Bachelor's thesis

Business Information Technology

2023

Taru Perkola

Identity and Access Management with a CIAM solution

– Case Azure Active Directory Business to Customer

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Bachelor’s Thesis | Abstract

Turku University of Applied Sciences

Business Information Technology

2023| 43 + 8 pages

Taru Perkola

Identity and Access Management with a CIAM solution

- Case Azure Active Directory Business to Customer

The object of this thesis was to study a single CIAM solution and test how it can be implemented into two web applications and how it can be customized.

This thesis is handling the basics of cloud services and key elements of Identity and Access Management as well as authentication and authorization, focusing on most commonly used methods and protocols.

Two web applications were created for testing purposes. Azure AD B2C solution was implemented on both applications, though they utilize the solution differently. The first application showcases the customization opportunities that the solution has to offer, these were made with JavaScript programming language. External Identity Providers, such as Facebook and Google were also joined into the first application.

The second application is significantly lighter solution, which does not require programming, but enables minor customization fairly quickly.

After testing, implementing and customizing the solution, the results were gained, and they will be used for the KPMG’s employees when they are familiarilizing themselves to Azure AD B2C.

Keywords: IAM (Identity & Access Management), CIAM, Microsoft Azure AD B2C, digital identity

Opinnäytetyö (AMK) | Tiivistelmä

Turun ammattikorkeakoulu

Tietojenkäsittely

2023 | 43 + 8 sivua

Taru Perkola

Identiteetin ja pääsynhallinta CIAM-ratkaisulla

- Case Azure Active Directory Business to Customer

Tämän opinnäytetyön tavoitteena oli perehtyä yksittäiseen CIAM-järjestelmään ja testata sen implementaatiota kahteen sovellukseen sekä selvittää, minkälaisia kustomointimahdollisuuksia se tarjoaa. Työssä käsiteltiin pilvipalveluiden perusteita sekä identiteetin ja pääsynhallinnan tärkeimpiä elementtejä. Lisäksi työssä käsiteltiin todennuksen sekä varmennuksen yleisimpiä menetelmiä ja protokollia.

Testausta varten luotiin kaksi verkkosovellusta, joihin liitettiin Azure AD B2C -järjestelmä. Molemmat sovellukset hyödynsivät järjestelmää eri tavoin. Ensimmäinen sovellus ilmensi järjestelmän tarjoamia kustomointimahdollisuuksia, jotka toteutettiin JavaScript-ohjelmointikielellä. Ensimmäiseen sovellukseen liitettiin myös ulkoisia identiteetin tarjoajia, kuten Facebook ja Google.

Toinen sovellus edusti huomattavasti kevyempää ratkaisua, joka ei edellytä ohjelmointitaitoa, mutta mahdollisti pienimuotoisen kustomoinnin hyvinkin nopeasti.

Järjestelmän huolellisella testauksella, kustomoinnilla ja sovelluksiin integroimalla saavutettiin tuloksia, joita voidaan hyödyntää tulevaisuudessa toimeksiantajan yrityksessä, kun työntekijät perehtyvät Azuren AD B2C -järjestelmän käyttöön.

Asiasanat:

IAM, CIAM, Microsoft Azure AD B2C, digitaalinen identiteetti

Contents

Appendices

Pictures

List of abbreviations

AAD	Azure Active Directory
API	Application Programming Interface
B2B	Business to Business
B2C	Business to Customer
CIAM	Customer Identity and Access Management
IAM	Identity and Access Management
IdP	Identity Provider
JSON	JavaScript Object Notation
MFA	Multi-Factor Authentication
SMS	Short Message Service
SSO	Single Sign On
SP	Service Provider
SPA	Single Page Application
URI	Uniform Resource Identifier

1 Introduction

This thesis was commissioned by KPMG Finland Oy Ab. KPMG Finland is part of the KPMG International. KPMG is a global network of professional service firms that provide audit and assurance, tax and legal, and advisory services.

The objective of this thesis is to demonstrate Azure Active Directory B2C solution with two web applications and study its adequacy as being a finalized product that can be sold to customers in the future.

Customers have various needs and desires, so as a company it is important to understand the need of educating employees and keeping their knowledge updated, regarding the new alternative solutions in the market.

In the chapters two to four, this thesis will study cloud computing services, main elements of Identity and Access Management and most commonly used authentication and authorization protocols.

In chapter five, this thesis will demonstrate Azure AD B2C solution, how it operates and what are its main properties such as customization features, and security enhancing options, such as multifactor authentication. External Identity Providers are also integrated into the service, so that users can login to the application with their social accounts, such as Facebook and Google.

All the images in this thesis have been created by the author or taken as screenshots from the author's Azure Portal or from an application that the author has created for demonstration purposes. The demonstrated applications will not be publicly available on the Internet and are tested only locally.

In chapter six, the conclusions of this thesis are focusing on the benefits of the Azure AD B2C solution. The conclusions are based on the solutions' pricing, practicality, and what kind of customers the solution would be beneficial.

The expected result from this thesis is to provide useful information for KPMG, that they can utilize in the future, when they are training more employees to use Azure Active Directory B2C solution.

2 Cloud services

Cloud services or cloud computing is a method of providing services over the internet. When accessing an application or a file that is not located on local computer, or at the organizations' servers, that file or application is located at the cloud service providers' servers. (Vento 2021.) Many people are using cloud services on regular basis, even they might not be aware of it and they are accessible for everyone, individuals and organizations. (Citrix, 2023).

Cloud services were designed to be affordable and easy to implement on demand (Citrix, 2023). Mostly cloud services are used by purchasing only those resources that are needed and then paying for only what is being used. Cloud can provide multiple services, including servers, databases, storage, application hosting, analytics and even machine learning functionalities. (Vento 2021.)

Cloud can be divided into three main sections which are (Vento 2021)

- public cloud
- private cloud
- hybrid cloud.

Public cloud is a cloud computing service that is hosted by third party cloud service provider. With this type of solution, the cloud service provider is responsible for updating and maintaining the infrastructure for the cloud service. (Vento 2021.)

Private cloud is designed so that only a particular company can access its resources. Private cloud can be in the physical server room of the company or hosted by third party cloud service provider. (Vento 2021.)

Hybrid cloud is a combination of different environments. This means that it is possible having services running on-premises and in the cloud. This is a common solution when a company has invested plenty of money into on-premises infrastructure and doesn't want to move to cloud completely. (Google Cloud, 2023.)

There are also solutions where a company is using multiple cloud service providers at the same time, which is known as multicloud (Vento 2021).

The most common cloud vendors at the market currently are (Vento 2021)

- Microsoft Azure
- Amazon Web Services
- IBM Cloud
- Alibaba Cloud.

2.1 Identity and Access Management in cloud

This thesis examines one cloud service provider, which is Microsoft Azure. Microsoft Azure provides two solutions that can be used for Identity and Access Management. They are Azure AD Business to Customer, (B2C) and Azure AD Business to Business (B2B). B2C is more commonly used as it offers Identity and Access Management for external users. B2B is used for providing access for companys' business partners' employees, so that they can access appropriate resources when needed. (Kosunen 2021.) This thesis will demonstrate and provide guidance on how to use Azure AD B2C solution in Chapter 5.

3 Identity and Access Management – IAM

Identity and Access Management (IAM) is a collection of procedures, policies, and tools that can be used to define and manage the roles and access rights of an individual entity. This type of entity can be a user, application or a device and it can have access rights to applications that are cloud based or on-premises. When an individual entity is representing a user, that user can be a customer, partner, or an employee. These types of individual entities can also be represented as a device, which can be e.g., computer, smartphone, router, server, controller, or sensor (Strom, 2021).

The main purpose of IAM solution is that one entity has their own digital identity that belongs to only that entity. After digital identity has been created, its lifecycle can be managed and maintained by modifying and monitoring the identity when needed. (Strom, 2021.)

Identity and Access Management takes care of verifying the entity's identity and then controls their access rights to different resources. IAM enables the right individual to gain access to the right resources at the right time for the right reason. (Gontovnikas, 2021.)

IAM solutions provide the right tools for managing the user roles, tracking user activities, ability to create reports based on those activities and enforcing custom policies. The idea is to provide an effective way to administer user access rights across the organization and make certain that the compliance requirements are met as well with the company policies and government regulations. (Strom, 2021)

3.1 Customer Identity and Access Management – CIAM

Identity and Access Management can be divided into multiple subsections. This thesis will mainly focus on one subsection, which is CIAM, also known as Customer Identity and Access Management. CIAM is used for controlling access for external applications. External application means that the application is

directed at customers or consumers. Social login options are commonly used with CIAM solutions, because giving the customer an opportunity to use an already existing account, makes the login process smoother for the customer. (Gontovnikas, 2021.)

CIAM is considered more than just a technical security solution, that can handle customer login features. CIAM provides basic functions, such as customer sign up, login, own profile, and consent controlling, but in advance to those, it provides an easy to use, and uniformed experience, no matter what type of device or platform is being used. (Häkkinen, 2023.)

CIAM solutions are widely spread, because it is common these days, that people need to login to multiple devices and services. From a company's perspective, CIAM can provide valuable information about company's customers. (Gontovnikas, 2021.)

To provide best possible service to customers, it's important to know them. Understanding customers will require having access and visibility to the data, of how service is being used. One key feature of CIAM is to provide a way of knowing customers and then use that information for company improvement. (Häkkinen, 2023.) Although, the collected data about customers, can be used for improving companies, it does come with a great responsibility, as data privacy laws need to be followed (Gontovnikas, 2021).

4 Authentication and authorization

Authentication is used for referring to a user's identity: who is that user and has the user's identity been confirmed by a login process. Authorization is referring to a user's permissions and privileges, focusing on what type of actions is that user allowed to do within different systems. (Cloudflare, 2023.)

Main difference between authentication and authorization can be easily described with an example: Let us say a person is wanting to participate in a certain event, and that person buys a ticket for e.g., a music concert. When arriving at destination and at the gates of the event, a valid ticket needs to be presented to the event organizer. Personal ID needs to be presented as well, because proof of that the age and the name in Personal ID are matching the information in the ticket. After this step is done, authentication is ready and proceeding into the concert is allowed. Next step is the authorization. Authenticated people are allowed to find a seat and see the artist presenting on the stage. However, being authorized does not allow people doing whatever they like at the concert, even though possesing a valid ticket. Climbing up to the stage and greeting the artist is not allowed, this would require more access. By purchasing a more expensive ticket, it could be possible to gain this type of access and visit the backstage. (Cloudflare, 2023)

4.1 SAML

SAML is abbreviation for Security Assertion Markup Language, which is a standardized way to inform external applications and services, if a user is who they say they are (Kennedy, 2022). With SAML, SingleSign-On technology can be used, because it provides a way to authenticate a user once and then forward that authentication to various applications. At time of writing this report, SAML 2.0 is the most recent version of SAML. (Cloudflare, 2023.)

SAML authentication can be seen as a way to provide information about who someone is, in a simple and standardized way, just like an identification card.

SAML is considered as an interoperable standard, which means that it can work with systems and devices that were built by different vendors and for completely different purposes, but they still must interact with each other. SAML is using Extensible Markup Language (XML) for standardizing communications (OneLogin, 2023). SAML is acknowledged as a way to provide user's identity to cloud service providers (Cloudflare, 2023).

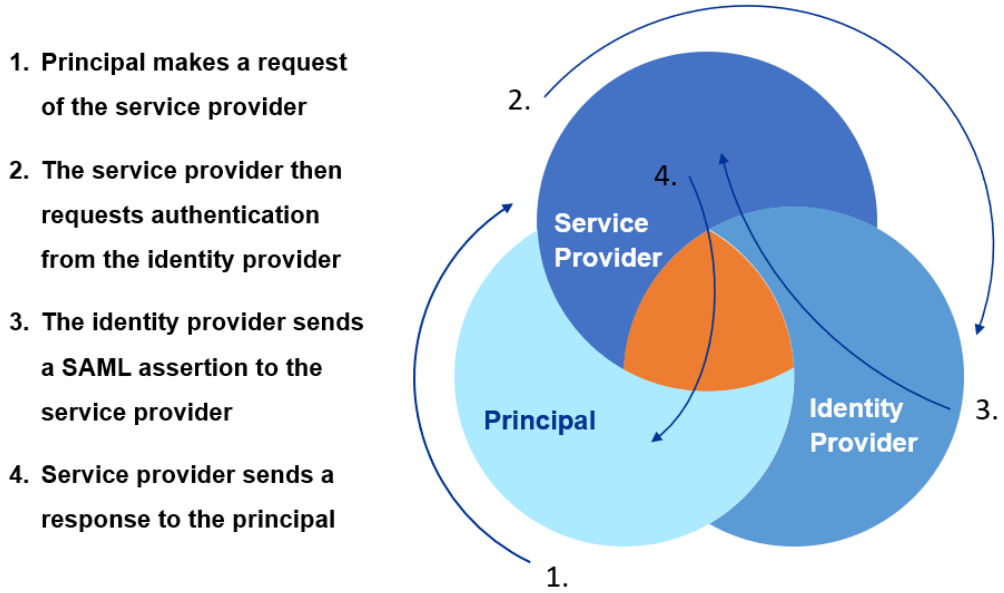
4.2 Single Sign-On (SSO)

Single Sign-On enables access to multiple resources at once, as long as they are located in a single organization or domain (McKeown, 2021). This is possible because of SAML, as it can forward authentication to various applications. (Cloudflare, 2023.) SSO is often used without the user even noticing it, for example with Google accounts, users are gaining direct access to Gmail and YouTube accounts, even they are completely different services. Google account is mentioned here to provide a simple example of how SSO works. (Gontovnikas, 2021.)

