Network Working Group
Internet-Draft
Intended status: Informational
Expires: 21 August 2025

I. Y. Eroglu
independent

17 February 2025

Usage specification of the otpauth URI format for TOTP and HOTP token generators
draft-linuxgemini-otpauth-uri-02

Abstract

This document describes a foundational schema for the otpauth URI, utilized by TOTP (and/or HOTP) based authenticators.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 21 August 2025.

Table of Contents

1. Discussion 2
2. Introduction 2
2.1. Conventions and Terminology 3
3. Syntax 3
3.1. TYPE entry (REQUIRED) 4
3.2. LABEL entry (REQUIRED) 4
3.3. PARAMETERS entry (REQUIRED) 5
3.3.1. secret parameter (REQUIRED) 5
3.3.2. algorithm parameter (OPTIONAL) 5
3.3.3. digits parameter (OPTIONAL) 5
3.3.4. counter parameter (REQUIRED if HOTP) 5
3.3.5. period parameter (OPTIONAL, only TOTP) 6
3.3.6. issuer parameter (OPTIONAL) 6
3.3.7. Other parameters (OPTIONAL) 6
4. Examples 6
5. Security Considerations 6
6. IANA Considerations 6
7. References 6
7.1. Normative References 6
7.2. Informative References 7
Appendix A. Acknowledgements 8
Appendix B. Document History 8
Author’s Address 8

1. Discussion

This note is to be removed before publishing as an RFC.

Source for this draft and an issue tracker can be found at https://github.com/linuxgemini/otpauth-spec-draft (https://github.com/linuxgemini/otpauth-spec-draft).

2. Introduction

The otpauth URI is used for easy addition of accounts to Time-Based One-Time Password (TOTP) and/or HMAC-based One-Time Password (HOTP) authenticators with various options [Google.Authenticator.OSS.Wiki.Key.Format].

Although available as a provisional scheme at IANA [IANA.URISchemes.Prov.otpauth], there are many deviations of the specification usage per authenticator hardware and software [Edent.Blog.Post].

This document aims to provide foundational boundaries for the URI format and standardize the secret sharing of One-Time Password (OTP) tokens.

2.1. Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

This specification uses the Augmented Backus-Naur Form (ABNF) notation of [RFC5234].

This specification uses terms "TOTP" defined by [RFC6238] and "HOTP" defined by [RFC4226]. Both RFCs also mention "secret", "issuer", and "account".

The term "URI" is imported from [RFC3986]. Mentions of "query string" in this document references the "Query" parameter (in section 3.4) of this RFC.

The Base16, Base32, and Base64 Data Encodings mentioned here are imported from [RFC4648] with the same name.

3. Syntax

The URI MUST be formatted like below:

otpauth://TYPE/LABEL?PARAMETERS

An approximate ABNF representation of this is like below:

```
otpauth-uri    = "otpauth://" uri-type "/" uri-label "?" uri-parameters
uri-type       = "totp" / "hotp"
uri-label      = *VCHAR
uri-parameters = "secret=" *base-32 [ *uri-opt-parameters ]

uri-opt-parameters =  ("&algorithm=" otp-algorithm)
uri-opt-parameters =/ ("&digits=" otp-digits)
uri-opt-parameters =/ ("&counter=" *DIGIT) / ("&period=" *DIGIT)
uri-opt-parameters =/ ("&issuer=" *VCHAR) / ("&" *VCHAR "=" *VCHAR)
                        ; Please refer to RFC3986 for handling
                        ; complex names

otp-algorithm = "SHA1" / "SHA256" / "SHA512"

otp-digits    = %x36-38
                ; 6-8

base-32 = %x41-5A / %x32-37
                ; A-Z2-7
DIGIT   = %x30-39
                ; 0-9
VCHAR   = %x21-7E
                ; visible (printing) characters
```

3.1. TYPE entry (REQUIRED)

The type entry MUST be one of totp or hotp, depending on the One-Time Password (OTP) type.

3.2. LABEL entry (REQUIRED)

The label entry MUST be an identifier representing the user. For example, can be a username, nickname or a person’s name.

The label entry MUST be considered as a Path per section 3.3. of [RFC3986].

Although the Authenticator Team at Google recommends including the secret issuer to be prepended to the label with the colon character (: or %3A) as a separator in [Google.Authenticator.OSS.Wiki.Key.Format], the authors of this document believe that the issuer should only be appended as a separate parameter (see next division).

3.3. PARAMETERS entry (REQUIRED)

This entry is a URI query string. Each parameter MUST be separated by the & character and SHOULD BE "URI Safe" (see section 2.2. Reserved Characters in [RFC3986]).

