



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

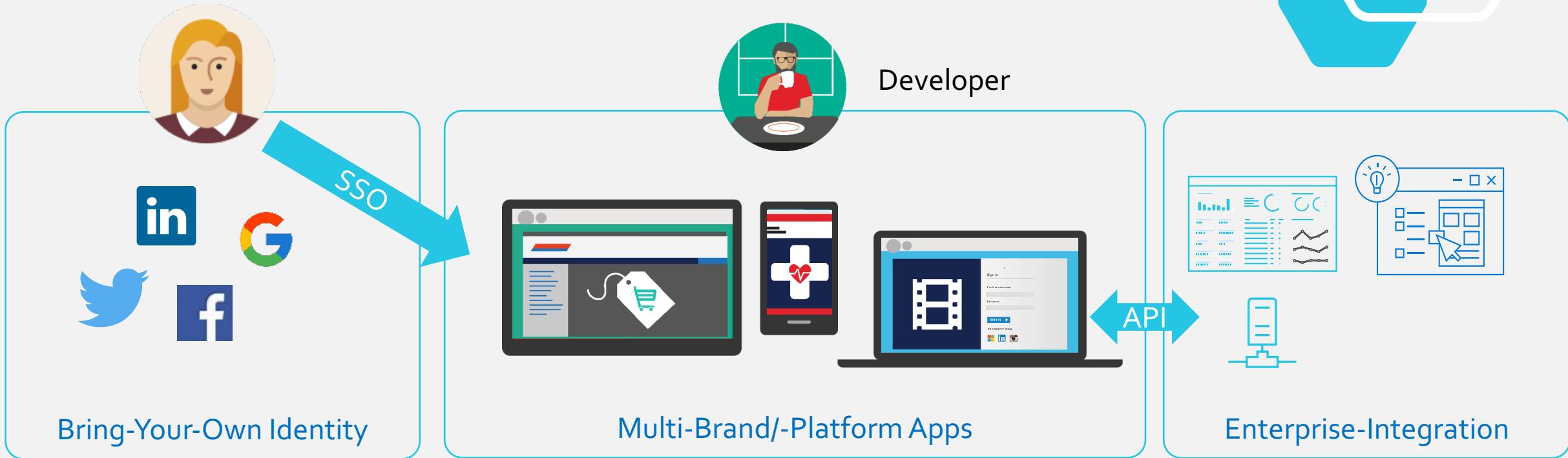
 www.cloud-architekt.net





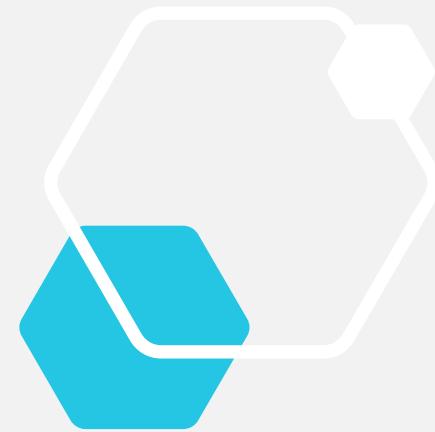
Azure AD B2C Overview

Requirements for Customer Identity & Access Management (CIAM)



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



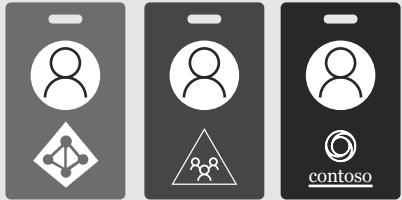
Azure AD B2C

Customers

Social IDs, email, or local accounts

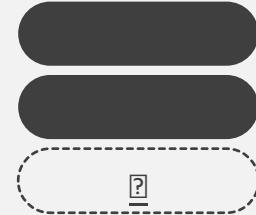
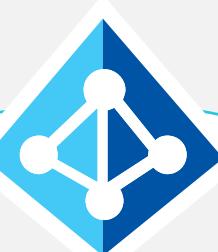