Single Sign-On makes login processes more efficient because the user does not need to confirm who they are, every single time they need to use an application or a service. (Cloudflare 2023). From a user's perspective, SSO will simplify things since people do not need to remember multiple credentials to every single application. SSO provides valuable information for organizations, because it can track when users are moving from one application to another. (Gontovnikas, 2021.) Single Sign-On system must be able to communicate with every external application and let them know that the user is signed in and this is the part where SAML is needed (Cloudflare, 2023).

Single Sign-On authentication process usually involves three main parts that are principal, Identity Provider and service provider (Cloudflare, 2023). Principal is usually a user who is trying to access an application that is being hosted in the cloud. Identity Provider or IdP, is a cloud-based software service that can store and confirm a user's identity. This is typically done through a login process.

Service provider is the application or a service that is hosted in the cloud and the user wants to use or access. Normally, if people want to use an application, they just directly log into it, and then gain access to it. With SSO, people are logging into the SSO, and then gain access to multiple applications through SAML. (Cloudflare 2023.) Typical flow of requests can be seen in the Picture 1.



Picture 1. Request flow.

In Picture 1, section 3, the Identity Provider sends a SAML assertion to the service provider. SAML assertion is a message that lets the service provider know that a user is signed in. This message contains all the necessary information that is required by a service provider to confirm the user's identity. This includes the source of the message, the time it was issued and the conditions that make the message valid. (Cloudflare 2023.)

4.3 Federated Identity Management (FIM)

Federated Identity Management, also known as FIM, makes it possible for people to gain access to multiple applications and domains with single credentials

(OneLogin, 2023). Federated Identity Management can also be called as Federated SSO, however SSO and FIM are not the same thing, even they work in a similar way. The main difference between Federated Identity Management and SSO is the level of access, because with SSO people can gain access to resources that are in a single domain. With Federated Identity Management people can access multiple domains and organizations, and this can be very useful, for e.g., employees or students who need quick access to third party applications which are located outside their organization. (McKeown, 2021)

FIM provides a link between the user's identity and various identity management systems, which enables that the user can use many applications in a secure and efficient way. Federated Identity Management solutions are common with organizations, since they can have a lot of users that need to gain access for multiple resources, such as applications, websites, and Active Directory, without logging in separately to each service. (OneLogin, 2023.)

Federated identity is based on trust (Gontovnikas, 2021). This means that there is a mutual understanding between the two parties. These two parties are usually known as service provider (SP) and the Identity Provider (IdP). The Identity Provider takes care of the user's credentials by storing them into IdP's database and together with the service provider they agree on authentication process. One Identity Provider can interact with multiple service providers. (OneLogin, 2023.)

Federated identity benefits from multiple standard protocols, one of them being SAML. SAML is used for simplifying password management and authentication of the user in a federated system. With SAML it is possible to send the user's information from the Identity Provider to the Service Provider in a secure way. (OneLogin, 2023.)

4.4 OAuth

OAuth means "Open Authorization" (Okta, 2023). OAuth is an authorization protocol that enables third-party services e.g., websites and applications to exchange user information. This type of information exchange happens without

the user’s password. The user can grant authorization for the chosen application and after that, the application can access the user’s e.g., Facebook profile information. OAuth does not share the user’s password to the application, but instead it uses access tokens for verifying the user’s identity to target application. (OneLogin, 2023.)

Access token is used for representing the authorization to access the chosen resources. These access tokens are often using JSON Web Token (JWT) format, even there is no specific format required for the tokens. (Okta, 2023.)

It is important to realise that OAuth is not an authentication protocol, it is authorization protocol, and it was designed to be used for granting access to certain resources (Okta, 2023).

4.5 OpenID Connect

OpenID Connect is a separate layer that focuses on identity and is built on top of the OAuth 2.0 protocol (OpenID, 2023). OpenID Connect is a protocol that was designed for authentication, and it is used for securely log in users into applications (Microsoft, 2022c).

With OpenID Connect clients can verify the identity of an end user, based on the authentication that was performed by an authorization server. Basic information about the end users' profile can be gained in an interoperable way. (OpenID, 2023.)

OpenID Connect makes it possible for several types of clients, such as web-based, mobile and JavaScript clients, to receive and request information about authenticated sessions and end users (OpenID, 2023).

Azure AD B2C implements OpenID Connect and provides an outsourced way to perform user sign up and sign in into web applications through Azure Active Directory (Microsoft, 2022c).

OpenID Connect is extending the OAuth 2.0 authorization protocol in a way that it can be used for authentication but Azure AD B2C extends these use cases. With Azure AD B2C developers can use user flows, which enable the use of OpenID Connect to add user experiences in to application. These user experiences can include such as sign up, sign in and profile editing. (Microsoft, 2022c).

5 CIAM Solution with Azure Active Directory B2C

The idea of Azure AD B2C is to create a B2C tenant for an organization and then make an application available to the organizations' customers. Azure AD B2C is not same service as Azure AD, although it is based on the same technology. (Microsoft, 2022a.)

With B2C, customers can use their favorite social media accounts, since there are a lot of options to choose from. Some of the currently available options are Facebook, Google, Amazon, Twitter, LinkedIn, and GitHub. If desired, it is possible to add multiple Identity Providers into application or leave them out completely.

This thesis will demonstrate Facebook and Google as external Identity Providers, and how they are connected into the application.

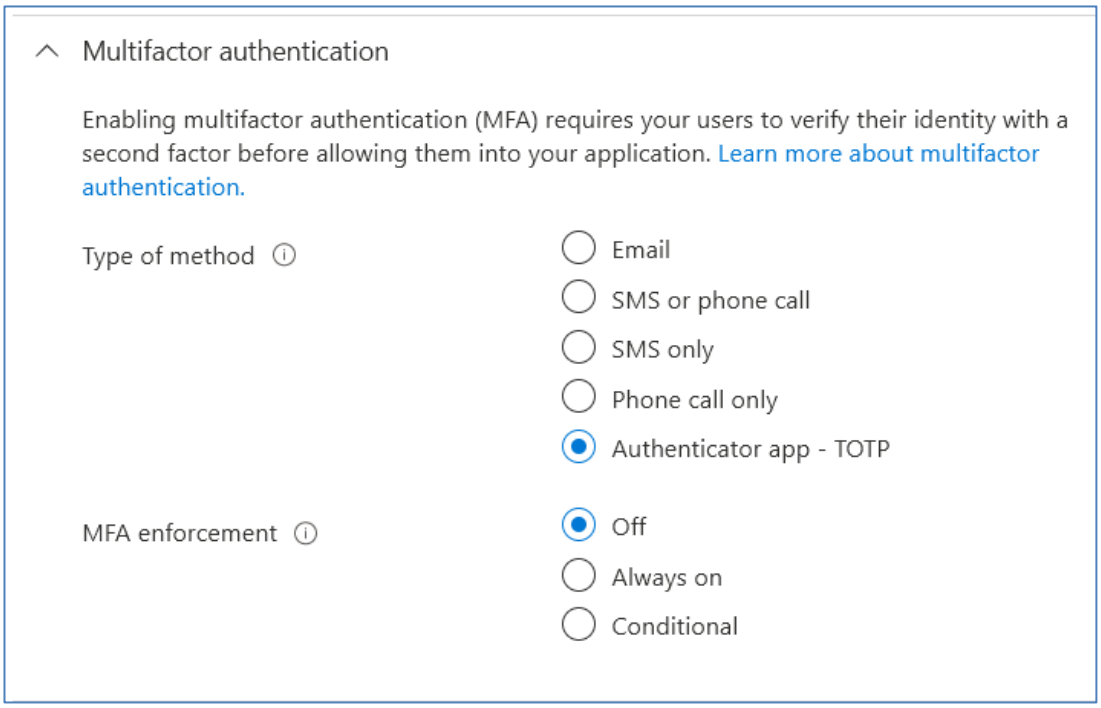
Multi-factor Authentication (MFA)

Azure AD B2C provides additional security measures for an application, such as multi-factor authentication (Microsoft, 2022d). Multi-factor means that there are multiple factors used for authentication. Additional factors can involve using (Strom, 2021)

- verification code in mobile phone (SMS message or application)
- smart card (physical card with a chip in it)
- biometrical requirement (fingerprint).

The idea of using multiple factors for authentication is to reduce the risk of cyber-attacks, data breaches and identity thefts. Security of an application can strengthen by using MFA. (CyberArk, 2023.)

Azure AD B2C makes adding MFA easy, since it can be activated from Azure portal. Possible options, when activating MFA are shown in Picture 2.



Picture 2. Enable Multi-factor authentication.

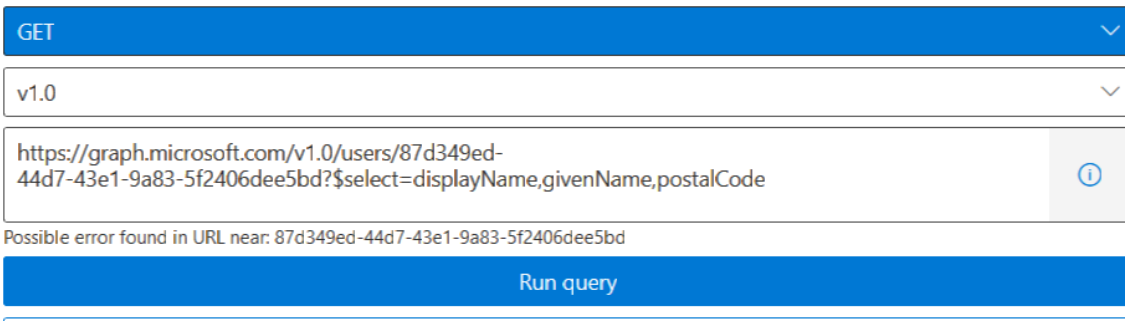
Microsoft recommends using an application for authentication and they consider email to be the most unsecure option. (Microsoft, 2022d.)

Microsoft Graph (MS Graph)

Azure AD B2C also supports Microsoft Graph, which is a service that provides access to data, that is being stored in Microsoft 365 services, including the B2C tenant. Scripts or an application that connects to Microsoft Graph API can be created. Automated tasks that are relevant for the tenant can be created with MS Graph. These types of tasks could be:

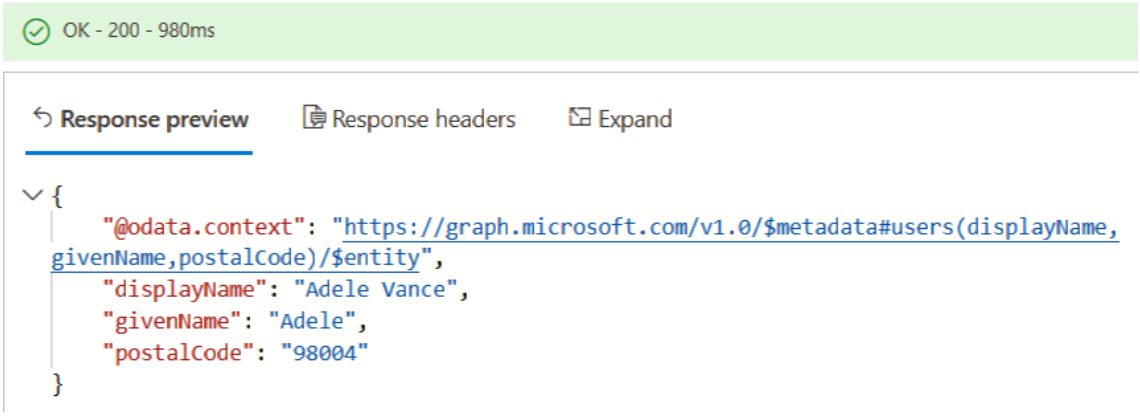
- migrating already existing users into new B2C tenant
- creating new users
- accessing audit logs

MS Graph Explorer enables running queries on the tenant, for e.g., sending an HTTP GET request like in Picture 3. This query is an example from Microsoft, and they are providing guidance, on how to use MS Graph with the B2C tenant.



Picture 3. MS Graph query.

The query in Picture 3, will return a response containing information about the user, such as display name, given name, and postal code, as shown in Picture 4. (Microsoft, 2022e.)



Picture 4. MS Graph response.

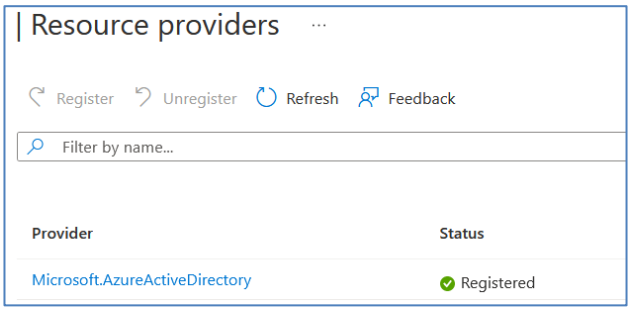
Overall, Azure AD B2C is highly customizable service, and it provides an option for deciding if users are able to log in just with their local, enterprise, or social media accounts. User accounts can be created by an administrator beforehand, or if a user has the ability to create their own accounts and sign up for the application.

