PROTECTIMUS

Protectimus FLEX

Programmable TOTP tokens in a key fob format

Programmable OTP tokens Protectimus Flex are designed to be used instead of 2FA apps to reliably secure services that don't offer native support for hardware token authentication: Office 365, Azure MFA, Google, PayPal, Dropbox, GitHub, most payment systems, cryptocurrency exchanges, social networks, and so on. All you need to program a Protectimus Flex token is Android smartphone with NFC support.

Protectimus Limited
Carrick house, 49 Fitzwilliam Square,
Dublin D02 N578, Ireland

PROTECTIMUS

Protectimus FLEX

Programmable TOTP tokens in a key fob format

PROTECTIMUS

RoHS

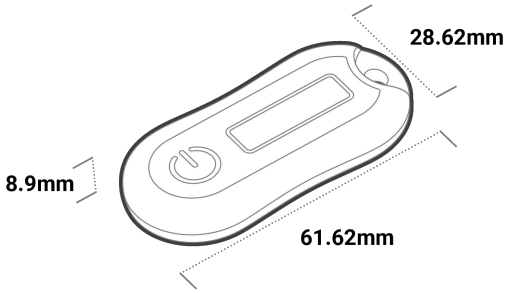
IP67

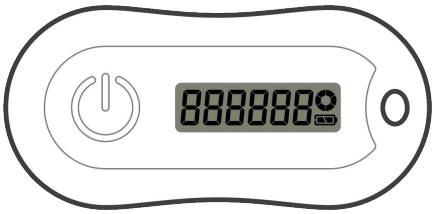
oath
initiative for open authentication
CERTIFIED

PROTECTIMUS

Protectimus FLEX

Technical Specification





Weight	16.1 g (0.57 oz)
Display	LCD 6 digits
Algorithm	OATH compliant time based TOTP
Cryptographics	SHA-1
Time Interval	30/60 seconds (Time Synchronization Support)
Programmable Protocol	NFC
Operating Temperature	0°C - 40°C (32°F - 104°F)
Humidity	0 - 90% without condensation
Battery	Up to 5 years
Material	PC+ABS
Physical Resistance	Tamper evident, IP68 for Glue Injection

The warranty period is 12 months

PROTECTIMUS

RoHS

IP67

oath initiative for open authentication CERTIFIED

www.protectimus.com
sales@protectimus.com

Key Features

Easy to use and portable

- Designed in a key fob format
- Supports 16- to 32-character long secret keys (Base32)
- Simple one-click generation of one-time-passwords
- Independent of the end-user environment
- No external connection is required
- Minimum change to the existing password authentication system
- Secure, robust and long life hardware design

Secure

- Compliant with open OATH authentication standards
- Can be easily integrated with 3rd party OATH authentication systems
- Your company controls the turnover of secret keys

Can be programmed over NFC (Android smartphone is required)

IP67

PROTECTIMUS

Protectimus FLEX

An unbreakable hardware OTP token

PROTECTIMUS

RoHS

IP67

oath
initiative for open authentication
CERTIFIED

www.protectimus.com
sales@protectimus.com

Convenience and security

Secure
The programmable TOTP token Protectimus Flex doesn't connect to the internet or to a GSM network, eliminating the possibility of a one-time password being intercepted when delivered in an SMS, or being read by malware on a smartphone. With this one-time password generation token, unlike standard hardware tokens, only you will know your secret key, thanks to the setup over NFC.

Universal
The Protectimus Flex was developed as a hardware alternative for the Google Authenticator and other OATH-compliant software tokens. It's suitable for authentication systems that support TOTP tokens. If you're not sure whether a token is right for you, just ask us!

Reprogrammable
One Protectimus Flex TOTP token can hold a single secret key, but the secret key can be changed an unlimited number of times. This is convenient for businesses, as it allows the same token to be re-assigned multiple times for use with different services, unlike non-programmable OTP tokens. It's convenient for clients, too, since the secret key can be changed if necessary.

