**SQRL** (pronounced "squirrel")[[3]](https://en.wikipedia.org/wiki/SQRL#cite_note-grc-3) or **Secure, Quick, Reliable Login** (formerly **Secure QR Login**) is a [draft](https://en.wikipedia.org/wiki/Draft_document) [open standard](https://en.wikipedia.org/wiki/Open_standard) for secure [website](https://en.wikipedia.org/wiki/Website) [login](https://en.wikipedia.org/wiki/Login) and [authentication](https://en.wikipedia.org/wiki/Authentication). The [software](https://en.wikipedia.org/wiki/Computer_software) typically uses a [link of the scheme](https://en.wikipedia.org/wiki/Uniform_Resource_Identifier) sqrl:// or optionally a [QR code](https://en.wikipedia.org/wiki/QR_code), where a user identifies via a [pseudonymous](https://en.wikipedia.org/wiki/Pseudonymous) [zero-knowledge proof](https://en.wikipedia.org/wiki/Zero-knowledge_proof) rather than providing a [user ID](https://en.wikipedia.org/wiki/User_ID) and [password](https://en.wikipedia.org/wiki/Password). This method is thought to be impervious to a [brute force](https://en.wikipedia.org/wiki/Brute-force_attack) password attack or [data breach](https://en.wikipedia.org/wiki/Data_breach). It shifts the burden of security away from the party requesting the authentication and closer to the operating system [implementation](https://en.wikipedia.org/wiki/Implementation_(computing)) of what is possible on the [hardware](https://en.wikipedia.org/wiki/Computer_hardware), as well as to the user. SQRL was proposed by [Steve Gibson](https://en.wikipedia.org/wiki/Steve_Gibson_(computer_programmer)) of Gibson Research Corporation in October 2013 as a way to simplify the process of [authentication](https://en.wikipedia.org/wiki/Authentication_protocol) without the risk of revelation of information about the transaction to a [third party](https://en.wikipedia.org/wiki/Third-party_verification).

History[[edit](https://en.wikipedia.org/w/index.php?title=SQRL&action=edit&section=1)]

The [acronym](https://en.wikipedia.org/wiki/Acronym) SQRL was coined by Steve Gibson and the protocol drafted, discussed and analyzed in-depth, by himself and a community of [Internet security](https://en.wikipedia.org/wiki/Internet_security) [enthusiasts](https://en.wikipedia.org/wiki/Enthusiasts) on the news.grc.com [newsgroups](https://en.wikipedia.org/wiki/Newsgroups) and during his weekly [podcast](https://en.wikipedia.org/wiki/Podcast), [*Security Now!*](https://en.wikipedia.org/wiki/Security_Now), on October 2, 2013. Within two days of the airing of this podcast, the [W3C](https://en.wikipedia.org/wiki/W3C) expressed interest in working on the standard.[[4]](https://en.wikipedia.org/wiki/SQRL#cite_note-4) Ian Maddox and Kyle Moschetto, [Google](https://en.wikipedia.org/wiki/Google) Cloud Solutions Architects mention SQRL in their document "Modern password security for system designers".[[5]](https://en.wikipedia.org/wiki/SQRL#cite_note-5)

A thesis on SQRL analyzed and found that "it appears to be an interesting approach, both in terms of the envisioned user experience as well as the underlying cryptography. SQRL is mostly combining well established cryptography in a novel way."[[6]](https://en.wikipedia.org/wiki/SQRL#cite_note-6)

Benefits[[edit](https://en.wikipedia.org/w/index.php?title=SQRL&action=edit&section=2)]

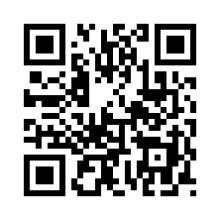
The protocol is an answer to a problem of [identity](https://en.wikipedia.org/wiki/Online_identity) [fragmentation](https://en.wikipedia.org/wiki/Fragmentation_(programming)). It improves on protocols such as [OAuth](https://en.wikipedia.org/wiki/OAuth) and [OpenID](https://en.wikipedia.org/wiki/OpenID) by not requiring a [third party](https://en.wikipedia.org/wiki/Third-party_verification) to broker the transaction, and by not giving a server any secrets to protect, such as username and password.

Additionally, it provides a standard that can be freely used to simplify the login processes available to [password manager](https://en.wikipedia.org/wiki/Password_manager) applications. More importantly the standard is open so no one company can benefit from owning the technology. According to Gibson's website,[[7]](https://en.wikipedia.org/wiki/SQRL#cite_note-7) such a robust technology should be in the public domain so the security and cryptography can be verified, and not deliberately restricted for commercial or other reasons.

