant

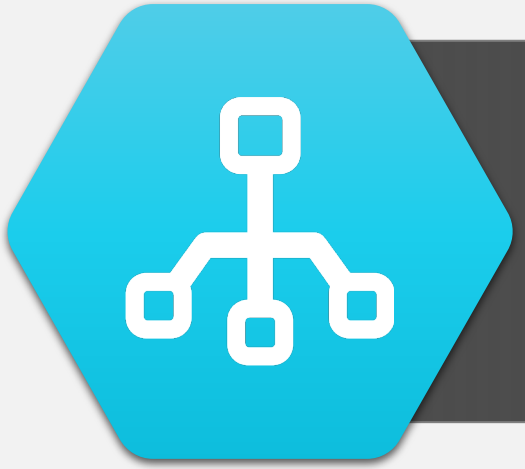
Integration of **Apps and APIs**

Libraries for App Integration



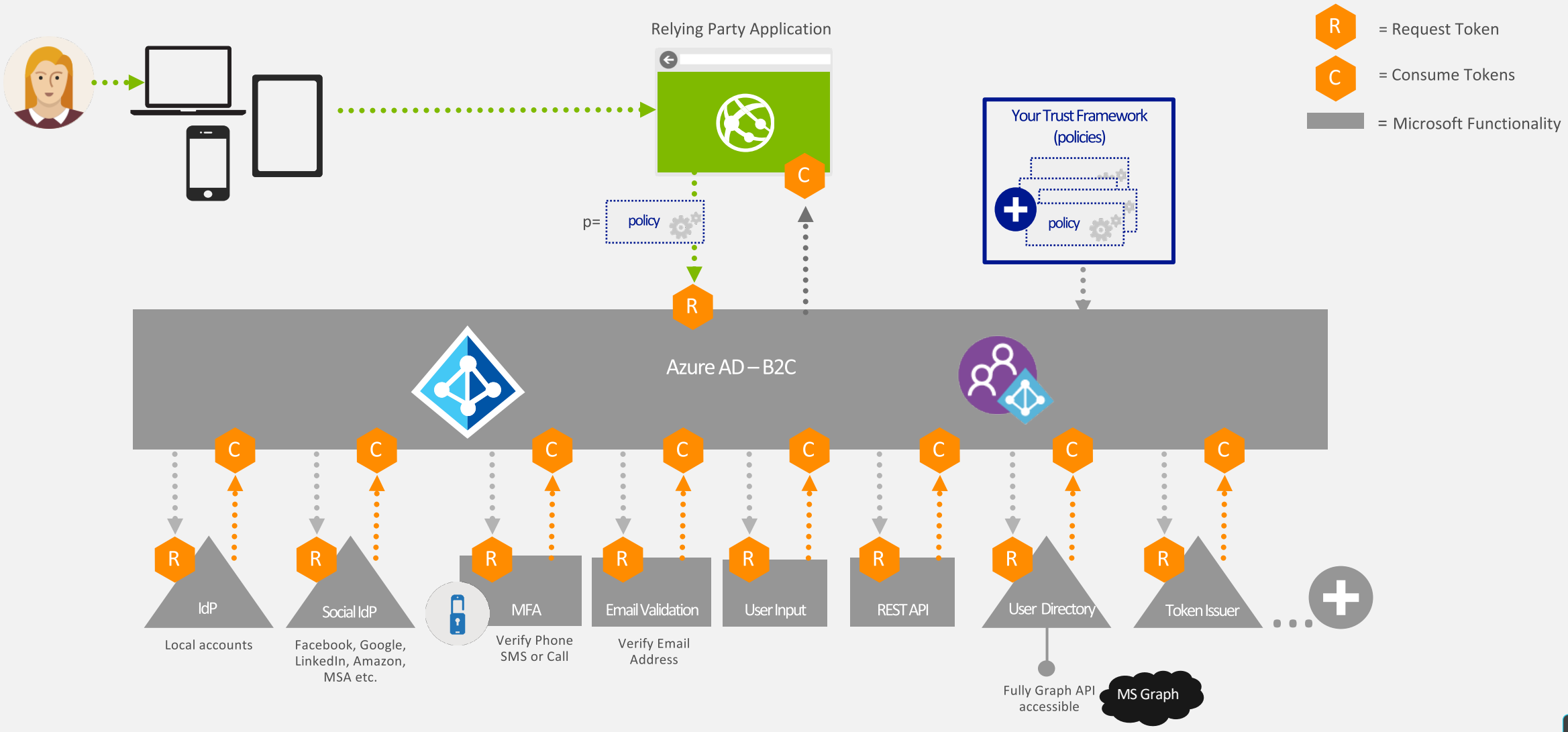
- **Any OpenID Connect compliant library will work with Azure AD B2C**
- **Samples available for:**
  - MSAL (.NET, JavaScript, Android, iOS)
  - AppAuth (Android, iOS)
  - Hello JS (Javascript)


Microsoft Azure
Search resou
Home > Azure AD B2C - Applications
Azure AD B2C - Applications
wolke7.onmicrosoft.com
Search (Cmd+/)
Add
Overview
Manage
Applications
App registrations (Preview)
Identity providers
User attributes
Users
Roles and administrators
Policies
User flows (policies)
Identity Experience Framework
Security
Authentication methods (Previe...
Activities
Audit logs
Create a resource
Azure Active Directory
Azure AD B2C
Azure Cosmos DB
Storage accounts
Monitor
Advisor
Security Center
Cost Management + Billing
Help + support
W7-API
W7-App
WebApplication1
Hands-on:
Management of
Application
(Registration)



User flows and policies in Azure AD B2C

Cloud secure identity and data orchestration



Source: Microsoft (BRK3240 „Secure customer identity and access management using Azure Active Directory B2C “)

Redirect to Azure AD B2C

Sample request

```
https://wolke7.b2clogin.com/wolke7.onmicrosoft.com/
oauth2/v2.0/authorize
p=B2C_1_susi&
client_id=f99657fc-e116-4865-a32c-72293aceae7c&
nonce=defaultNonce&
redirect_uri=https%3A%2F%2Flocalhost%3A44321%2F&
scope=openid&
response_type=id_token
```

