IdentoGO®

IDEMIA CARES Solution

Multi-Factor Authentication Applications

This document contains references or links to web sites or application developers that were current at the time of publication, but that may have moved or become inactive since. This document includes references to application developers which are owned and operated by third parties. IDEMIA is not responsible for the content of any such third party sites.

Guidance on Authenticator Application Setup

An authenticator application is a software-based tool that provides an additional layer of security to protect your online accounts from unauthorized access. It generates time-based one-time passwords (TOTP) or event-based codes that are used as a second factor in multi-factor authentication (MFA) process, alongside your regular password. This means that even if someone manages to obtain your password, they would still need the unique code generated by the authenticator app to gain access to your account.

Getting an authenticator application is simple and easy. Below is a step-by-step guide on how to get one for a person who has a phone or a laptop:

Choose an Authenticator App: There are several authenticator apps available for use, and the choice may depend on your device and personal preferences. Below are some popular authenticator apps:

- Google Authenticator: Developed by Google, this app is available for both Android and iOS devices. It supports multi-factor authentication (MFA) for various online accounts, including Google accounts, social media, and many other popular services.

- Duo Mobile: Developed by Duo Security, a trusted provider of multi-factor authentication solutions, Duo Mobile is available for both Android and iOS devices. It supports MFA for Duo-protected accounts, as well as other services that use the TOTP or event-based One-Time Password (OTP) protocols.

- Microsoft Authenticator: Created by Microsoft, this app is available for both Android and iOS devices. It supports MFA for Microsoft accounts, as well as other services that use the Time-based One-Time Password (TOTP) protocol.

- Authy: Authy is a popular authenticator app available for Android, iOS, and desktop platforms (Windows, macOS, and Linux). Authy allows you to sync your accounts across multiple devices, making it convenient for users who want to use an authenticator app on different devices.

- LastPass Authenticator: Offered by LastPass, a popular password manager, this app is available for Android and iOS devices. It provides an additional layer of security for LastPass accounts, as well as other services that support TOTP-based authentication.

- YubiKey Authenticator: This app is designed specifically for use with YubiKey hardware security keys, which are physical devices that provide an additional layer of security. The YubiKey Authenticator app is available for Android and iOS devices and supports TOTP and HOTP protocols.

Download and Install the Authenticator App: If you have a smartphone, go to the respective app store for your device (e.g., Google Play Store for Android or App Store for iOS) and search for the authenticator app you've chosen. Download and install the app on your phone. If you have a laptop, visit the website of the authenticator app you've chosen and download the software for your operating system (e.g., Windows, macOS, or Linux) and install it on your laptop.

Set up the Authenticator App: Once you have the authenticator app installed on your device, open it and follow the instructions to set it up. Typically, you'll need to scan a QR code or enter a secret key provided by the service you want to enable two-factor authentication for. This links your authenticator app to your account.

Verify the Authenticator App: After setting up the authenticator app, you'll usually need to verify it to ensure it's working correctly. This usually involves entering a code generated by the app into the service you're trying to secure. This step confirms that the authenticator app is generating the correct codes and is ready to be used as a second factor in the authentication process.

Use the Authenticator App: Once the authenticator app is set up and verified, it's ready to use. Whenever you log in to an account that has two-factor authentication enabled, you'll need to enter the code generated by the authenticator app in addition to your regular password. The app will generate a new code every few seconds or after each use, ensuring that the second factor is dynamic and constantly changing, adding an extra layer of security to your accounts.