Business & Government IDs



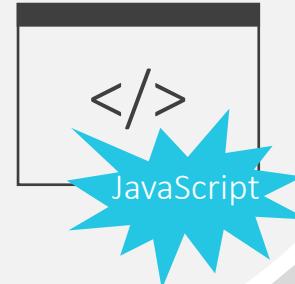
Use social accounts

Protect your users with MFA



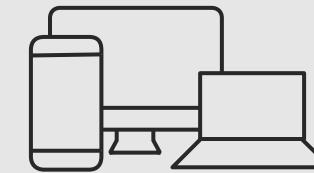
Create custom user attributes

Customize your pages using HTML and CSS

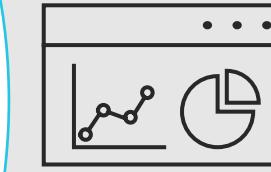


Business

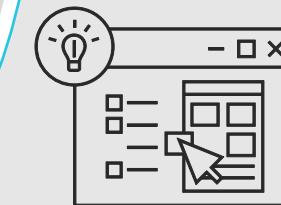
Apps and APIs



Analytics



Integration with other systems



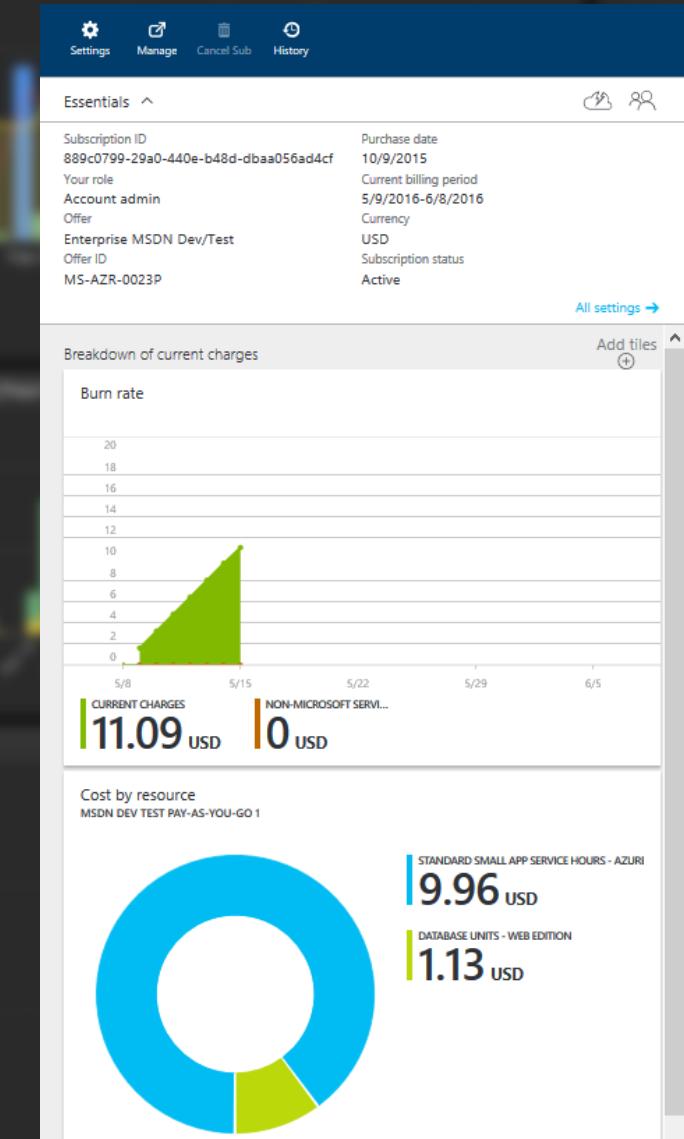
Azure AD B2C Customer Identity Access Management (CIAM) Features

 Azure AD Integration	 Connect with existing systems	 Connect to a store	 Smart Lockout protection
 SSO to customer apps	 Self-Service capabilities	 Audit and login reports	 Multi-Factor Authentication
 Native sign-in experience	 User Journeys	 Scale to millions of users	 Identity Protection
 Conditional Branching	 Migrate existing users	 Compliance	 Custom Attributes addition
 SAML  Open standards	 Identity Experience Framework	 Enrich user journeys	 Security Reporting
 Social accounts	 Customize with HTML and CSS	 White-label: Use your own brand	 Workflows

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)
 $(50,000 \text{ MAUs} \times 0 \text{ EUR (Free tier)})$
 $+ (50,000 \text{ MAUs} \times 0,00464 \text{ EUR})$
 $= 232 \text{ EUR}$



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



Azure AD B2C

wolke7.onmicrosoft.com

Search (Cmd+/)



Troubleshoot

Domain name : wolke7.onmicrosoft.com

Billable Units : Monthly Active Users

Subscription ID : 0f1ba8a3-e8a5-4252-bf36-4f3cfedfb1b6

Tenant type : Production-scale tenant

Subscription status : Registered

Resource name : wolke7.onmicrosoft.com

Welcome to Azure Active Directory B2C

1 Register an application

The application registration is used to secure your directory by allowing only your applications to make requests and to make sure your users are sent to a trusted place after signing in. Get started

2 Add identity provider(s)

Identity providers are the different types of accounts your users can use to sign in to your application. Get started

3 Create a user flow

User flows define the experience for your users signing up and signing into your application. Get started

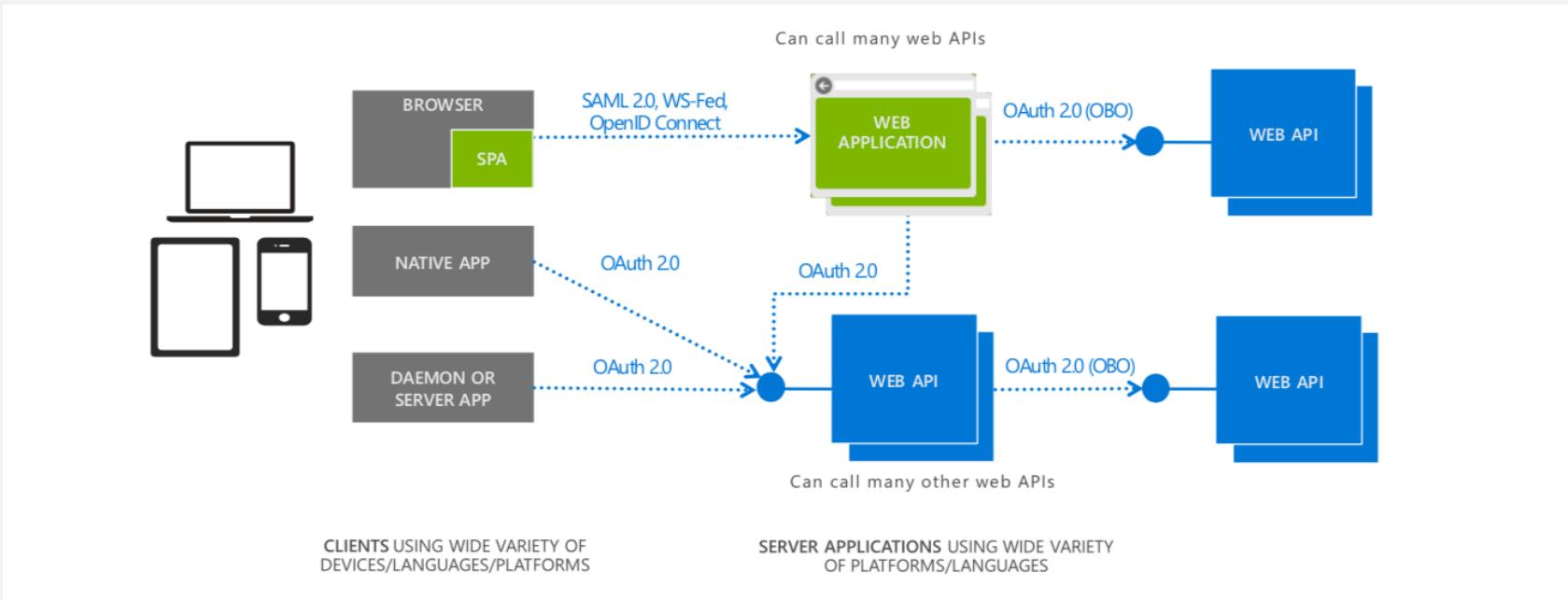
Hands-on: Create and Manage B2C Tenant

Provide feedback



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)

Azure AD B2C - Applications

wolke7.onmicrosoft.com

Search (Cmd+/)

Add



The preview experience for App registrations is

Overview

Manage

Applications

App registrations (Preview)

Identity providers

User attributes

Users

Roles and administrators

Policies

User flows (policies)

Identity Experience Framework

Security

Authentication methods (Preview...)

