



#ScottishSummit2021



Thomas Naunheim

Manage and Secure Your Customer
Identities with Azure AD B2C!

GERMAN 13:00

Our Sponsors



Cloud Architect

Speaker & Blogger

Work and live in Koblenz, Germany

Focus on Identity + Security in Microsoft Azure

Member of „Azure Meetup Bonn“ Orga Team

@Thomas_Live

www.cloud-architekt.net

Thomas Naunheim



Agenda



Overview
and B2C Tenant



User Flows and
App Integration



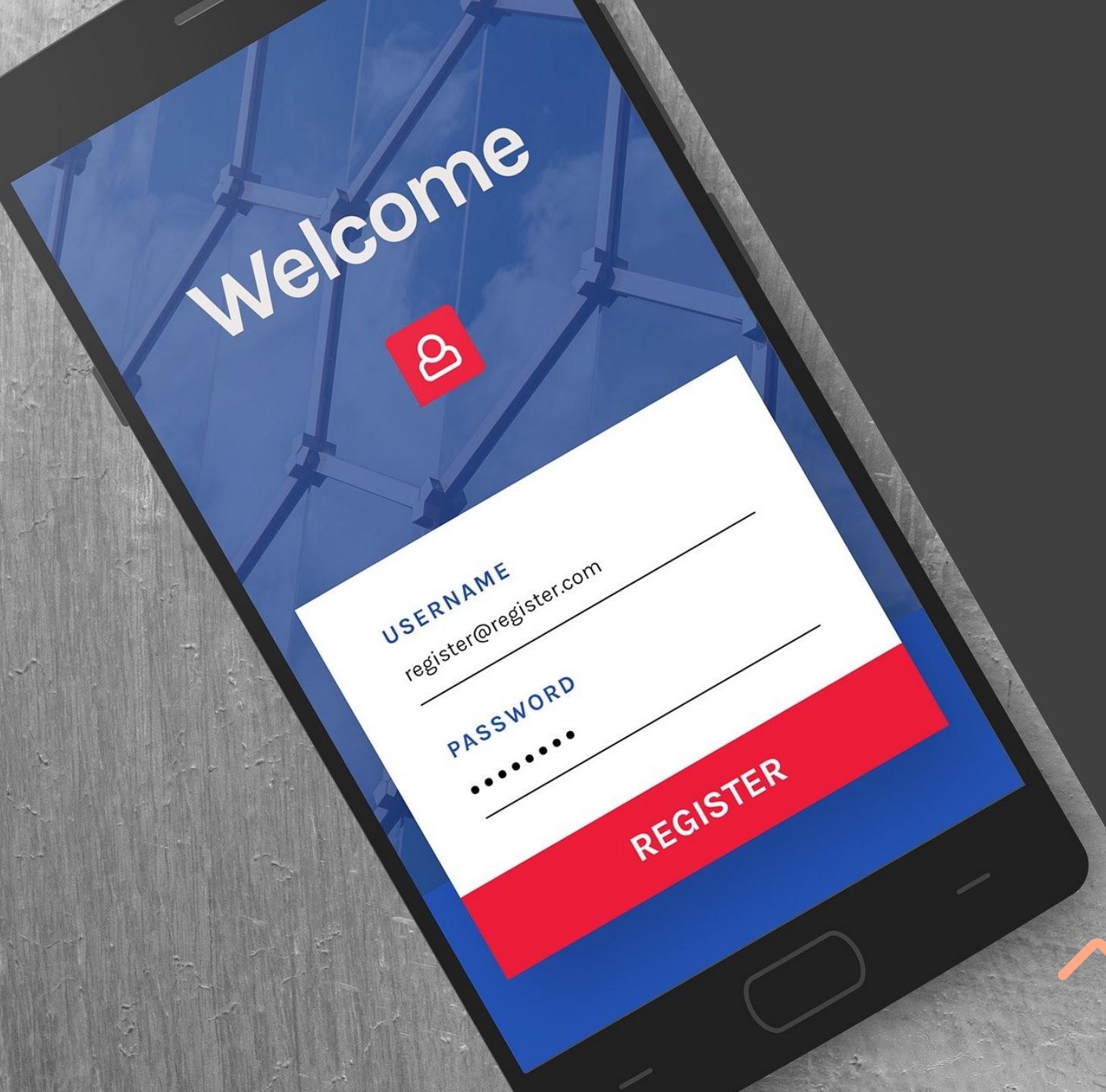
Branding and
Customizing



Protection of
B2C Identities



Monitoring and
Operations



Azure AD B2C

Overview and B2C Tenant



Azure Active Directory B2C

Customers

Social IDs, email, or local accounts



Any SAML Provider

Business & Government IDs



Any OIDC Provider

Protect your users with MFA



Use social accounts



Create custom user attributes

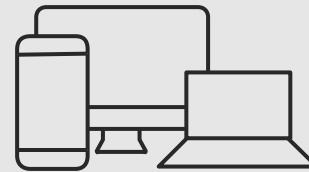


Customize your pages using HTML and CSS



Business

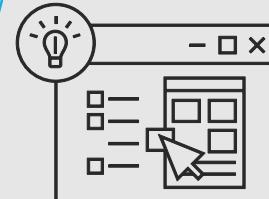
Apps and APIs
OAuth2 / SAML



Analytics



Integration with other systems





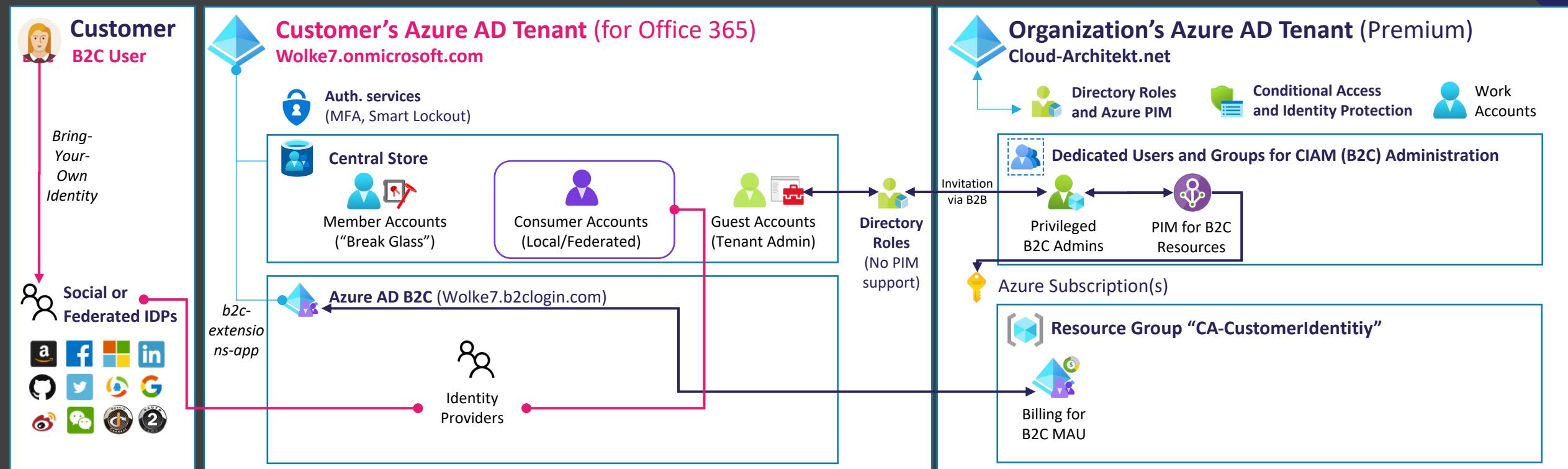
Azure AD B2C

Overview of B2C Tenant



A screenshot of the Microsoft Azure portal. The URL in the address bar is "https://portal.azure.com/#blade/Microsoft_AAD_B2C/B2C_OverviewBlade/overview". The page title is "Azure Active Directory B2C". It features a "Create" button and navigation links for Overview, Plans, Usage Information + Support, and Reviews. Below this, there's a section titled "Customer Identity and Access Management (CIAM) in the cloud" with a brief description and a bulleted list of benefits. At the bottom, it mentions a free tier of 50,000 monthly active users (MAUs) and notes that Multi-Factor Authentication (MFA) activity is billed separately. A "Media" section shows thumbnail images of various Azure services.

Azure AD (B2C) Tenant(s)