The following parameters SHOULD BE included:

3.3.1. secret parameter (REQUIRED)

The secret of the OTP MUST be provided within this parameter. The secret MUST be encoded in Base32. The padding specified in [RFC4648] section 3.2 is not required and SHOULD BE omitted.

For example:

otpauth://totp/ietfuser?secret=NBSWY3DPFQQHO33SNRSAU

3.3.2. algorithm parameter (OPTIONAL)

The algorithm used for TOTP or HOTP tokens SHOULD BE provided in this parameter. When not provided, SHA1 is assumed by default.

The ABNF representation is defined below:

otp-algorithm = "SHA1" / "SHA256" / "SHA512"

Some authenticators at the time of writing this document ignore this parameter. The authors of this document believe that this parameter MUST be supported in all cases.

3.3.3. digits parameter (OPTIONAL)

The number of digits in the output for TOTP or HOTP tokens SHOULD BE provided in this parameter. This value MUST be between 6 and 8. When not provided, 6 digits is assumed by default.

Some authenticators at the time of writing this document ignore this parameter. The authors of this document believe that this parameter MUST be supported in all cases.

3.3.4. counter parameter (REQUIRED if HOTP)

The provisioning counter for HOTP tokens MUST BE provided in this parameter.

This parameter is ignored if the token type is TOTP.

3.3.5. period parameter (OPTIONAL, only TOTP)

The refresh period (in seconds) for TOTP tokens SHOULD BE provided in this parameter. When not provided, 30 seconds is assumed by default.

Some authenticators at the time of writing this document ignore this parameter. The authors of this document believe that this parameter MUST BE supported in all cases.

This parameter is ignored if the token type is HOTP.

3.3.6. issuer parameter (OPTIONAL)

The issuer name of TOTP or HOTP tokens SHOULD BE provided in this parameter.

3.3.7. Other parameters (OPTIONAL)

Vendors MAY include other parameters in their issued otpauth URIs. These parameters are OPTIONAL for the function of TOTP or HOTP tokens and not necessary to be included in this document.

4. Examples

otpauth://totp/ietfuser?secret=NBSWY3DP

otpauth://hotp/13tfus3r?secret=NBSWY3DP&counter=192

otpauth://totp/big?issuer=IETF&secret=NBSWY3DP&period=5&algorithm=SHA256

5. Security Considerations

This URI format does not in itself pose a security threat. However, the Security Considerations of [RFC3986] SHOULD BE followed.

6. IANA Considerations

This format is already available as a provisional entry [IANA.URISchemes.Prov.otpauth]. IANA is asked to change the provisional URI scheme to reference [[this RFC]].

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <https://www.rfc-editor.org/info/rfc3986>.

[RFC4226] M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., and O. Ranen, "HOTP: An HMAC-Based One-Time Password Algorithm", RFC 4226, DOI 10.17487/RFC4226, December 2005, <https://www.rfc-editor.org/info/rfc4226>.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <https://www.rfc-editor.org/info/rfc4648>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <https://www.rfc-editor.org/info/rfc5234>.

[RFC6238] M'Raihi, D., Machani, S., Pei, M., and J. Rydell, "TOTP: Time-Based One-Time Password Algorithm", RFC 6238, DOI 10.17487/RFC6238, May 2011, <https://www.rfc-editor.org/info/rfc6238>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

7.2. Informative References

[Edent.Blog.Post] "Why is there no formal specification for otpauth URls?", <https://shkspr.mobi/blog/2022/05/why-is-there-no-formal-specification-for-otpauth-urls/>.

[Edent.Mastodon.Post] "Fediverse post for "Why is there no formal specification for otpauth URls?"", <https://mastodon.social/@Edent/108266107975107228>.

[Google.Authenticator.OSS.Wiki.Key.Format]
Google, "Google Authenticator Key Uri Format", <https://github.com/google/google-authenticator/wiki/Key-Uri-Format>.

[IANA.URISchemes.Prov.otpauth]
IANA, "Provisional scheme for the otpauth URI", <https://www.iana.org/assignments/uri-schemes/prov/otpauth>.

Appendix A. Acknowledgements

We would like to thank Q Misell, Terence Eden, The Google Authenticator Team at Google, Eugene Fox, Seonghyeon Cho, and others (please let us know, if you've been mistakenly omitted) for their valuable input, feedback and general support of this work.

This document originated from discussions at the Fediverse initially written by Terence Eden [Edent.Mastodon.Post].

Appendix B. Document History

[[To be removed from the final specification]]

-02

* various typo corrections
* various phrasing changes

-01

* corrected Terence's name
* corrected parameter confusion between TOTP and HOTP

-00

* first draft

Author's Address

Ilteris Yagiztegin Eroglu
independent
/Ankara
T端rkiye
Email: ietf@linuxgemini.space
URI: https://linuxgemini.space