Activities

Audit logs

me

JWT. s

AzureSamplesWebApp

W7-API

W7-App

AzureSamplesRt

AzureSamplesWeb

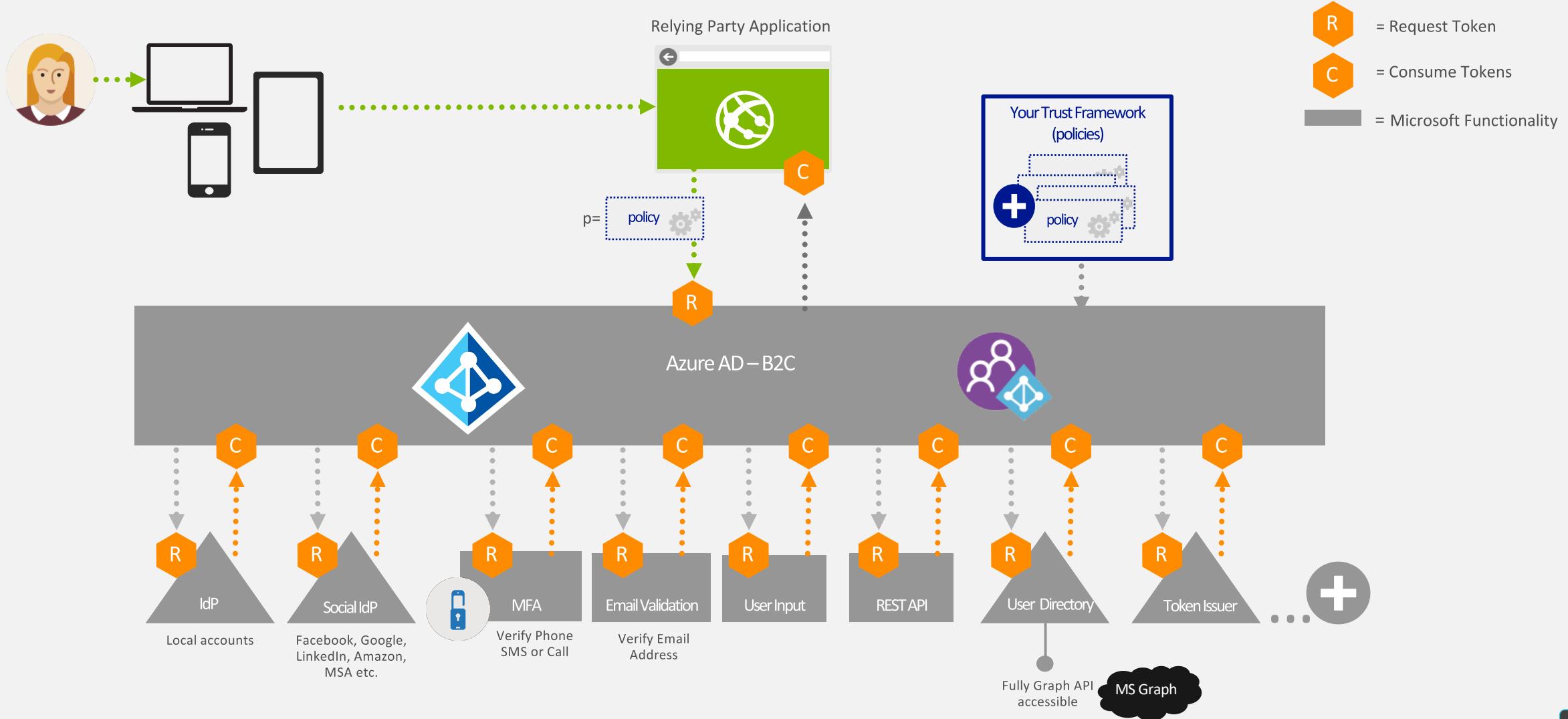
WebApplication1

Hands-on: Management of Application (Registration)