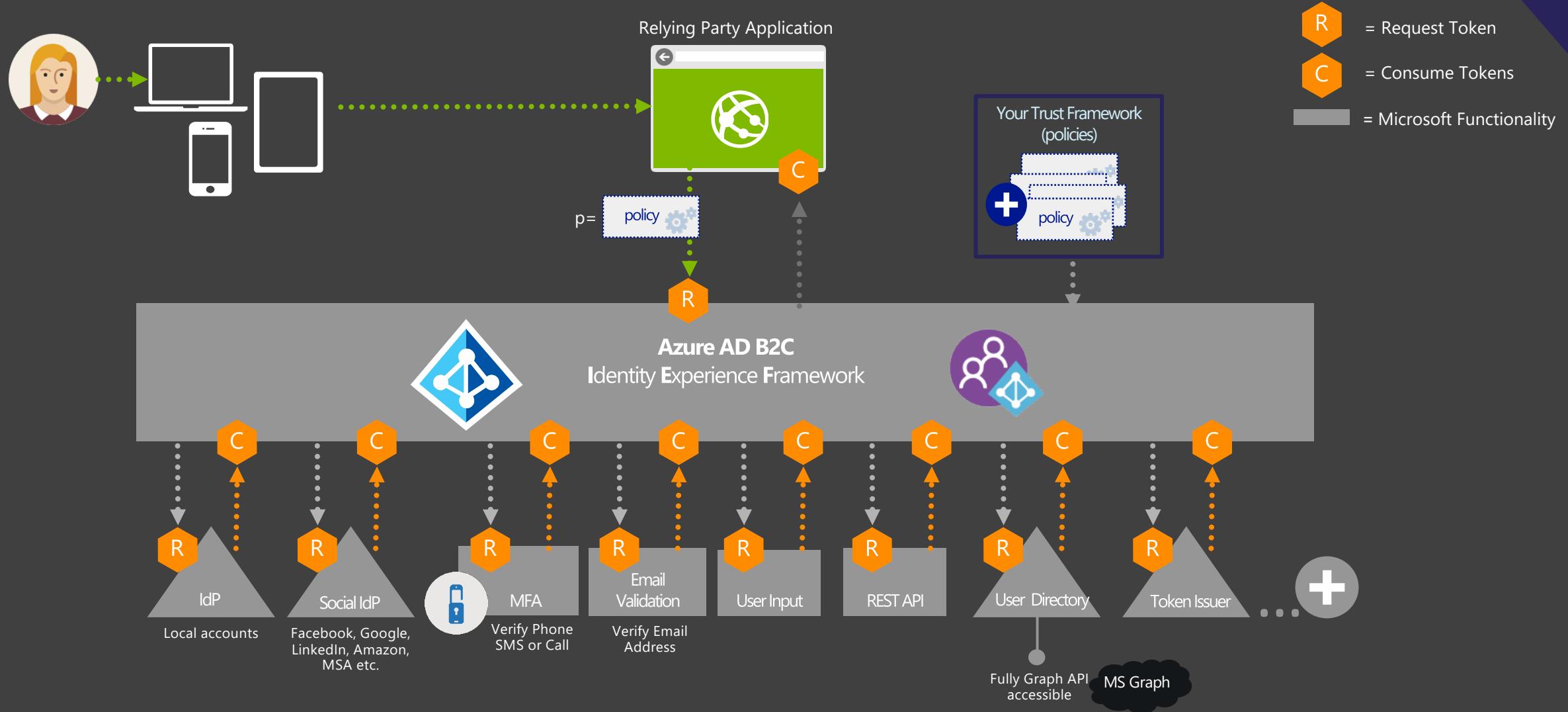




Azure AD B2C *App Integration and User Flows*

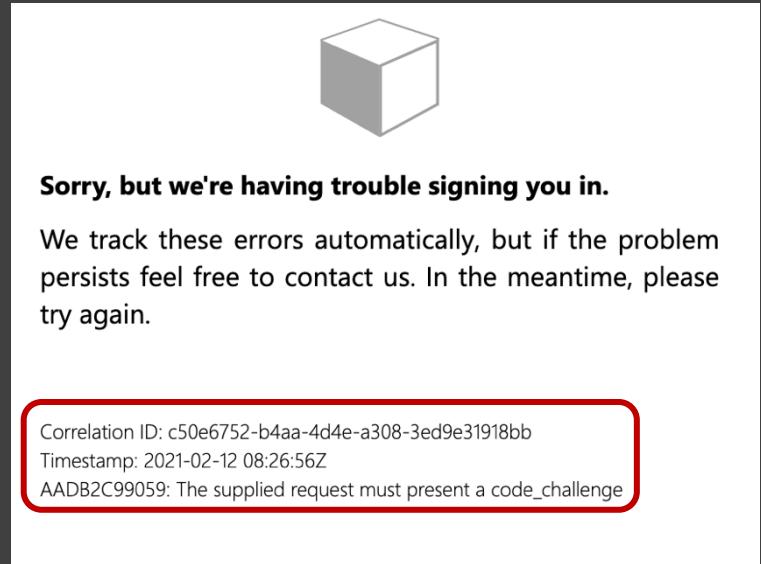


Orchestration and Flows



Error Codes and Throttling

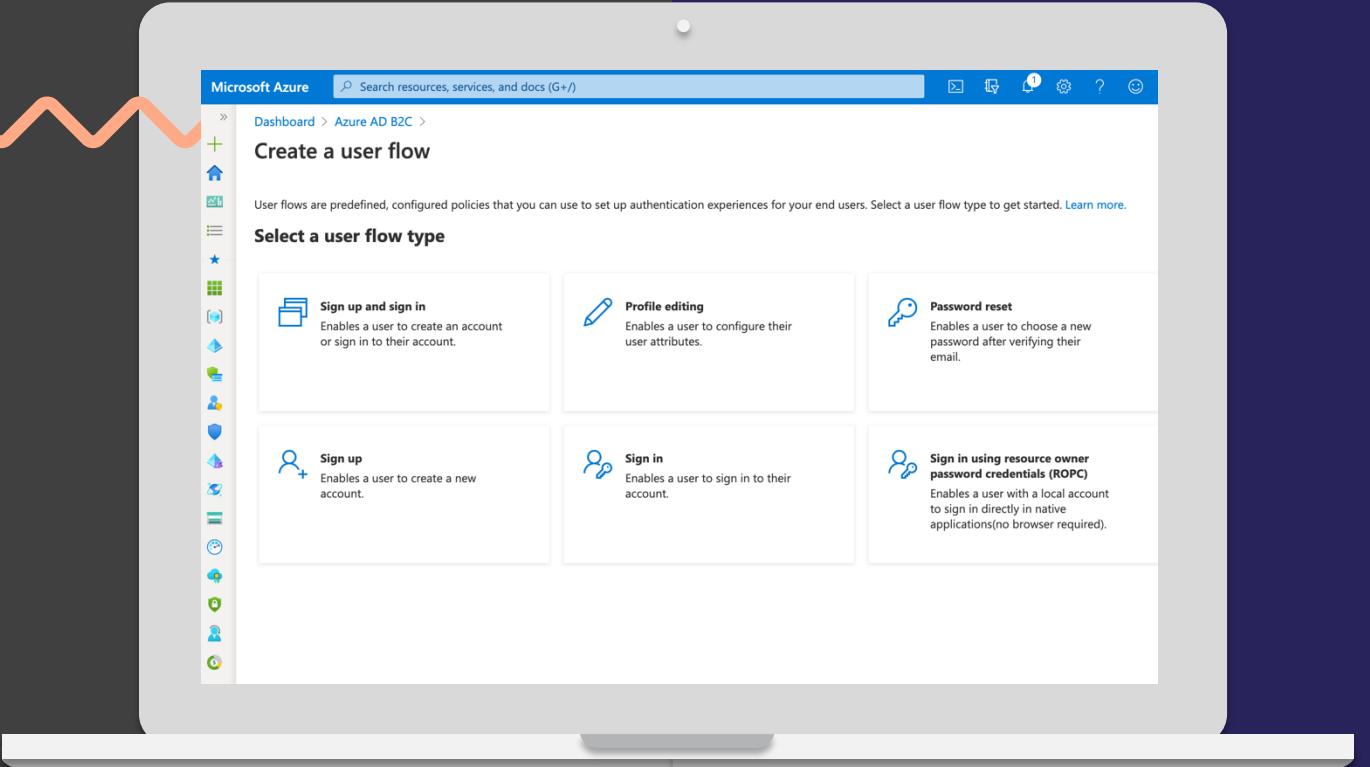
- Error Codes returned by B2C Service
 - “AADB2C90118”: Returned to app for invoking SSPR flow
