Internet-Draft
Expires: May 23 2016

Ben Golightly
20 November 2015

A Method for Verification of Domain Name Ownership
draft-bsag-domain-ownership-00

Abstract

This document defines a method for website administrators to verify ownership of a domain name to third party service providers.

1. 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 http://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."

Comments are solicited and should be addressed to the working group's mailing list and/or the author(s).

This Internet-Draft will expire on May 23, 2016.

2. Copyright Notice

3. Introduction

Website administrators are often required to verify ownership of a domain name to a third party service provider. This verification process may form a part of access control, privacy control, or security and fraud prevention more generally.

Examples:

* a webmaster may verify their ownership of a domain with a search engine in order to change how the website is displayed in search, diagnose issues, and access search analytics.

* a digital Certificate Authority issuing an SSL certificate will verify domain name ownership to prevent a "man in the middle" attacker from being able to act as an imposter when intercepting HTTPS connections to the targeted domain name.

To date, there is no standard way to do this. The service provider will normally specify a method such as:

* Adding a vendor-specific meta tag to the home page of the website accessible at the given domain, or more generally add some specific HTML to the website.

* Uploading a HTML file with a specific file name and content to the root directory of the website accessible at the given domain.

* Modifying the DNS records for the domain.

* Emails sent to a specific administrator e-mail address for a domain.

Domain names expire or change ownership. Therefore, these methods of verification must be permanently maintained by the website administrator and regularly checked by the service provider.

These vendor-specific HTML files are often cryptically named, and clutter the root directory of a website.

The method specified in this memo allows website administrators to simplify webserver and domain name maintanence by centralising verification information, and allows service providers to streamline the verification process by avoiding vendor-specific verification methods.

4. Specification

This memo specifies a format for encoding domain name verification information provided by a service provider, and a method for retrieving this information. Service providers may retrieve this information and treat it as current evidence of domain ownership.

4.1 Access method

The verification information must be accessible via HTTP from the domain requiring verification, under a standard relative path on the server: "/verify.txt".

For convenience this resource may be referred to as a "verify.txt file", though the resource need in fact not originate from a file-system.

This file must be served with a MIME Type of "text/plain". The character encoding must be UTF-8.

4.2 File Format Description

The format consists of a list of records, separated by blank lines and comment lines.

A comment line takes the form:

```
# <comment>
```

Each record takes the form:

```
<Domain> <ServiceProvider> [<value>]
```

For example:

```
# verify.txt example
example.org          ExampleServiceProvider1  exampleAccountId-1234
example.org          ExampleServiceProvider1  exampleAccountId-5678
example.com          ExampleServiceProvider2  example-ABCDEF
example.com          ExampleServiceProvider3
testing.example.com  Example4                 v=1;u=123;d=20150102
```

4.2.1 The Domain field

One webserver may be accessible from several different domain names. The Domain field identifies to which domain name the verification record applies.

The content of the domain field must be any validly formatted domain name or IP address.

4.2.2 The ServiceProvider field

This is a field identifying the service provider requiring the verification. There is no restriction on the format of this field, except that it may not contain whitespace. Service providers should pick descriptive names that uniquely identify an organisation or service. This could be the URL of the service.

The length of this field should not exceed 256 bytes.

4.2.3 The value field

This is an optional field containing a value assigned by the service provider. This may be used, for example, to associate a specific

account with the service provider with the verified domain. There is no restriction on the format of this field, except that it may not contain whitespace.

The length of this field should not exceed 4096 bytes.

4.3 Interoperability

Service providers should be liberal in accepting files with different end-of-line conventions, specifically CR and LF in addition to CRLF.

With the exception of line breaks, service providers should ignore whitespace except as a separator between fields in a record.

5. Security Considerations

Website administrators should prevent unauthorised users from creating verify.txt files at the root of any domain (including subdomains).

Website administrators should be cautious of the verify.txt file being maliciously modified, and used to verify unauthorised users to service providers. Website administrators should use appropriate best practice, such as audited source control, to detect and trace modifications.

Service providers are encouraged to place limits on the resources spent on processing verify.txt files.

Service providers should be aware that domain names expire or change ownership, and take steps to reverify as appropriate.

Service providers should be aware that, as with any verification method, it may be possible for a user to impersonate a domain administrator. The required strength of verification should be balanced against the desired ease of verification.

6. IANA Considerations

This document has no actions for IANA.

7. Author's Address

Ben Golightly
Tawesoft Ltd
Email: ben@tawesoft.co.uk