**Phishing protections**[[edit](https://en.wikipedia.org/w/index.php?title=SQRL&action=edit&section=3)]

SQRL has some design-inherent and intentional [phishing](https://en.wikipedia.org/wiki/Phishing) defenses,[[8]](https://en.wikipedia.org/wiki/SQRL#cite_note-8) but it is mainly intended to be for authentication, not anti-phishing, despite having some anti-phishing properties.[[9]](https://en.wikipedia.org/wiki/SQRL#cite_note-9)

Example use case[[edit](https://en.wikipedia.org/w/index.php?title=SQRL&action=edit&section=4)]

[](https://en.wikipedia.org/wiki/File:QR_code_for_mobile_English_Wikipedia.svg)

Example of a SQRL-URL / QR-code, which could be clicked, tapped, or scanned for website authentication.

For the protocol to be used on a website, two components are necessary: an [implementation](https://en.wikipedia.org/wiki/Implementation), that is part of the [Web service](https://en.wikipedia.org/wiki/Web_service) to which the implementation authenticates, which displays a [QR code](https://en.wikipedia.org/wiki/QR_code) or specially crafted [URL](https://en.wikipedia.org/wiki/URL) according to the [specifications](https://en.wikipedia.org/wiki/Specifications) of the protocol, and a [browser plugin](https://en.wikipedia.org/wiki/Browser_plugin) or a [mobile application](https://en.wikipedia.org/wiki/Mobile_application), which can read this code in order to provide secure authentication.

The SQRL client uses ["one-way" functions](https://en.wikipedia.org/wiki/One-way_function) and the user's single master password to decrypt a secret master key, from which it generates in combination with the site name (comprising the domain name and optionally an additional sub-site identifier: "example.com", "example.edu/chessclub") a (sub-)site-specific public/private key pair. It signs the [transaction tokens](https://en.wikipedia.org/wiki/Authentication_token) with the private key and gives the public key to the site, so it can verify the encrypted data.

There are no "shared secrets" which a compromise of the site could expose to allow attacks on accounts at other sites. The only thing a successful attacker could get, the public key, would be limited to verifying signatures that are only used at the same site. Even though the user unlocks the master key with a single password, it never leaves the SQRL client; the individual sites do not receive any information from the SQRL process that could be used at any other site.

SQRL implementations[[edit](https://en.wikipedia.org/w/index.php?title=SQRL&action=edit&section=5)]

A number of [proof-of-concept](https://en.wikipedia.org/wiki/Proof-of-concept) implementations have been made for various platforms, including for the server ([PHP](https://en.wikipedia.org/wiki/PHP),[[10]](https://en.wikipedia.org/wiki/SQRL#cite_note-10) [Drupal](https://en.wikipedia.org/wiki/Drupal),[[11]](https://en.wikipedia.org/wiki/SQRL#cite_note-11), and [C# .NET](https://en.wikipedia.org/wiki/C_Sharp_(programming_language))[[12]](https://en.wikipedia.org/wiki/SQRL#cite_note-12)[[13]](https://en.wikipedia.org/wiki/SQRL#cite_note-13)) and for the client ([Android](https://en.wikipedia.org/wiki/Android_(operating_system)),[[14]](https://en.wikipedia.org/wiki/SQRL#cite_note-14)[[15]](https://en.wikipedia.org/wiki/SQRL#cite_note-15)[[16]](https://en.wikipedia.org/wiki/SQRL#cite_note-16) [C# .NET](https://en.wikipedia.org/wiki/C_Sharp_(programming_language)),[[17]](https://en.wikipedia.org/wiki/SQRL#cite_note-17) [Java](https://en.wikipedia.org/wiki/Java_(programming_language)) [[18]](https://en.wikipedia.org/wiki/SQRL#cite_note-18), and [Python](https://en.wikipedia.org/wiki/Python_(programming_language))[[19]](https://en.wikipedia.org/wiki/SQRL#cite_note-19)). There are also various server-end test and debugging sites available.[[20]](https://en.wikipedia.org/wiki/SQRL#cite_note-20)[[21]](https://en.wikipedia.org/wiki/SQRL#cite_note-21)[[22]](https://en.wikipedia.org/wiki/SQRL#cite_note-22)[[23]](https://en.wikipedia.org/wiki/SQRL#cite_note-23)