 - [Reference list of error codes](#)
- Throttling
 - B2C throttles traffic if too many requests are sent (from the same source in a short period of time).
 - **Monitoring and handle error code “AADB2C90229”**





Azure AD B2C

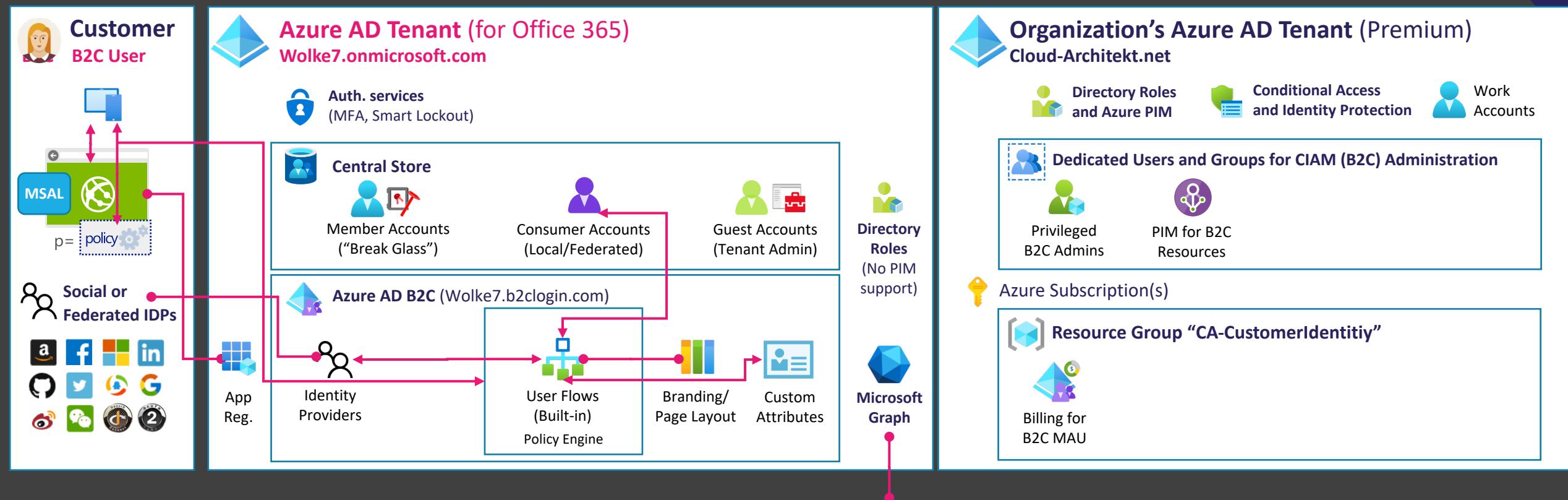
Built-in User Flow Capabilities (Zero-Code)