User flows and policies in Azure AD B2C

Cloud secure identity and data orchestration



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
```

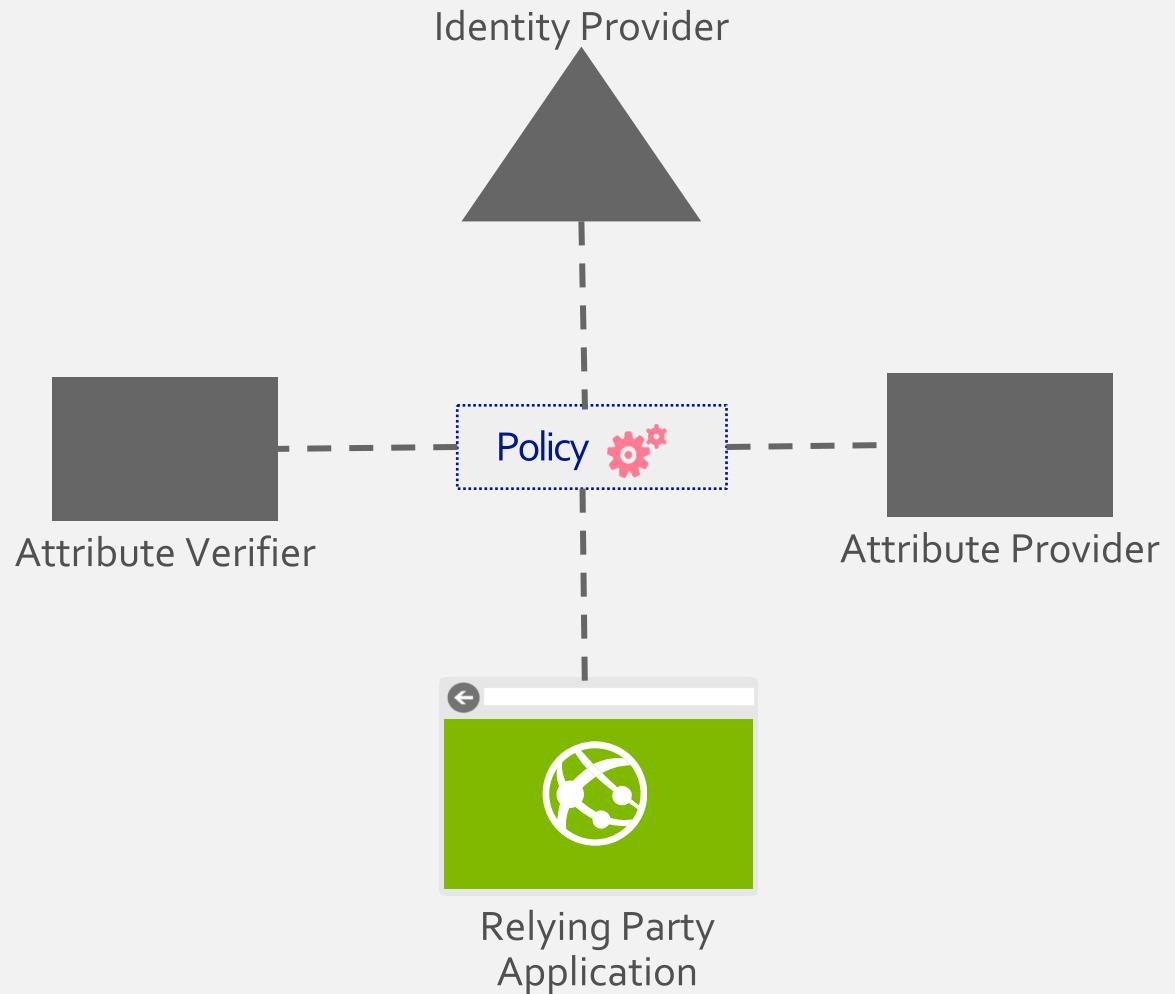
What is a policy?

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



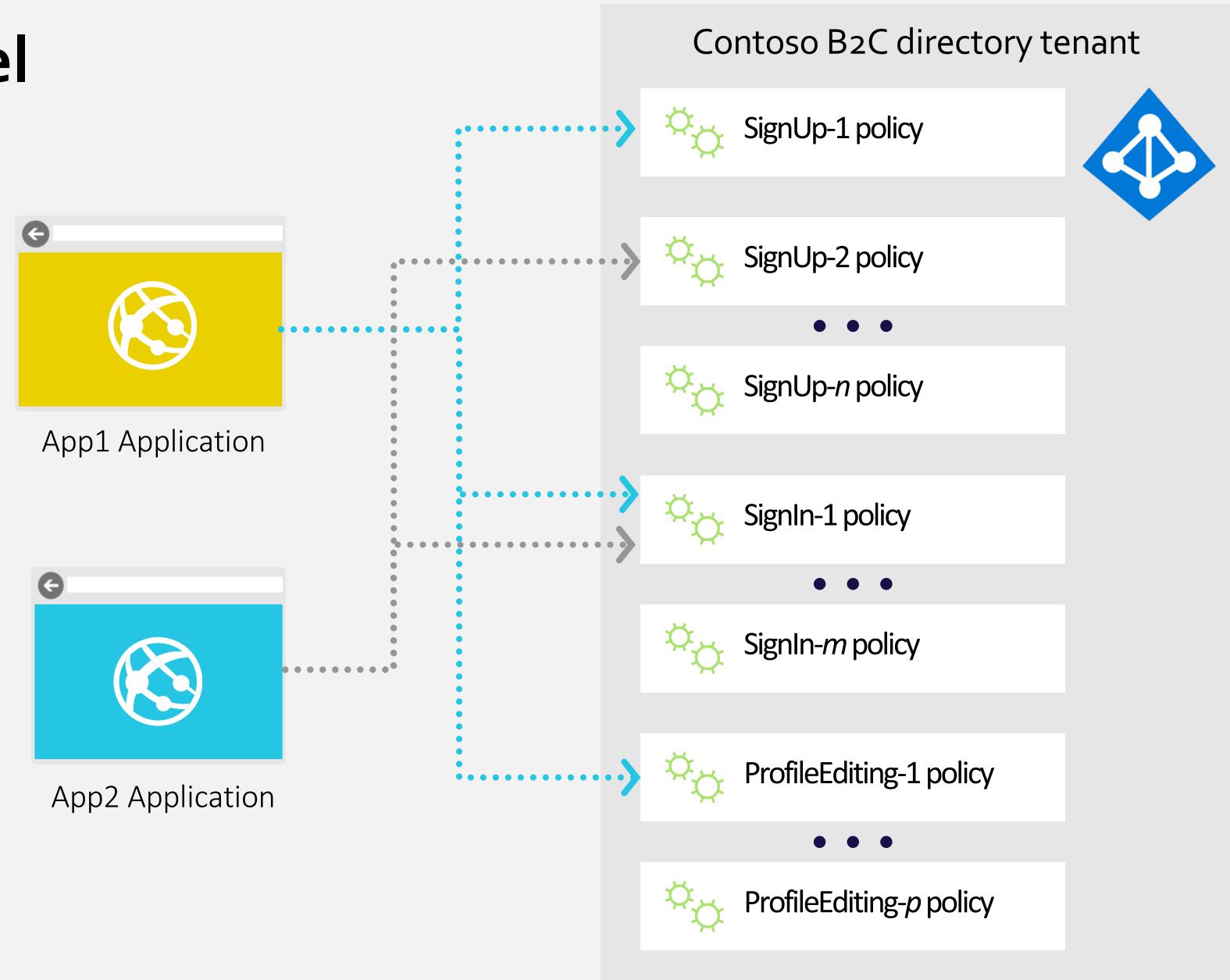
Policy-based model

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



- Create a resource
- me
- oard
- s
- groups
- Active Directory
- Azure AD B2C
- Azure Cosmos DB
- Storage accounts
- Monitor
- Advisor
- Security Center
- Cost Management + Billing
- Help + support

 **B2C_1_su**
Sign up and sign in

Search (Cmd+/) Run user flow Delete Download

Got a second? We would love your feedback on the user flows management experience →

Settings

Properties	Multifactor authentication Enabled
Identity providers	Password complexity Strong
User attributes	Hub
Application claims	City Country, Region 3 more
Customize	Identity Pro
Page layouts	Classic (Default)
Languages	English

Properties

Identity providers

User attributes

Application claims

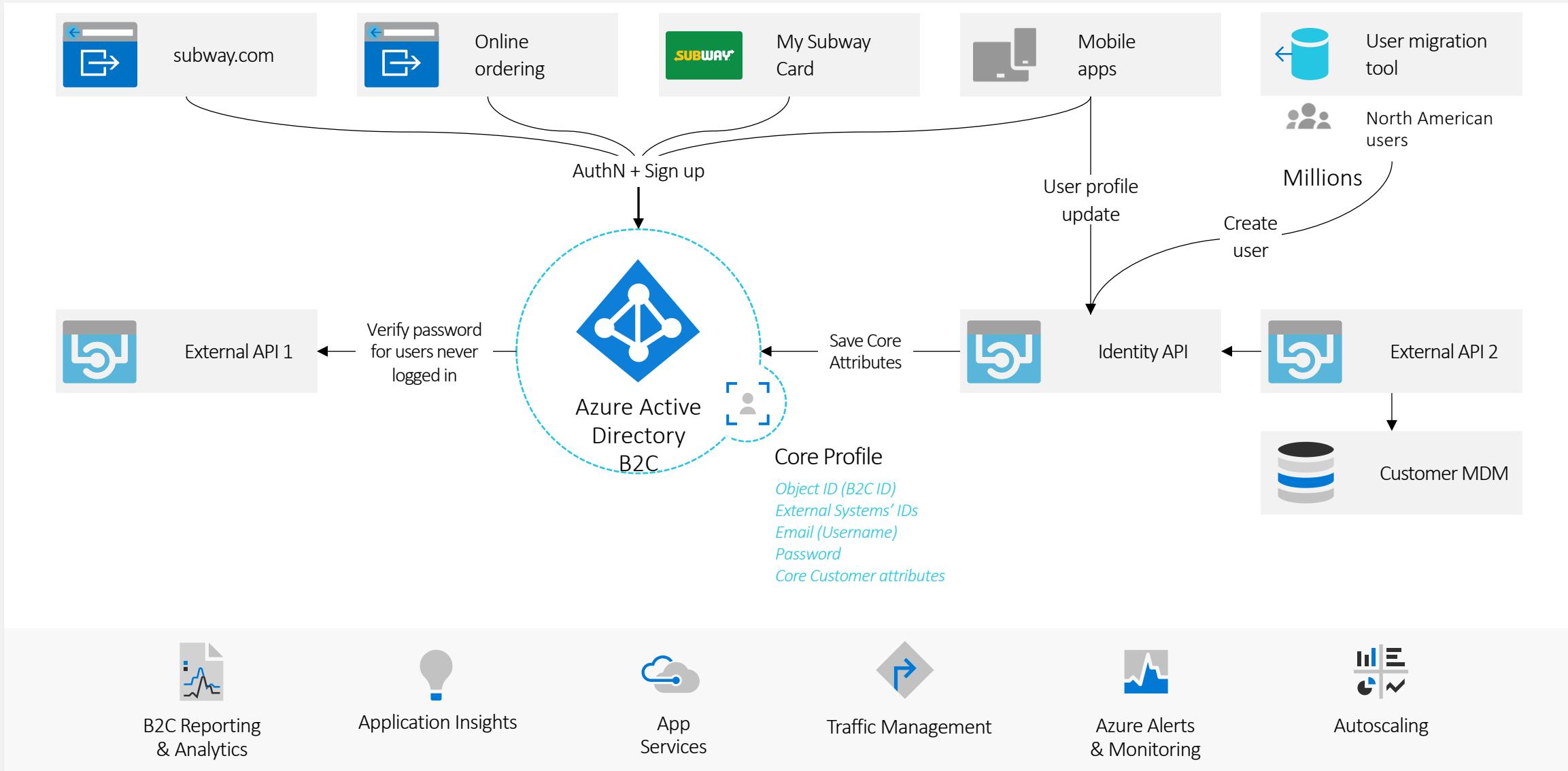
Customize

Page layouts

Languages

Hands-on: Using zero-code user flows and built-in policies

Case Study: Subway Customer Identity Architecture



Azure AD B2C

Types of policies

User flows

→ Built-in policies

Identity Experience Framework (IEF)

→ Custom policies

The screenshot shows the Microsoft Azure portal interface for the Azure AD B2C service. The left sidebar includes options like 'Create a resource', 'Home', 'Dashboard', 'All services', 'FAVORITES' (with 'All resources', 'Resource groups', 'Azure Active Directory', 'Azure AD B2C', 'Azure Cosmos DB', 'Storage accounts', 'Monitor', 'Advisor', 'Security