Network Working Group F. Brezo
Internet-Draft Y. Rubio
Intended status: Informational Telefonica
Expires: June 6, 2019 December 03, 2018

A Method for Deactivation and Deletion Policies
draft-brezorubio-wg-oblivion-00

Abstract

The existing methods for opting out or asking for users data stored by a service are far from being standard. This fact makes the process of deactivating or deleting an account from a website difficult to find since each platform provides the link in a different way. This document defines a standard ("oblivion.txt") to help organizations to describe the steps to follow by a user for deactivating or deleting an account from their websites as well as shipping the personal data linked to its users in a secure and standard way.

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 June 6, 2019.

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

1. Introduction

1.1. Motivation and Previous Work

Many of the standard interaction of end users with online services involve creating and managing personal accounts. Even when the creation of these accounts may seem easy to control, generally, the deletion and deactivation of an account does not fulfill with any type of standards making each experience look differently. Regarding this issue, there has been efforts to list the procedures followed by different platforms to conduct this task. For example, the project JustDelete.me shows a list of direct links to deletion URLs on different platforms. However, this process is mainly curated by contributors, which is an approach that does not scale well.

Similarly, the processes of requesting all the personal data stored by a service or even the management of the consents collected by it usually involve manual interactions withnon-standarized systems. These processes, enforced by law in many countries, are no longer easy to identify by the end user, hindering the exercise of rights inherent to the citizens.

In this document, we define a machine-readable and extensible way of communicating how users can interact with a service to deactivate their accounts or fully deleting them. This standard is thought to assist companies on providing a transparent and reachable way of giving access to their opt-out procedures so as to give back to the users the right to keep control of their own digital footprint.

1.2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119 [RFC2119].

2. The Specification

This standard defines a text file to be placed in a known location that provides information for users and applications to assist them in the process of finding the tools to delete or remove accounts and services.

The file is named "oblivion.txt", and this file SHOULD be placed under the Well-Known path ("/.well-known/oblivion.txt") [RFC5785] of a domain name or IP address for web properties. If it is not possible to place the "oblivion.txt" file in the Well-Known path or setup a redirect, web-based services MAY place the file in the top-level path of a given web domain or IP address ("/oblivion.txt") as a fall back option. For web-based services, the instructions MUST be accessible via the Hypertext Transfer Protocol [RFC1945] as a resource of Internet Media Type "text/plain" with the default charset parameter set to "utf-8" per section 4.1.3 of [RFC2046]. For file systems and version control repositories an ".oblivion.txt" file SHOULD be placed in the root directory of a particular file system or source code project.

This text file contains multiple directives with different values. The "directive" is the first part of a field all the way up to the colon ("Contact:"). Directives MUST be case-insensitive. The "value" comes after the directive ("https://example.com/oblivion"). A "field" MUST alway consist of a directive and a value ("Contact: https://example.com/oblivion"). An "oblivion.txt" file can have an unlimited number of fields. It is important to note that you MUST have a separate line for every field. One MUST NOT chain multiple values for a single directive and everything MUST be in a separate field. Unless otherwise indicated in a definition of a particular field, any directive MAY appear multiple times.

2.1. Scope

An "oblivion.txt" file MUST apply to the domain in the URI used to retrieve it and to any of its subdomains or parent domains. However, an "oblivion.txt" file that is found in a file system or version control repository MUST only apply to the folder or repository in which it is located, and not to any of its parent or sibling folders, or repositories.

Some examples appear below:

The following only applies to example.com and subdomain.example.com

https://example.com/.well-known/oblivion.txt

This only applies to subdomain.example.com but not to example.com

https://subdomain.example.com/.well-known/oblivion.txt

This oblivion.txt file applies to IPv4 address of 192.0.2.0.

http://192.0.2.0/.well-known/oblivion.txt

```
# This oblivion.txt file applies to IPv6 address of 2001:db8:8:4::2.

http://[2001:db8:8:4::2]/.well-known/oblivion.txt

# This oblivion.txt file applies to the /example/folder1 directory.

/example/folder1/oblivion.txt
```

2.2. Comments

Any line beginning with the "#" (%x30) symbol MUST be interpreted as a comment.

Example:

```
# This is a comment.
```

You MAY use one or more comments as descriptive text immediately before the field. Parsers SHOULD associate the comments with the respective field.

2.3. Separate Fields

A separate line is REQUIRED for every new value and field. You MUST NOT chain everything into a single field. Every line MUST end either with a carriage return and line feed characters (CRLF / %x0D %x0A) or just a line feed character (LF / %x0A).

