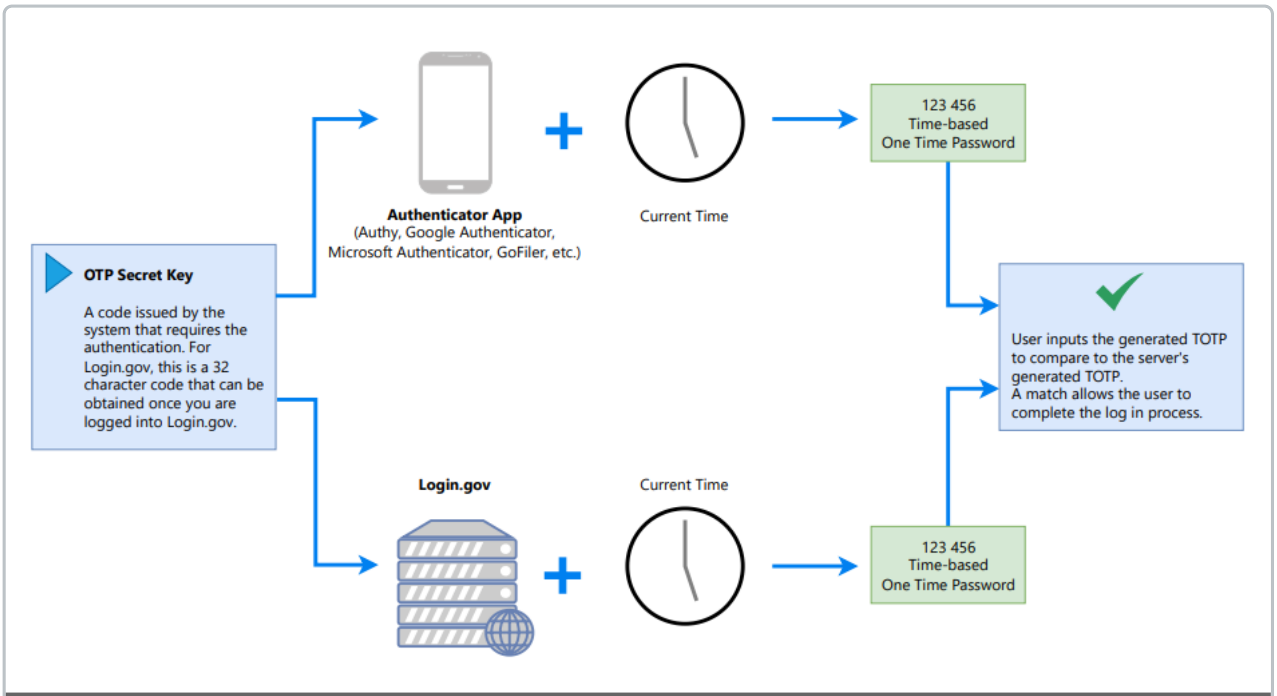
What is a TOTP secret key?

Last Modified on 10/23/2023 11:32 am EDT

TOTP stands for **Time-based One-Time Passwords**, and they are used as a common form of two factor or multi-factor authentication (2FA and MFA, respectively). Multi-factor authentication schemes can use the following common authentication factors: something the user has; something the user knows; and something the user is (i.e. a physical characteristic of the user such as a fingerprint or voice). TOTP authentication is considered to be **something the user has** because it requires a third-party authenticator (TPA) application.

TOTP is also referred to as "app-based authentication", "software tokens", or "soft tokens". Many apps support the TOTP standard for generating passwords.

TOTP authentication generates unique numeric passwords with a standardized algorithm that uses the current time as an input.The one-time password can be generated by a TPA that knows the OTP secret key. The TOTP can then be verified by the server which can generate the same code independently. Because the current time is used as an input when creating the password (in addition to the secret key), this password will expire – hence "time-based".


OTP Secret Key
A code issued by the system that requires the authentication. For Login.gov, this is a 32 character code that can be obtained once you are logged into Login.gov.
Authenticator App
(Authy, Google Authenticator, Microsoft Authenticator, GoFiler, etc.)
Current Time
123 456
Time-based
One Time Password
User inputs the generated TOTP to compare to the server's generated TOTP.
A match allows the user to complete the log in process.
Login.gov
Current Time
123 456
Time-based
One Time Password

The above image illustrates how the OTP secret key is used by the TPA as well as the server seeking the authentication (in this case Login.gov) to generate the OTOP. If the OTOP matches, the user may complete the log in process and log into the server. If the codes do not match, the user will be forced to try another code or use a different method of authentication.

The EDGAR Next system uses **Login.gov** to authenticate a user to the system. **Login.gov** requires 2FA and can be set to use TOTP authentication as a method of verifying a user. Users can choose one or more authentication apps that use TOTP authentication in order to verify their identity when logging into **Login.gov**.

The OTP secret key only needs to be added to an authentication app once. The app will then be able to generate the TOTP (or passcode) whenever the user requests a TOTP to log into **Login.gov**. **Learn how GoFiler can be set up as your authentication app.**