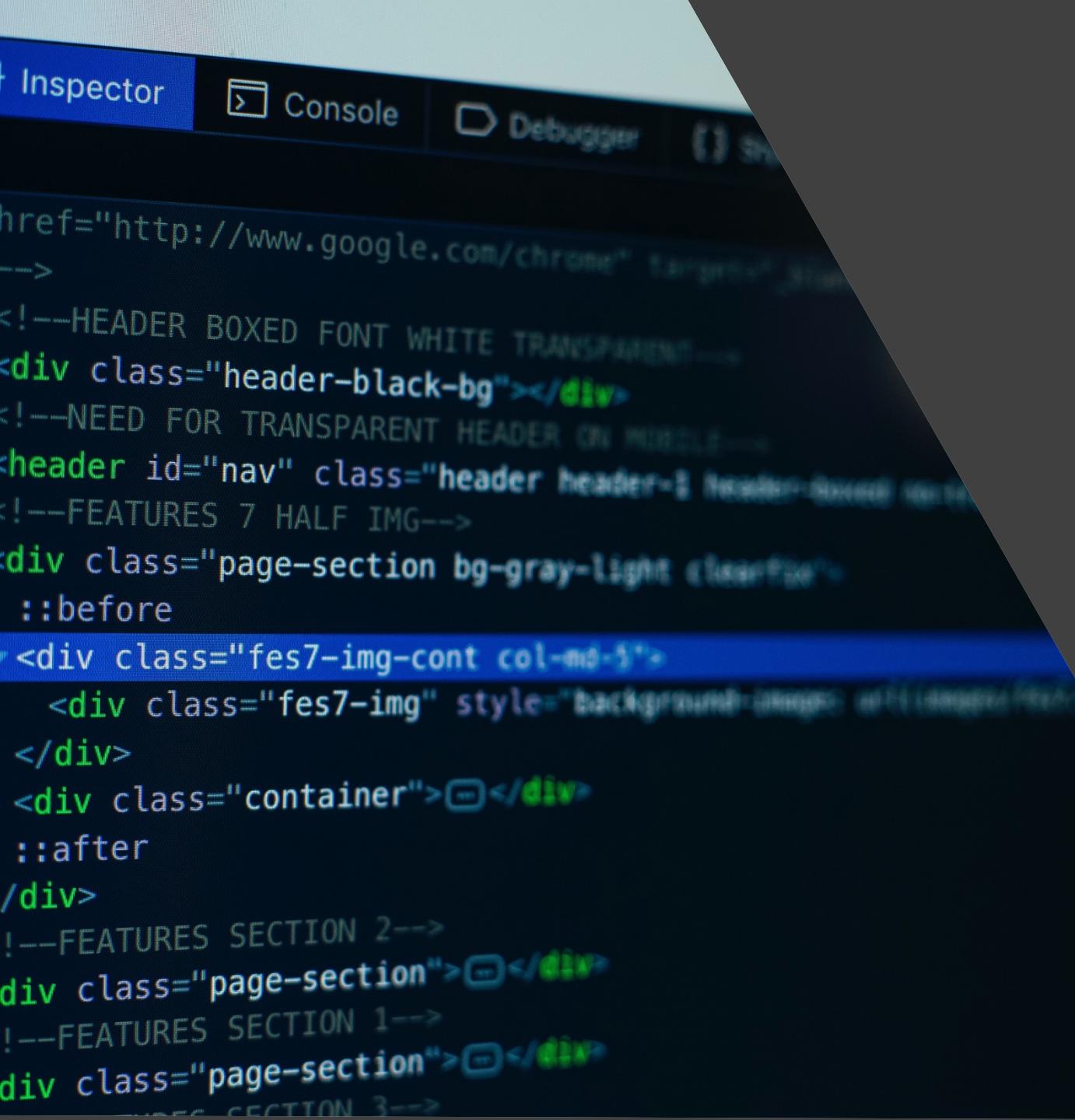


The screenshot shows the 'Create a user flow' page in the Microsoft Azure portal. The top navigation bar includes 'Microsoft Azure', a search bar, and various icons. The main content area has a title 'Create a user flow' and a subtitle 'User flows are predefined, configured policies that you can use to set up authentication experiences for your end users. Select a user flow type to get started.' Below this is a section titled 'Select a user flow type' with six cards arranged in a 2x3 grid:

User Flow Type	Description
Sign up and sign in	Enables a user to create an account or sign in to their account.
Profile editing	Enables a user to configure their user attributes.
Sign up	Enables a user to create a new account.
Sign in	Enables a user to sign in to their account.
Password reset	Enables a user to choose a new password after verifying their email.
Sign in using resource owner password credentials (ROPC)	Enables a user with a local account to sign in directly in native applications (no browser required).

User Flows and App Integration





A screenshot of a browser's developer tools, specifically the Inspector tab. The code displayed is a portion of an HTML file, likely a landing page or features section. It includes elements like a header with a black background, a main content area with a gray background, and several 'page-section' divs containing placeholder text. The code uses CSS classes such as 'header-black-bg', 'bg-gray-light', and 'fes7-img-cont'. There are also some inline styles and comments throughout the code.

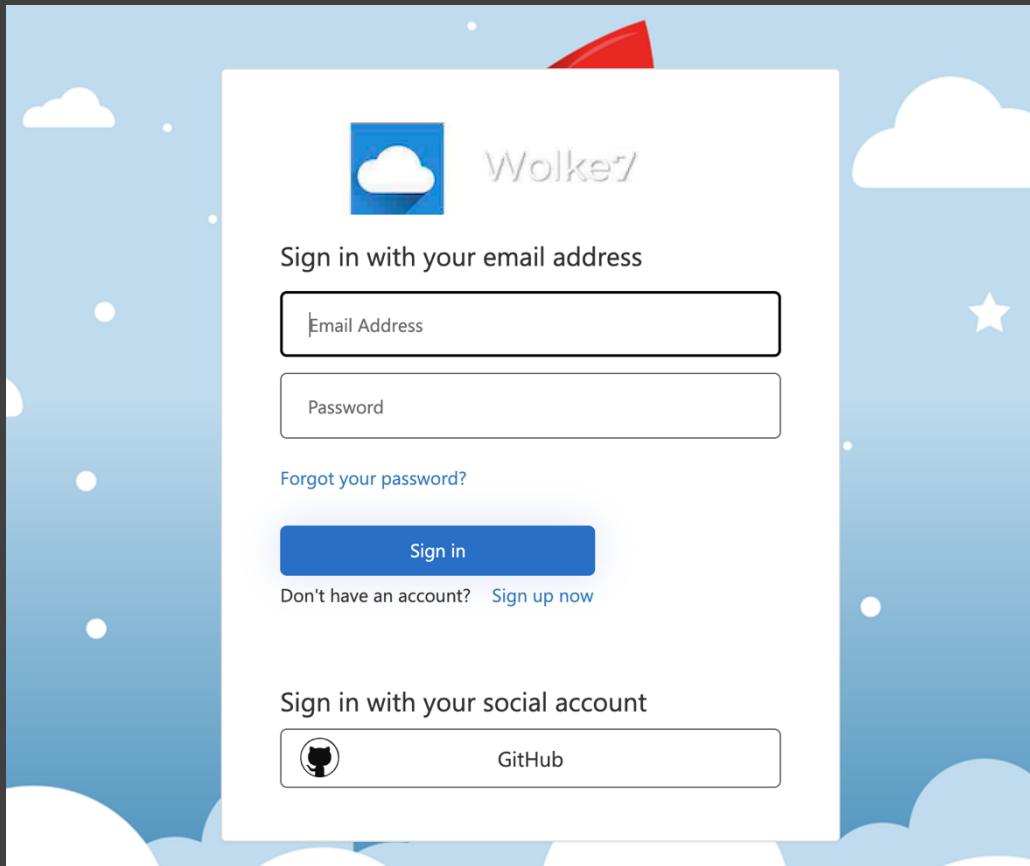
```
href="http://www.google.com/chrome" target="blank">-->
<!--HEADER BOXED FONT WHITE TRANSPARENT-->
<div class="header-black-bg"></div>
<!--NEED FOR TRANSPARENT HEADER ON MOBILE-->
<header id="nav" class="header header--l header-transparent">
<!--FEATURES 7 HALF IMG-->
<div class="page-section bg-gray-light clearfix">
  ::before
  <div class="fes7-img-cont col-md-5">
    <div class="fes7-img" style="background-image: url('https://image.flaticon.com/icons/png/512/145/145855.png');">
  </div>
  <div class="container">■</div>
  ::after
</div>
<!--FEATURES SECTION 2-->
<div class="page-section">■</div>
<!--FEATURES SECTION 1-->
<div class="page-section">■</div>
<!--FEATURES SECTION 3-->
```