2.4. Field Definitions

2.4.1. Claim

The "Claim" directive is used for linking to the process of claiming the delivery of all the data stored about a user in a system. If this directive indicates a web URL, then it SHOULD begin with "https://".

```
Claim: https://example.com/claim.html
```

2.4.2. Consents

The "Consents" directive is used for linking to the consent management website. If this directive indicates a web URL, then it SHOULD begin with "https://".

```
Consents: https://example.com/consents.html
```

2.4.3. Contact

This directive allows you to provide an address where users CAN ask for additional information to delete their accounts. The value MAY be an email address, a phone number and/or a contact page with more information. The "Contact:" directive MUST always be present in an "oblivion.txt" file. If this directive indicates a web URL, then it MUST be begin with "https://". Contact email addresses SHOULD use the conventions defined in section 4 of [RFC2142], but there is no requirement for this directive to be an email address.

The value MUST follow the general syntax described in [RFC3986]. This means that "mailto" and "tel" URI schemes MUST be used when specifying email addresses and telephone numbers.

The precedence SHOULD be in listed order. The first field is the preferred method of contact. In the example below, the e-mail address is the preferred method of contact.

Contact: mailto:oblivion@example.com

Contact: tel:+1-201-555-0123

Contact: https://example.com/oblivion-contact.html

2.4.4. Deactivate

The "Deactivate" directive is used for linking to the deactivation procedure. If this directive indicates a web URL, then it SHOULD begin with "https://".

Deactivate: https://example.com/deactivate-account.html

2.4.5. Delete

The "Delete" directive is used for linking to the deletion procedure. If this directive indicates a web URL, then it SHOULD begin with "https://".

Delete: https://example.com/delete-account.html

2.4.6. Encryption

This directive allows you to point to an encryption key that any user or application SHOULD use for encrypted communication. You MUST NOT directly add your key to the field. Instead the value of this field MUST be a URI pointing to a location where the key can be retrieved

from. If this directive indicates a web URL, then it SHOULD begin with "https://".

When it comes to verifying the authenticity of the key, it is always the user's responsibility to make sure the key being specified is indeed one they trust. Users MUST NOT assume that this key is used to generate the signature file referenced in Section 2.4.6.

Example of a PGP key available from a web server:

Encryption: https://example.com/pgp-key.txt

Example of a PGP key available from an OPENPGPKEY DNS:

Encryption: dns:5d2d37ab76d47d36._pgp.example.com?type=OPENPGPKEY

Example of a PGP key being referenced by its fingerprint:

Encryption: openpgp4fpr:5f2de5521c63a801ab59ccb603d49de44b29100f

2.4.7. Policy

This directive allows you to link to where your privacy policy and/or terms and conditions policy is located. This can help end users to understand what are the conditions to opt-out in the service. If this directive indicates a web URL, then it SHOULD begin with "https://".

Example:

Policy: https://example.com/privacy-policy.html

2.4.8. Signature

This directive allows you to specify a full URI (as per [RFC3986]) of an external signature file that can be used to check the authenticity of a "oblivion.txt" file. External signature files SHOULD be named "oblivion.txt.sig" and SHOULD be placed under the Well-Known path ("/.well-known/oblivion.txt.sig"). If this directive indicates a web URL, then it MUST be begin with "https://". This directive MUST NOT appear more than once.

It is RECOMMENDED to implementors that this directive is always used.

When it comes to verifying the authenticity of the file, it is always the user's responsibility to make sure the key being specified is indeed one they trust.

Here is an example of an external signature file.

Signature: https://example.com/.well-known/oblivion.txt.sig

2.5. Example of an "oblivion.txt" File

```
# Our oblivion address
Contact: mailto:oblivion@example.com
# Claim your data
Claim: https://example.com/claim.txt
# Manage your consents
Consents: https://example.com/consents.txt
# Our PGP key
Encryption: https://example.com/pgp-key.txt
# Our privacy policy
Policy: https://example.com/privacy-policy.html
# Deactivate from our service
Deactivate: https://example.com/deactivate-account.html
# Delete your account from our service
Delete: https://example.com/delete-account.html
# Verify this oblivion.txt file
Signature: https://example.com/.well-known/oblivion.txt.sig
```

3. Location of the "oblivion.txt" File

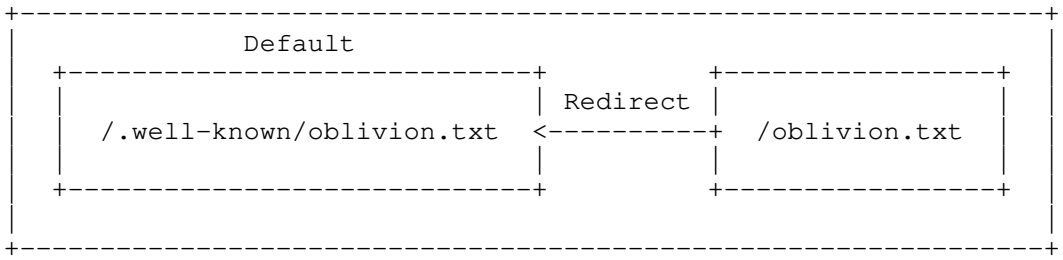

Figure 1: External Location of the "oblivion.txt" File.