This thesis will demonstrate two applications that can handle user login, sign up, profile editing and resetting user passwords through Azure AD B2C user flows.

5.1 Azure AD B2C tenant

A tenant is a describing object of an organization that needs to be represented. Through this tenant developers can control applications that are registered into it. Tenants can be found from Azure portal by selecting the “Directories + Subscriptions”.

This thesis will demonstrate two applications that are connected into Azure AD B2C tenants. To be able to connect an application into AD B2C tenant, an active Azure subscription is needed. Free subscription is an option to start with or pay as you go, but administrative access to the Azure environment is required. After the subscription is active, Azure AD service needs to be activated in default directory. This can be done by going to the subscription and then opening the link to “Resource providers”. The picture 5. shows the status of Azure Active Directory as “Registered”.

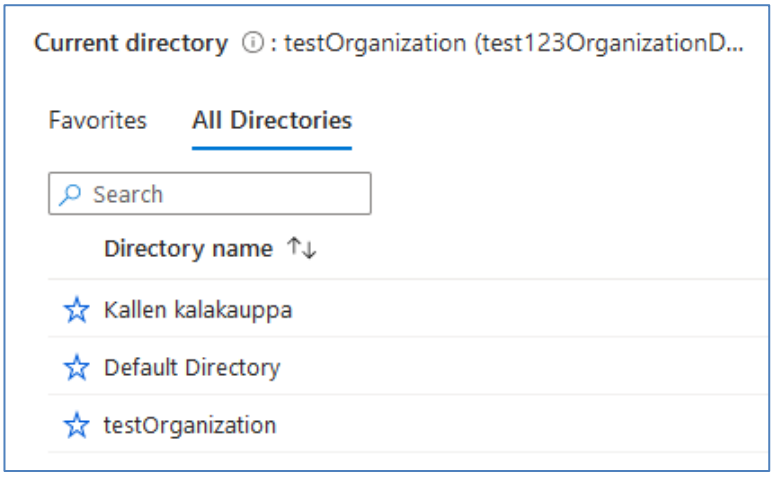


Picture 5. Azure Resource providers.

If the status is not registered, click the status and change it to registered and then click save. If the status doesn’t update immediately, try refreshing the page, for the changes to appear. When the status is registered, Azure AD B2C tenant can be created.

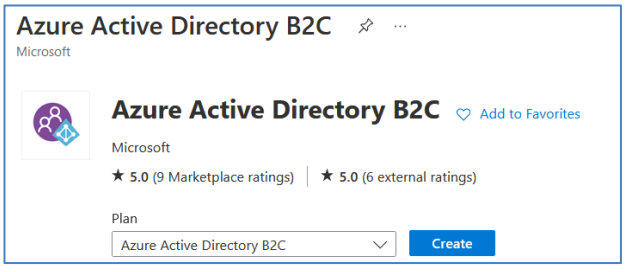
These B2C tenants live inside the default tenant because that is where the Azure AD is also activated. To make changes into the tenant, navigation between these directories is required, because some of the functionalities are created inside of default tenant instead of B2C tenant.

To create a B2C tenant, current location needs to be inside the “Default Directory”. Checking current location is possible from “Directories + Subscriptions” as shown in Picture 6.



Picture 6. Directories.

Search bar can be used to find the Azure AD B2C service in Azure portal. Similar view as in Picture 7 should be found and then choose ”Create.” Next, define a name for the organization, a domain name, pick a country or a region, subscription, and a resource group. When all the required information is filled out, go and click ”Create and review.” This is a common way that is being used in Azure services, it enables checking once more, if everything is as originally planned it to be, and then finally create the chosen resource.



Picture 7. Creating Azure AD B2C.

5.2 Application registration

After the B2C directory is created, Azure portal will show a notification about it, and then it can be accessed. When the tenant has been accessed, application registration can be added to it. Every application that will be used with the tenant, needs to be registered separately. First the decision of what type of an application is being used needs to made. Web applications that are built on ASP.NET Core (C#), Maven (Java), Flask (Python) or Express (Node.js) can be used.

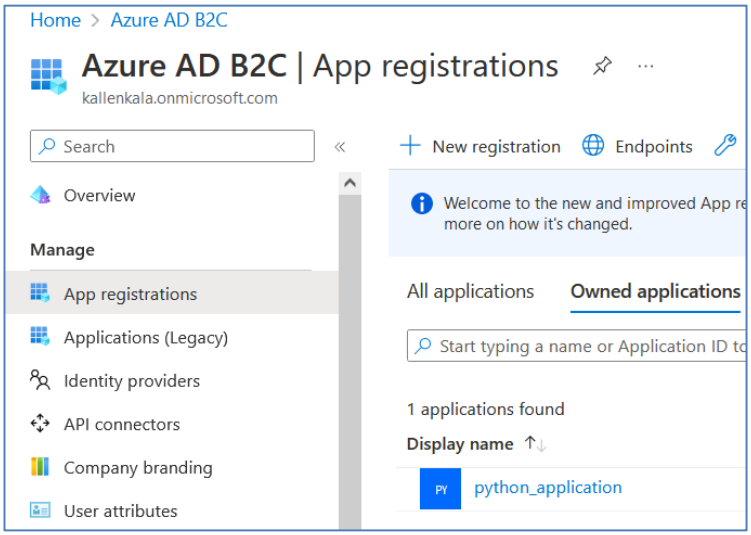
Azure AD B2C supports also single page applications (SPA's) that are using React, Vue or Angular. This thesis will focus on demonstrating two web applications based on Express (Node.js) and Flask (Python) frameworks.

Application is registered by accessing the tenant and then clicking "App registrations" and then choosing "New registration." Next, definition of a display name, what type of user accounts are used, a redirect URI, and appropriate platform needs to be made. This thesis will demonstrate two applications that are using "Accounts in any Identity Provider or organizational directory." This means we will use user flows for our user authentication.

Redirect URI is an address that can be changed later, but it needs to be specified, because it is the route that will redirect users into the application, after they are successfully authenticated. There are multiple platforms to choose from, such as:

- web application
- mobile and desktop application
- single page application (SPA)

After the application has been registered, its' information can be accessed by clicking its name, e.g., "python_application" as shown in Picture 8.



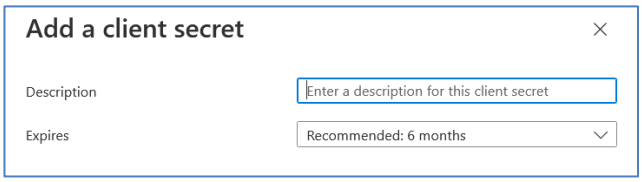
Picture 8. Application registration.

Accessing this will provide information about the application such as:

- Application (client) ID
- Display name
- Object ID
- Directory (tenant) ID
- Supported account types
- Client credentials (certificates and secrets)
- Redirect URIs
- Application ID URI

To connect the application into Azure, some of these values are needed. Application (client) ID is a unique value that is assigned to the application, when it is registered into the tenant. Certificate or an application secret needs to be createad for the application. This thesis will use application secrets when demonstrating both Express and Flask application. Application secret is easy to create from accessing the registered application, and then choosing "Certificates and secrets".

Then choose ”Create a new client secret” and fill out the description for the secret and choose an expiration date as shown in Picture 9. The options for expiration times are in months being 3, 6, 12, 18, 24, or custom amount. When application secret is created, its value is shown only once, and after that it cannot be accessed anymore. Keep record of the application secret in a safe place and access it in the application code securely.

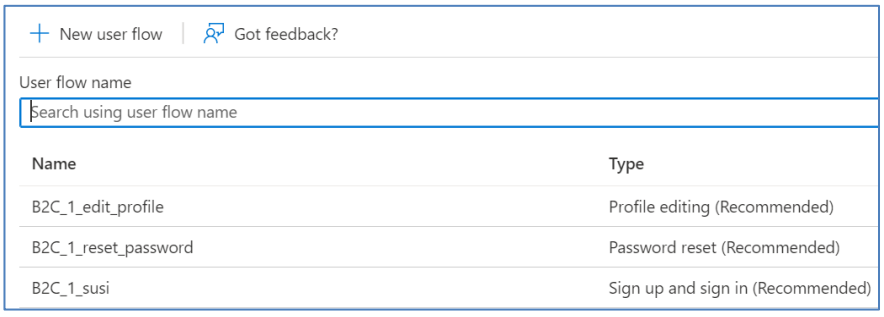


Picture 9. Create a client secret.

This thesis will access application secrets through environmental variables, which is achieved by using dotenv package and .env file in application development process. This is a more secure way to store secrets, rather than writing them in code as plain text.

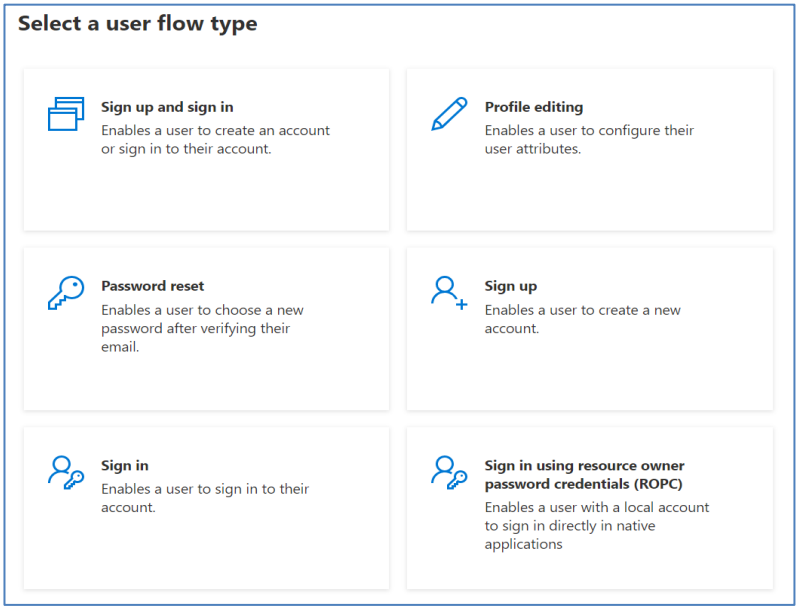
5.3 User flows

Another term used for a user flow would be policy. Policy defines how something is or must be done. This applies to Azure AD B2C as well, but these policies are known as user flows. User flows can be created directly from the Azure portal and the process is straightforward. Creating a new user flow can be done by opening the AD B2C tenant and clicking “User flows” and then “New user flow”. Picture 10, shows three different user flows that are used in this demonstration.



Picture 10. User flow list.

Azure recommends to use certain user flows. From Picture 11, can be seen what the view looks like when selecting new user flows.



Picture 11. Selecting a new user flow.

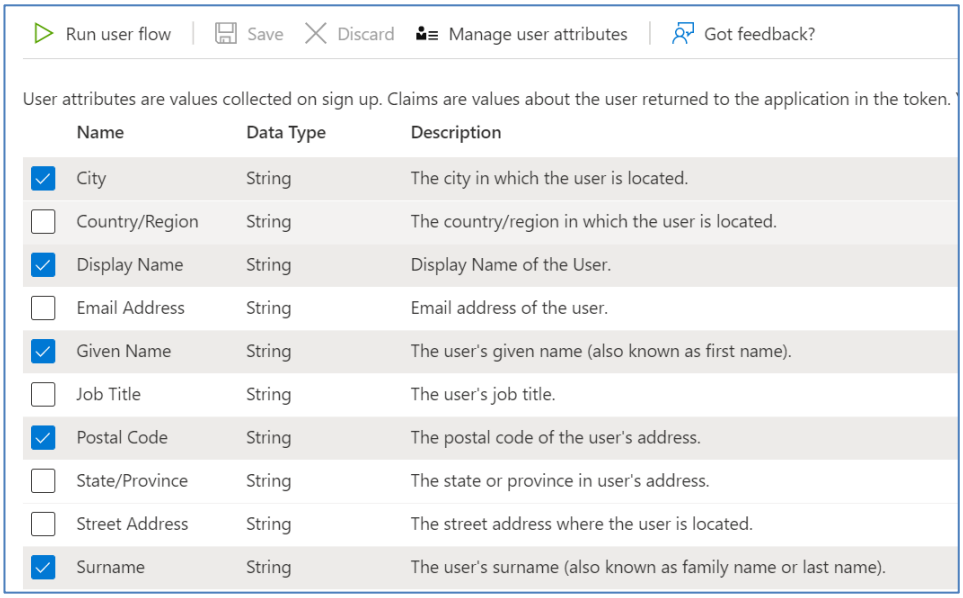
To open the user flow, click its name, so that more details about it comes available, as in Picture 10. From this view changes to a specific user flow, for e.g., activating additional Identity Providers or defining custom page layouts can be made. Application claims are used can also be defined here.

5.4 Application claims

Demonstrated application is currently using City, Display Name, Given Name, Postal Code and Surname as application claims. This means that when creating a new user, these claims need to be filled.

The view in Picture 12, shows how these claims can be altered, added or removed from the user flows.

Application claims are accessible from application code, e.g., using the “Display Name” application claim, we could show a greet message for the user that just logged in.