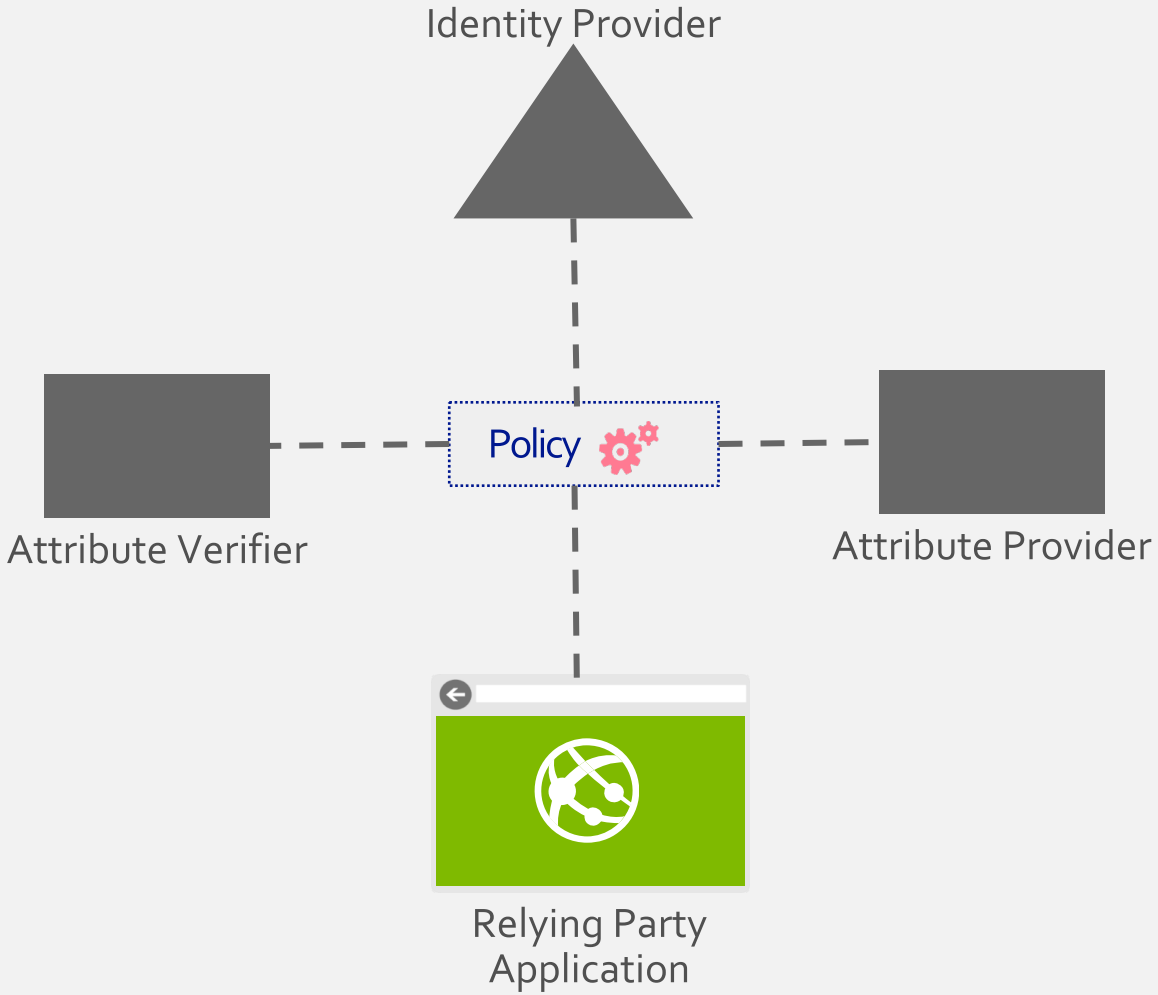
What is a policy?

Defines

- Claims Providers and Relying Parties
- Relationships between the entities
- Identity data available to the entities
- User Experience

Domain-Specific Language

- XML-based
- Mashable flows



Source: Microsoft "Introduction to B2C (Office Hours Jul 26th 2018)"