Azure AD B2C *Branding and Customizing*



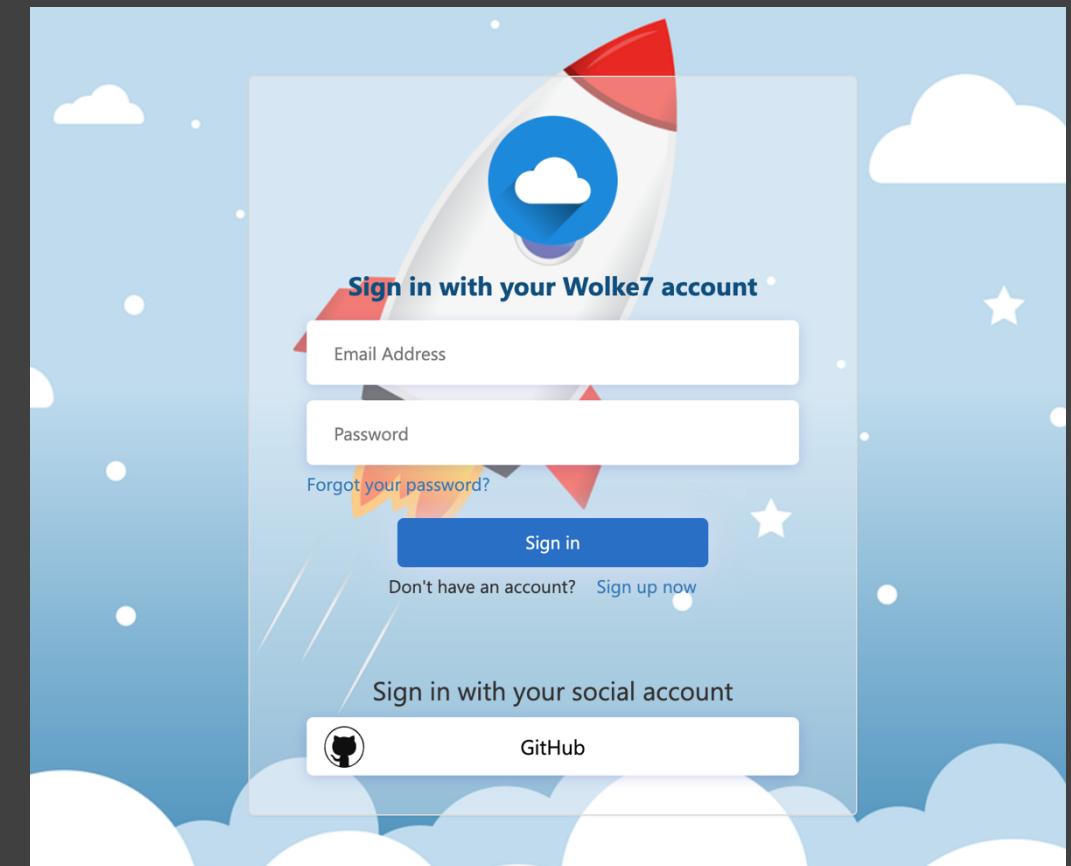
Options for UI Customizing

Company Branding (Recommended Policies)



Limitation of Azure AD's Company Branding

Custom Page Layout (All Policies)



Customizing of Template "Ocean Blue"

Options for UI Customizing

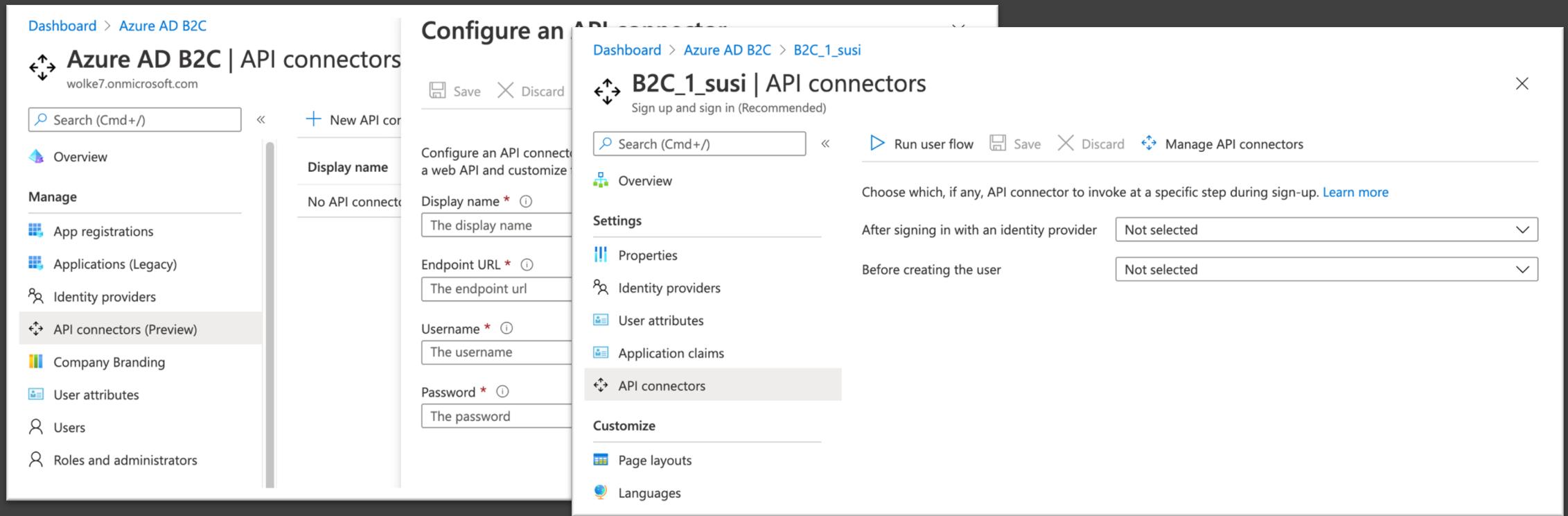
- **Custom Page Layout**
 - Customize UI with (hosted) HTML/CSS files
 - Sample HTML and CSS files available on [GitHub](#)
 - Hosting the page content (publicly available HTTP endpoint that supports CORS, CDN recommended)
 - Your own JavaScript client-side code, consider guidelines!
- **Domain Customization**
 - Default: <https://{{your-tenant-name}}.b2clogin.com/{{your-tenant-id}}>
 - Customer-Owned Domains: Announced as Public Preview in 2021 → [UserVoice](#)

Custom email verification (Custom Policies only)

- Send customized email using 3rd party provider ([SendGrid](#), [Mailjet](#),...)

