Workgroup: Privacy Pass
Internet-Draft:
draft-hendrickson-privacypass-geo-extension-00
Published: 10 July 2023
Intended Status: Informational
Expires: 11 January 2024
Authors: S. Hendrickson C. A. Wood
Google Cloudflare, Inc.

Privacy Pass Geolocation Hint Extension

Abstract

This document describes an extension for Privacy Pass that allows tokens to encode geolocation hints.

About This Document

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

The latest revision of this draft can be found at https://chris-wood.github.io/draft-hendrickson-privacypass-geolocation-extension/draft-hendrickson-privacypass-expiration-extension.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-hendrickson-privacypass-geo-extension/.

Discussion of this document takes place on the Privacy Pass Working Group mailing list (mailto:privacy-pass@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/privacy-pass/. Subscribe at https://www.ietf.org/mailman/listinfo/privacy-pass/.

Source for this draft and an issue tracker can be found at https://github.com/chris-wood/draft-hendrickson-privacypass-geolocation-extension.

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 11 January 2024.

Table of Contents

1. Introduction

Some Privacy Pass token types support binding additional information to the tokens, often referred to as public metadata. [AUTH-EXTENSIONS] describes an extension parameter to the basic PrivateToken HTTP authentication scheme [AUTH-SCHEME] for supplying this metadata alongside a token. [EXTENDED-ISSUANCE] describes variants of the basic Privacy Pass issuance protocols [BASIC-ISSUANCE] that support issuing tokens with public metadata. However, there are no existing extensions defined to make use of these protocol extensions.

This document describes an extension for Privacy Pass that allows tokens to encode geolocation hints. These hints can be used by origins that redeem tokens to influence its behavior in various ways, such as determining the content of HTTP responses.

2. Conventions and Definitions

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.

3. Geolocation Hint Extension

The geolocation hint extension is an extension used to convey rough geolocation hints to origins that do not already have accurate or authoritative mappings for the IP addresses of clients. This can be particularly useful for cases where IP geolocation mappings have changed recently, or a client is using a VPN or proxy that may not be commonly recognized by servers.

The value of this extension is an GeoHintTimestamp, defined as follows.

```
struct {
   opaque geo_hint<1..2^16-1>;
} GeoHint;
```

The GeoHintTimestamp fields are defined as follows:

* "geo_hint" is a string formatted as defined in Section 2.1.1 of [GEOFEED]. It contains a comma-separated list of Alpha2code, Region, and City. The value **SHOULD NOT** contain a Postal Code.

As an example, a GeoHint structure corresponding to the "192.0.2.5,US,US-AL,Alabaster" entry would be:

```
struct {
   opaque geo_hint<1..2^16-1>; // "US,US-AL,Alabaster"
} GeoHint;
```

4. Security Considerations

Geolocation information can contribute to a client's fingerprint. Exposing precise geolocation information can therefore lead to anonymity set partitioning, as described in [ARCHITECTURE]. More general information regarding the use of extensions and their possible impact on client privacy can be found in [ARCHITECTURE].

Servers **MUST NOT** use IP Geolocation Client Hints for making security or access-control decisions, as the value can be spoofed by a client. The hint is intended only for use in optimizing behavior.

5. IANA Considerations

This document registers the following entry into the "Privacy Pass PrivateToken Extensions" registry.

*Expiration extension

-Type: 0x0002

-Name: Geolocation hint

-Value: GeoHint value as defined in Section 3

-Reference: This document

-Notes: None

6. Normative References

[ARCHITECTURE] Davidson, A., Iyengar, J., and C. A. Wood, "The Privacy Pass Architecture", Work in Progress, Internet-Draft, draft-ietf-privacypass-architecture-13, 15 June 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-privacypass-architecture-13>.

[AUTH-EXTENSIONS] Hendrickson, S. and C. A. Wood, "The PrivateToken HTTP Authentication Scheme Extensions Parameter", Work in Progress, Internet-Draft, draft-wood-privacypass-auth-scheme-extensions-00, 10 July 2023, <https://datatracker.ietf.org/doc/html/draft-wood-privacypass-auth-scheme-extensions-00>.

[AUTH-SCHEME] Pauly, T., Valdez, S., and C. A. Wood, "The Privacy Pass HTTP Authentication Scheme", Work in Progress, Internet-Draft, draft-ietf-privacypass-auth-scheme-11, 23 June 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-privacypass-auth-scheme-11>.

[BASIC-ISSUANCE] Celi, S., Davidson, A., Valdez, S., and C. A. Wood, "Privacy Pass Issuance Protocol", Work in Progress, Internet-Draft, draft-ietf-privacypass-protocol-11, 26 June 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-privacypass-protocol-11>.

[EXTENDED-ISSUANCE] "*** BROKEN REFERENCE ***".

[GEOFEED] Kline, E., Duleba, K., Szamonek, Z., Moser, S., and W. Kumari, "A Format for Self-Published IP Geolocation Feeds", RFC 8805, DOI 10.17487/RFC8805, August 2020, <https://www.rfc-editor.org/rfc/rfc8805>.

[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/rfc/rfc2119>.

[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/rfc/rfc8174>.

Acknowledgments

This document received input and feedback from Jim Laskey.

Authors' Addresses

Scott Hendrickson
Google

Email: scott@shendrickson.com

Christopher A. Wood
Cloudflare, Inc.

Email: caw@heapingbits.net