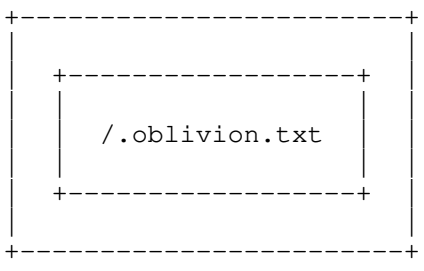

Figure 2: Internal Location of the "oblivion.txt" File.

3.1. Web-based services

Web-based services SHOULD place the "oblivion.txt" file under the Well-Known path (e. g., "https://example.com/.well-known/oblivion.txt"). An "oblivion.txt" file located under the top-level path SHOULD either redirect (as per section 6.4 of [RFC7231]) to the "oblivion.txt" file under the Well-Known path or be used as a fall back.

3.2. Filesystems

File systems SHOULD place the "oblivion.txt" file under the root directory (e. g., "/.oblivion.txt", "C:\.oblivion.txt").

```
user:/$ l

.oblivion.txt

example-directory-1/

example-directory-2/

example-directory-3/
```

example-file

3.3. Internal hosts

An ".oblivion.txt" file SHOULD be placed in the root directory of an internal host.

3.4. Extensibility

Like many other formats and protocols, this format may need to be extended over time to fit the ever-changing landscape of the Internet. Therefore, extensibility is provided via an IANA registry for directives as defined in Section 6.2 of this document. Any directives registered via that process MUST be considered optional. To encourage extensibility and interoperability, implementors MUST ignore any fields they do not explicitly support.

4. File Format Description and ABNF Grammar

The expected file format of the "oblivion.txt" file is plain text (MIME type "text/plain") as defined in section 4.1.3 of [RFC2046] and is encoded using UTF-8 [RFC3629] in Net-Unicode form [RFC5198].

The following is an ABNF definition of the "oblivion.txt" format, using the conventions defined in [RFC5234] and [RFC5322].

```
body = *line (permission-field eol) (signature-field eol) *line

line = *1(field / comment) eol

eol = *WSP [CR] LF

field = claim-field / consents-field / contact-field / deactivate-
field / delete-field / encryption-field / policy-field / ext-field

fs = ":"

email = <Email address as per [RFC5322]>

phone = "+" *1(DIGIT / "-" / "(" / ")" / SP)

uri = <URI as per [RFC3986]>

comment = "#" *(WSP / VCHAR / %xA0-E007F)

claim-field = "Claim" fs SP (email / uri / phone)

consents-field = "Consents" fs SP (email / uri / phone)
```

```
contact-field = "Contact" fs SP (email / uri / phone)

deactivate-field = "Deactivate" fs SP uri

delete-field = "Delete" fs SP uri

encryption-field = "Encryption" fs SP uri

policy-field = "Policy" fs SP uri

signature-field = "Signature" fs SP uri

ext-field = field-name fs SP unstructured

field-name = <as per section 3.6.8 of [RFC5322]>

unstructured = <as per section 3.2.5 of [RFC5322]>
```

"ext-field" refers to extension fields, which are discussed in Section 3.4 of this document

5. Security Considerations

Organizations creating "oblivion.txt" files will need to consider several security-related issues. These include exposure to sensitive information and attacks where limited access to a server could grant the ability to modify the contents of the "oblivion.txt" file or affect how it is served. Organizations SHOULD also monitor their "oblivion.txt" files regularly to detect tampering. Organizations SHOULD also ensure that any resources such as web pages, email addresses and telephone numbers references by an "oblivion.txt" file are kept current, are accessible and controlled by the organization, and are kept secure.

To ensure the authenticity of the "oblivion.txt" file, organizations SHOULD sign the file and include the signature using the "Signature" directive (Section 2.4.6). As stated in Section 2.4.4 and Section 2.4.6, both encryption keys and external signature files MUST be loaded over HTTPS.

Websites SHOULD reserve the "oblivion.txt" namespace to ensure no third-party can create a page with the "oblivion.txt" name.

6. IANA Considerations

"example.com" is used in this document following the uses indicated in [RFC2606].

