Sample of Project Notes

**Authenticator App: Microsoft Or Google?**

**An authenticator app provides an additional layer of security that is more than just a username and password.**

Let’s start with the basics…

Authentication is the process a user goes through to validate who they are by way of logging basic identification details such as an email address or username followed by a [password](https://www.uniserveit.com/password-security-and-best-practices/). To protect high-valued accounts, passwords aren’t always enough.

**How does multi-factor authentication play a role in preventing intruders from stealing your data?**

Multi-factor authentication (MFA) or two-factor authentication (2FA) provides an additional layer of security to avoid [phishing](https://www.uniserveit.com/blog/top-tips-to-identify-and-block-phishing-attacks/). Passwords can be forgotten or compromised and MFA or 2FA helps access accounts more securely making it harder for other people to break in.

There are numerous factors of multi-factor authentication:

* What the user knows: This includes security questions or PINs, wherein the user is the only one who knows the answer.
* What the user has: This includes mobile phones where it can give codes or a one-time password or even smart cards.
* What the user is: This includes a part of the human body such as fingerprints or facial recognition.

The combination of two or all these types creates the multi-factor authentication method, and this is where Microsoft, Google, or any other authenticator app comes into play.

**Microsoft Authenticator or Google Authenticator App?**

Both app’s interface might look the same but there are a few features that differentiate them.

It both generates time-based 6 or 8-digit codes during the verification process when you sign in on your online accounts and the apps work for mobile and tablet devices running on iOS and Android.

Aside from Microsoft accounts or Google accounts, it can also be used as an authenticator for other products such as GitHub, Dropbox, Facebook, or interchangeably.

Microsoft list the following ways to use Microsoft Authenticator app on its [documentation:](https://docs.microsoft.com/en-us/azure/active-directory/user-help/user-help-auth-app-download-install)

* *Two-factor verification. The standard verification method, where one of the factors is your password. After you sign-in using your username and password, you can either approve a notification or enter a provided verification code.*
* *Phone sign-in. A version of two-factor verification that lets you sign-in without requiring a password, using your username and your mobile device with your fingerprint, face, or PIN.*
* *Code generation. As a code generator for any other accounts that support authenticator apps.*

**What Are The Differences?**

1. Microsoft Authenticator can support one account on multiple devices while Google Authenticator doesn’t.
2. Microsoft Authenticator has a feature that lets you hide the code useful to protect your account.
3. Google automatically syncs the time between the mobile device and app while Microsoft desyncs it, resulting in invalid codes.
4. Microsoft offers a backup feature essential when the device is lost or stolen.
5. Microsoft supports custom icons that make it easier to locate each account and code, which Google doesn’t have.

No matter the app, it is vital to implement multi-factor authentication to prove a user’s identity and protect individuals from data theft.

[Contact us](tel:+8522036228500) today if you have any questions on setting up multi-factor authentication for your devices.