Center', 'Cost Management + Billing', and 'Help + support'), and a 'Search' bar. The main content area displays the 'Overview' of the Azure AD B2C service, showing domain name (wolke7.onmicrosoft.com), billable units (Monthly Active Users), and subscription ID (0f1ba8a3-e8a5-4252-bf36-4fcfedfb1b6). Below the overview, there's a 'Manage' section with links for 'Applications', 'App registrations (Preview)', 'Identity providers', 'User attributes', 'Users', 'Roles and administrators', and 'Policies'. The 'Policies' section is further divided into 'User flows (policies)' and 'Identity Experience Framework'. The 'User flows (policies)' link is highlighted with a red box. To the right of the main content, there's a 'Welcome to Azure Active Directory B2C' section with three numbered steps: 1. Register an application, 2. Add identity provider, and 3. Create a user flow.

Microsoft Azure

Home > Azure AD B2C

Azure AD B2C
wolke7.onmicrosoft.com

Search (Cmd+ /)

Troubleshoot

Overview

Domain name : wolke7.onmicrosoft.com
Billable Units : Monthly Active Users
Subscription ID : 0f1ba8a3-e8a5-4252-bf36-4fcfedfb1b6

Manage

Applications

App registrations (Preview)

Identity providers

User attributes

Users

Roles and administrators

Policies

User flows (policies)

Identity Experience Framework

Welcome to Azure Active Directory B2C

1 Register an application

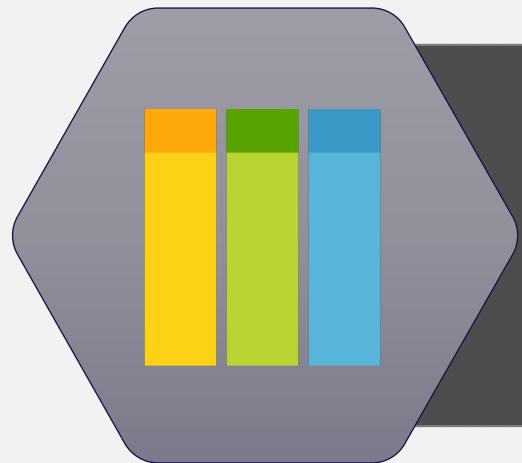
The application registration is used to secure your directory by allowing only your applications to make requests and to make sure your users are sent to a trusted place after signing in. [Get started](#)

2 Add identity provider

Identity providers are the accounts your users can use with your application. [Get started](#)