API Connectors (Preview)

- Simple and secure customization and extension of user flows for
 - Protect against automated fraud abuse (CAPTCHA)
 - Use invitation codes or perform identity verification
 - Reformat of attribute values or update from/to corporate database



The screenshot shows the Azure AD B2C API connectors configuration interface. On the left, the navigation menu includes options like Overview, App registrations, Applications (Legacy), Identity providers, API connectors (Preview) (which is selected and highlighted in grey), Company Branding, User attributes, Users, and Roles and administrators. The main area displays a modal window titled "Configure an API connector" for a connector named "B2C_1_susi". The modal has sections for "Display name" (set to "The display name"), "Endpoint URL" (set to "The endpoint url"), "Username" (set to "The username"), and "Password" (set to "The password"). To the right of the modal, the "B2C_1_susi | API connectors" page is shown, featuring tabs for Overview, Settings, and Customize. Under Settings, there are dropdown menus for "After signing in with an identity provider" (set to "Not selected") and "Before creating the user" (set to "Not selected"). The "API connectors" tab is currently selected in the navigation bar.



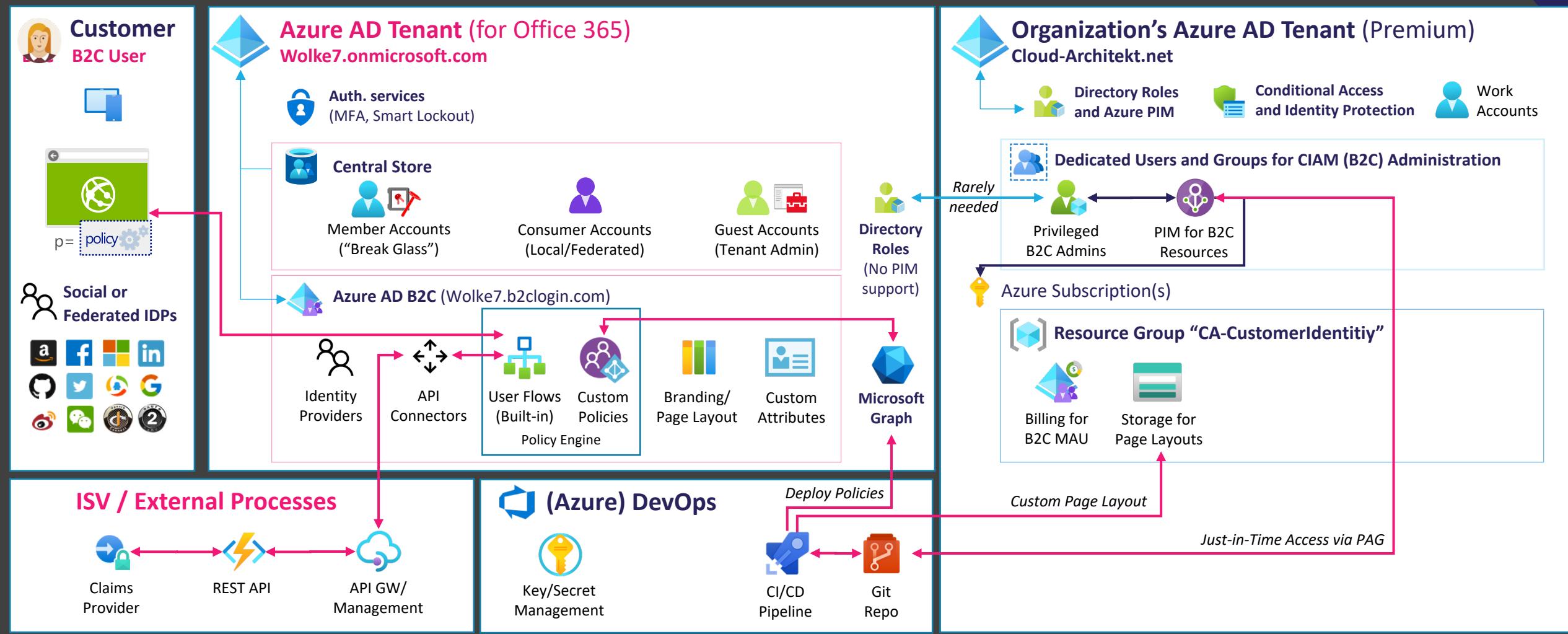
Azure AD B2C

Custom Policies (Templates) & Deployment

A screenshot of the Microsoft Azure Identity Experience Framework (B2C) custom policies page. The page shows a list of custom policies including "B2C_1A_TrustFrameworkBase", "B2C_1A_CAPolicySample", "B2C_1A_phone_SSUI", "B2C_1A_ProfileEdit", "B2C_1A_signup_signin", "B2C_1A_TrustFrameworkExtensions", and "B2C_1A_TrustFrameworkBase". The "B2C_1A_TrustFrameworkBase" policy is selected and shown in detail. The interface includes navigation menus for "Custom policies", "Manage", and "App registrations", as well as links to "Documentation" and "Scenarios".

The screenshot illustrates the deployment of a custom policy named "B2C_1A_TrustFrameworkBase" within the Azure AD B2C service. The policy is described as a "custom policy" and includes a note about its requirements for a relying party section. The page also provides links to "What are custom policies?", "Get started with custom policies", and "Your custom policies".

