Identity

In computing, “identity” is a representation of a person, application or device.

Example: person, email, application, a printer

Usually requires a password, a secrete key or a certificate (multi-factor authentication) to prove identity.

Many applications require you to log in to use some of functionality. Thus, different people have different permissions.

Before Microsoft standardize / cloud, identity is handled as follows:

Client App, Web browser, Mobile App (username & password) --> Server, Web site --> Database

Over the time, people found ways (cache instead of plain text) to save password, but they are also hacked.

Microsoft came up with “Active Directory” (for cloud we have Azure Active Directory / Microsoft Entra ID). Activate Directory uses protocols such as LDAP and Kerberos for communication.

Thus, as a user, instead of coding your own security backend, you can use APIs to Entra ID to handle authentication and authorization.

Benefits of using Entra ID as a service (for third party application and custom applications)

- Security
- Reduced development time + easier support
- There are additional features: Use AI to logging patterns (logging someone from country/region where you do not have any business), Audit features
- Centralized administration (can flag some users)
- Single sign-on (SSO) (same username can be used to logging company laptop and then also Azure)
- Integrates with other Azure services

Authentication and Authorization

Authentication is a user providing who they are (user Id and password).

Authorization is ensuring that a user is permitted to perform an action (read/edit/delete a certain file)

Nowadays we are moving away from all authenticated users having admin access.

External Identities in Azure

In here, we see how Azure help with users who are not in company internal directory (that is, partners, contactors, end users). This is where B2B B2C comes in.

- In simple terms, the ability to give secure access to your resources or applications for people outside of your organization.

Business-to-Business (B2B)

Can view as collaborators (formal relationships).

B2B means inviting partners, contractors or vendors into your organization.

These are guests (guest users). They use their own credentials to log in (Gmail, company log in). We can assign roles and permissions, same as internal users.

Business-to-Consumer (B2C)

B2C means inviting customers/end users to use your applications. They do not appear in your organization at all.

Users use “social identities” to sign like FB, Google, ...

Single Sign-On (SSO)

Example: We may log into Microsoft 365 and then we will be using Microsoft Words, outlook, Excel, … without typing password every time.

Imagine your company has 10 apps for various things such as time entry, file storage, design software, etc. In typical set up here we may need unique usernames and passwords. However, when try to change it, we may have to change it in every place. The solution is SSO.

This is a feature of Entra ID. Entra ID uses a token that proves who you are. That token is trusted by all other applications in your company. Instead of your password, it checks your token. Authenticated once, trusted everywhere.

How it works?

- Every application is registered with your Entra ID
- The app trusts your Entra ID
- The token was encrypted by Entra ID and can only be decrypted because of your public key

This enables fewer logins, strong password. For organization, it gives better security, simplified management (instead of 10 passwords for 1 user, one password for one user).

Entra Conditional Access

These are options we can enable, and we may have to pay for these services.

It is important to note not all attempts to log into a system are equally safe. We can set rules to identity risky attempts to log into the system.

Safe attempt: When someone logs in to an application from inside your office building as do every day.

Risky attempts: (1) Someone try to log in from a country that particular employee has never logged in. It could be someone on a sales trip and try to log from there. (2) Try to log in after long time. (3) Try to log with a new device.

Thus, Entra Conditional Access will use different signals (location, time, device) to determine whether it is a risky attempt. Then, either block or require multi factor authorization (MFA).