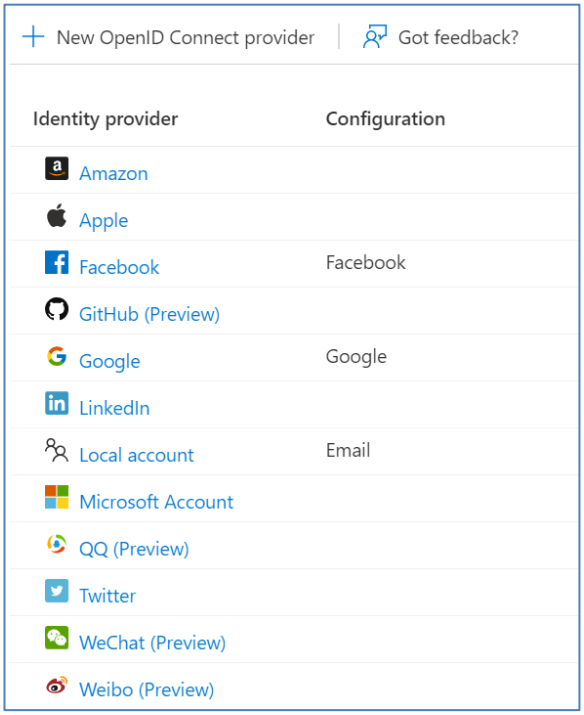
Picture 12. Application claims.

If the application needs an additional application claim, it can be created by using custom claims, these are also called external claims. Example of an external application claim can be seen in Picture 13, claim is called “Partner ID,” and it has a data type of string and a description of “This is Custom.”

Picture 13. External application claims.

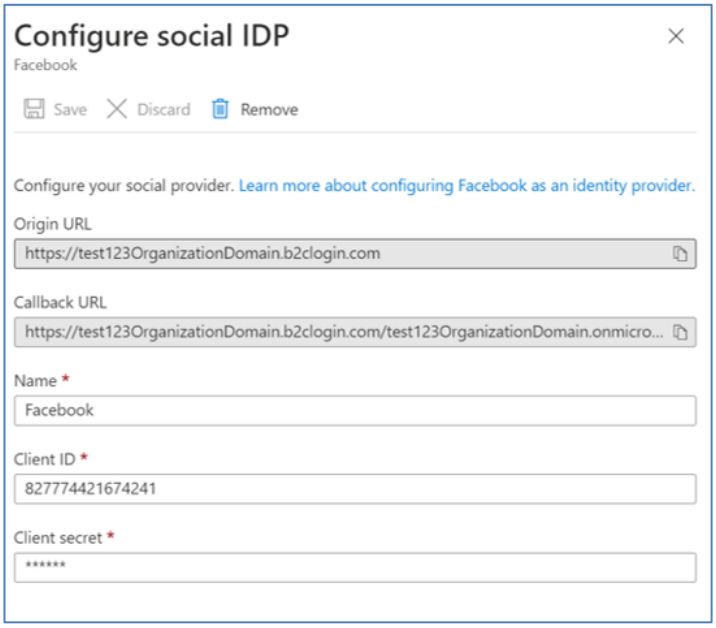
5.5 Identity Providers

New Identity Providers can be added by clicking “New OpenID Connect provider”. This B2C tenant is currently using Facebook, Google, and local accounts, as can be seen from the Picture 14.



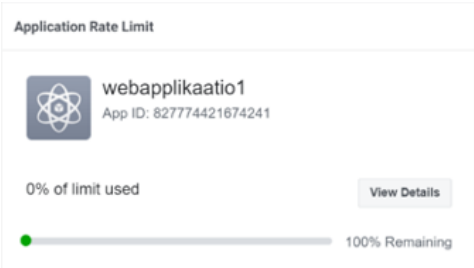
Picture 14. Identity Provider list.

The Social Identity Provider can be configured by clicking its name and then filling out the required information fields, see Picture 15. This will require the B2C tenant domain name and a callback URL, that is used for user authentication. Identity Provider should also have a name, Client ID, and Client secret.



Picture 15. Social IDP configuration.

Generating these values inside the social Identity Provider's service is required. In Picture 16, is a screenshot from Facebook web application that was created in Facebook Developer service. To create a Facebook web application, a Facebook Developer account is needed and then Facebook web applications and application secrets can be created.



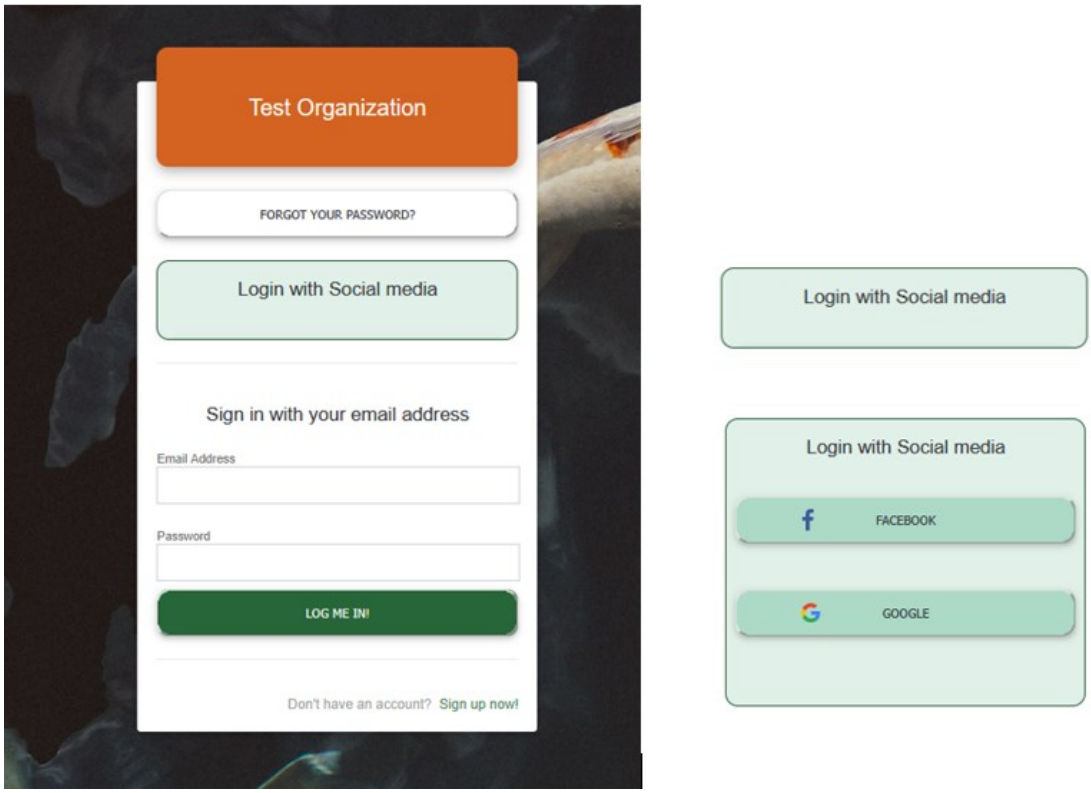
Picture 16. Facebook web application.

This thesis will be using Google as an Identity Provider as well, and it is registered in a comparable way as Facebook. Access to Google Cloud dashboard is required for being able to create a web application and client secret in their service.

5.6 Running user flows

After deciding of what user flows and application claims the application needs, they can be tested. User flows can be run from Azure portal, choose the user flow that needs to be tested and click “run user flow.”

In Picture 17, can be seen what does user flow for the sign in page looks like. This user flow was customized for B2C tenant, TestOrganization. The external Identity Provider buttons are hidden in the dropdown menu called “Login with Social media”, until dropdown is clicked open. On the right side of Picture 17, can be seen how the dropdown element is open and the buttons are appearing for each social Identity Provider.

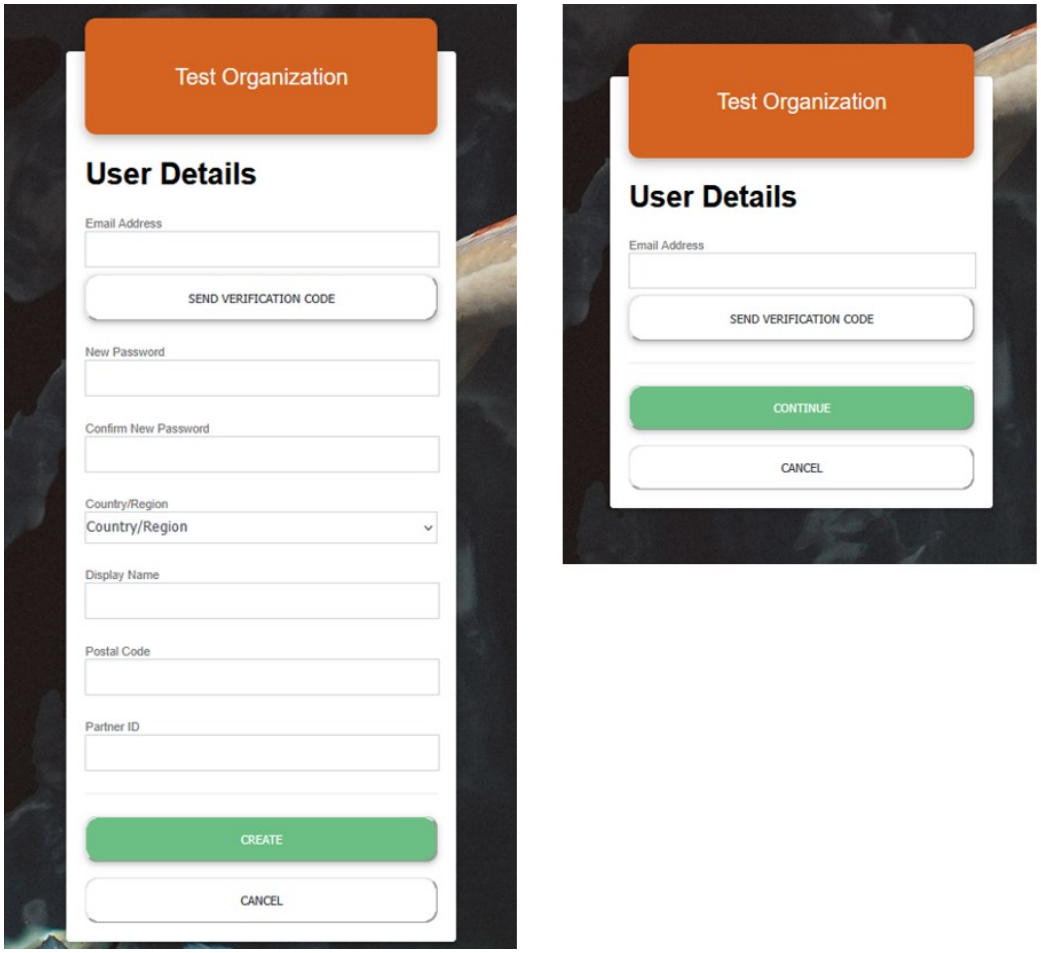


Picture 17. User flow for sign up and sign in with dropdown menu.

The login page for application also contains options for a password resetting and signing up for the application. These are convenient options to have on the first page, as user can access them directly.

Picture 18, shows how the user flow for signing up to the application and password resetting look like. Both user flows are defined in a way that they require a valid email address from the user. This means that when a user tries to sign up for the application, they must verify their email address with a separate code. This same functionality is used when logged in users are trying to reset their passwords, or if they request a new password.

By asking the user for a valid email address during registration process, will reduce the number of unnecessary accounts, which is important, since the B2C pricing is based on the amount of monthly active users.



Picture 18. Sign up and password resetting forms.

5.7 Custom page layouts

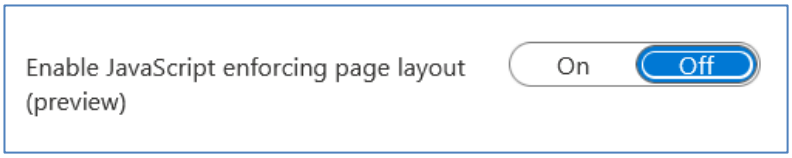
Storage account is needed for using custom styles for the user flows. Storage account is created inside the Default Directory, so switching directories in Azure portal is needed, if current directory is the AD B2C tenant.

This thesis will use a storage account that uses a blob storage as storage service. All custom html templates that are used in user flow customization are uploaded inside Azure blob storage. Microsoft currently offers three different templates that can be used in user flows:

- Azure Blue
- Classic
- Slate Gray

These templates can be downloaded from Microsoft and then added to the blob storage. It is recommended to start with Microsoft's templates and then trying to customize own templates.

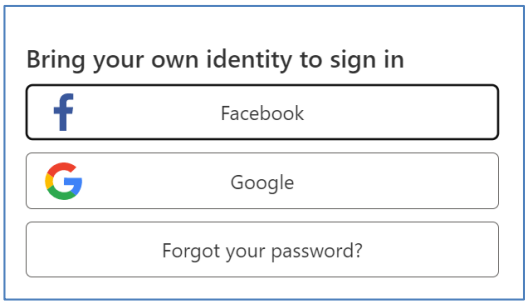
This thesis demonstrates custom page for login page, where html elements are altered with JavaScript. JavaScript needs to be enabled from Azure portal, before it can be runned in user flows, otherwise the page gets rendered without the script running. Picture 19 shows how JavaScript can enabled from Azure portal and that JavaScript feature is still in preview mode. Azure uses the term preview for services that are not completely ready, and they are being evaluated, so they might still go through some changes and evolve. Microsoft does offer support for preview features, but normal service level agreements do not apply to preview features.



