Thank you for inquiry and interest! Below is information you are free to use when talking about Yubico and the YubiKey.

While your integration is under review, we kindly request that you include the disclaimer in this document in your content. Once your integration is Yubico certified, we will be able to add your solution to our partner listing.

Disclaimer

"[Name of your company] and our products are not affiliated with or endorsed by Yubico, Inc. Our integration is currently under validation testing, and we are seeking certification from Yubico."

If you do not plan to seek certification from Yubico: "[Name of your company] and our products are not affiliated with or endorsed by Yubico, Inc. We do not intend to seek certification from Yubico."

Company Description

Yubico sets new global standards for simple and secure access to computers, servers, and internet accounts. Founded in 2007, Yubico is privately held, with offices in Australia, Germany, Singapore, Sweden, UK, and USA.

Yubico is a leading contributor to both the FIDO2 and FIDO Universal 2nd Factor (U2F) open authentication standards. The company's technology is deployed and loved by 9 of the top 10 internet brands and millions of users in more than 160 countries.

Elevator Pitch

The YubiKey combines public key cryptography with hardware-backed protection to deliver an easy to use and secure authentication solution.

Why the YubiKey

The YubiKey is a security key used for two-factor authentication (2FA).

- **Strong Phishing Defense -** The YubiKey combines hardware-backed authentication and public key cryptography to protect against phishing and account takeovers.
- **Easy, Fast, Reliable -** Logging in with the YubiKey requires just a touch, making it 4 times faster than typing codes.
- **Trusted Leader** - The YubiKey is the trusted secure authentication choice for the largest internet, finance, and retail companies in the world, including 9 of the top 10 internet companies.
- **Affordable -** The YubiKey comes in durable, water-resistant, and battery-free designs with varying capabilities starting at $20 USD.

Features and Benefits

- **Multi-protocol -** The YubiKey offers flexibility for users looking to deploy more than one authentication protocol (e.g. FIDO2, U2F, smart card, Yubico One Time Password) for a variety of services.
- **Compatibility -** The YubiKey works on major browsers, such as Google Chrome and Firefox, and operating systems, including but not limited to Microsoft Windows, MacOS, Linux, and Chrome OS.
- **Robust -** The YubiKey comes in different form factors for semi-permanent installation on a USB-port or for everyday mobility on a keyring.

Form Factors and Features

Security Key by Yubico

The Security Key by Yubico combines the U2F and FIDO2 protocols to eliminate account takeovers. It provides the strongest level of authentication to hundreds of U2F and FIDO2 compatible services.

- For USB-A ports
- Designed for keychains
- Supports: U2F, FIDO2

YubiKey NEO

The YubiKey NEO has both contact (USB) and contactless (NFC) communications. It supports multiple authentication protocols, and works with NFC phones and tablets.

- For USB-A ports and NFC active devices
- Designed for keychains
- Supports: Static Password, Yubico OTP, OATH - HOTP (Event), OATH - TOTP (Time), PIV-Compliant Smart Card/CCID, OpenPGP, U2F

**Note: Apple currently provides only limited support for NFC. The YubiKey NEO can be used to perform OTP-based authentication for iOS devices over NFC.*

YubiKey 4 Series

The YubiKey 4 Series of security keys brings strong cryptographic protection with seamless touch-to-sign functions to an unlimited number of accounts.

- Same capabilities in four form factors:
  - YubiKey 4: For USB-A ports, designed for keychains
  - YubiKey 4 Nano: For USB-A ports, designed to remain inside USB port
  - YubiKey 4C: For USB-C ports, designed for keychains
  - YubiKey 4C Nano: For USB-C ports, designed to remain inside USB port
- Supports: Static Password, Yubico OTP, OATH - HOTP (Event), OATH - TOTP (Time), PIV-Compliant Smart Card/CCID, OpenPGP, U2F

Authentication Protocols

Smart Card (PIV)
The YubiKey allows 3 different smart card protocols to be used simultaneously—PIV, as defined by the NIST standard for authentication; OpenPGP for encryption, decryption, and signing; and OATH, for client apps like Yubico Authenticator and Windows Hello.

FIDO U2F
U2F is an open authentication standard that enables keychain devices, mobile phones and other devices to securely access any number of web-based services — instantly and with no drivers or client software needed.

FIDO2
FIDO2 marks an evolution of the U2F open authentication standard and enables strong passwordless authentication built on public key cryptography using hardware devices like security keys, mobile phones, and other built-in devices.

Yubico One Time Password
Integrate YubiOTP natively with the free YubiCloud authentication service, or program your own TOTP or HOTP secrets.

Learn more: https://developers.yubico.com/

Useful Resources

Yubico Blog

Yubico Customers & Case Studies

Yubico Webinars

Yubico White Papers

Yubico Awards

Yubico in the News

Yubico for Developers

Imagery

Approved product images can be downloaded here. General usage guidelines here.

Updated April 10, 2018