The **Time-based One-time Password algorithm** (**TOTP**) is an extension of the [HMAC-based One-time Password algorithm](https://en.wikipedia.org/wiki/HMAC-based_One-time_Password_algorithm) (HOTP) that generates a [one-time password](https://en.wikipedia.org/wiki/One-time_password) (OTP) by instead taking uniqueness from the current time. It has been adopted as [Internet Engineering Task Force](https://en.wikipedia.org/wiki/Internet_Engineering_Task_Force) (IETF)[[1]](https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm#cite_note-RFC6238-1) standard [RFC 6238](https://tools.ietf.org/html/rfc6238),[[1]](https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm#cite_note-RFC6238-1) is the cornerstone of [Initiative for Open Authentication](https://en.wikipedia.org/wiki/Initiative_for_Open_Authentication) (OATH), and is used in a number of [two-factor authentication](https://en.wikipedia.org/wiki/Two-factor_authentication) (2FA) systems.

Because of [latency](https://en.wikipedia.org/wiki/Latency_(engineering)), both network and human, and [unsynchronised clocks](https://en.wikipedia.org/wiki/Clock_synchronisation), the one-time password must validate over a range of times between the [authenticator](https://en.wikipedia.org/wiki/Authenticator) and the authenticatee. Here, time is downsampled into larger durations (e.g., 30 seconds) to allow for validity between the parties.

Algorithm[[edit](https://en.wikipedia.org/w/index.php?title=Time-based_One-time_Password_algorithm&action=edit&section=1)]

|  |  |
| --- | --- |
|  | This section **does not**[**cite**](https://en.wikipedia.org/wiki/Wikipedia:Citing_sources)**any**[**sources**](https://en.wikipedia.org/wiki/Wikipedia:Verifiability). Please help [improve this section](https://en.wikipedia.org/w/index.php?title=Time-based_One-time_Password_algorithm&action=edit) by [adding citations to reliable sources](https://en.wikipedia.org/wiki/Help:Referencing_for_beginners). Unsourced material may be challenged and [removed](https://en.wikipedia.org/wiki/Wikipedia:Verifiability#Burden_of_evidence). *(August 2020) (*[*Learn how and when to remove this template message*](https://en.wikipedia.org/wiki/Help:Maintenance_template_removal)*)* |

To establish TOTP authentication, the authenticatee and authenticator must pre-establish both the [HOTP parameters](https://en.wikipedia.org/wiki/HMAC-based_One-time_Password_algorithm#parameters) and the following TOTP parameters:

* *T*0, the [Unix time](https://en.wikipedia.org/wiki/Unix_time) from which to start counting time steps (default is 0)
* *TX*, an interval which will be used to calculate the value of the counter *CT* (default is 30 seconds)

Both the authenticator and the authenticatee compute the TOTP value, then the authenticator checks if the TOTP value supplied by the authenticatee matches the locally generated TOTP value. Some authenticators allow values that should have been generated before or after the current time in order to account for slight [clock skews](https://en.wikipedia.org/wiki/Clock_skew), network latency and user delays.

**TOTP value**[[edit](https://en.wikipedia.org/w/index.php?title=Time-based_One-time_Password_algorithm&action=edit&section=2)]

TOTP uses the HOTP algorithm, substituting the counter with a [non-decreasing](https://en.wikipedia.org/wiki/Increasing) value based on the current time.

TOTP value(*K*) = [HOTP value](https://en.wikipedia.org/wiki/HMAC-based_One-time_Password_Algorithm#Definition)(*K*, *CT*)

**Calculating counter value**

{\displaystyle C\_{T}=\left\lfloor {\frac {T-T\_{0}}{T\_{X}}}\right\rfloor }

|  |  |  |
| --- | --- | --- |
| *CT* | Count of the number of durations *TX* between *T*0 and *T* | *integer* |
| *T* | Current time or [Unix time](https://en.wikipedia.org/wiki/Unix_time) | *integer* |
| *T*0 | some epoch (eg. Unix epoch is 0) | *integer* |
| *TX* | length of one time duration (eg 30 seconds) | *integer* |

Note that Unix time is not strictly increasing. When a [leap second](https://en.wikipedia.org/wiki/Leap_second) is inserted into UTC, Unix time repeats one second. But a single leap second does not cause the [integer part](https://en.wikipedia.org/wiki/Floor_function) of Unix time to decrease, and *CT* is non-decreasing as well so long as *TX* is a multiple of one second.