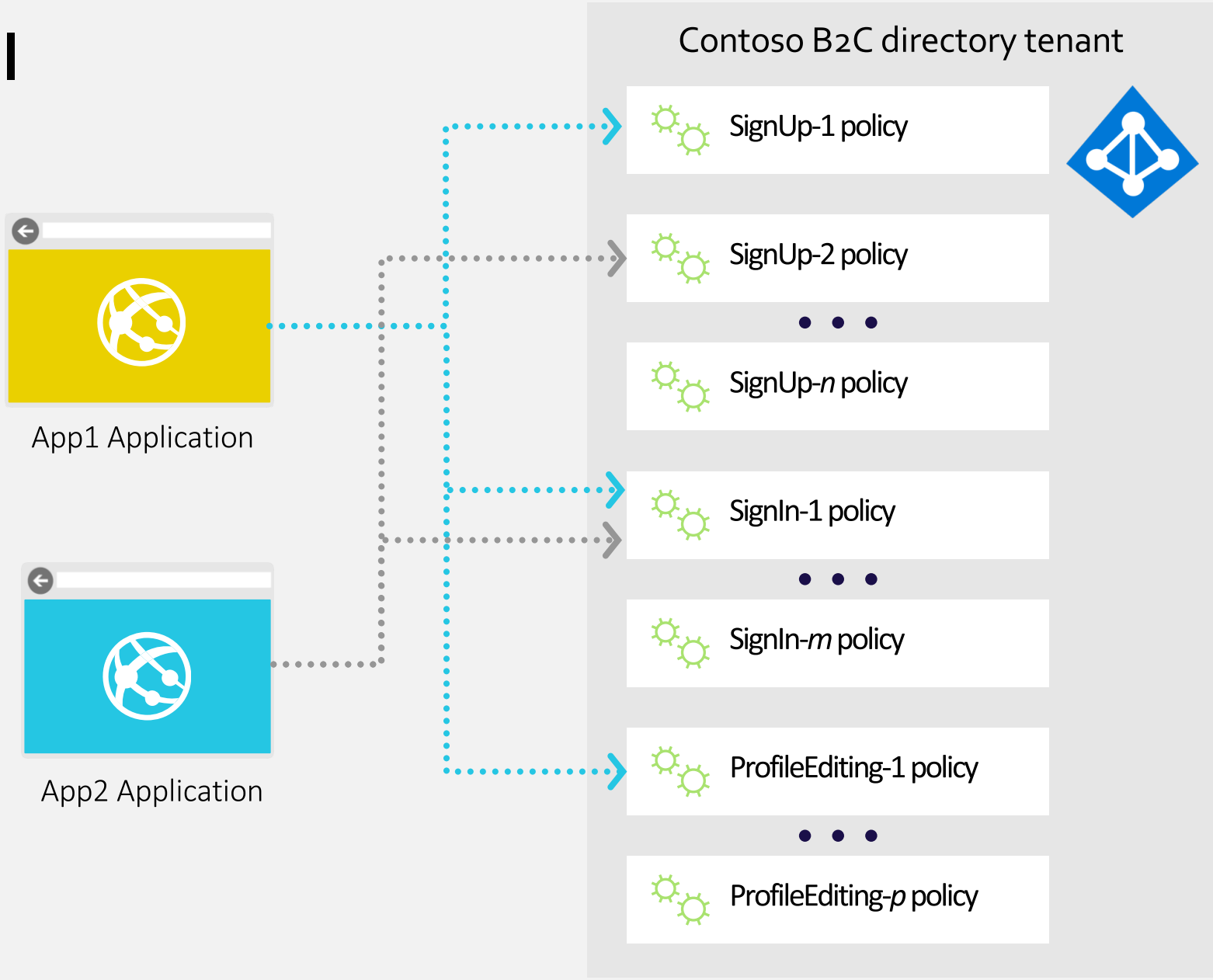
Policy-based model

Types of policies

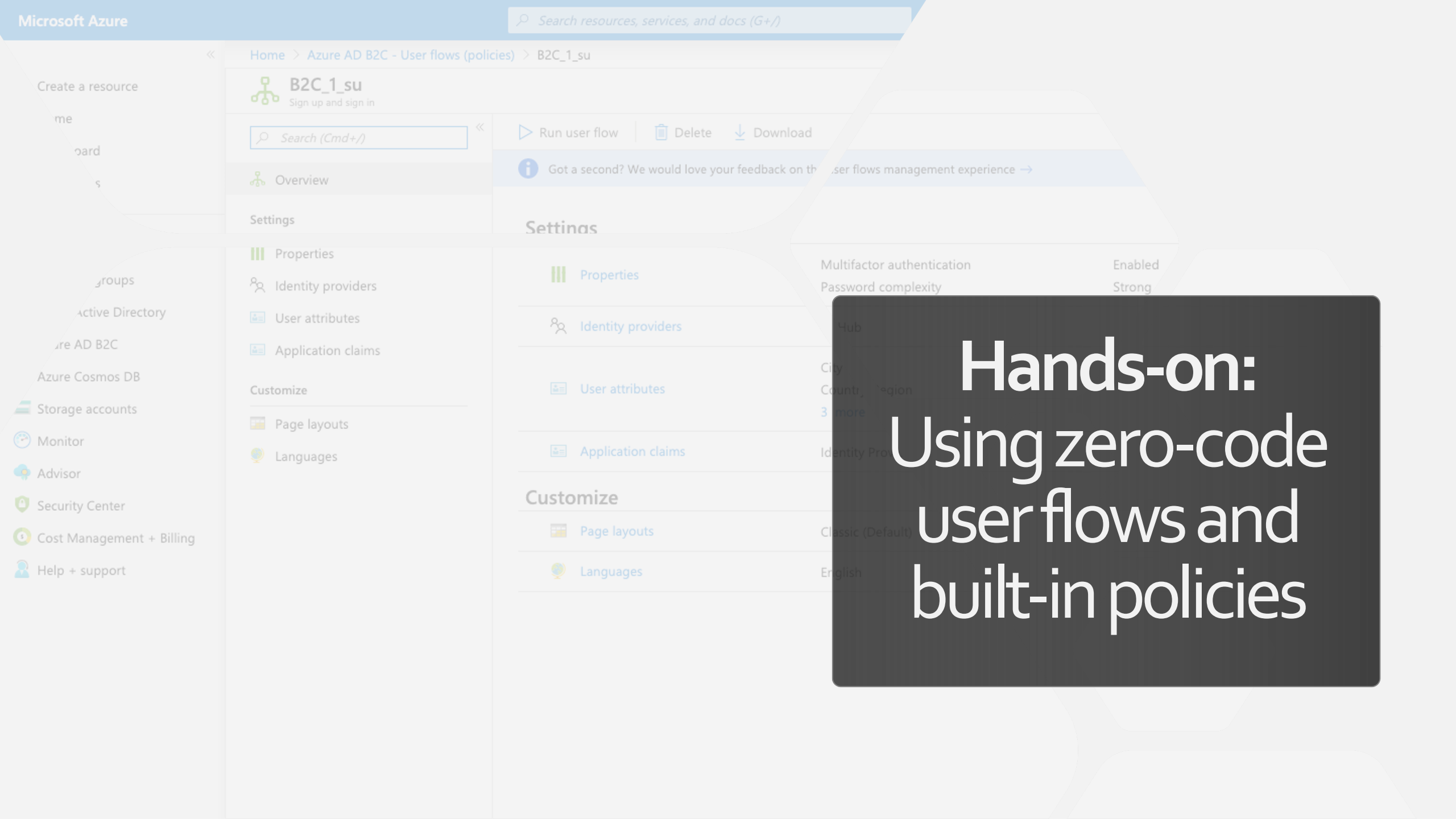
- Sign-Up
- Sign-In
- Combined Sign-Up/Sign-In
- Profile Editing
- Password Reset