The best choice for:
1. Corporate use with Google Authenticator based authentication systems as well as Microsoft Azure MFA, Office365, Duo, Okta, etc.
2. Personal use with Google, Dropbox, GitHub, Kickstarter, Mailchimp, Microsoft, Facebook, many cryptocurrency exchanges, etc.

IP67

Protectimus FLEX

How to program?

Download the app

If you have an NFC-enabled phone running Android OS, just download and run the TOTP Burner app to program your OTP token.

Enabling 2FA

Initiate the token setup on the system where you require enhanced security. Save the secret key in a SAFE place so that you can easily restore the security token.

Scanning the key

Scan the secret key using the TOTP Burner app, or input it manually. We recommend the automatic method.

Programming

Activate the OTP token and place it near your phone's NFC antenna. While holding it near the NFC antenna, tap "Burn the seed" and wait for a message confirming that the 2FA token was programmed successfully.

Protection, everywhere and always!

Enjoy reliable and convenient protection for your account on any service — make hackers' lives difficult.

PROTECTIMUS

RoHS

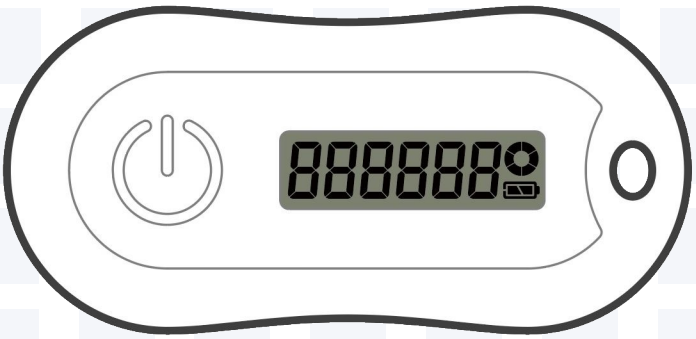
IP67

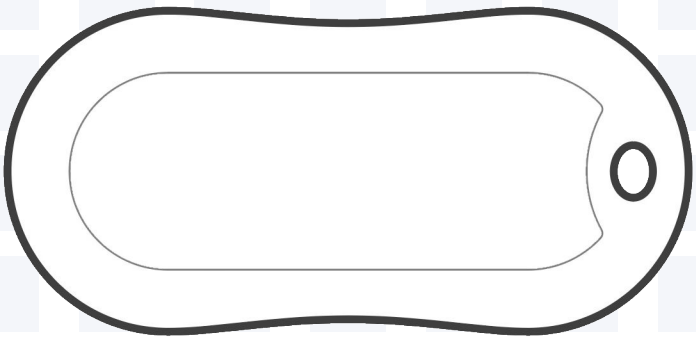
oath initiative for open authentication CERTIFIED

Protectimus FLEX

How to use

1. Press the button, the One-Time-Password code will appear on the screen.
2. The screen may go off because of the expiration of the OTP lifetime (i.e. 30 or 60 seconds), you can press the button again to generate a new code.
3. Input the code to the web page or application.
4. The screen will go off automatically once the code expires.
5. You can also close the screen by pressing the button.





www.protectimus.com
sales@protectimus.com

White-Labeling and Delivery Options

Protectimus can offer a comprehensive white-label solution.
Depending on your preferences, we can place your company's logo and other visual features on the device; you can also choose the color of your OTP token.

Want OATH tokens with custom branding?
We can make them for you! Branding is available for orders of 1000 tokens or more. It costs $1 per token.

The price of tokens does not include shipping and delivery costs and other additional charges, such as taxes and customs duties.

Delivery times depend on several factors, in particular: lot/consignment size, token availability at our warehouse, and postal service. Besides, the delivery time will depend on whether additional visual features need to be placed on the products. Typically, if there is a sufficient quantity of products at the warehouse, orders are delivered within 2 to 6 weeks.

How to buy?
You can easily become a happy owner of this device. To place an order, please, fill out the form on our website or write an email to sales@protectimus.com, and our specialist will contact you promptly.