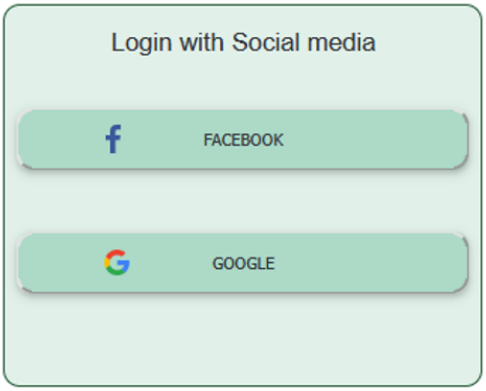
Picture 19. Enable JavaScript.

Without JavaScript, the buttons for social Identity Providers would be shown on the page as individual buttons, one below another. In Picture 20, can be seen an example of how the buttons are being rendered to the page without custom JavaScript.

However, the styling of the elements require knowing what elements are being accessed. To know what elements, should be accessed, finding the appropriate class and id names from the default page that is rendered by Azure is required. For example, the dropdown menu is created by finding the correct element from html file and then finding the social Identity Provider buttons from this html element. When the buttons are found, a new list element is being created and those buttons will be joined into the list as list elements. From Picture 21, can be seen what the dropdown menu on the login page looks like, when using JavaScript.



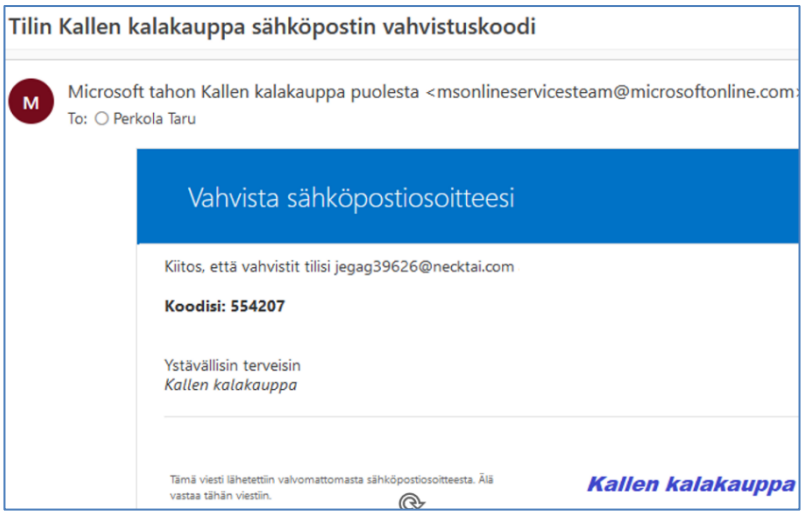
Picture 21. Identity Provider buttons without JavaScript customization.



Picture 20. Dropdown menu for buttons created with JavaScript.

5.8 Company Branding

There is also another customization option for user flows, called “Company Branding”. This is demonstrated with our second AD B2C tenant, Kallen kalakauppa. Company Branding allows defining a company logo, that is also used in email verification messages, as seen in Picture 22. Content of the email verification message is automatically translated into Finnish, because Azure B2C can be translated to multiple languages, based on location of the browser that is being used.

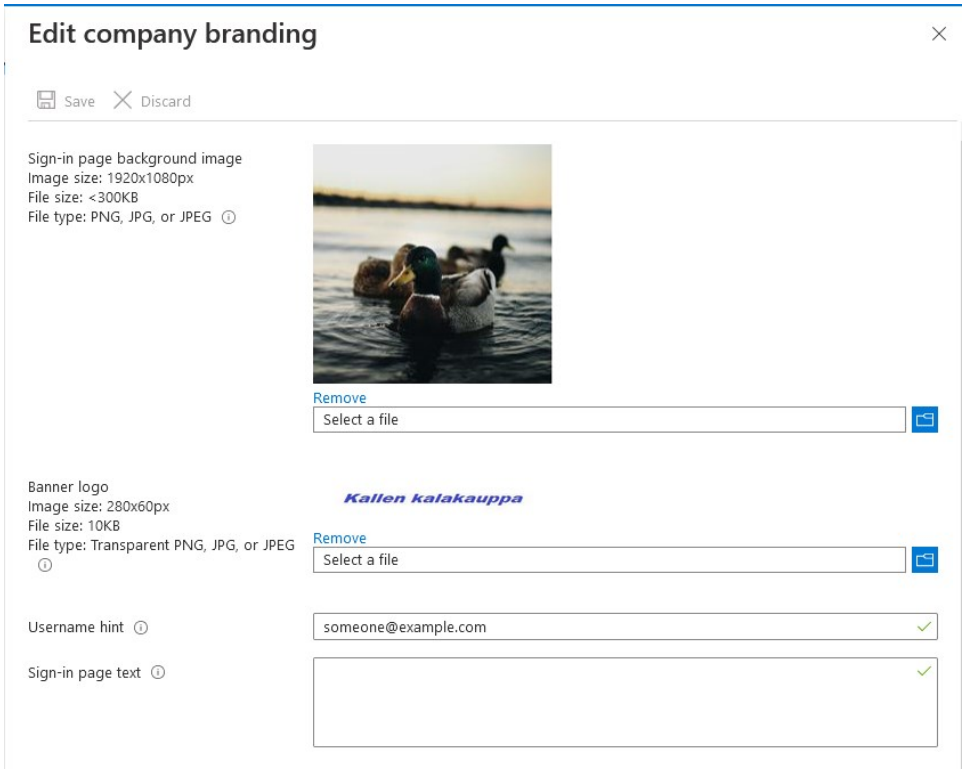


Picture 22. Company Branding email verification.

With Kallen kalakauppa, chosen languages are English and Finnish. It is possible to choose from many languages and even provide own translations if the default values are not sufficient. Azure allows editing these values, by downloading default json file from the portal and then adding new changes into json file. To make the changes appear into B2C tenant, the override value has to be set equal to true, so that Azure will know some default values are being overridden.

Main advantage in Company Branding is, that even without creating a storage account, creating user flows that makes application to stand out is still possible. With Company branding there is an option for choosing a logo, background image, and background color.

There are some limitations to image sizes, as can be seen from the Picture 23. There is also an option for ”Username hint” which means that when a user accesses the Kallen kalakauppa login page, there is a hint provided in the username input field. The hint can be customized based on organization’s needs. Sign-in page text that is visible for the user, when they access to the login page can also be defined. This text is visible to all who can access the login page, so it should not contain any secret information, but act more like guidance to the new users.



Picture 23. Edit Company Branding.

5.9 Connecting an application to B2C

This thesis demonstrates connecting two different applications into the AD B2C tenant. First application is created with Express framework (Node.js) and connected to our TestOrganization tenant.

The second application is created with Flask (Python) framework, and it is connected to our tenant, Kallen kalakauppa.

Both applications are using Microsoft Authentication Library, MSAL. MSAL is a tool that makes it possible for developers to gain access to security token from the Microsoft identity platform. These security tokens are used for authenticating the users and there for accessing to secured web APIs (Application Programming Interfaces). MSAL enables accessing Microsoft Graph and it is supported by multiple platforms such as .NET, JavaScript, Java, Python, Android, and iOS.

5.10 Custom policies

Custom policies are used when regular user flows don't provide enough control. Microsoft recommends using user flows, but if the application requires more complex user journeys, then using custom policies is a good option. (Microsoft, 2022b.) Custom policies are used for defining the behavior of the tenant. They are completely configurable, and policy driven. (Sadasivan, 2021.) They allow building more complicated scenarios for identities, which is key feature of custom policies (Microsoft, 2022b). If the application e.g., needs to use only Facebook as a login option, that can be achieved with custom policies (Sadasivan, 2021).

Custom policies consist of many XML files that are referencing each other, doing so in a hierarchical order (Microsoft, 2022b).

XML file can contain various elements that are used for defining (Microsoft, 2021)

- building blocks
- interaction with the user
- other parties
- business logic.

Microsoft provides an easy solution to start with custom policies, since it is possible to download their starter pack from the internet. Their starter pack includes multiple pre-built policies, and it provides a simple way to start practicing with custom policies and later on adjusting them based on more demanding needs. (Microsoft, 2021)

6 Conclusion

The objective of this thesis was to demonstrate Azure Active Directory B2C solution with two web applications and study its adequacy as being a finalized product that can be sold to customers in the future.

The objective was achieved by testing, implementing and customizing Azure AD B2C solution.

Based on all the testing that was performed on Azure AD B2C, it seems to be providing a diverse and easy to use solution for Customer Identity and Access Management. Customized solution that has a unified look can be achieved by using custom html files or the readymade templates that Microsoft is currently offering. Company branding feature is providing fast results, and it is simple to implement, but it does not provide a unique solution that is custom made.

Using custom html pages require knowledge of creating html webpages and CSS styling. If more customization is required, than can be achieved with CSS, and by altering the elements directly from Azure portal, then knowledge of JavaScript is needed as well.

By using JavaScript, visually striking results can be achieved, such as custom styled elements. Although there are some limitations with this approach. Microsoft recommends that if something can be edited by using custom policies, then custom policies should be used. Using JavaScript comes with rules that need to apply in order for the content to be rendered correctly. Microsoft provides guidance on how to use JavaScript on custom html pages, so paying attention in their guidance before adding any JavaScript is recommended.

JavaScript can be used for moving the elements and re-arrange them as desired, e.g., demonstrated application for TestOrganization is using JavaScript for creating the dropdown menu on login page.

By using JavaScript, html page content can be edited, but since it is a feature in preview, there might appear some issues with it. At the time of writing this report,

there is a slight problem with the custom page rendering. The content is rendered to the page correctly when inspecting it from a browser. Although it does require adding one line of code into the custom html file, so that the scripts and styles are being loaded, before the page is shown to the user. This can be easily fixed, by adding the html property data-preload=”true” into the header section of the html file. Using this property for the style and script files is recommended. After this property is added, the page flickering should stop, although there might still be some flickering when opening the application for the first time. When the application is opened and the login page is accessed for the first time, that’s when the styling and script files are being loaded into the cache. After this, all pages of the application should work without flickering, but if the cache is removed, then that content needs to be loaded again, which will result in slight flickering. Trying to compress the background image, might help with this issue, since larger images can take some time to be fully loaded.

Pricing is based on amount of active unique users per month. There is a free tier for the first 50 000 monthly active users, so if the application has less users than that, this might be a good option. When total amount of monthly active users exceeds the 50 000 limit, the price is 0,003061€ for each unique user. If multi-factor authentication (MFA) is activated, it will come with extra cost, and every login attempt using it, will cost 0,0029€. Customization comes with minor cost, since it only requires a storage account, where images, html, styling, and script files can be stored. Storage account will be charged based on the file structure, redundancy, region, volume of data, and type and quantity of operations that are perform in the storage, including data transfer. Only the files that are used for customization will be uploaded to the storage, so there should be no worries regarding storage expenses.

Overall, Azure AD B2C provides a decent solution for applications that are designed to be used by customers or consumers. It is easy to implement and it does not take a long time to learn the basics of it. Pricing for this service is reasonable and it can work for many companies, especially if they can estimate how many active users their application will have in the future. It provides multiple

options for customization, which makes it possible to offer unique and one-of-a-kind solutions. If even more control over user journeys is required, custom policies can be used, and achieve completely customized solution that is specially designed to fulfill the company’s needs.