Relation app to policy

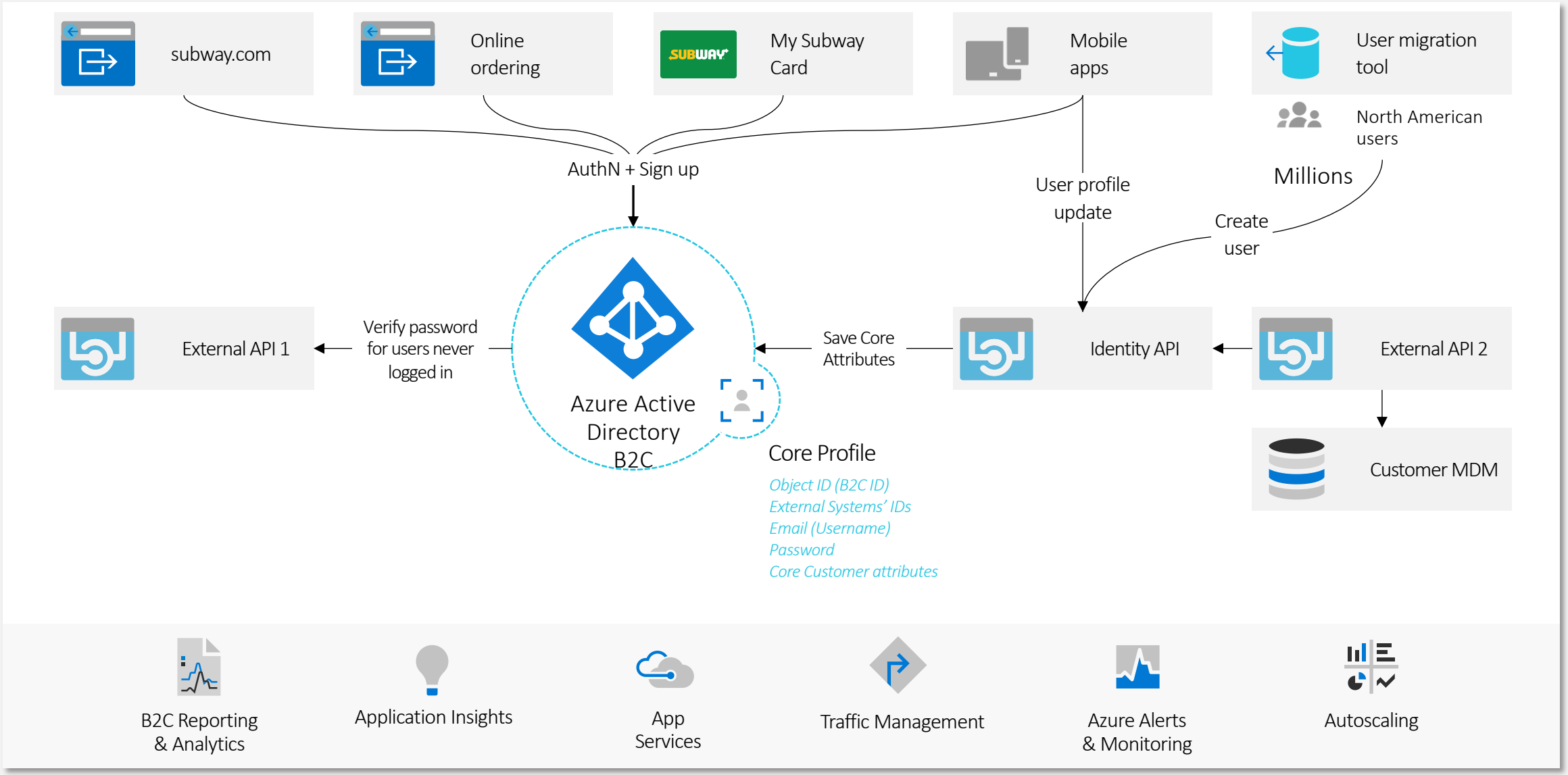
- 1 to many
- Many to 1



Source: Microsoft "Introduction to B2C (Office Hours Jul 26th 2018)"


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Azure AD B2C - User flows (policies) > B2C_1_su
B2C_1_su
Sign up and sign in
Search (Cmd+/)
Run user flow
Delete
Download
Got a second? We would love your feedback on th ser flows management experience
Overview
Settings
Properties
Identity providers
User attributes
Application claims
Customize
Page layouts
Languages
Settings
Properties
Identity providers
User attributes
Application claims
Customize
Page layouts
Languages
Multifactor authentication
Enabled
Password complexity
Strong
Classic (Default)
English
Create a resource
Azure Cosmos DB
Storage accounts
Monitor
Advisor
Security Center
Cost Management + Billing
Help + support
Hands-on:
Using zero-code user flows and built-in policies

Case Study: **Subway Customer Identity Architecture**

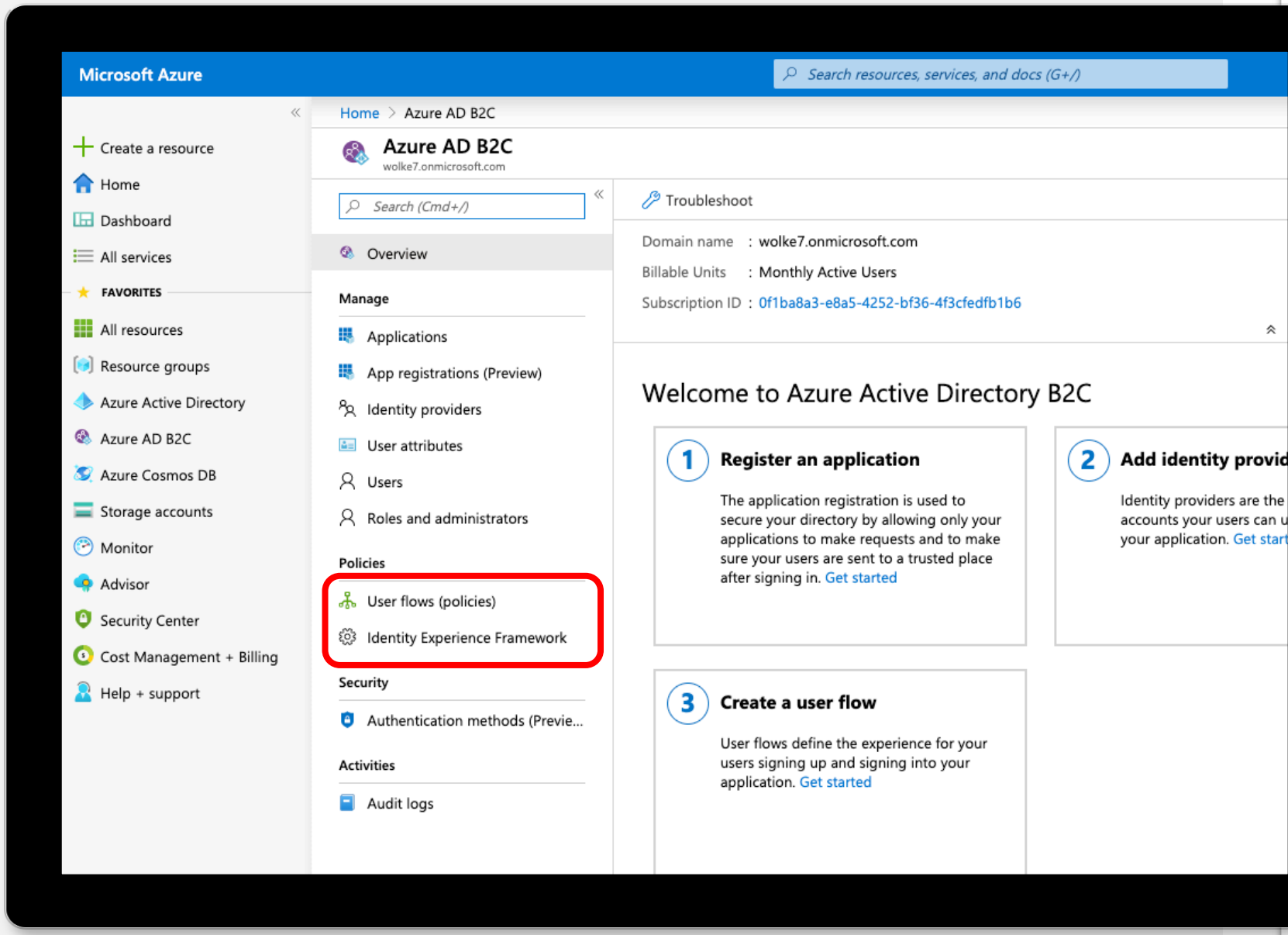


Source: Microsoft (BRK3240 „Secure customer identity and access management using Azure Active Directory B2C “)