Legal aspects[[edit](https://en.wikipedia.org/w/index.php?title=SQRL&action=edit&section=6)]

|  |  |
| --- | --- |
|  | This article **may rely excessively on sources**[**too closely associated with the subject**](https://en.wikipedia.org/wiki/Wikipedia:Verifiability#Self-published_sources), potentially preventing the article from being [verifiable](https://en.wikipedia.org/wiki/Wikipedia:Verifiability) and [neutral](https://en.wikipedia.org/wiki/Wikipedia:Neutral_point_of_view). Please help [improve it](https://en.wikipedia.org/w/index.php?title=SQRL&action=edit) by replacing them with more appropriate [citations](https://en.wikipedia.org/wiki/Wikipedia:Citing_sources) to [reliable, independent, third-party sources](https://en.wikipedia.org/wiki/Wikipedia:Identifying_and_using_independent_sources). *(August 2019) (*[*Learn how and when to remove this template message*](https://en.wikipedia.org/wiki/Help:Maintenance_template_removal)*)* |

Steve Gibson states that SQRL is "open and free as it should be", and that the solution is "unencumbered by patents".[[3]](https://en.wikipedia.org/wiki/SQRL#cite_note-grc-3) While SQRL brought a lot of attention to QR code based authentication mechanisms, the suggested protocol is said to have been patented earlier and is not generally available for royalty free use.[[24]](https://en.wikipedia.org/wiki/SQRL#cite_note-24) But Gibson says "What those guys are doing as described in that patent[[25]](https://en.wikipedia.org/wiki/SQRL#cite_note-patents-25) is completely different from the way SQRL operates, so there would be no conflict between SQRL and their patent. Superficially, anything that uses a 2D code for authentication seems "similar"... and superficially all such solutions are. But the details matter, and the way SQRL operates is entirely different in the details."[[26]](https://en.wikipedia.org/wiki/SQRL#cite_note-26)

See also[[edit](https://en.wikipedia.org/w/index.php?title=SQRL&action=edit&section=7)]

* [BrowserID](https://en.wikipedia.org/wiki/BrowserID)
* [Central Authentication Service](https://en.wikipedia.org/wiki/Central_Authentication_Service)
* [Information Card](https://en.wikipedia.org/wiki/Information_Card)
* [Light-Weight Identity](https://en.wikipedia.org/wiki/Light-Weight_Identity)
* [OAuth](https://en.wikipedia.org/wiki/OAuth)
* [OpenID Connect](https://en.wikipedia.org/wiki/OpenID_Connect)
* [Single sign-on](https://en.wikipedia.org/wiki/Single_sign-on)
* [WebID](https://en.wikipedia.org/wiki/WebID)
* [FIDO Alliance](https://en.wikipedia.org/wiki/FIDO_Alliance)

References[[edit](https://en.wikipedia.org/w/index.php?title=SQRL&action=edit&section=8)]