References

Citrix. (2023). *What is a cloud service - Cloud Services Solutions*. Retrieved January 7th, 2023, from Citrix Systems: https://www.citrix.com/solutions/digital-workspace/what-is-a-cloud-service.html

Cloudflare. (2023). *What is SAML | How SAML authentication works?* Retrieved January 7th, 2023, from Cloudfare: https://www.cloudflare.com/learning/access-management/what-is-saml/

CyberArk. (2023). *Multi-Factor Authentication (MFA).* Retrieved January 8th, 2023, from https://www.cyberark.com/what-is/mfa/

Gontovnikas, M. (2021, June 8th). *What is IAM*. Retrieved January 10th, 2023, from Auth0 blog By Okta: https://auth0.com/blog/what-is-iam/

Google Cloud. (2023). *What is hybrid cloud?* Retrieved January 10th, 2023, from https://cloud.google.com/learn/what-is-hybrid-cloud

Häkkinen, N. (2023). *CIAM 2020-luvulla 1/2*. Retrieved January 11th, 2023, from Sogeti: https://www.sogeti.fi/media/blog-posts/ciam-2020-luvulla-asiakkaiden-identiteetin--ja-p%C3%A4%C3%A4synhallinta-on-keskeinen-osa-palvelukokemusta/

Kennedy, B. (2022, August). *What is SAML?* Retrieved January 13th, 2023, from Linux Hint: https://linuxhint.com/saml/

Kosunen, K. (2021, October 11th). *Azure ja tunnistautuminen - Mitä ovat Azure B2C ja B2B*. Retrieved January 22nd, 2023, from Cloudamite: https://cloudamite.com/azure-ja-tunnistautuminen-mita-ovat-azure-b2c-ja-b2b/

McKeown, E. (2021, March 3rd). *Single Sign-on vs. Federated Identity Management - Complete Guide.* Retrieved January 21st, 2023, from PingIdentity: https://www.pingidentity.com/en/resources/blog/post/sso-vs-federated-identity-management.html

Microsoft. (2021, October 21st). *Azure AD B2C custom policy overview.* Retrieved January 9th, 2023, from https://learn.microsoft.com/en-us/azure/active-directory-b2c/custom-policy-overview

Microsoft. (2022a, December 5th). *What is Azure Active Directory B2C?* Retrieved January 21st, 2023, from Microsoft: https://learn.microsoft.com/en-us/azure/active-directory-b2c/overview

Microsoft. (2022b, December 5th). *User flows and custom policies overview.* Retrieved January 15th, 2023, from https://learn.microsoft.com/en-us/azure/active-directory-b2c/user-flow-overview

Microsoft. (2022c, August 19th). *Web sign in with OpenID Connect in Azure Active Directory B2C*. Retrieved January 14th, 2023, from https://learn.microsoft.com/en-us/azure/active-directory-b2c/openid-connect

Microsoft. (2022d, July 20th). *Enable multifactor authentication in Azure Active Directory B2C.* Retrieved January 20th, 2023, from https://learn.microsoft.com/en-us/azure/active-directory-b2c/multi-factor-authentication?pivots=b2c-user-flow

Microsoft. (2022e, June 25th). *Register a Microsoft Graph application.* Retrieved January 15th, 2023, from https://learn.microsoft.com/en-us/azure/active-directory-b2c/microsoft-graph-get-started?tabs=app-reg-ga

Okta. (2023). *Intro to IAM / What is OAuth 2.0?* Retrieved January 21st, 2023, from authO by Okta: https://auth0.com/intro-to-iam/what-is-oauth-2

OneLogin. (2023). *What is Federated Identity*. Retrieved January 18th, 2023, from https://www.onelogin.com/learn/federated-identity

OpenID. (2023). *Welcome to OpenID Connect - What is OpenID Connect*. Retrieved January 19th, 2023, from https://openid.net/connect/

Poza, D. (2020, September 6th). *What is IDaaS*. Retrieved January 23rd, 2022, from Auth0 blog by Okta: https://auth0.com/blog/what-is-idaas/

Poza, D. (2021, June 8th). *What is CIAM*. Retrieved January 23rd, 2023, from Auth0 blog by Okta: https://auth0.com/blog/what-is-ciam/

Raible, M. (2017, July 21st). *What is OAuth?* Retrieved January 22nd, 2022, from Okta Developer: https://developer.okta.com/blog/2017/06/21/what-the-heck-is-oauth

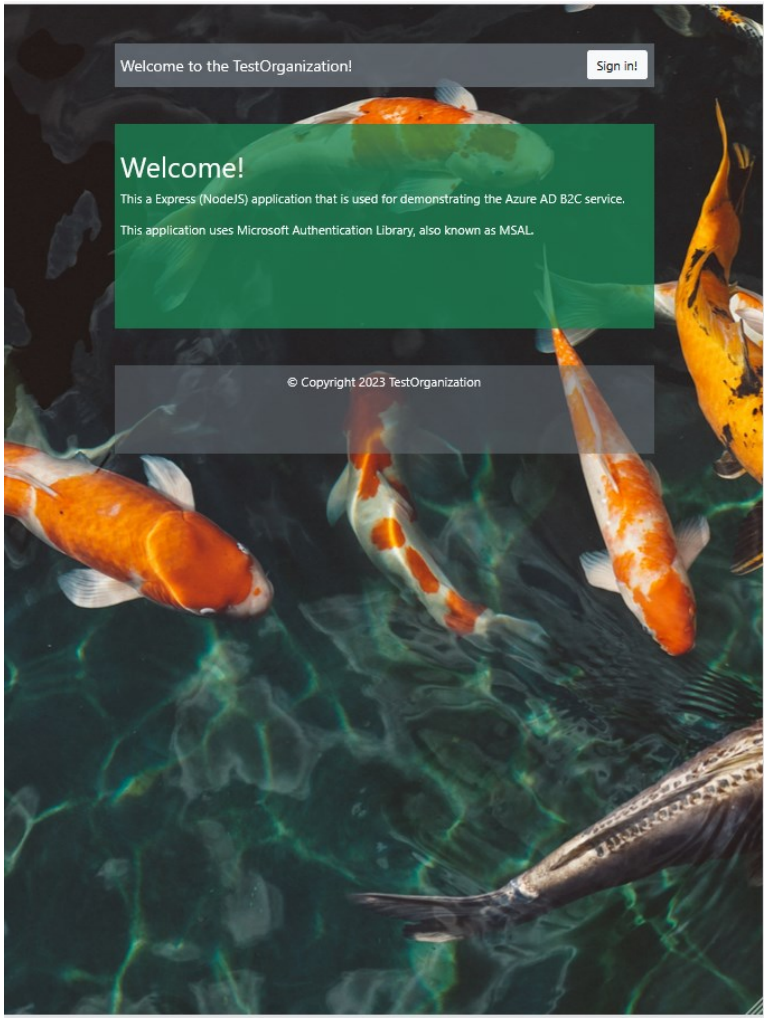
Sadasivan, B. (2021, September 2nd). *Deep Dive into Azure AD B2C custom policies.* Retrieved January 19th, 2023, from Youtube: https://www.youtube.com/watch?v=6GiYx205SZE

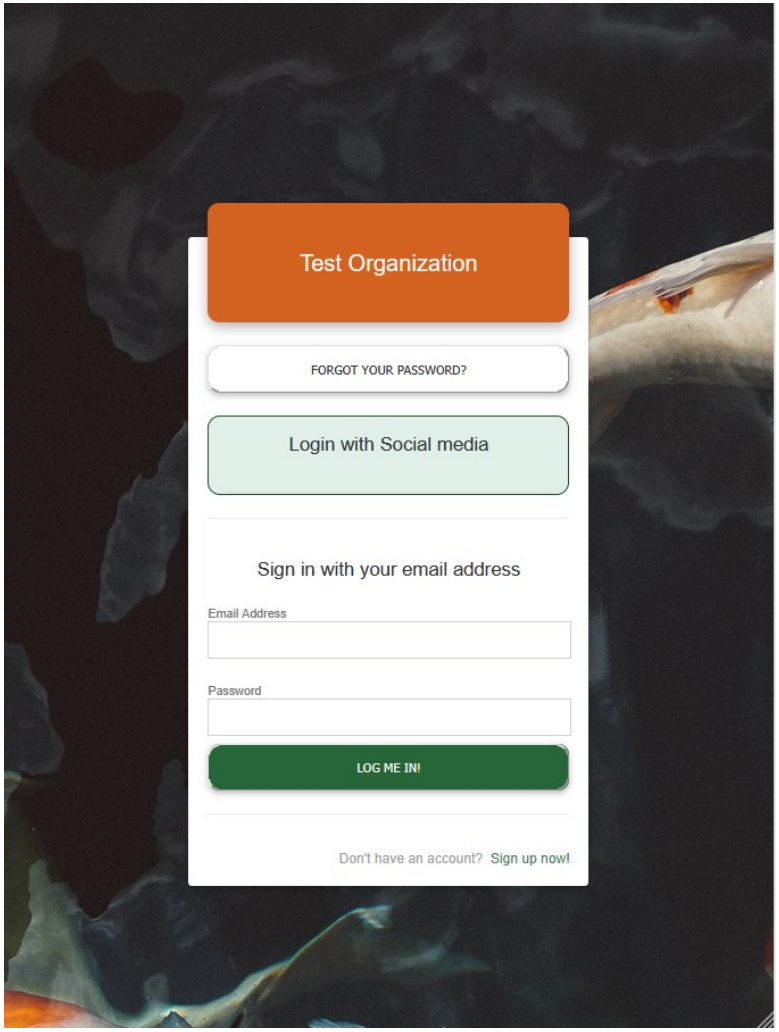
Strom, D. (2021, April 8th). *What is IAM? Identity and access management explained*. Retrieved January 20th, 2022, from CSO: https://www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html

Vento, J. (2021, February 4th). *Mikä on pilvipalvelu?* Retrieved January 16th, 2023, from onrego Blogi: https://onrego.fi/mika-on-pilvipalvelu/