Azure AD B2C
Types of policies

User flows
→ Built-in policies

Identity Experience Framework (IEF)
→ Custom policies



Branding & Customizing of Azure AD B2C

Branding and Customizing

Built-in options

- **UI Customization**
  - Using built-in page layout templates or own HTML/CSS files
    - Sample HTML and CSS files available on GitHub
    - Blob Storage to host custom page/themes
  - Your own JavaScript client-side code as part of your custom policy

- **Domain Customization**
  - https://{your-tenant-name}.b2clogin.com/{your-tenant-id}
  - No longer reference "login.microsoftonline.com"
    - Move onto B2Clogin , Previous endpoint depecated on December 2020
  - JavaScript client-side code is supported (currently in preview) in customized pages

- **Multi-Language Support**
  - Convert language files using Azure Cognitive Services

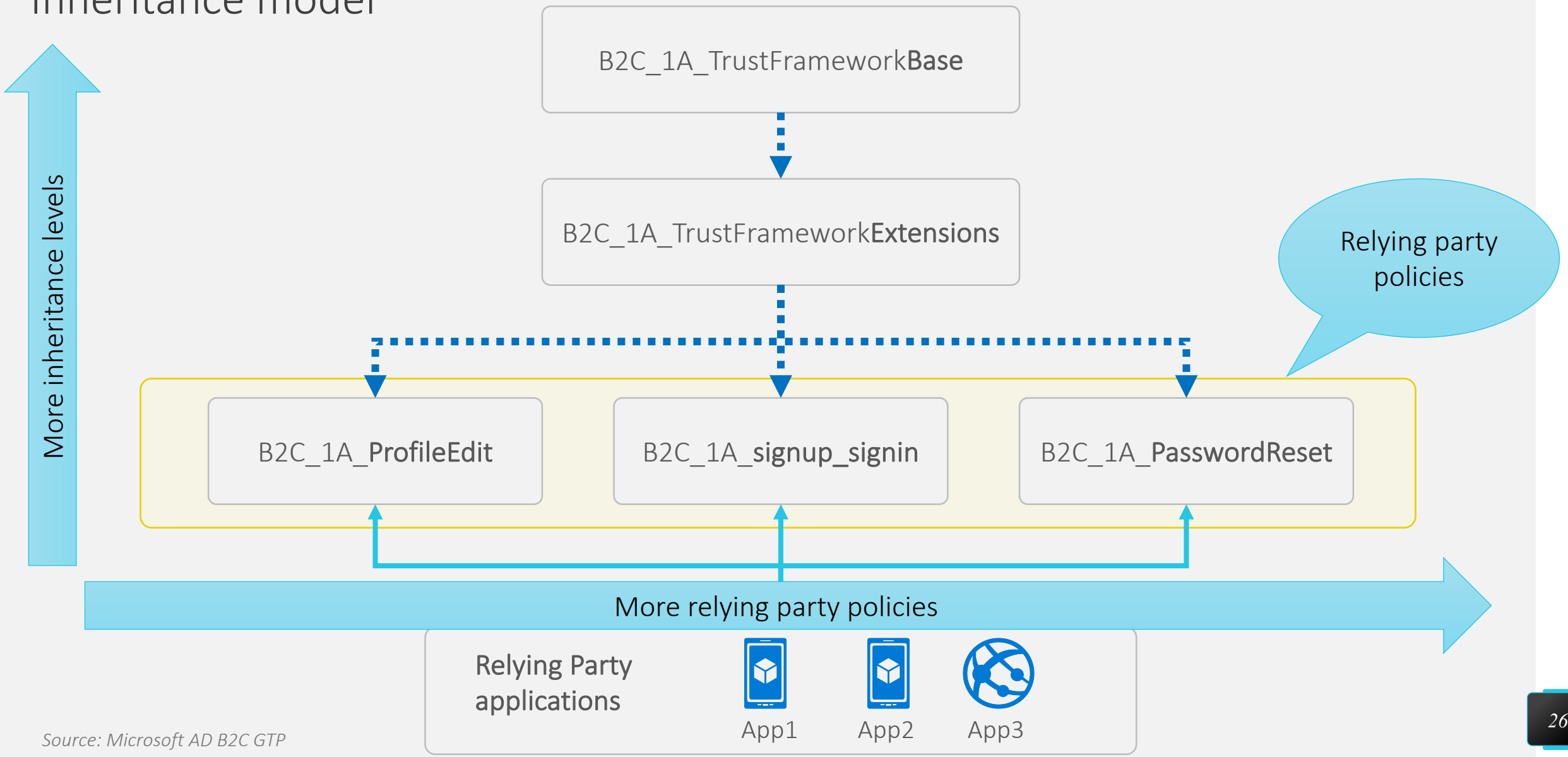
Identity Experience Framework (IEF)