Branding and Customizing





Azure AD B2C *Protection of B2C identities*



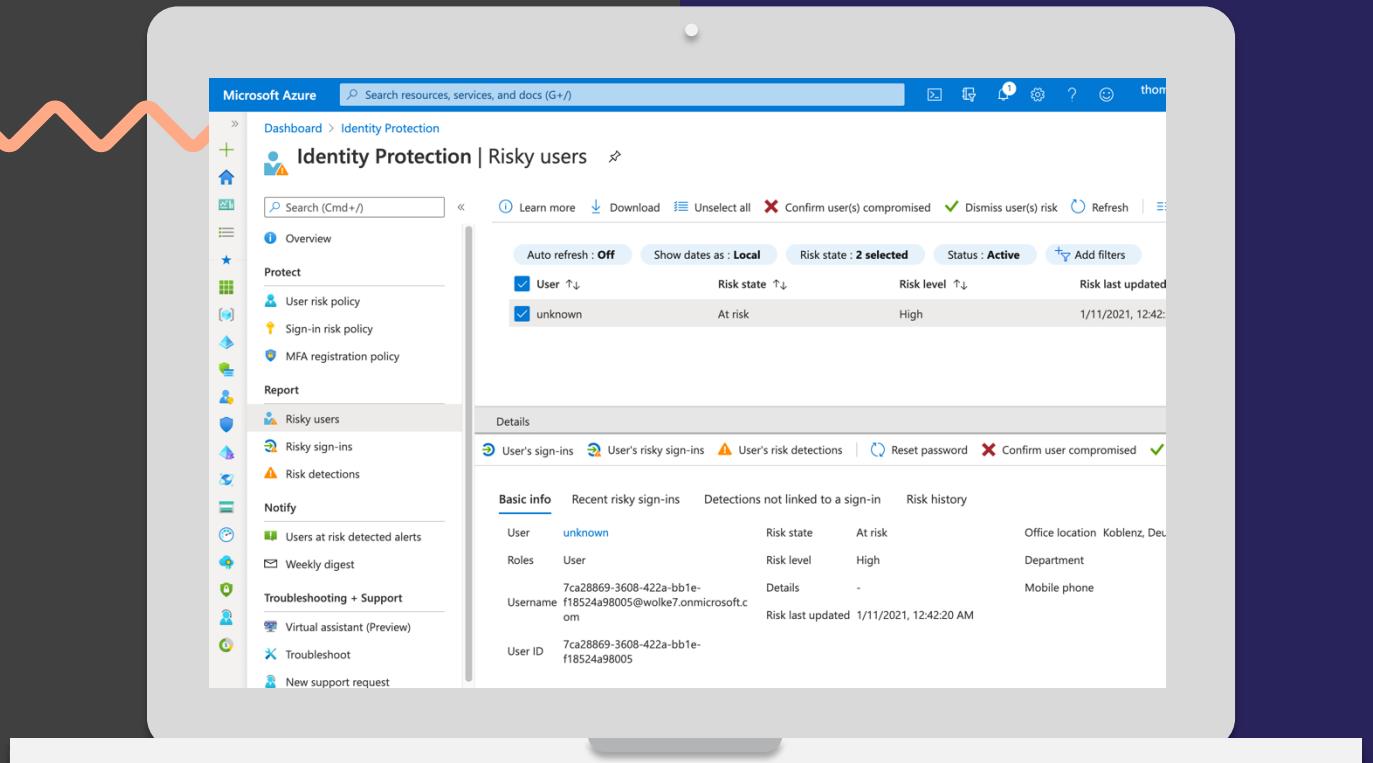
Conditional Access in B2C





Azure AD B2C

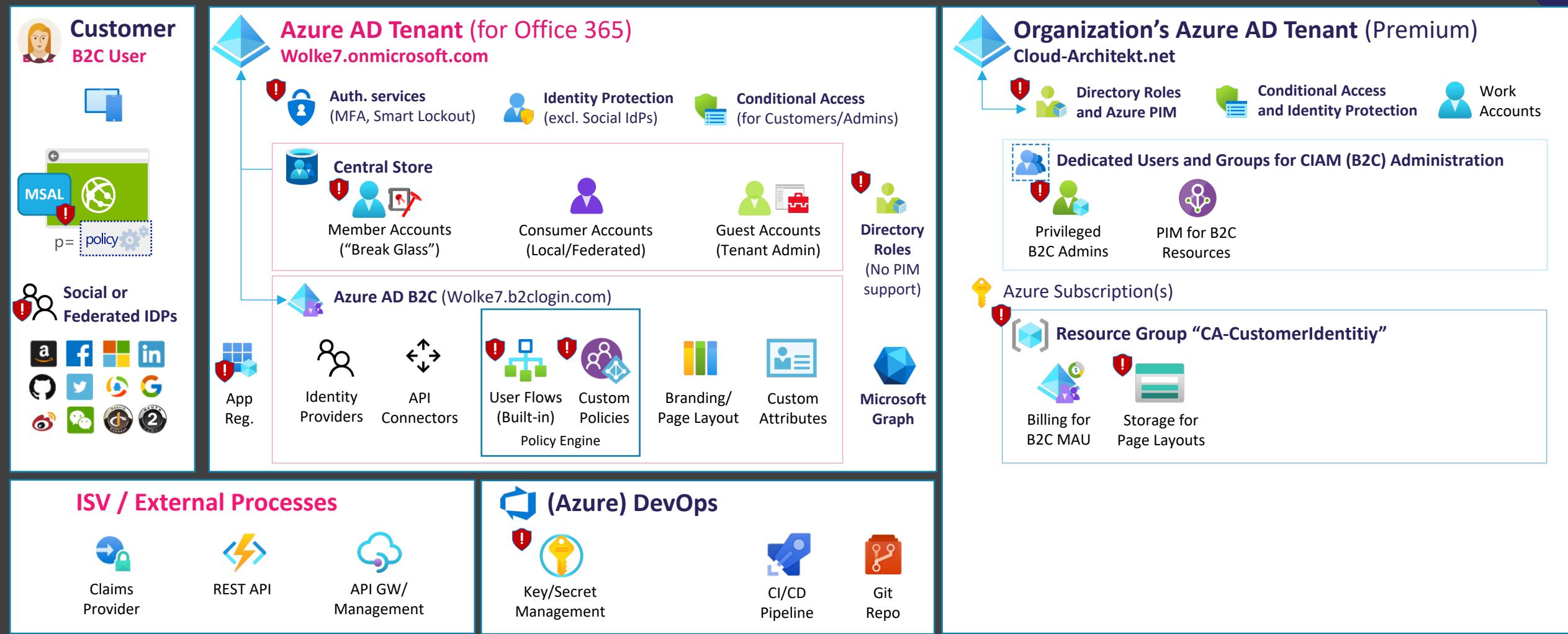
Identity Protection & Conditional Access



The screenshot shows the Microsoft Azure Identity Protection interface, specifically the 'Risky users' section. The left sidebar includes options like 'Overview', 'Protect' (with 'User risk policy', 'Sign-in risk policy', and 'MFA registration policy'), 'Report' (with 'Risky users' selected), 'Notify' (with 'Users at risk detected alerts' and 'Weekly digest'), 'Troubleshooting + Support' (with 'Virtual assistant (Preview)', 'Troubleshoot', and 'New support request'), and 'Support' (with 'Feedback'). The main content area displays two risky users: one labeled 'User' with 'unknown' as the user and 'At risk' as the risk level, and another labeled 'unknown' with 'At risk' as the risk level. Both have 'High' as the risk level. The 'Details' section provides basic information for the first user, including their user ID (7ca28869-3608-422a-bb1e-f1852498005) and email (wolke7.onmicrosoft.com). It also shows recent risky sign-ins, detections not linked to a sign-in, and risk history.

