

Technical Note on TOTP MFA Use

The Multi Factor Authentication (MFA) used in our systems is compliant with the [Time-Based One-Time Password Algorithm](#) (TOTP). Any authenticator that complies with TOTP should be able to generate the appropriate code for authentication with our systems.

There are implementations of the TOTP code generator available on variety of platforms and a list of examples is shown below. For the avoidance of doubt, inclusion in this list is not a recommendation by EMIS and any software used must first be validated as being secure by the user.

iOS Devices (iPhone, iPad etc)

- Native support (available in **Settings > Passwords > (Website) > Set Up Verification Code**)
- [Microsoft Authenticator](#)
- [Google Authenticator](#)
- [Duo Mobile](#)
- [Twilio Authy](#)
- [Authenticator App](#)

Android Devices

- [Microsoft Authenticator](#)
- [MFA Authenticator](#)
- [Google Authenticator](#)
- [2FA Authenticator \(2FAS\)](#)

Windows Desktop

- [OTPKEY Authenticator](#)
- [2FA Authenticator](#)
- [Enpass Password Manager](#)
- [KeePassXC](#)

Apple Mac Desktop

- [KeePassXC](#)
- [Enpass Password Manager](#)
- [G2FA for Google Authenticator](#)
- [Authenticator App](#)
- [Sentinel Authenticator](#)

EDGE Browser Plugin

- [2FAS – Two Factor Authentication](#)
- [Open Two-Factor Authenticator](#)
- [web2FA - Browser Authenticator](#)

Chrome Browser Plugin

- [TOTP Authenticator](#)
- [Authenticator.cc](#)
- [KeePassXC](#)