Use Cases

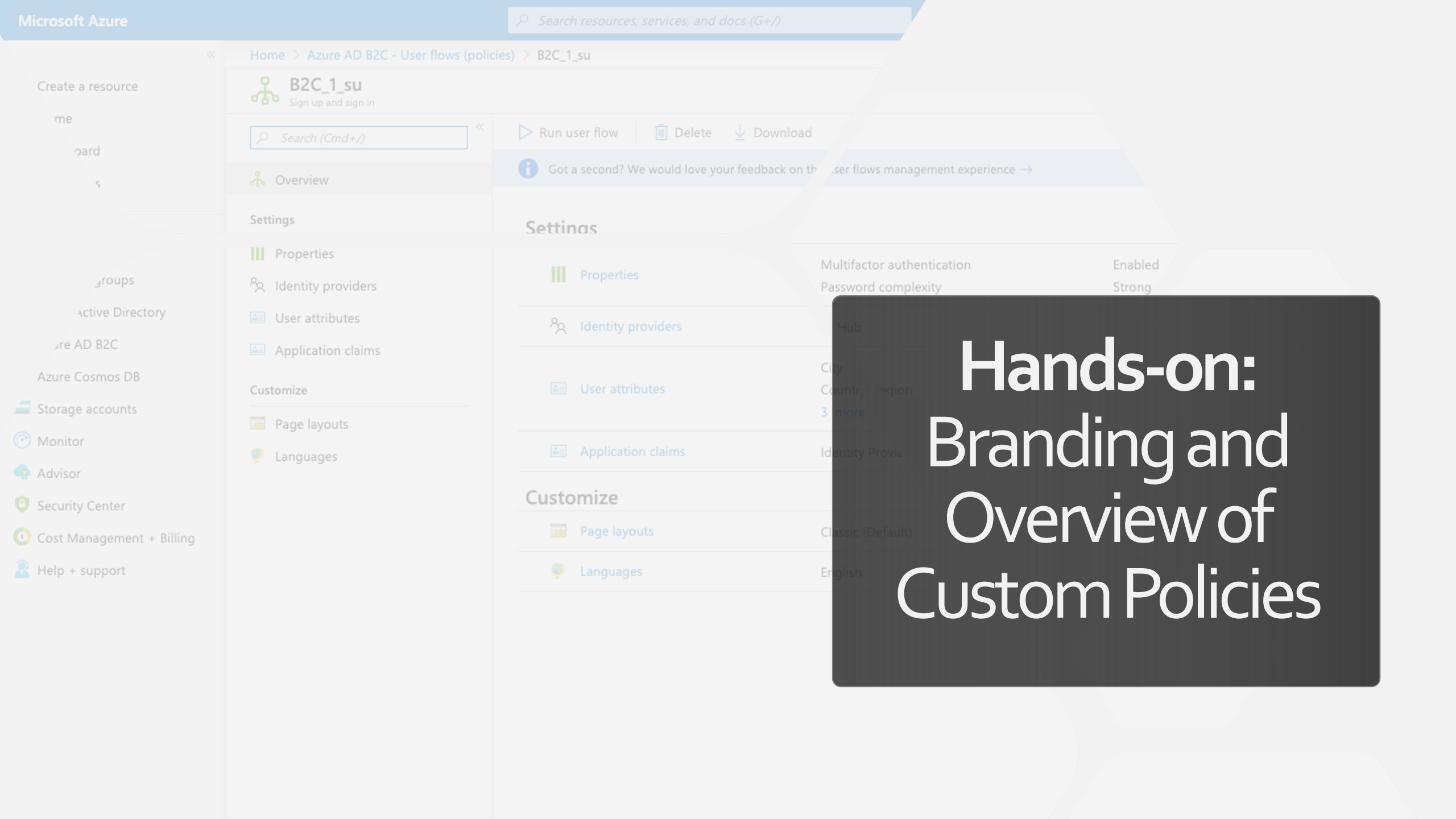
- **Option to customize identity tasks with IEF**
  - User invitation via mail
  - Link and unlink a social account
  - Validate user provided information from trusted (external) system via API
  - User store outside of B2C
  - Advanced progressive profiles
  - ….
- **Integration with REST APIs to Standards-based OIDC, OAUTH and SAML** (instead of using predefined local or social provider)
- **Samples of Custom CIAM User Journeys on GitHub**
- **Quickstart: Collection "Custom Policy Starter Kit"**

Identity Experience Framework

Inheritance model



Source: Microsoft AD B2C GTP


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Azure AD B2C - User flows (policies) > B2C_1_su
B2C_1_su
Sign up and sign in
Search (Cmd+/)
Run user flow
Delete
Download
Got a second? We would love your feedback on th ser flows management experience
Overview
Settings
Properties
Identity providers
User attributes
Application claims
Customize
Page layouts
Languages
Settings
Properties
Identity providers
User attributes
Application claims
Customize
Page layouts
Languages
Multifactor authentication
Enabled
Password complexity
Strong
Classic (Default)
English
Create a resource
Azure Cosmos DB
Storage accounts
Monitor
Advisor
Security Center
Cost Management + Billing
Help + support
Hands-on:
Branding and
Overview of
Custom Policies

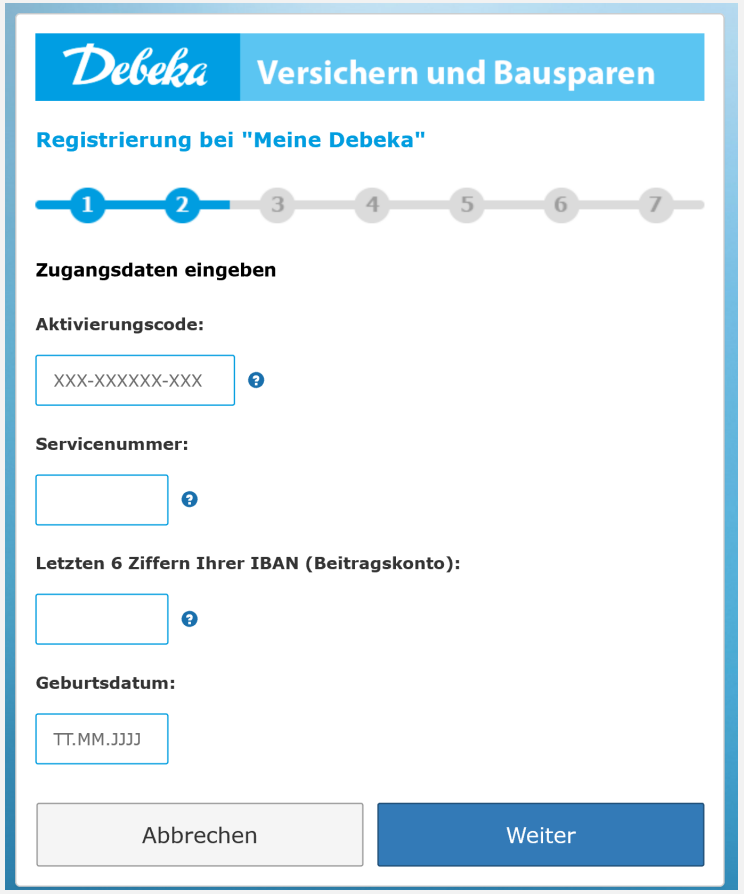
Branding & Customized User Journey

Debeka

Source: Microsoft (BRK3112 „Love all your identities – Building digital relationships with your customers and partners “)