* 1. [**^**](https://en.wikipedia.org/wiki/SQRL#cite_ref-1) [*"SQRL Translations"*](https://crowdin.com/project/sqrl)*. crowdin.com. Retrieved 16 July 2015.*
  2. [**^**](https://en.wikipedia.org/wiki/SQRL#cite_ref-2) [Secure Quick Reliable Login](https://www.grc.com/sqrl/sqrl.htm) on www.grc.com/sqrl *"Open & free, as it should be: The component techniques and technologies employed by this solution are all well known, well tested, well understood, unencumbered by patents, and exist in the public domain. [...] With this publication of every detail, I hereby release and disclaim any and all proprietary rights to any new ideas developed and presented herein. This work is thereby added to the public domain."*
  3. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/SQRL#cite_ref-grc_3-0) [***b***](https://en.wikipedia.org/wiki/SQRL#cite_ref-grc_3-1) [*"SQRL / Gibson Research"*](https://www.grc.com/sqrl/sqrl.htm)*. grc.com. Retrieved 2014-05-12.*
  4. [**^**](https://en.wikipedia.org/wiki/SQRL#cite_ref-4) [*"Security Now! #425 SQRL Q&A #176 (Transcript)"*](https://www.grc.com/sn/sn-425.txt)*. 2013-10-09. Retrieved 2013-10-16.*
  5. [**^**](https://en.wikipedia.org/wiki/SQRL#cite_ref-5) [*"Modern password security for system designers"*](https://cloud.google.com/solutions/modern-password-security-for-system-designers.pdf)*(PDF).*
  6. [**^**](https://en.wikipedia.org/wiki/SQRL#cite_ref-6) [*"Security Analysis and Implementation of the SQRL Authentication Scheme"*](https://web.archive.org/web/20150402182457/https:/www.sec.in.tum.de/finished-work/publication/318)*. Archived from*[*the original*](https://www.sec.in.tum.de/finished-work/publication/318)*on 2015-04-02. Retrieved 2015-03-18.*[[*dead link*](https://en.wikipedia.org/wiki/Wikipedia:Link_rot)]
  7. [**^**](https://en.wikipedia.org/wiki/SQRL#cite_ref-7) [*"GRC's SQRL Secure Quick Reliable Login"*](https://www.grc.com/sqrl/sqrl.htm)*. www.grc.com. Retrieved 2016-06-02.*
  8. [**^**](https://en.wikipedia.org/wiki/SQRL#cite_ref-8) *Gibson, Steve (2014). DigiCert Security Summit (ed.).*[*"Revolutionizing Website Login and Authentication with SQRL"*](https://vimeo.com/112444120)*. Vimeo.*
  9. [**^**](https://en.wikipedia.org/wiki/SQRL#cite_ref-9) [*"Details about phishing defenses and limitations"*](https://www.grc.com/sqrl/phishing.htm)*. grc.com. 2013-12-06. Retrieved 2013-12-06.*
  10. [**^**](https://en.wikipedia.org/wiki/SQRL#cite_ref-10) <https://github.com/trianglman/sqrl>
  11. [**^**](https://en.wikipedia.org/wiki/SQRL#cite_ref-11) <https://www.drupal.org/project/sqrl>
  12. [**^**](https://en.wikipedia.org/wiki/SQRL#cite_ref-12) <https://github.com/jestin/SqrlNet>
  13. [**^**](https://en.wikipedia.org/wiki/SQRL#cite_ref-13) <https://github.com/TechLiam/SQRL-For-Dot-Net-Standard>
  14. [**^**](https://en.wikipedia.org/wiki/SQRL#cite_ref-14) <https://github.com/geir54/android-sqrl>
  15. [**^**](https://en.wikipedia.org/wiki/SQRL#cite_ref-15) [*"Archived copy"*](https://web.archive.org/web/20150402132412/https:/www.paulstechtalk.com/2014/12/sqrl-implementations-on-android-and-it-works/)*. Archived from*[*the original*](https://www.paulstechtalk.com/2014/12/sqrl-implementations-on-android-and-it-works/)*on 2015-04-02. Retrieved 2015-03-17.*
  16. [**^**](https://en.wikipedia.org/wiki/SQRL#cite_ref-16) <https://play.google.com/store/apps/details?id=net.vrallev.android.sqrl>
  17. [**^**](https://en.wikipedia.org/wiki/SQRL#cite_ref-17) <https://github.com/jestin/SqrlNet>
  18. [**^**](https://en.wikipedia.org/wiki/SQRL#cite_ref-18) [[1]](https://archive.today/20150317214235/https:/github.com/TheBigS/SQRL)
  19. [**^**](https://en.wikipedia.org/wiki/SQRL#cite_ref-19) <https://github.com/bushxnyc/sqrl>
  20. [**^**](https://en.wikipedia.org/wiki/SQRL#cite_ref-20) <https://www.grc.com/sqrl/demo.htm>
  21. [**^**](https://en.wikipedia.org/wiki/SQRL#cite_ref-21) <https://www.grc.com/sqrl/diag.htm>
  22. [**^**](https://en.wikipedia.org/wiki/SQRL#cite_ref-22) [https://sqrl-test.paragon-es.de](https://sqrl-test.paragon-es.de/) [Archived](https://web.archive.org/web/20150402131033/https:/sqrl-test.paragon-es.de/) 2015-04-02 at the [Wayback Machine](https://en.wikipedia.org/wiki/Wayback_Machine)
  23. [**^**](https://en.wikipedia.org/wiki/SQRL#cite_ref-23) [http://sw.squaltech.com:8080](http://sw.squaltech.com:8080/) [Archived](https://web.archive.org/web/20150316131413/http:/sw.squaltech.com:8080/) 2015-03-16 at the [Wayback Machine](https://en.wikipedia.org/wiki/Wayback_Machine)
  24. [**^**](https://en.wikipedia.org/wiki/SQRL#cite_ref-24) [*"SQRL is not really new"*](http://www.michael.beiter.org/2013/10/04/steve-gibsons-sqrl-is-not-really-new/)*. Mike Beiter. October 4, 2013. Retrieved 2014-05-12.*
  25. [**^**](https://en.wikipedia.org/wiki/SQRL#cite_ref-patents_25-0) [Method and system for authenticating a user by means of a mobile device US 20100070759 A1](https://www.google.com/patents/US20100070759)
  26. [**^**](https://en.wikipedia.org/wiki/SQRL#cite_ref-26) [*"Secure Quick Reliable Login"*](https://www.grc.com/sqrl/other.htm)*. grc.com. Retrieved 22 September 2015.*