Practical considerations[[edit](https://en.wikipedia.org/w/index.php?title=Time-based_One-time_Password_algorithm&action=edit&section=3)]

For subsequent authentications to work, the clocks of the authenticatee and the authenticator need to be roughly synchronized (the authenticator will typically accept one-time passwords generated from timestamps that differ by ±1 time interval from the authenticatee's timestamp).[[1]](https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm#cite_note-RFC6238-1)

Weaknesses and vulnerabilities[[edit](https://en.wikipedia.org/w/index.php?title=Time-based_One-time_Password_algorithm&action=edit&section=4)]

TOTP values can be phished like passwords, though this requires attackers to proxy the credentials in real time.[[2]](https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm#cite_note-2)

An attacker who steals the shared secret can generate new, valid TOTP values at will. This can be a particular problem if the attacker breaches a large authentication database.[[3]](https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm#cite_note-3)

TOTP values are typically valid for longer than 30 seconds so that client and server time delays are accounted for.[[1]](https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm#cite_note-RFC6238-1)

History[[edit](https://en.wikipedia.org/w/index.php?title=Time-based_One-time_Password_algorithm&action=edit&section=5)]

A TOTP draft was developed through the collaboration of several OATH members in order to create an industry-backed standard. It complements the event-based one-time standard HOTP, and it offers end user organizations and enterprises more choice in selecting technologies that best fit their application requirements and security guidelines. In 2008, OATH submitted a draft version of the specification to the IETF. This version incorporates all the feedback and commentary that the authors received from the technical community based on the prior versions submitted to the IETF.[[4]](https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm#cite_note-4) In May, 2011, TOTP officially became [RFC](https://en.wikipedia.org/wiki/Request_for_Comments) 6238.[[1]](https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm#cite_note-RFC6238-1)

See also[[edit](https://en.wikipedia.org/w/index.php?title=Time-based_One-time_Password_algorithm&action=edit&section=6)]

* [Botan](https://en.wikipedia.org/wiki/Botan_(programming_library)), C++ cryptography library with HOTP/TOTP support
* [FreeOTP](https://en.wikipedia.org/wiki/FreeOTP), an open-source software that implements HOTP and TOTP for two-factor authentication (2FA)
* [multiOTP](https://en.wikipedia.org/wiki/MultiOTP), open-source PHP programming library that implements several OTP algorithms

References[[edit](https://en.wikipedia.org/w/index.php?title=Time-based_One-time_Password_algorithm&action=edit&section=7)]

* 1. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm#cite_ref-RFC6238_1-0) [***b***](https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm#cite_ref-RFC6238_1-1) [***c***](https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm#cite_ref-RFC6238_1-2) [***d***](https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm#cite_ref-RFC6238_1-3) [***e***](https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm#cite_ref-RFC6238_1-4) [*"RFC 6238 – TOTP: Time-Based One-Time Password Algorithm"*](https://tools.ietf.org/html/rfc6238)*. Retrieved July 13, 2011.*
  2. [**^**](https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm#cite_ref-2) *Umawing, Jovi (21 January 2019).*[*"Has two-factor authentication been defeated? A spotlight on 2FA's latest challenge"*](https://blog.malwarebytes.com/cybercrime/2019/01/two-factor-authentication-defeated-spotlight-2fas-latest-challenge/)*. Malwarebytes Labs. Retrieved 9 August 2020.*
  3. [**^**](https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm#cite_ref-3) *Zetter, Kim.*[*"RSA Agrees to Replace Security Tokens After Admitting Compromise"*](https://www.wired.com/2011/06/rsa-replaces-securid-tokens/)*. WIRED. Retrieved 17 February 2017.*
  4. [**^**](https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm#cite_ref-4) *Alexander, Madison.*[*"OATH Submits TOTP: Time-Based One Time Password Specification to IETF"*](http://www.openauthentication.org/news/20080408)*. Open Authentication. Retrieved 22 February 2010.*

External links[[edit](https://en.wikipedia.org/w/index.php?title=Time-based_One-time_Password_algorithm&action=edit&section=8)]

* [Step by step Python implementation in a Jupyter Notebook](https://nbviewer.jupyter.org/github/algorithmic-space/cryptoy/blob/master/rfc6238.ipynb)
* [Designing Docker Hub Two-Factor Authentication](https://www.docker.com/blog/designing-docker-hub-2fa/), (section "Using Time-Based One-Time Password (TOTP) Authentication").