Branding & Customized User Journey

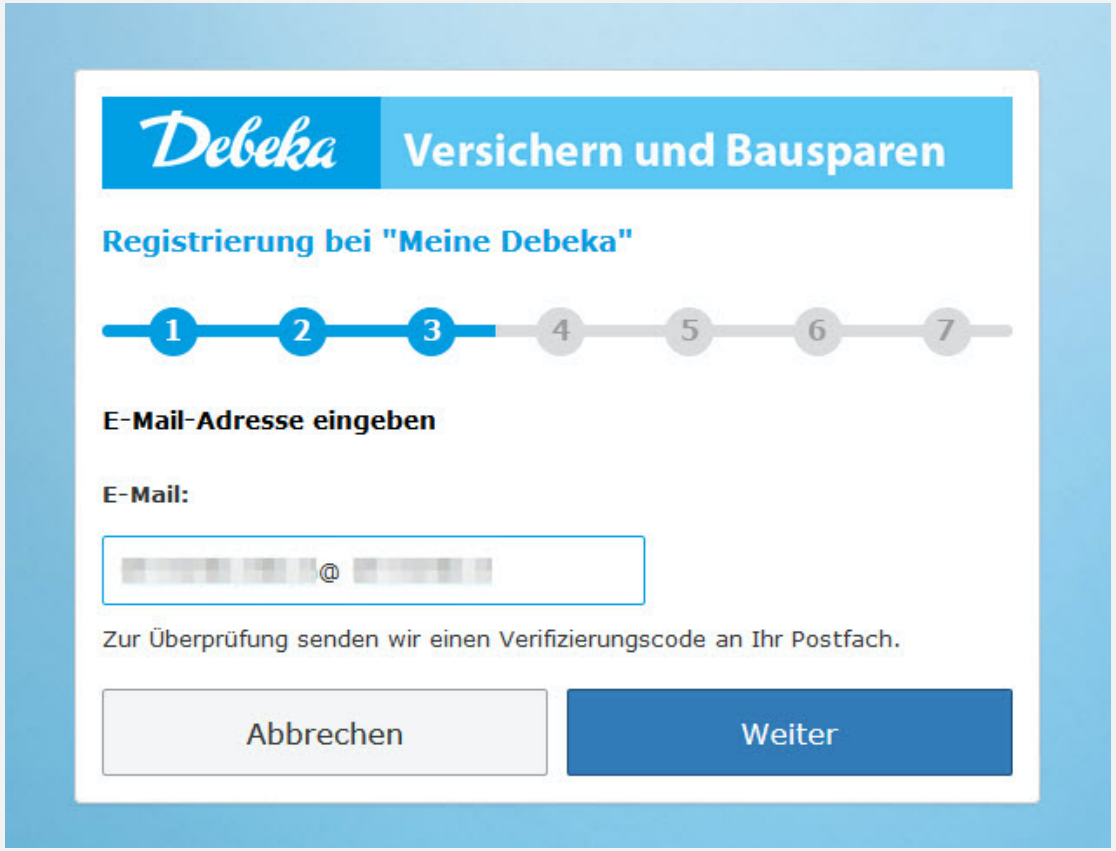
Debeka



Source: Microsoft (BRK3112 „Love all your identities – Building digital relationships with your customers and partners “)

Branding & Customized User Journey

Debeka



Source: Microsoft (BRK3112 „Love all your identities – Building digital relationships with your customers and partners “)

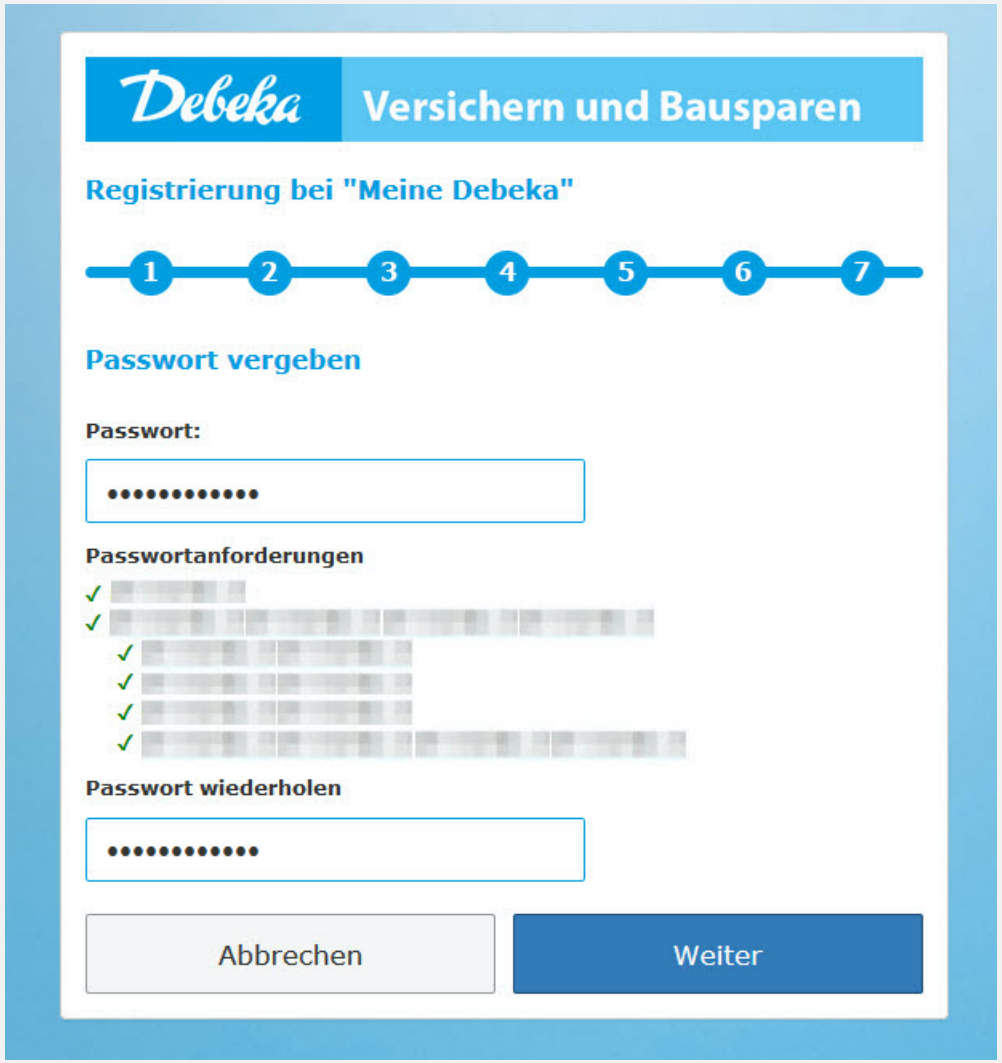
Branding & Customized User Journey

Debeka

Source: Microsoft (BRK3112 „Love all your identities – Building digital relationships with your customers and partners “)