3 Create a user flow

User flows define the experience for your users signing up and signing into your application. [Get started](#)



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)

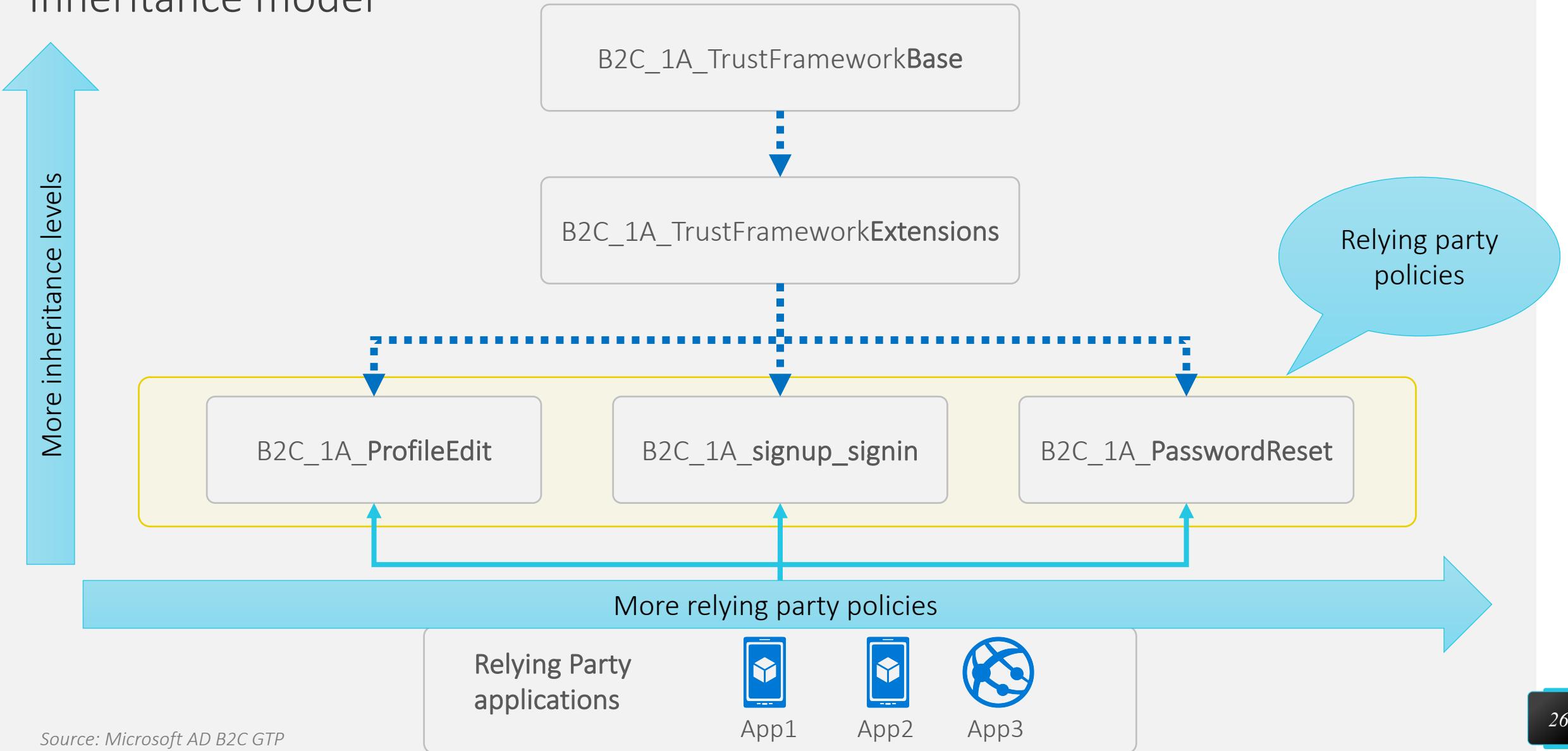
Use Cases



- **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



- Create a resource
- me
- oard
- s
- groups
- Active Directory
- Azure AD B2C
- Azure Cosmos DB
- Storage accounts
- Monitor
- Advisor
- Security Center
- Cost Management + Billing
- Help + support

 **B2C_1_su**
Sign up and sign in

Search (Cmd+/) Run user flow Delete Download

Got a second? We would love your feedback on the user flows management experience →

Settings

 Properties	Multifactor authentication Enabled
 Identity providers	Password complexity Strong
 User attributes	Hub
 Application claims	City Country, Region 3 more
 Customize	Identity Providers
 Page layouts	Classic (Default)
 Languages	English

Hands-on:
Branding and
Overview of
Custom Policies

Branding & Customized User Journey

Debeka



Branding & Customized User Journey

Debeka

Debeka Versichern und Bausparen

Registrierung bei "Meine Debeka"

1 2 3 4 5 6 7

Nutzungsbedingungen und Datenschutz

Ich akzeptiere die [Nutzungsbedingungen](#).

Die [Datenschutzerklärung](#) habe ich zur Kenntnis genommen.
Diese Einwilligung kann ich jederzeit mit Wirkung für die Zukunft widerrufen.

[Abbrechen](#) [Weiter](#)

Debeka Versichern und Bausparen

Registrierung bei "Meine Debeka"

1 2 3 4 5 6 7

Zugangsdaten eingeben

Aktivierungscode:

XXX-XXXXXX-XXX

Servicenummer:

Letzten 6 Ziffern Ihrer IBAN (Beitragskonto):

Geburtsdatum:

TT.MM.JJJJ

[Abbrechen](#) [Weiter](#)



Branding & Customized User Journey

