YubiKey NEO

- YubiKey NEO offers strong authentication via Yubico one-time passwords (OTP), FIDO Universal 2nd Factor (U2F), and smart card (PIV, OpenPGP, OATH-TOTP, and OATH-HOTP) — all with a simple tap or touch of a button
- Works instantly with no need to re-type passcodes — replacing SMS texts, authenticator apps, RSA tokens, and similar devices
- Identifies as a USB keyboard, smart card, and smart card reader — no client software or drivers need to be installed, no batteries, no moving parts — and works over USB or NFC
- Crush-resistant and waterproof, YubiKey NEO is practically indestructible during normal use — weighs only 3g, and attaches to your keychain alongside your house and car keys
- Manufactured in USA and Sweden with high security and quality

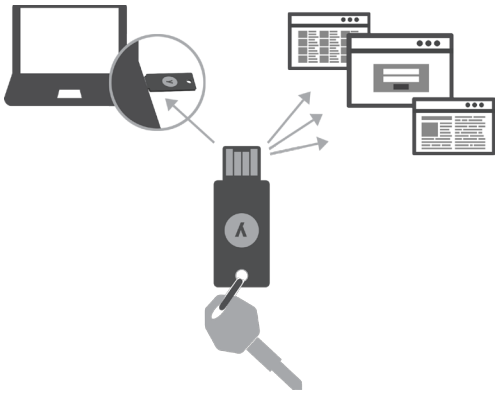
Description:
YubiKey NEO is a small USB and NFC device supporting multiple authentication and cryptographic protocols. With a simple touch, YubiKey NEO protects access to computers, networks, and online services for everyone from individual consumers to the world's largest organizations. YubiKey NEO works on Microsoft Windows, Mac OS X, Linux operating systems; major browsers; and Android NFC phones and tablets.

Note: If NFC is not required, or if the smaller Nano form factor is preferred, Yubico recommends you purchase the YubiKey 4 or YubiKey 4 Nano. The YubiKey 4 and YubiKey 4 Nano are Yubico's latest generation YubiKeys and include faster and stronger crypto compared to the YubiKey NEO.

Product Identification Information

	YubiKey NEO
Size	*18mm x 45mm x 3.3mm*
Weight	*3g*
FIDO Certified™	*Yes*
BIS Classification	*ECCN 5A992.a, CCATS G153476*

One key many services:



YubiKey NEO

Where Can You Use Your YubiKey?

Use the YubiKey NEO to secure a wide range of applications, including remote access and VPN, password managers, computer login, development platforms, identity and access management systems, popular online services, and much more. Log in to your Gmail, Google, GitHub, or Dropbox accounts using the emerging FIDO Universal 2nd Factor (U2F) protocol. Find out more about the wide range of open source and enterprise solutions at yubico.com.

For IT Departments

The YubiKey can be deployed across an entire enterprise quickly and easily using your own tools or tools from our enterprise partners. Deployment is easy, because people love using the YubiKey. Find out more at yubico.com/biz.

For Businesses and Organizations

Integrate the YubiKey within your systems and applications to secure access to your intellectual property. Or integrate the YubiKey with your own product to secure access to your service for your customers. Use your own tools or integrate with tools from our enterprise partners. Find out more at yubico.com/biz.

For Developers

Use the YubiKey NEO as soon as you receive it to secure your Google, Gmail, GitHub, or Dropbox accounts. Then use our developer tools to integrate the YubiKey into your own service, website, or application. Or set up your YubiKey so you can sign code or SSH into a server. Learn more on our developer site at dev.yubico.com.

For Home Use

Use the YubiKey NEO as soon as you receive it to secure your Google, Gmail, Dropbox, and Dashlane accounts. Protect your computer login for Windows, Mac, and Linux. Find out more at yubico.com/indiv.

Google Dropbox GitHub GitLab Bitbucket

dashlane DUO Shibboleth Sentry COMPOSE AN IBM COMPANY WSO2

What Can Your YubiKey Do?