Branding & Customized User Journey

Debeka



Source: Microsoft (BRK3112 „Love all your identities – Building digital relationships with your customers and partners “)

Management and Operations of B2C

Management and Operations of B2C Tenant

Audit logs and reporting

- **Azure AD (Core) Directory and B2C**
  - Audit Logs
  - Sign-In Logs
  - LoggedByService "B2C"

- **Export B2C Logs via Microsoft Graph API**

- **Correlation ID** (rendered in HTML of user's browser)

- **Advanced queries with Log Analytics** (e.g. Anomalous User App Sign-in)

- **Usage Reports via API or User Insights (in private preview)**

Management and Operations of B2C Tenant

- Custom Policy Management and Testing

- **Automate policy deployment** via Azure DevOps Pipeline (manual management via Policy Manager)
- **VSCode Extension** „Azure AD B2C Tools“
- Load testing solution to **simulate sign-in and sign-up with local accounts**
- **Monitoring availability and responsiveness** via Web Tests
- **Service Health Alerts** for notification of B2C platform incidents or maintenance

Management and Operations of B2C Tenant

- User Account Management

- Microsoft Graph API to manage user accounts in B2C
  (Migration, Profile update, back-end synchronization,…)

- Management of Key Container or Application via B2C PowerShell Module

- Code Sample: Manage users by Azure AD Graph API via .NET Client

- Migrating users from application authentication
  - Whitepaper and Sample of Just-in-Time Migration

Identity Protection of B2C local users

Identity Protection

Protection of customer identities in B2C

- **Configure the following settings based on your security requirements/concept:**
  - "Smart Lockout" Controls (Tenant-Level)
  - Password policy (for each user flow)
  - Token lifetime and Session behavior (for each user flow)
  - Password expiration?
  - Enforce MFA (on critical operations or activities)
  - Password Expiration (in case of security incidents)

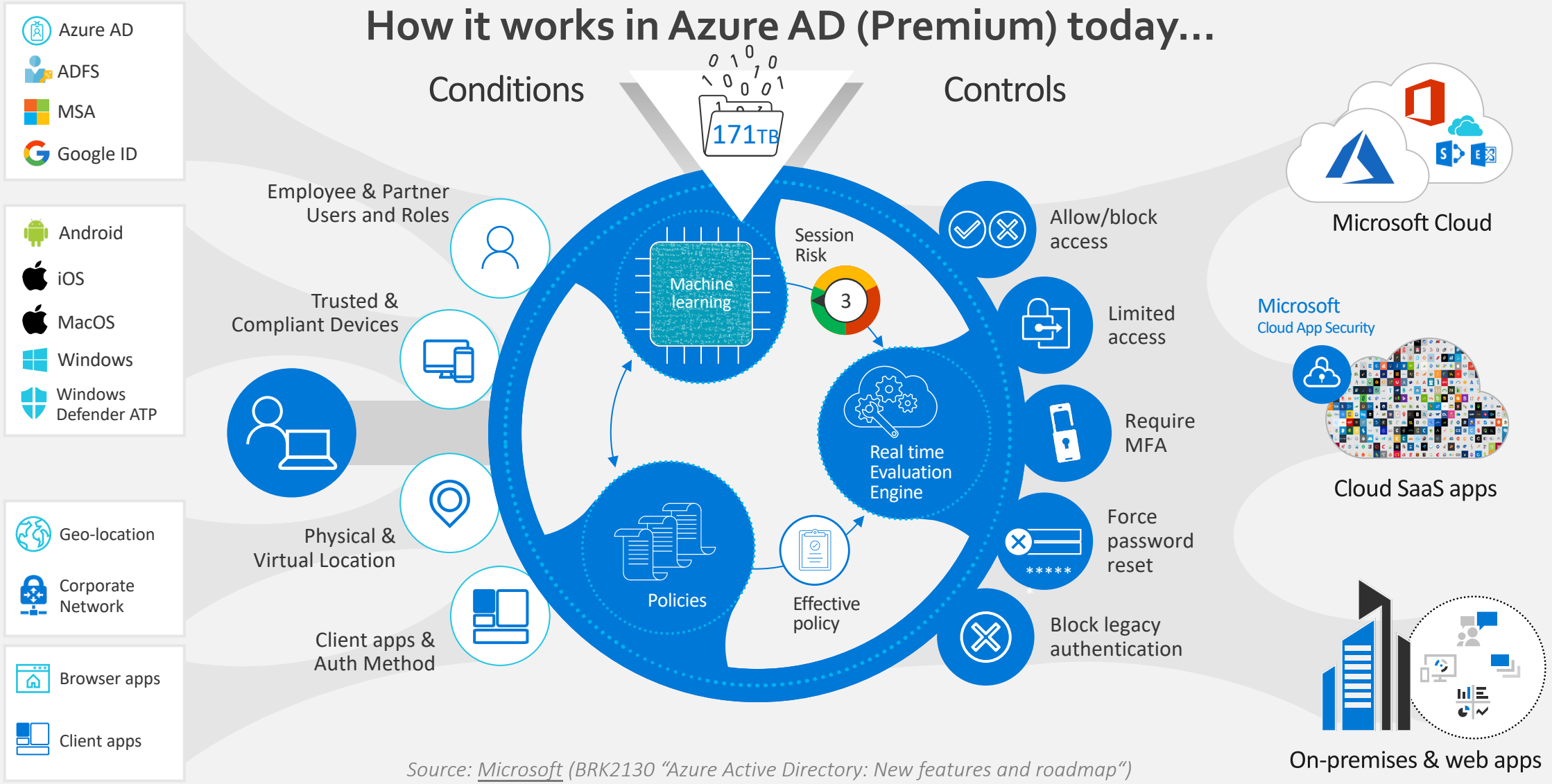
- **Mail validation** as part of user sign-up and e-mail address change ("Double-Opt-in")

- **Notification for unusual login behavior or (high number of) sign-in attempts to users**

- **Validating the user password selection by** invoking Troy Hunt's "Pwned Passwords" API

Announced features (Ignite 2019)

Identity protection and Conditional Access for B2C



Source: Microsoft (BRK2130 "Azure Active Directory: New features and roadmap")

Thank You

@Thomas_Live

Thomas@Naunheim.net

www.cloud-architekt.net