Debeka

Debeka Versichern und Bausparen

Registrierung bei "Meine Debeka"

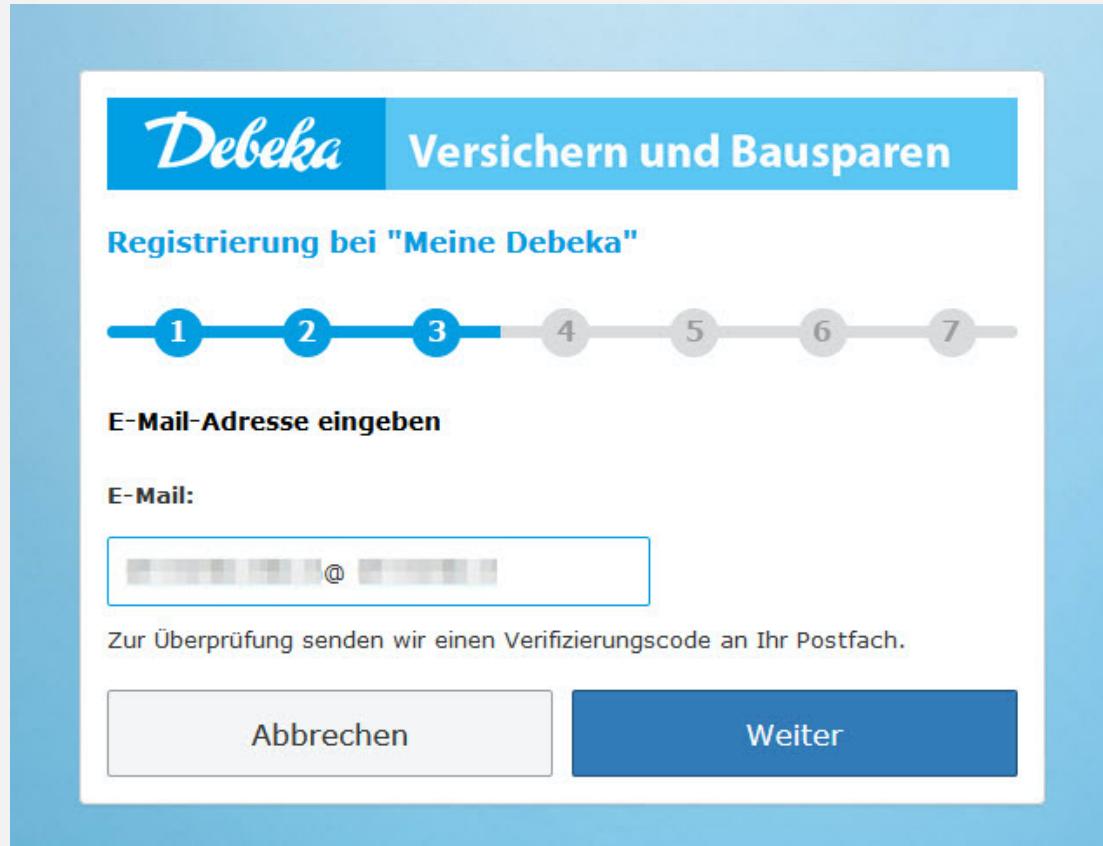
1 2 3 4 5 6 7

E-Mail-Adresse eingeben

E-Mail:

Zur Überprüfung senden wir einen Verifizierungscode an Ihr Postfach.

Abbrechen Weiter



Debeka Versichern und Bausparen

Registrierung bei "Meine Debeka"

1 2 3 4 5 6 7

E-Mail-Adresse bestätigen

Bitte geben Sie Ihren Verifizierungscode ein, den Sie per E-Mail erhalten haben.

Verifizierungscode:

Sie haben keinen Verifizierungscode erhalten? Bitte überprüfen Sie Ihren SPAM-Ordner oder fordern Sie hier neuen Verifizierungscode an (Schritt zurück).

Abbrechen Weiter



Branding & Customized User Journey

Debeka

The screenshot shows the fifth step of a seven-step registration process. The header reads "Debeka Versichern und Bausparen" and the sub-header "Registrierung bei 'Meine Debeka'". A progress bar at the top shows steps 1 through 7, with steps 1-5 in blue and steps 6-7 in grey. The main content asks for a phone number entry. It includes a note that a security factor is required for all functions. A dropdown menu for entering a phone number (+49) is shown. Below it, a note says users will receive a verification code via SMS or phone call. A question "Wie möchten Sie den Verifizierungscode erhalten?" has two options: "per SMS" (selected) and "als Anruf". At the bottom are "Abbrechen" and "Weiter" buttons.

The screenshot shows the sixth step of the registration process. The header and sub-header are identical to the previous screen. The progress bar now shows steps 1-6 in blue and step 7 in grey. The main content asks for a verification code. It includes a note that users can request a new code if none was received. A text input field for the verification code is shown. At the bottom are "Abbrechen" and "Weiter" buttons.

