Home (/) / OATH

OATH (/OATH)

YKOATH Protocol (/OATH/YKOATH_Protocol.html)
YubiKey OATH software (/OATH/YubiKey_OATH_software.html)

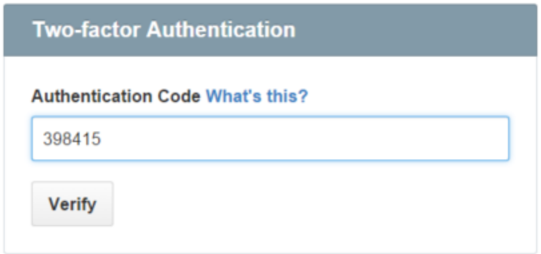
Suggest Edits (https://github.com/Yubico/developers.yubico.com/issues/new?title=Suggested%20edit%20for%20OATH/index)

What is OATH?

OATH (Initiative for Open Authentication) is an organization that specifies two open authentication standards: TOTP (Time-based One-time Password Algorithm) and HOTP (HMAC-based One-time Password Algorithm).

TOTP

To authenticate using TOTP, the user enters a 6-8 digit code that changes every 30 seconds. It can look like this:



Two-factor Authentication

Authentication Code What's this?

398415

The code is generated using `HMAC(sharedSecret, timestamp)` , where timestamp changes every 30 seconds. The shared secret is often provisioned as a QR-code or preprogrammed into a hardware token.

Websites with TOTP support

The website twofactorauth.org (https://twofactorauth.org) lists common websites that supports TOTP.

HOTP

HOTP works just like TOTP, except that an authentication counter is used instead of a timestamp. The advantage of this is that HOTP devices requires no clock.

HOTP is susceptible to losing counter sync. That is, if the user generates an OTP without authenticating with it, the device counter will no longer match the server counter. This can be mitigated on the server by testing several subequent counter values. This can not happen with Yubico OTP (/OTP) since its counter is encrypted (as opposed to hashed).

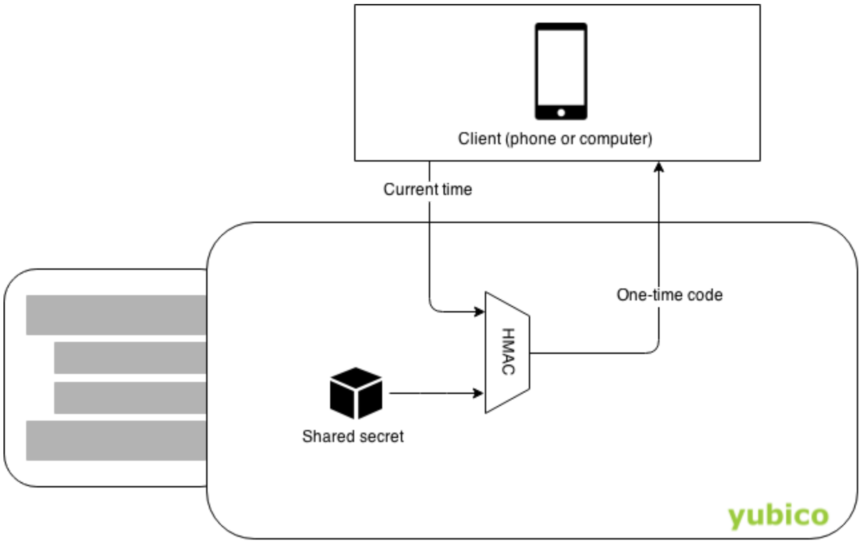
Use OATH with the YubiKey

When using OATH with a YubiKey, the shared secrets are stored and processed in the YubiKey's secure element. This has two advantages over storing secrets on a phone:

Security
The secrets always stay within the YubiKey. A phone can get stolen, sold, infected by malware, have its storage read by a connected computer, etc.

Accessibility
You can display OATH codes on more than one phone or computer. If your phone runs out of battery, you can get a code using a friend's phone or your computer.

A YubiKey can emit a HOTP code when its button is pressed. This is configured using Yubikey Personalization GUI (/yubikey-personalization-gui). For TOTP you need an application that can read OATH codes from YubiKeys (YubiKey_OATH_software.html), since YubiKeys does not have an internal clock.



DEV.YUBICO (https://developers.yubico.com/)

OTP (/OTP)

U2F (/U2F)

OATH (/OATH)

PGP (/PGP)

PIV (/PIV)

YubiHSM2 (/YubiHSM2)

Software Projects (/Software_Projects)

RESOURCES

Buy YubiKeys (https://store.yubico.com/)

Blog (https://www.yubico.com/blog/)

Newsletter (https://www.yubico.com/newsletter/)

Yubico Forum (http://forum.yubico.com/)

YUBICO.COM (https://www.yubico.com/)

YubiKey for Businesses (https://www.yubico.com/why-yubico/for-businesses/)

YubiKey for Individuals (https://www.yubico.com/why-yubico/for-individuals/)

What is a YubiKey? (https://www.yubico.com/faq/yubikey/)

About Yubico (https://www.yubico.com/about/)

co) (https://plus.google.com/114531431015898699937) (https://www.facebook.com/Yubikey) (https://www.youtube.com/c/Yubico) (https://github.com/Yubico)