"192.0.2.0" and "2001:db8:8:4::2" are used in this document following the uses indicated in [RFC6890].

6.1. Well-Known URIs registry

The "Well-Known URIs" registry should be updated with the following additional values (using the template from [RFC5785]):

URI suffix: oblivion.txt

URI suffix: oblivion.txt.sig

Change controller: IETF

Specification document(s): this document

6.2. Registry for "oblivion.txt" Header Fields

IANA is requested to create the "oblivion.txt Header Fields" registry in accordance with [RFC8126]. This registry will contain header fields for use in "oblivion.txt" files, defined by this specification.

New registrations or updates MUST be published in accordance with the "Expert Review" guidelines as described in section 4.5 of [RFC8126]. Any new field thus registered is considered optional by this specification unless a new version of this specification is published.

New registrations and updates MUST contain the following information:

1. Name of the field being registered or updated
2. Short description of the field
3. Whether the field can appear more than once
4. The document in which the specification of the field is published
5. New or updated status, which MUST be one of the following:
    1. "current". The field is in current use.
    2. "deprecated". The field is in current use, but its use is discouraged.
    3. "historic". The field is no longer in current use.

An update may make a notation on an existing registration indicating that a registered field is historical or deprecated if appropriate.

The initial registry contains these values:

Field Name: Claim

Description: contact information to use for opt-out related issues

Multiple Appearances: Yes

Published in: this document

Status: current

Field Name: Consents

Description: contact information to use for opt-out related issues

Multiple Appearances: Yes

Published in: this document

Status: current

Field Name: Contact

Description: contact information to use for opt-out related issues

Multiple Appearances: Yes

Published in: this document

Status: current

Field Name: Deactivate

Description: link to the deactivation

Multiple Appearances: No

Published in: this document

Status: current

Field Name: Delete

Description: link to the deletion page

Multiple Appearances: No

Published in: this document

Status: current

Field Name: Encryption

Description: link to a key to be used for encrypted communications

Multiple Appearances: Yes

Published in: this document

Status: current

Field Name: Policy

Description: link to privacy policy page

Multiple Appearances: Yes

Published in: this document

Status: current

Field Name: Signature

Description: signature used to verify the authenticity of the file

Multiple Appearances: No

Published in: this document

Status: current

7. Contributors

The authors would like to acknowledge the work started by E. Foudil, Y. Shafranovich et al. in defining the structure and purpouse of the "security.txt" file as shown in the Internet Draft "A Method for Web Security Policies". The structure of this document including several normartive and formal sections have been used as a referemce for the final structure of many of the normative parts in this document.

8. Normative References

[RFC1945] Berners-Lee, T., Fielding, R., and H. Frystyk, "Hypertext Transfer Protocol -- HTTP/1.0", RFC 1945, DOI 10.17487/RFC1945, May 1996, <https://www.rfc-editor.org/info/rfc1945>.

[RFC2046] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, DOI 10.17487/RFC2046, November 1996, <https://www.rfc-editor.org/info/rfc2046>.

[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>.

[RFC2142] Crocker, D., "Mailbox Names for Common Services, Roles and Functions", RFC 2142, DOI 10.17487/RFC2142, May 1997, <https://www.rfc-editor.org/info/rfc2142>.

[RFC2606] Eastlake 3rd, D. and A. Panitz, "Reserved Top Level DNS Names", BCP 32, RFC 2606, DOI 10.17487/RFC2606, June 1999, <https://www.rfc-editor.org/info/rfc2606>.

[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>.

[RFC5198] Klensin, J. and M. Padlipsky, "Unicode Format for Network Interchange", RFC 5198, DOI 10.17487/RFC5198, March 2008, <https://www.rfc-editor.org/info/rfc5198>.

[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>.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <https://www.rfc-editor.org/info/rfc5322>.

[RFC5785] Nottingham, M. and E. Hammer-Lahav, "Defining Well-Known Uniform Resource Identifiers (URIs)", RFC 5785, DOI 10.17487/RFC5785, April 2010, <https://www.rfc-editor.org/info/rfc5785>.

[RFC6890] Cotton, M., Vegoda, L., Bonica, R., Ed., and B. Haberman, "Special-Purpose IP Address Registries", BCP 153, RFC 6890, DOI 10.17487/RFC6890, April 2013, <https://www.rfc-editor.org/info/rfc6890>.

[RFC7231] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content", RFC 7231, DOI 10.17487/RFC7231, June 2014, <https://www.rfc-editor.org/info/rfc7231>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

Authors' Addresses

Felix Brezo
Telefonica

Email: felix.brezofernandez@telefonica.com

Yaiza Rubio
Telefonica

Email: yaiza.rubiovinuela@telefonica.com