# Identity Management Solutions

An identity management solution, or IdM is a key aspect of security in a cloud environment where digital identities for individuals, or applications are used to restrict and secure access to a cloud environments resources. An identity management solution can assist in securing access to users data, providing access control to resources and help ensure data privacy is maintained.

## Microsoft Entra ID

In the context of a popular cloud provider: Microsoft Azure, an identity management solution named Microsoft Entra ID (formerly Azure Active Directory) is available (Microsoft, 2024). Some of the core features provided by Microsoft Entra ID include:

* Single sign-on (SSO) and multifactor authentication
* Role-based access control (Azure RBAC)
* Consumer identity and access management
* Device registration
* Security monitoring and reporting
* Identity protection

## Single sign-on (SSO)

A key feature of an identity management solution is single sign-on, whereby users can access all applications available to them utilising a single account, or method of signing on. This is a widely used concept in Software as a Service (SaaS) applications, where users can register and sign-on using an account from other providers (i.e. Google, Apple). This mitigates against the need for users to recall multiple usernames and passwords (Microsoft, 2024).

## Multifactor authentication

Access security to a resource using single sign-on is one important factor in identity management, and this can be bolstered utilising multifactor authentication. Multifactor authentication requires that an authenticating user provide a secondary method of proving who they are when attempting to access a system. In terms of the IdM solution provided by Microsoft Entra ID, an SMS message, phone call, or the use of the Microsoft Authenticator mobile application are all used in conjunction with a password to complete an authentication journey (Microsoft, 2023).

Once a user is authenticated with Microsoft Azure, they are provided with a screen showing what exactly they have access to. Administrators can control what subscriptions and resources a user has via a conditional access. Role-based access control (RBAC) is another method of controlling what groups of users have access to which cloud resources. An example use case of employing RBAC in the Azure cloud environment is to grant database administrators access to database, or data lake resources only, while restricting application developers access to resource groups where application services, container apps or Azure functions are deployed.

## IdM in TU Dublin

Data privacy and access control are two key ethical considerations to make when planning to adopt any IdM in a University. One primary consideration to make in the context of data privacy is to ensure that user roles are absolutely clearly defined so that unauthorised intrusion on other students data is not a possibility. Carefully designed roles and use of role based access control (RBAC) are two important areas to emphasise.

Data storage location is another consideration to take into account. Since Azure is a cloud platform, it is possible to define where cloud components are located across the world. Ensuring that data protection (and ultimately GDPR) laws are adhered to, and user data is not being exported from the jurisdiction in which it is supposed to be stored must be taken into account.

Transparency and security are two other points to take into consideration. The cloud provider should employ clearly defined data storage auditing and reporting features. It should be possible to configure and deploy monitoring and alerting functionality, and the University should be clear on whom has access to these reports (Microsoft, 2023).

# Bibliography

Microsoft. (2023, October 23). *Data protection considerations.* Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/entra/fundamentals/data-protection-considerations

Microsoft. (2023, October 23). *How it works: Microsoft Entra multifactor authentication.* Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mfa-howitworks

Microsoft. (2024, January 1). *Azure identity management security overview.* Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/azure/security/fundamentals/identity-management-overview