Workgroup: Network Working Group
Internet-Draft:
draft-nottingham-how-did-that-get-into-the-repo-02
Published: 18 October 2020
Intended Status: Informational
Expires: 21 April 2021
Authors: M. Nottingham

The secret-token URI Scheme

Abstract

This document registers the "secret-token" URI scheme, to aid in the identification of authentication tokens.

Note to Readers

RFC EDITOR: please remove this section before publication

The issues list for this draft can be found at https://github.com/mnot/I-D/labels/how-did-that-get-into-the-repo.

The most recent (often, unpublished) draft is at https://mnot.github.io/I-D/how-did-that-get-into-the-repo/.

Recent changes are listed at https://github.com/mnot/I-D/commits/gh-pages/how-did-that-get-into-the-repo.

See also the draft's current status in the IETF datatracker, at https://datatracker.ietf.org/doc/draft-nottingham-how-did-that-get-into-the-repo/.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

It has become increasingly common to use bearer tokens as an authentication mechanism in various protocols.

A bearer token is a security token with the property that any party in possession of the token (a "bearer") can use the token in any way that any other party in possession of it can. Using a bearer token does not require a bearer to prove possession of cryptographic key material (proof-of-possession).

Unfortunately, the number of security incidents involving accidental disclosure of these tokens has also increased. For example, we now regularly hear about a developer committing an access token to a public source code repository, either because they didn't realise it was included in the committed code, or because they didn't realise the implications of its disclosure.

This specification registers the "secret-token" URI scheme to aid prevention of such accidental disclosures. When tokens are easier to unambiguously identify, they can trigger warnings in Continuous

Integration systems, or be used in source code repositories themselves. They can also be scanned for separately.

For example, if cloud.example.net issues access tokens to its clients for later use, and it does so by formatting them as secret-token URIs, tokens that "leak" into places that they don't belong are easier to identify. This could be through a variety of mechanisms; for example, if repo.example.com can be configured to refuse commits containing secret-token URIs, it helps its customers avoid accidental disclosures.

secret-token URIs are intended to aid in identification of generated secrets like API keys and similar tokens. They are not intended for use in controlled situations where ephemeral tokens are used, such as things like Cross-Site Request Forgery (CSRF) tokens.

1.1. Notational Conventions

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 document uses ABNF [RFC5234]. It also uses the pchar rule from [RFC3986].

2. The secret-token URI scheme

The secret-token URI scheme identifies a token that is intended to be a secret.

```
secret-token-URI    = secret-token-scheme ":" token
secret-token-scheme = "secret-token"
token               = 1*pchar
```

See [RFC3986], Section 3.3 for a definition of pchar. Disallowed characters - including non-ASCII characters - MUST be encoded into UTF-8 [RFC3629] and then percent-encoded ([RFC3986], Section 2.1).

When a token is both generated and presented for authentication, the entire URI MUST be used, without changes.

For example, given the URI:

```
secret-token:E92FB7EB-D882-47A4-A265-A0B6135DC842%20foo
```

This string (character-for-character, case-sensitive) will both be issued by the token authority, and required for later access.

Therefore, if the example above were used as a bearer token in [RFC6750], a client might send:

```
GET /authenticated/stuff HTTP/1.1
Host: www.example.com
Authorization: Bearer secret-token:E92FB7EB-D882-47A4-A265-A0B6135DC842%
```

3. IANA Considerations

This document registers the following value in the URI Scheme registry:

- *Scheme name: secret-token

- *Status: provisional

- *Applications / protocols that use this scheme: none yet

- *Contact: iesg@iesg.org

- *Change Controller: IESG

- *References: (this document)

4. Security Considerations

The token ABNF rule allows tokens as small as one character. This is not recommended practice; applications should evaluate their requirements for entropy and issue tokens correspondingly. See [RFC4086] for more information.

This URI scheme is intended to reduce the incidence of accidental disclosure; it cannot prevent intentional disclosure.

If it is difficult to correctly handle secret material, or unclear as to what the appropriate handling is, users might choose to obfuscate their secret tokens in order to evade detection (for example, removing the URI scheme for storage). Mitigating this risk is often beyond the reach of the system using the secret-token URI, but they can caution users against such practices, and provide tools to help.

5. References

5.1. 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>.

[RFC3629]
Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, DOI 10.17487/RFC3629, November 2003, <https://www.rfc-editor.org/info/rfc3629>.

[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>.

[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>.

[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>.

5.2. Informative References

[RFC4086] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, DOI 10.17487/RFC4086, June 2005, <https://www.rfc-editor.org/info/rfc4086>.

[RFC6750] Jones, M. and D. Hardt, "The OAuth 2.0 Authorization Framework: Bearer Token Usage", RFC 6750, DOI 10.17487/RFC6750, October 2012, <https://www.rfc-editor.org/info/rfc6750>.

Appendix A. Acknowledgements

The definition of bearer tokens is from [RFC6750].

Author's Address

Mark Nottingham
Prahran VIC
Australia

Email: mnot@mnot.net
URI: https://www.mnot.net/