How to simplify access to 50 systems with a single authentication portal

Identity and access management

Karol Krystkowiak

Digital Advisor

6 min read • Nov 17, 2021

Contents:

Your organization likely operates using dozens or even more different applications. Those services are meant to be used by your customers and partners, but also by employees.

So, you need a functionality that would identify those users and give them the necessary access. Securely.

But as you likely already know, it can be difficult.

Providing secure access to systems is not just about handling usernames and passwords. You need the right balance between the convenience of the user and the safety of your data. It needs to be an automated, but 100% failure-proof process.

Why? **Because the average cost of a data breach for businesses is $4.24 million.** And lack of significant security layers will result in a data breach in almost every case.

Achieving the right level of protection is getting harder with the growing number of users with different access permissions.

With many services available for clients and partners, eventually comes a need for **a single, secure and convenient platform.** A platform that will be used to log in to any of these services.

And that was exactly the need of one of our clients – a giant manufacturer, with over 50 different systems, used daily by different groups of users **(over 100 thousand users in total).**

We helped them solve this problem with **the Multi-Access Identity Platform.**

Key points:

- How does Multi-Access Identity Platform work?
- What is Azure AD B2C and what is its role in the platform?
- How does this solution improve the authentication experience?

What is the Multi-Access Identity Platform (MIP)?

MIP is a service that aggregates identity and access functionalities to all your applications and makes them accessible via a single login box.

No more multiple sets of credentials to remember. No more additional burden for your customer service, or your app developers.

The platform supports 3 types of users: customers, partners, and employees. Each of these groups can use different applications, but they all log in through the same platform.

Applications know that **if a user has come from the platform, then they are fully authenticated.** Therefore, the platform has a big responsibility – hundreds of applications trust it. That's why implementing the right security measures was the highest priority during its development.

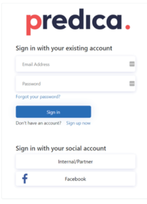
WHAT'S SO GREAT ABOUT THE PLATFORM?

The MIP provides key functionalities that make users' life easier:

- **Single sign-on**
- **Self-registration**
- **Integration with external identity providers**
- **Simplified registration with existing e-mail address**

What does it mean?

The platform enables users to securely authenticate with multiple applications **using just one set of credentials.** Additionally, customers can sign up, sign in, edit their profile, edit or reset their passwords. This way there is no need to engage IT teams in case of access issues.



Multi-Access Identity Platform: Example login screen using Azure AD B2C

Thanks to **the integration with external identity providers** (e.g. Google, Facebook, Twitter), users can also access the apps more easily, using their existing accounts. The same applies for partners who can register using their company e-mail, with no need for a separate account.

WHAT CHANGES AFTER MIP IMPLEMENTATION?

CUSTOMER EXPERIENCE

- **One login box**, providing access to multiple services across multiple devices contributes to a simplified experience for customers and partners.
- **One set of credentials** to remember, rather than several, makes it more convenient to use the services.
- **It also saves time** – users don't need to reset and change passwords as many times as before.
- **No service disruptions** – automated scalability makes it possible to handle an unpredictable number of users.

IMPROVED SECURITY

- Preventing account takeovers with **Multi-Factor Authentication** methods, such as SMS, authenticator app, or TOTP.
- Integration with the A-grade security intelligence of the **Azure cloud.**
- Ease of the information update for the user (password, e-mail).
- Immediate removal of access for the users who are no longer your employees or partners.

TIME & COST SAVINGS

- With the authentication and authorization covered, you can focus solely on building your app/service, shifting your resources to the core of it.

The difference between authentication and authorization:

- **Authentication** is about identifying users. Its goal is to verify if the users are who they claim to be, usually via username and password.
- **Authorization** is about granting access rights to resources like databases, applications, and other information. Its goal is to ensure that users can only access the services they are permitted to. Authorization happens after authentication.

WHAT'S THE TECHNOLOGY BEHIND IT?

The platform is built using Azure AD, as well as Azure AD B2C, provided by Microsoft. Their key functionalities are as follows:

1. **Azure AD (Active Directory)** delivers authentication, authorization, and access control across all Azure cloud services. Companies use it so that their employees could securely work with cloud applications.
2. **Azure AD B2C** is a service connected to Azure AD. It also allows to create a secure authentication directory for applications, but it is not attached to the particular company domain, meaning it can also serve te users from outside of the organization. They don't even have to be business users. It can be anyone, as long as they have an e-mail or social media account.

Therefore, Azure AD B2C makes it possible to create a single authentication gateway for all types of users – employees, partners, and customers.

Now, what about the authorization? With secure access guaranteed for anyone who may need it, we also have to make sure **they can only access the services they are permitted to.**

To do that, Azure AD B2C needs to connect with **the data source** (in this case provided by Cosmos DB) where all the permissions are stored. Database returns the users' data so that the application can decide whether they should have access to specific functionality or not.

User data appears in the database when they sign up for the first time. After successful login, anyone using the MIP can see the list of applications they can access on the personalized dashboard.

Why identity and access management matters

Consumer identity and access management solutions (CIAM) provide an additional layer of protection to your company's network. CIAM prevents your customers' data from falling in the wrong hands, and the consequent data breach.

Without a proper platform in place, tracking user information and related anomalies can become a complex matter. On the other hand, you don't want to make life difficult for your customers and partners, but simply supply them with safe access to the right resources.

With the right approach to the CIAM, your customers and partners get easy login and you can reap your own rewards – reliable safeguards against data leakage.

Wondering how to provide simplified access for your users? Read about our Multi-Access Identity Platform. We can help you design and build the right authentication solution for your business.

Key takeaways:

1. The platform supports 3 types of users: customers, partners, and employees. Each of these groups can use different applications, but they all log in through the same platform.
2. The platform enables users to securely authenticate with multiple applications using just one set of credentials. Additionally, customers can sign up, sign in, edit their profile, edit or reset their passwords.
3. The platform is built using Azure AD (Active Directory), as well as Azure AD B2C (a service connected to Azure AD), provided by Microsoft.