One single YubiKey NEO supports multiple authentication protocols, including Yubico One-Time Passwords (OTP), OATH (TOTP, HOTP), FIDO Universal 2nd Factor (U2F), and smart card (PIV, OpenPGP). Hardware secure elements guard your encryption keys. Free and open source software tools are available for download from the Yubico website so you can personalize and configure the YubiKey yourself.

What Is Really Inside the YubiKey?

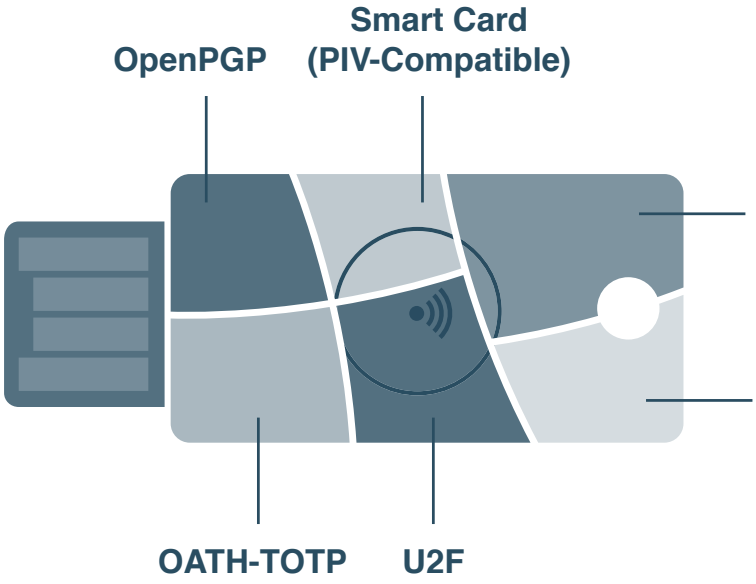
YubiKey NEO has two symmetric key "slots" that you can configure to store credentials, such as one for Yubico OTP (default in slot 1) and one for OATH-HOTP.

You can configure the same YubiKey as a smart card (PIV-compatible). You can store up to 32 OATH credentials (TOTP or HOTP) on the YubiKey NEO and access them using the Yubico Authenticator application. In addition, you can have an unlimited number of U2F credentials – these include Gmail plus other Google apps, GitHub, Dashlane, and Dropbox, and more.

Yubico provides the free and open source tools so individuals and admins can configure the YubiKey, or YubiKeys can be configured in bulk by Yubico (fee applies).

YubiKey NEO

One key — many functions!



CONFIG SET 1*
Yubico OTP
OATH-HOTP
Challenge-Response
Static Password
Symantec VIP

CONFIG SET 2*
Yubico OTP
OATH-HOTP
Challenge-Response
Static Password
Symantec VIP

* Configure using Yubico's free tools, except Symantec VIP which is programmed by Yubico (upon request)

Yubico changes the game for strong authentication, providing superior security with unmatched ease-of-use. Find out more at yubico.com.

	YubiKey 4/YubiKey 4 Nano	YubiKey NEO
Functions		
Yubico One-Time Password (OTP)	●	●
OATH-TOTP (Time)	●	●
OATH-HOTP (Event)	●	●
FIDO Universal 2nd Factor (U2F)	●	●
Challenge-Response	●	●
Static Password	●	●
Smart Card (PIV-compliant)	●	●
OpenPGP	●	●
Touch-to-sign	●	
Top Applications		
Google Apps (U2F)	●	●
GitHub (U2F)	●	●
Docker	●	
Dropbox (U2F)	●	●
LastPass	●	●
Communications Support		
USB	●	●
NFC		●
Certifications		
FIDO Certification Program	●	●
FIPS 140 Certification in Process	●	
Cryptographic Specifications		
2048 RSA Keys	●	●
4096 RSA Keys	●	
ECC p256 (PIV)	●	●
ECC p384 (PIV)	●	
Device Type		
HID Keyboard	●	●
CCID Smart Card	●	●
FIDO U2F HID Device	●	●