Appendix 1. Demo application for Azure AD B2C tenant, testOrganization

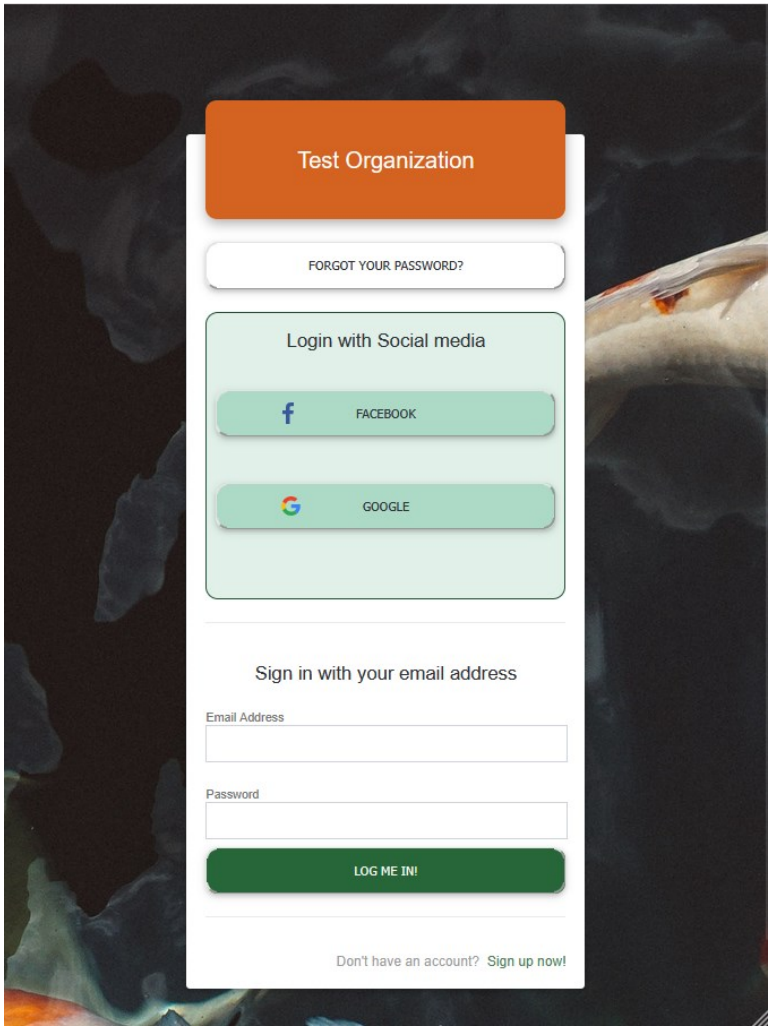
Front page and login form

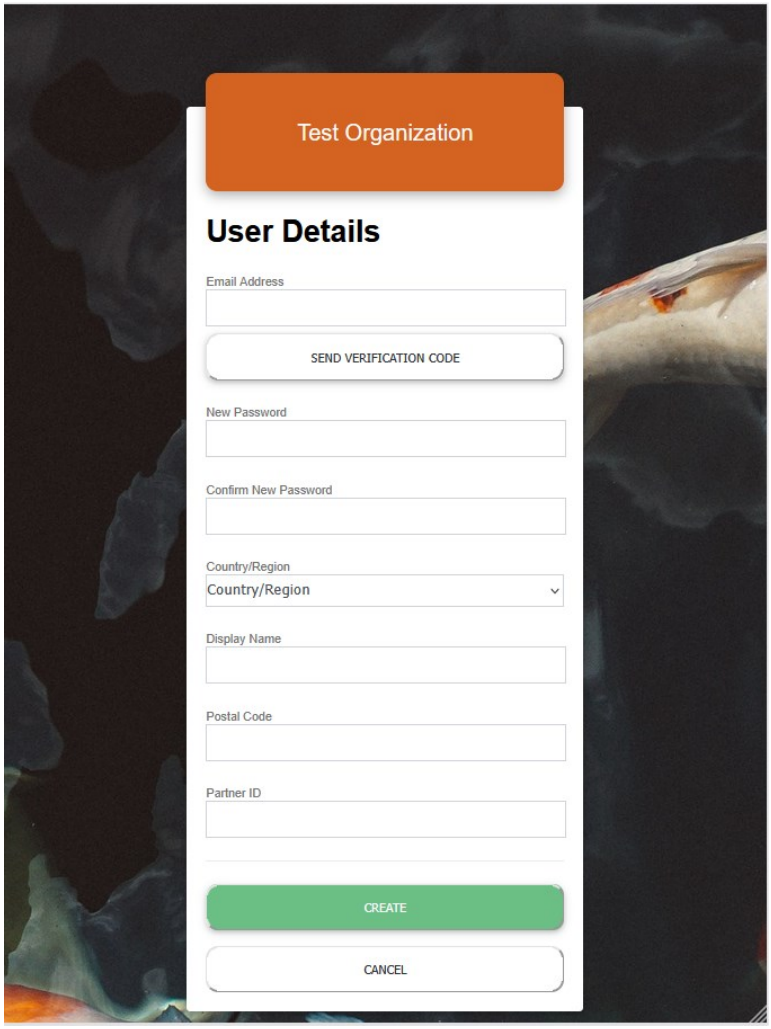




Appendix 1. Demo application for Azure AD B2C tenant, testOrganization

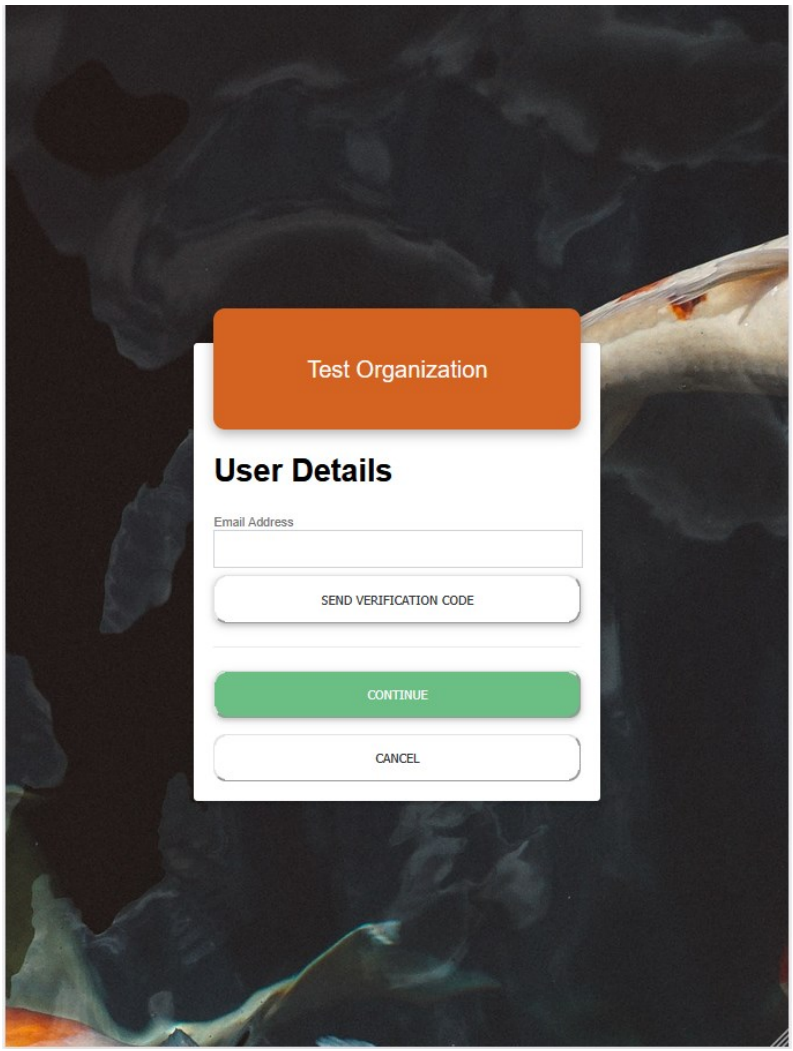
Social media options for login and registration form

