

Network Working Group
Internet-Draft
Intended status: Experimental
Expires: 11 March 2022

T. Pauly
F. Jacobs
Apple Inc.
C.A. Wood
Cloudflare
7 September 2021

The Privacy Token HTTP Authentication Scheme draft-privacy-token-01

Abstract

This documents defines an authentication scheme for HTTP called Privacy Token.

Discussion Venues

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/tfpaully/privacy-proxy>.

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 March 2022.

Copyright Notice

Copyright (c) 2021 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document.

Internet-Draft

HTTP Privacy Token

September 2021

Please review these documents carefully, as they describe your rights and restrictions with respect 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.

Table of Contents

1.	Introduction	2
1.1.	Requirements	2
2.	Privacy Token Structure	2
3.	PrivacyToken Authentication Scheme	3
4.	Security Considerations	3
5.	IANA Considerations	4
6.	Normative References	4
	Authors' Addresses	4

[1.](#) Introduction

This document defines a new HTTP authentication scheme [[RFC7235](#)] named "PrivacyToken".

This scheme is built to be used to authenticate to proxies, using the Proxy-Authorization header field, with a blind signature that allows a proxy to verify that a client has a token signed by a particular key, but without identifying the client. The initial version of this scheme is intended to be used with RSA Blind Signatures [[RSASIG](#)].

[1.1.](#) Requirements

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.

[2.](#) Privacy Token Structure

A privacy token is a structure that begins with a single byte that indicates a version. This document defines version, 1, which indicates use of private tokens based on RSA Blind Signatures [[RSASIG](#)], and determines the rest of the structure contents.

```
struct {  
    uint8_t version;  
    uint8_t key_id[32];  
    uint8_t message[32];  
    uint8_t signature[Nk];  
} Token;
```

The structure fields are defined as follows:

- * "version" is a 1-octet integer. This document defines version 1.
- * "key_id" is a collision-resistant hash that identifies the key used to produce the signature. This is generated as SHA256(public_key), where public_key is a DER-encoded SubjectPublicKeyInfo object carrying the public key.
- * "message" is a 32-octet random message that is signed by the signature.
- * "signature" is a Nk-octet RSA Blind Signature that covers the message. For version 1, Nk is indicated by size of the Token structure and may be 256, 384, or 512. These correspond to RSA 2048, 3072, and 4096 bit keys. Clients implementing version 1 MUST support signature sizes with Nk of 512 and 256.

[3.](#) PrivacyToken Authentication Scheme

The "PrivacyToken" authentication scheme defines one parameter, "token". All unknown or unsupported parameters to "PrivacyToken" authentication credentials MUST be ignored.

The value of the "token" parameter is a Privacy Token Structure [Section 2](#), encoded using base64url encoding [[RFC4648](#)].

As an example, a Proxy-Authorization field in an HTTP request would look like:

Proxy-Authorization: PrivacyToken token=abc...

4. Security Considerations

Note that the KeyID is only a hint to identify the public verification key. With a sufficiently large number of public keys, KeyID collisions may occur. By approximation, a KeyID collision between two distinct keys will occur with probability $\sqrt{p * 2^{33}}$. In such cases, servers SHOULD attempt verification using both keys.

Pauly, et al.

Expires 11 March 2022

[Page 3]

Internet-Draft

HTTP Privacy Token

September 2021

5. IANA Considerations

This document registers the "PrivacyToken" authentication scheme in the "Hypertext Transfer Protocol (HTTP) Authentication Scheme Registry" established by [\[RFC7235\]](#).

Authentication Scheme Name: PrivacyToken

Pointer to specification text: [Section 3](#) of this document

6. 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>>.
- [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>>.
- [RFC7235] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Authentication", [RFC 7235](#), DOI 10.17487/RFC7235, June 2014, <<https://www.rfc-editor.org/info/rfc7235>>.
- [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>>.

[RSASIG] Denis, F., Jacobs, F., and C. A. Wood, "RSA Blind Signatures", Work in Progress, Internet-Draft, [draft-irtf-cfrg-rsa-blind-signatures-02](https://www.ietf.org/archive/id/draft-irtf-cfrg-rsa-blind-signatures-02), 2 August 2021, <<https://www.ietf.org/archive/id/draft-irtf-cfrg-rsa-blind-signatures-02.txt>>.

Authors' Addresses

Tommy Pauly
Apple Inc.
One Apple Park Way
Cupertino, California 95014,
United States of America

Email: tpauly@apple.com

Pauly, et al.

Expires 11 March 2022

[Page 4]

Internet-Draft

HTTP Privacy Token

September 2021

Frederic Jacobs
Apple Inc.
One Apple Park Way
Cupertino, California 95014,
United States of America

Email: frederic.jacobs@apple.com

Christopher A. Wood
Cloudflare

Email: caw@heapingbits.net