User	Risk state	Risk level	Office location	Department
unknown	At risk	High	Koblenz, De	Mobile phone
7ca28869-3608-422a-bb1e-f1852498005	Details	-		
7ca28869-3608-422a-bb1e-f1852498005	Risk last updated	1/11/2021, 12:42:20 AM		

Protection of B2C identities





Azure AD B2C *Monitoring and Operations*



Monitoring

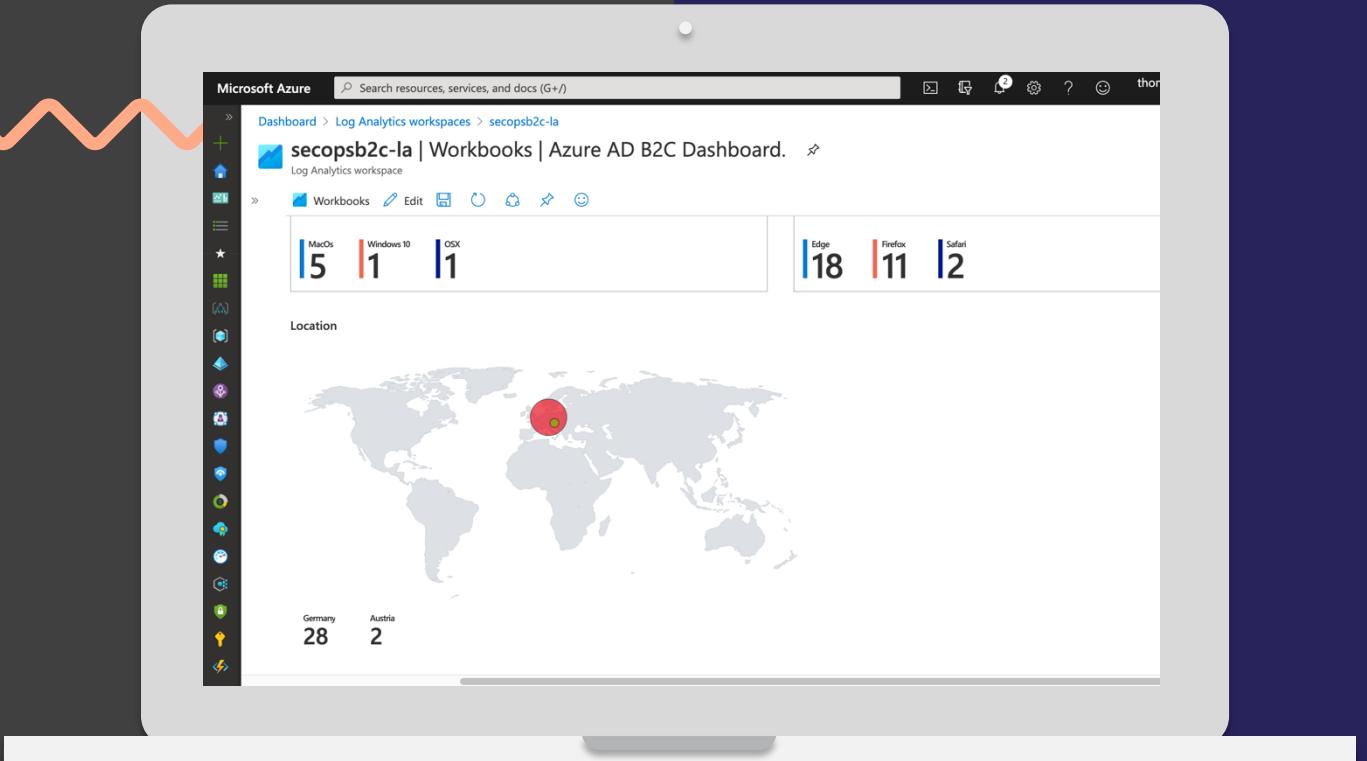
- Route logs to “[Azure Monitor](#)”, Storage (Long-term use) or 3rd Party SIEM (EventHub)

Service Health Alerts of B2C Platform and dependencies (incl. CDN, Functions, etc.)

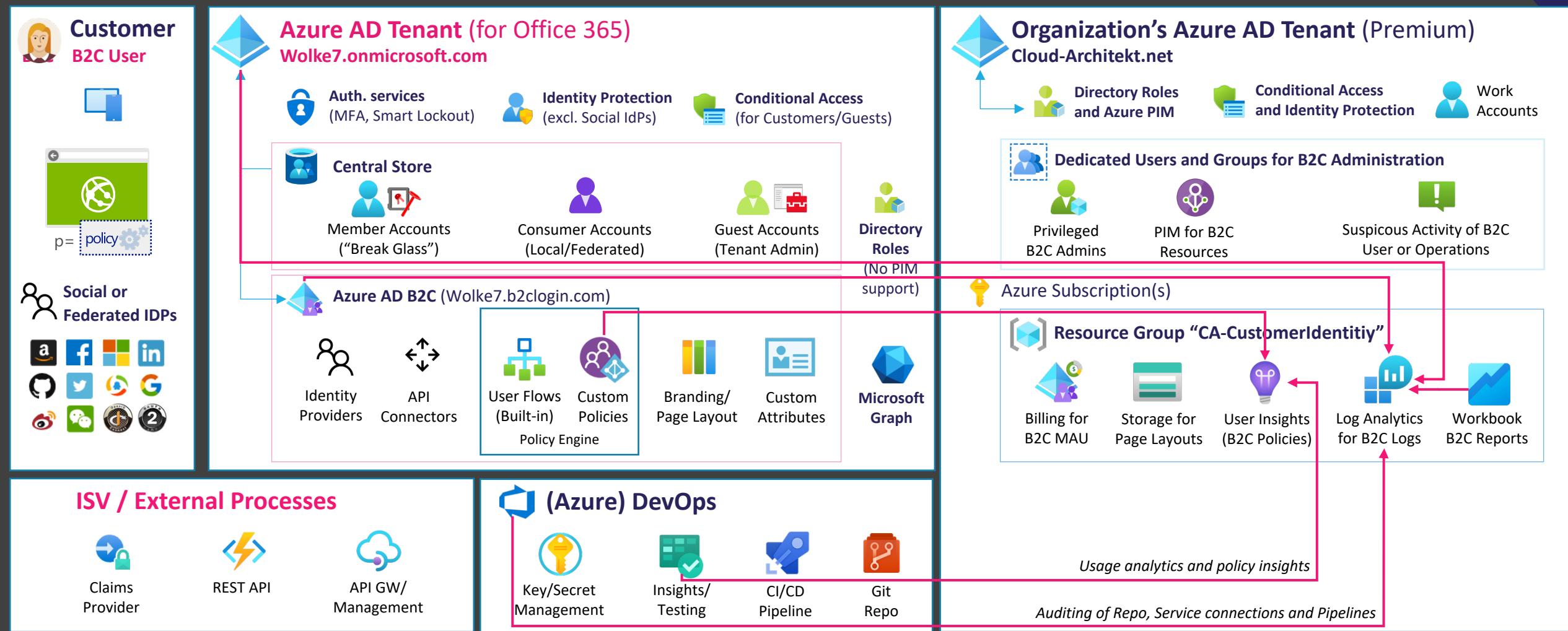
- Track “user behavior” (Usage Analytics) in Custom Policies with “[Application Insights](#)”



Azure AD B2C Dashboard *for Operations*



Management and Operations



#ScottishSummit2021



Thank You