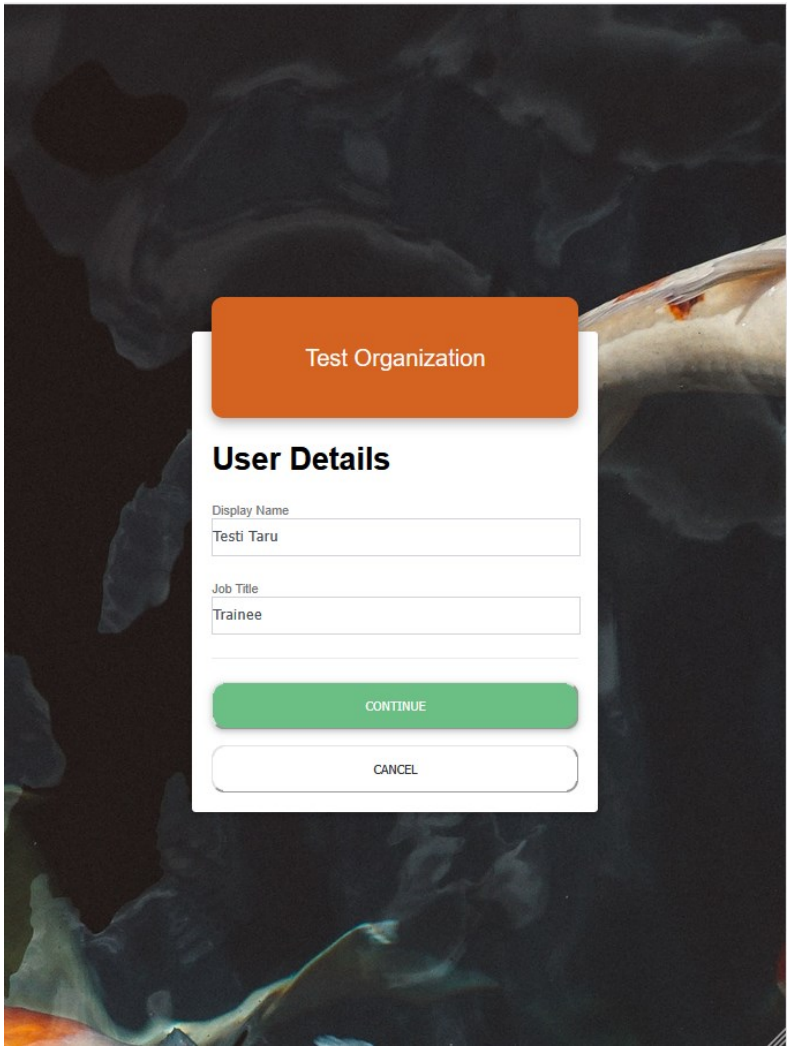




Appendix 1. Demo application for Azure AD B2C tenant, testOrganization

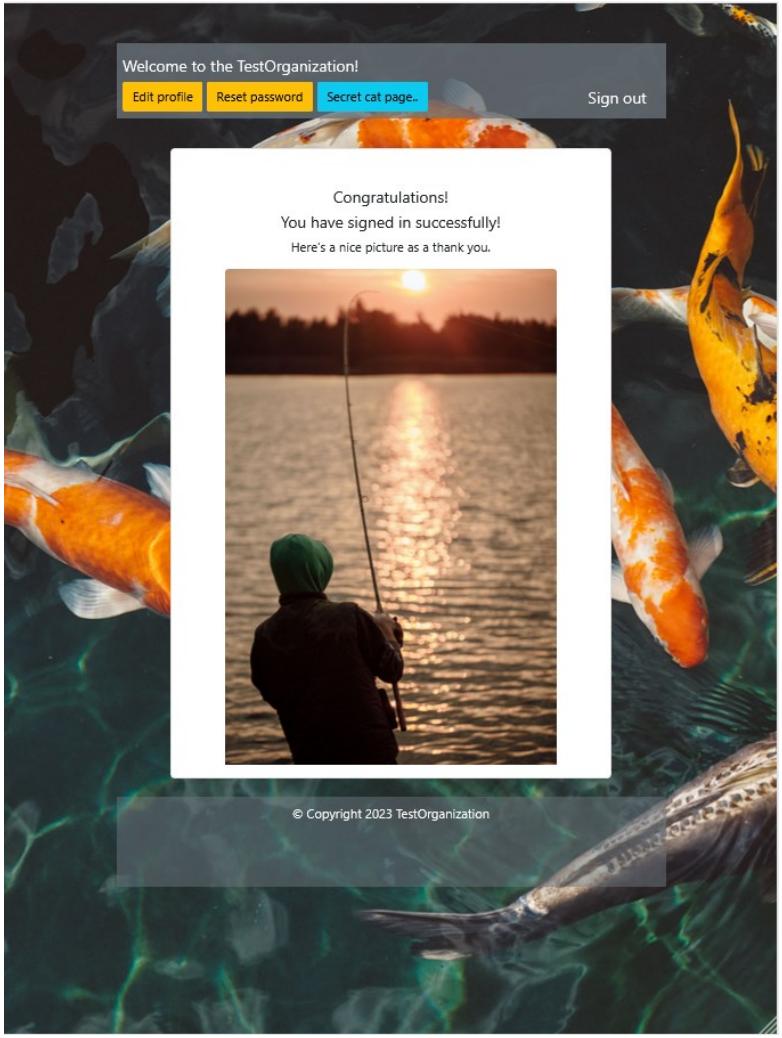
Password resetting and profile editing

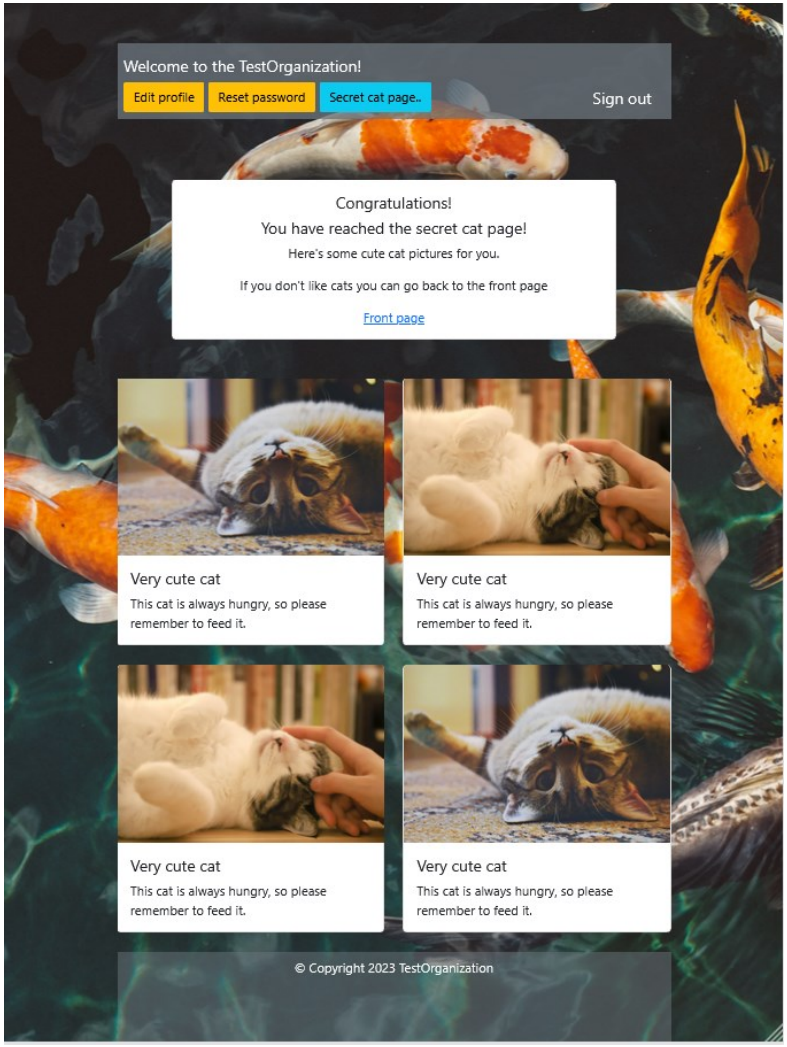




Appendix 1. Demo application for Azure AD B2C tenant, testOrganization

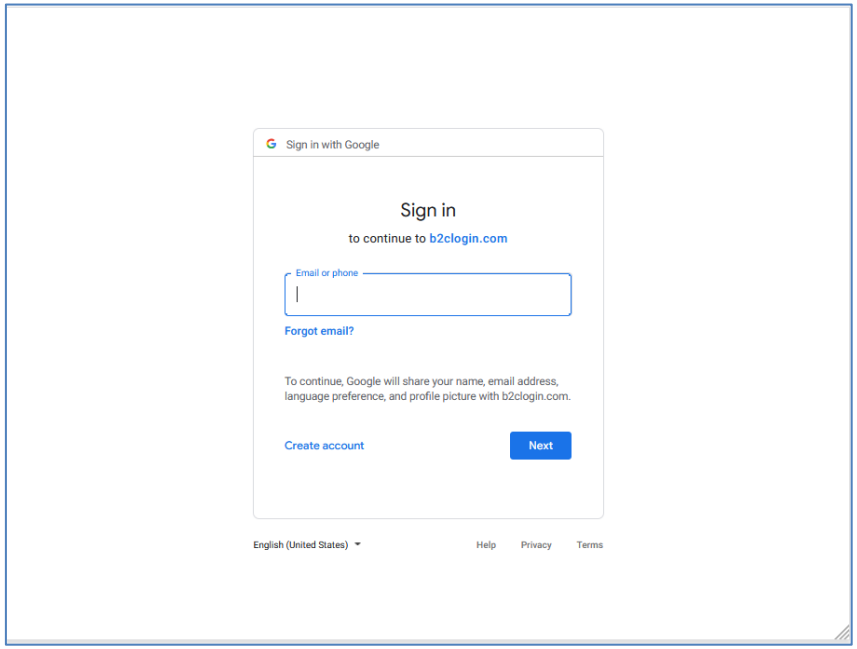
Application content as logged in user

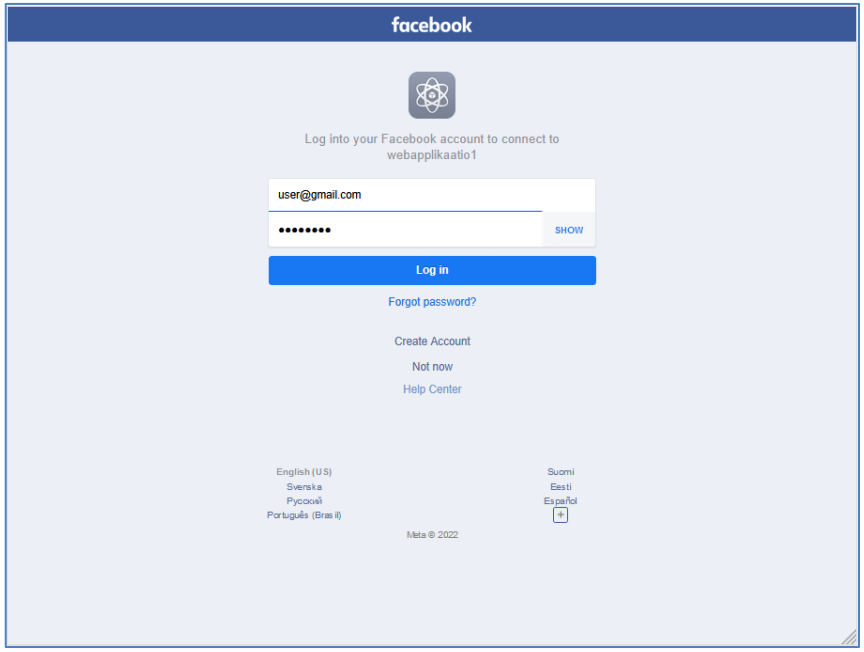




Appendix 1. Demo application for Azure AD B2C tenant, testOrganization

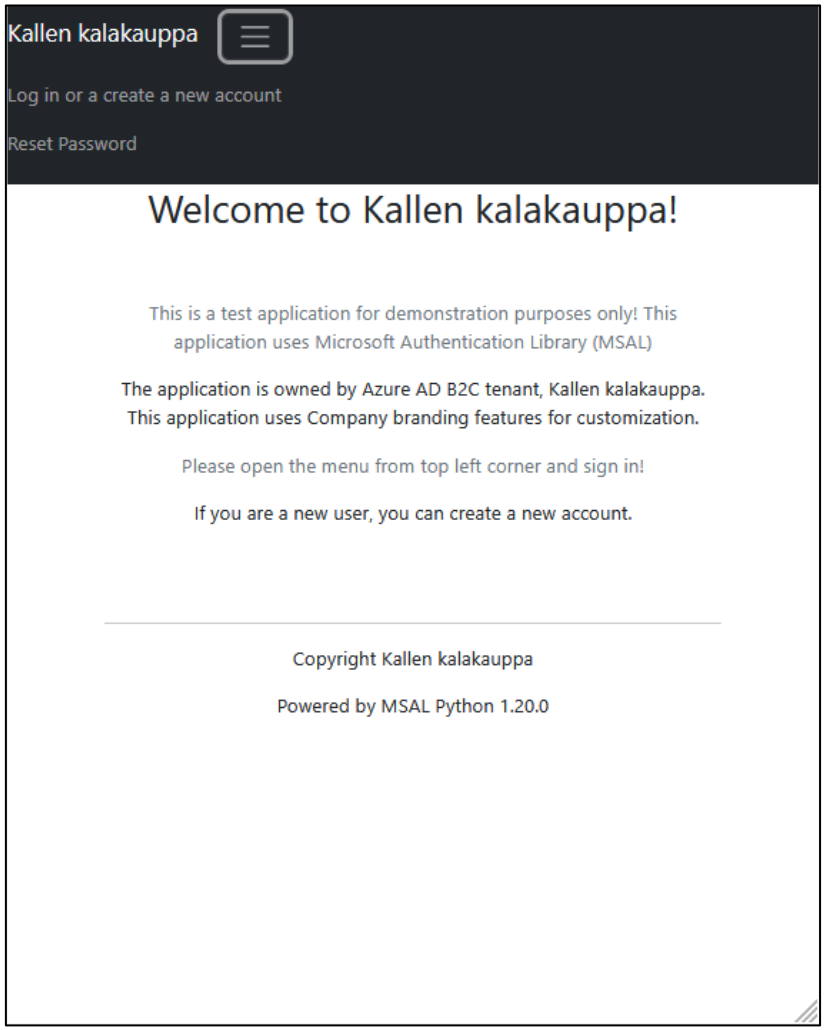
Google and Facebook login

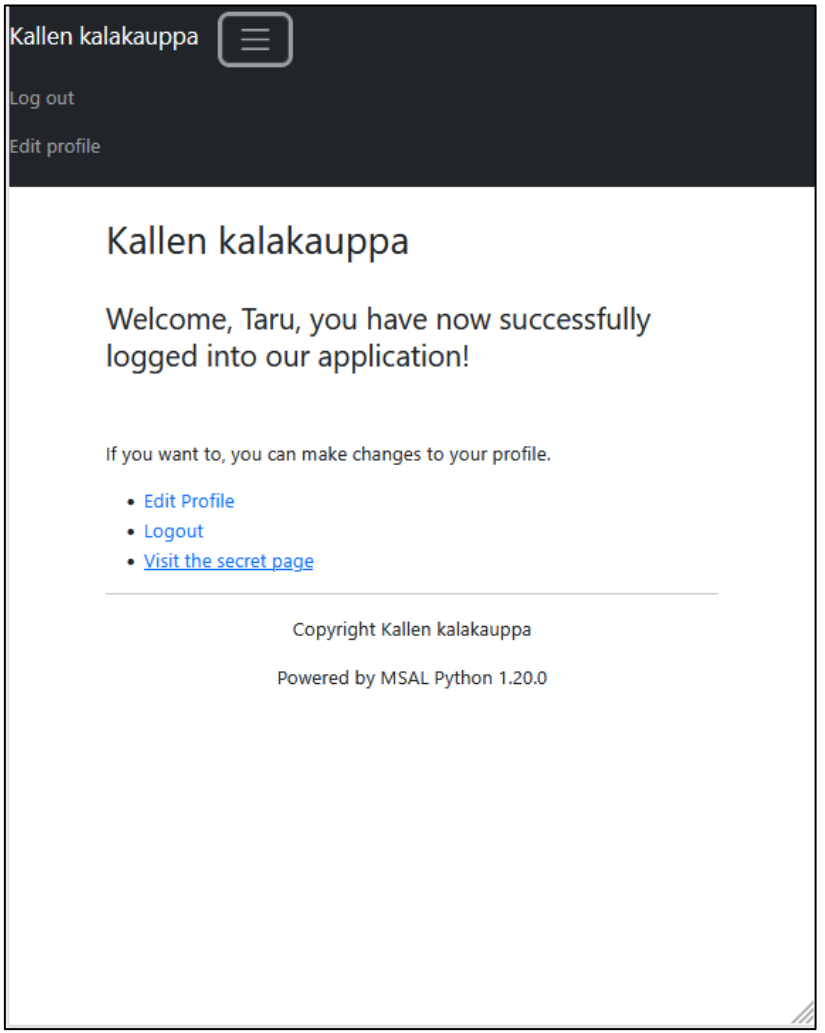




Appendix 2 Demo application for Azure AD B2C tenant, Kallen kalakauppa

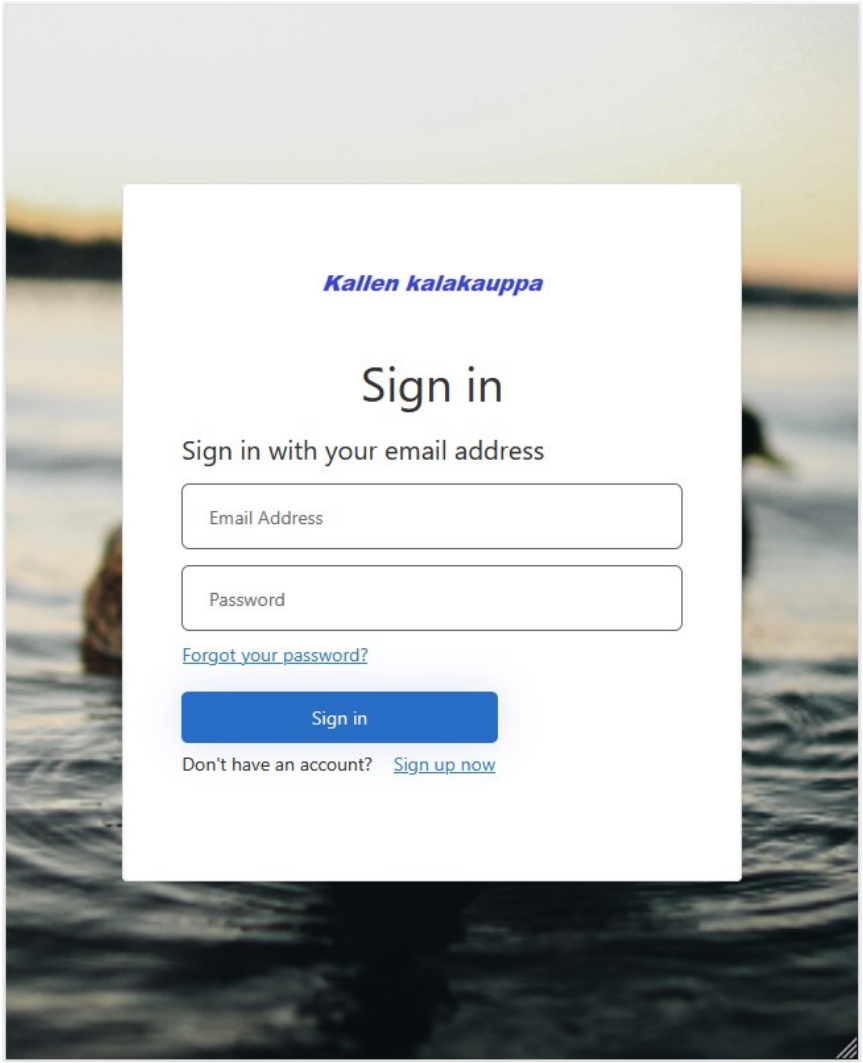
Front page and application content as a logged in user for Kallen kalakauppa

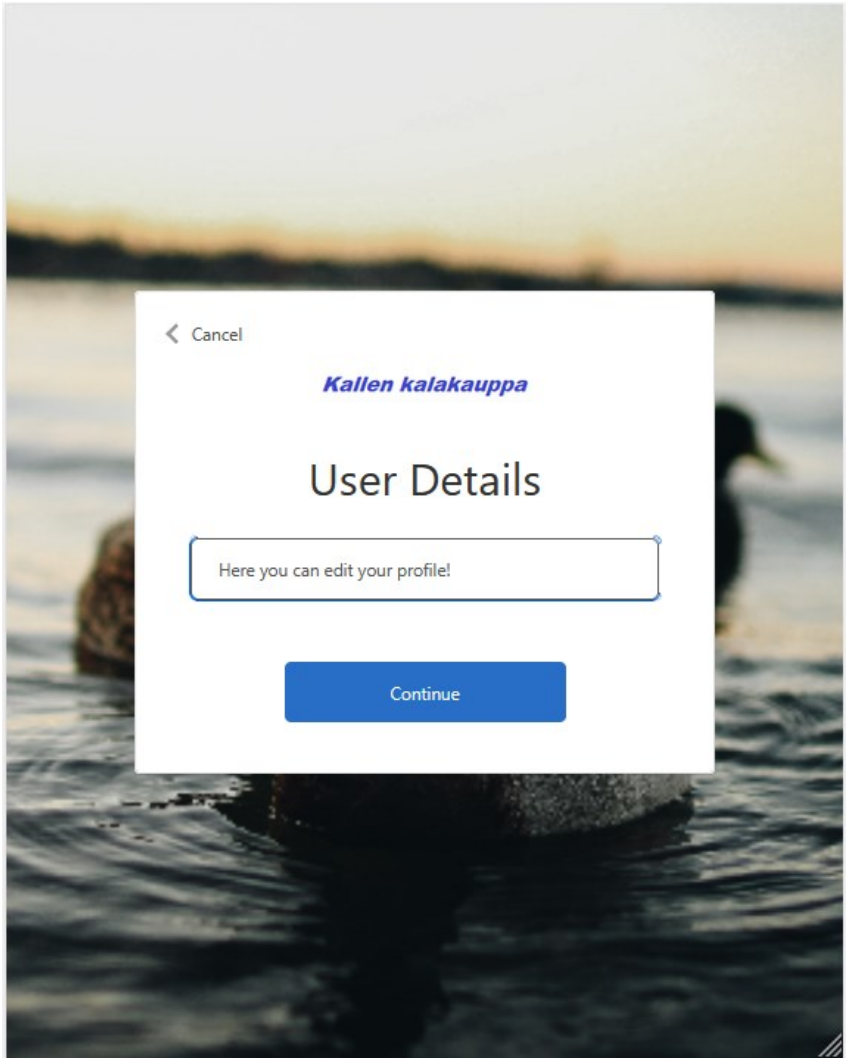




Appendix 2 Demo application for Azure AD B2C tenant, Kallen kalakauppa

Login page and user profile editing for Kallen kalakauppa





Appendix 2 Demo application for Azure AD B2C tenant, Kallen kalakauppa

Password resetting and registration forms for Kallen kalakauppa