Branding & Customized User Journey

Debeka

The screenshot shows the fourth step of a seven-step registration process. The top navigation bar includes the Debeka logo and the text "Versichern und Bausparen". The main title is "Registrierung bei "Meine Debeka"" and the step number is "4". The sub-section is "Passwort vergeben". A password field contains masked input. Below it, "Passwortanforderungen" are listed with several green checkmarks. The "Passwort wiederholen" field below contains masked input. At the bottom are "Abbrechen" and "Weiter" buttons.





Management and Operations of B2C

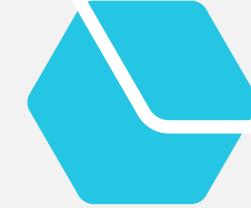
Management and Operations of B2C Tenant

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

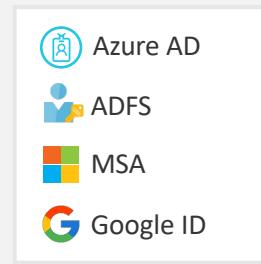
Identity Protection

Protection of customer identities in B2C

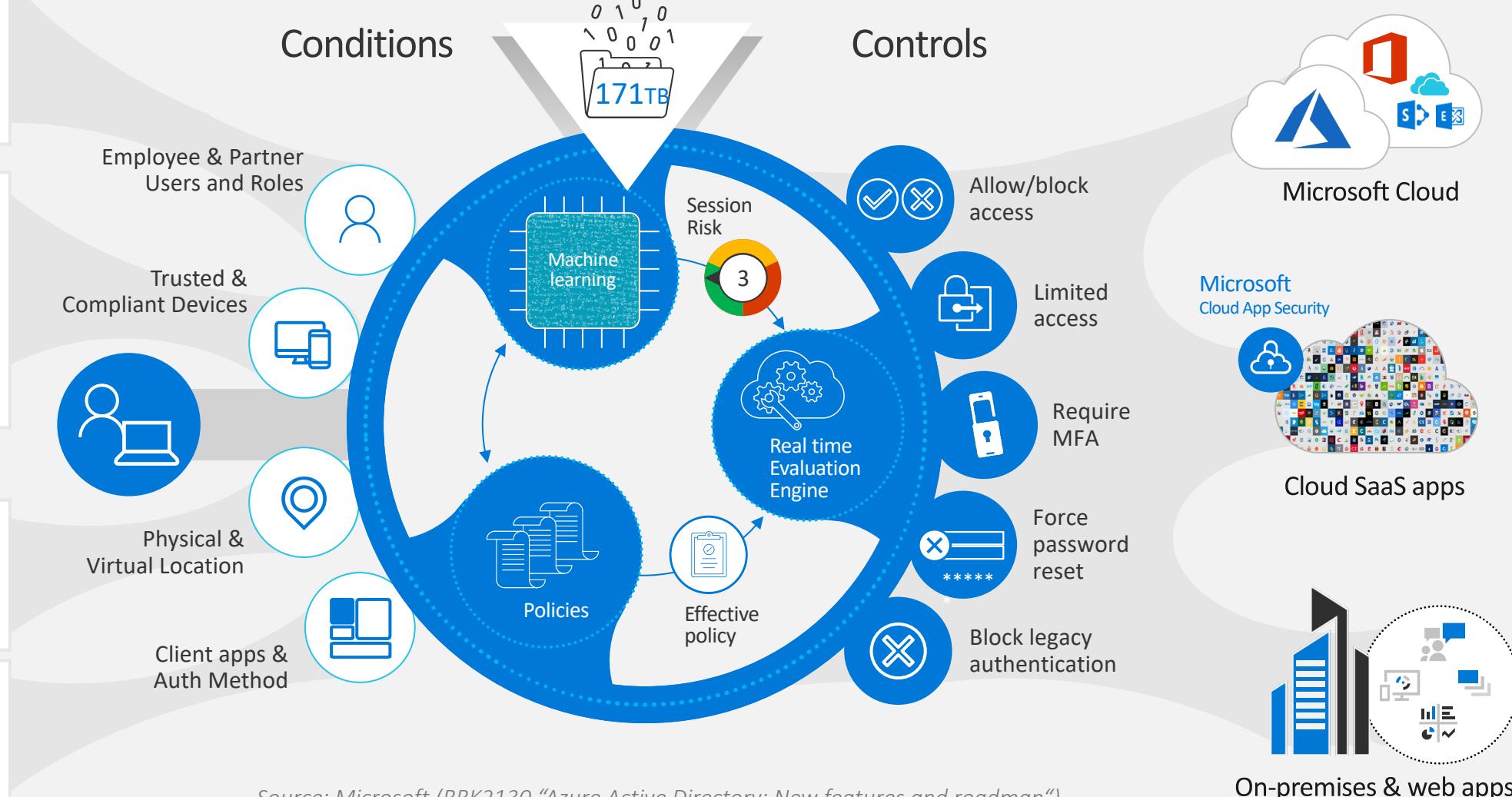
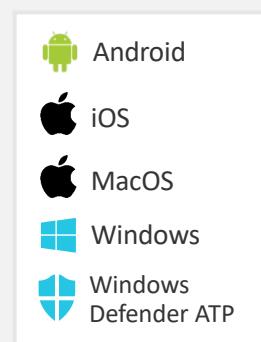
- Configure the following settings based on your security requirements/concept:
 - “Smart Lockout” Controls (Tenant-Level)
 - Password policy (for each user flow)
 - Token lifetime and Session behavior (for each user flow)
 - Password expiration?
 - Enforce MFA (on critical operations or activities)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



How it works in Azure AD (Premium) today...



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

A close-up photograph of a person's hands typing on a silver laptop keyboard. The background is blurred, showing what appears to be a window or a bright light source.

Thank You

 @Thomas_Live

 Thomas@Naunheim.net

 www.cloud-architekt.net