



# YubiKey 4 and YubiKey 4 Nano

- YubiKey 4 and YubiKey 4 Nano offer strong authentication via Yubico One-Time Passwords (OTP), OATH (TOTP, HOTP), FIDO Universal 2nd Factor (U2F), and smart card (PIV, OpenPGP) – 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
- Crush-resistant and waterproof, YubiKey 4 is practically indestructible during normal use – weighs only 3g, and attaches to your keychain alongside your house and car keys, while YubiKey 4 Nano fits inside a USB port
- Manufactured in USA and Sweden with high security and quality

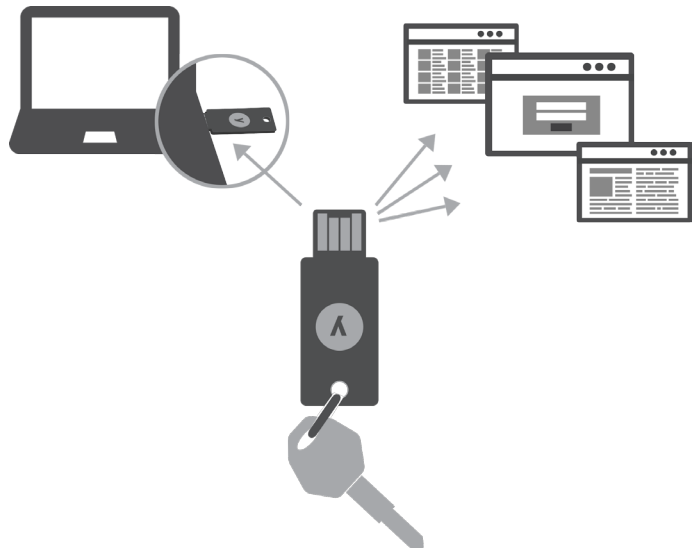
**Description:**

YubiKey 4 is a small USB device supporting multiple authentication and cryptographic protocols. With a simple touch, YubiKey protects access to computers, networks, and online services for everyone from individual consumers to the world’s largest organizations. YubiKey 4 works on Microsoft Windows, Mac OS X, and Linux operating systems, and on major browsers.

*Note: If you require NFC, the YubiKey NEO communicates using both USB and NFC.*

	YubiKey 4	YubiKey 4 Nano
Size	18mm x 45mm x 3.3mm	12mm x 13mm x 3.1mm
Weight	3g	1g
FIDO Certified™	Yes	Yes
FIPS 140	in process	in process
BIS Classification	ECCN 5A992.c CCATS G169868	ECCN 5A992.c CCATS G169868

One key many services:



# YubiKey 4 and YubiKey 4 Nano

## Where Can You Use Your YubiKey?

Use the YubiKey 4 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, and sign your code with Docker. Find out more about the wide range of open source and enterprise solutions at [yubico.com](http://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](http://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](http://yubico.com/biz).

### For Developers

Use the YubiKey 4 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 in Docker, or SSH into a server. Learn more on our developer site at [dev.yubico.com](http://dev.yubico.com).

### For Home Use

Use the YubiKey 4 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/individ](http://yubico.com/individ).



## What Can Your YubiKey Do?

One single YubiKey 4 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?

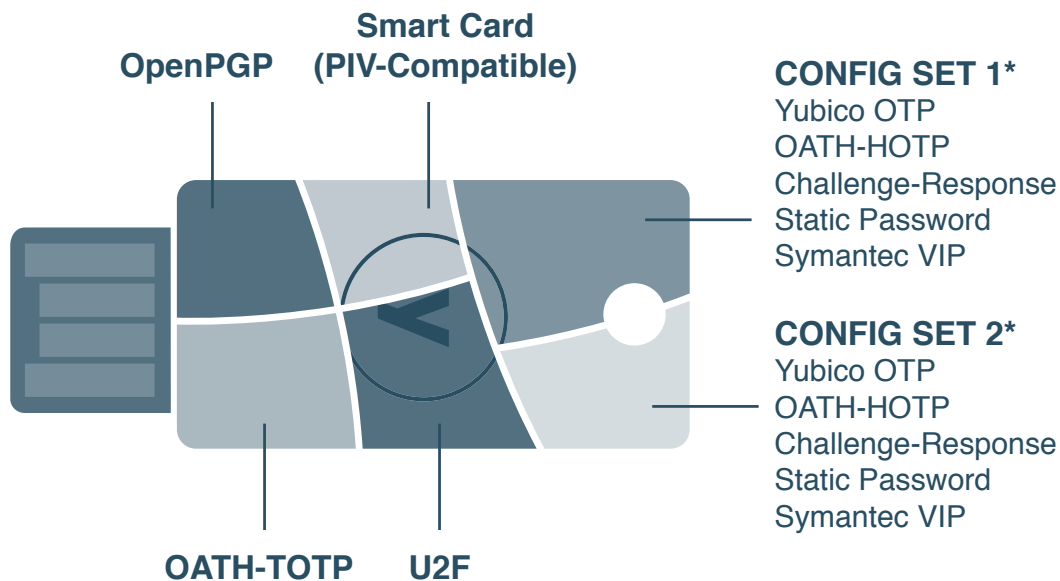
YubiKey 4 has two symmetric key “slots” that you can configure to store credentials, such as one for Yubico OTP (default in slot 1) and one for OATH-HOTP.

You can configure the same YubiKey as a smart card (PIV-compatible) and program the YubiKey for touch-to-sign code signing with Docker. You can store up to 32 OATH credentials (TOTP or HOTP) on the YubiKey 4 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 4

## One key — many functions!



\* 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](http://yubico.com).**

	YubiKey 4/YubiKey 4 Nano	YubiKey NEO
<b>Functions</b>		
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	●	
<b>Top Applications</b>		
Google Apps (U2F)	●	●
GitHub (U2F)	●	●
Docker	●	
Dropbox (U2F)	●	●
LastPass	●	●
<b>Communications Support</b>		
USB	●	●
NFC		●
<b>Certifications</b>		
FIDO Certification Program	●	●
FIPS 140 Certification in Process	●	
<b>Cryptographic Specifications</b>		
2048 RSA Keys	●	●
4096 RSA Keys	●	
ECC p256 (PIV)	●	●
ECC p384 (PIV)	●	
<b>Device Type</b>		
HID Keyboard	●	●
CCID Smart Card	●	●
FIDO U2F HID Device	●	●