USEFOR Working Group S. Lyall
INTERNET-DRAFT November 1998
Expires May 1999

**Cancel-Locks in Usenet articles.**
**draft-ietf-usefor-cancel-lock-01.txt**

Status of this memo



Abstract

This document outlines a method that may be used by authors of successor (or canceling) articles to authenticate their authorship of the original article.

As a proto-article article passes through various agents they may include the hash of a secret string in a Cancel-Key header. Later if they wish to use a standard mechanism to remove the original article (eg Cancel or Supersede) they can include this string in the Cancel-Lock header to verify that they are entitled to perform this operation.

Familiarity with the current News Article Format draft [ARTICLE] is assumed.

## 1. Introduction: The Cancel-Key & Cancel-Lock headers

These two headers MAY be used by posters, posting agents, moderators and
injecting agents in order to mark articles they process and to verify
canceling, superseding and replacing articles that may subsequently be
issued for those originals. They MUST NOT be altered or created by any
other agents.

The scheme works by including a "Cancel-Lock: " header and contents in an
article. Further articles that wish to cancel, supersede or replace this
article can include a "Cancel-Key: " header which contains a code-string
that when hashed yields one of the code-strings in the "Cancel-Lock: "
header of the original article.

These headers are intended to be used as a simple method to verify that
the author of an article which removes another one is either the poster,
posting agent, moderator or injecting agent that processed the original
article when it was in its proto-article form.

## 2. Format

```
   Cancel-Lock-content = cancel-lock *( CFWS cancel-lock ) [CFWS]
    Cancel-Key-content = cancel-key *( CFWS cancel-key ) [CFWS]
           cancel-lock = scheme ":" code-string
            cancel-key = scheme ":" code-string
                scheme = token
           code-string = 1*base64-octet
          base64-octet = ALPHA / DIGIT / "+" / "/" / "="
```

### 2.1 The "scheme" element

The scheme is the format that is used to encode the code-string. This
document only defines the scheme of "SHA1" which corresponds to the
SHA1 algorithm [SHA1]. Other schemes MAY be defined by further IETF
standards. This element is case insensitive.

### 2.2 The "code-string" element

The code-string is a series of base-64-octets. The code-string in a
cancel-lock is the hash of the corresponding code-string in a cancel-key.
The encoding of the binary key or lock is performed in accordance with
the Base64 Transfer Encoding defined in [RFC-2045].

Under scheme "sha1" the code-string element of a cancel-lock is the
output of a hash operation (using the SHA1 algorithm) performed on the
code-string of the cancel-key.

## 3. Use

In order for an article removal to be allowed under the Cancel-Lock method
the following takes place:

When a serving agent receives an article that attempts to remove a previous article via Cancel, Supersedes or Replaces, then if the original
article contains a valid cancel-lock the replacing article MUST contain a
valid cancel-key (or keys) that corresponds to at least one of the cancel-lock's in the original article.

### 3.1 Adding an initial "Cancel-Lock: " header to a proto-article

A Cancel-Lock header MAY be added to a proto-article by the poster or posting agent which will include one or more cancel-locks in its Cancel-Lock-content.

If the poster or posting agent does not add a Cancel-Lock header to an article then an injecting-agent (or moderator) MAY add one provided that
it positively authenticates the author. The injecting-agent (or moderator) MUST NOT add this header to an article unless it is able to authenticate all cancels, replaces and supersedes from the poster and automatically add the correct Cancel-Key header (and content) for such articles.

Other agents MUST NOT add this header to articles or proto-articles that
they process.

### 3.2 Extending the "Cancel-Lock: " header of a proto-article

If a "Cancel-Lock: " header has already been added to a proto-article then any agent (prior to the article being injected) further processing the proto-article (ie moderators and injection-agents) MAY append a single
cancel-lock to those already in the header.

No more than one cancel-lock SHOULD be added by each agent that processes the proto-article.

Once an article is injected then this header MUST NOT be altered. In particular, relaying agents beyond the injecting agent MUST NOT alter it.

### 3.3 Adding a "Cancel-Key: " header to a proto-article.

The Cancel-Key header MAY be added to a proto-article containing a "Cancel: ", "Replaces: " or "Supersedes: " header by the poster or posting agent which will include one or more cancel-keys in its Cancel-Key-content. These cancel-keys will correspond to some or all of the cancel-locks in articles listed in the "Cancel: " , "Replaces: " and
"Supersedes: " headers.

If, as mentioned in 3.1 an injecting agent (or moderator) has added a "Cancel-Lock: " header to an article listed in the "Cancel: " , "Replaces:
" or  "Supersedes: " headers then (assuming it authenticates the poster as
being the same as the poster of the original article(s) ) it MUST add a "Cancel-Key: " header with the cancel-key(s) that correspond to those article(s).

Other Agents MUST NOT alter this header.

## 4. Creating the cancel-lock

It is suggested that when creating a cancel-lock the function HMAC(message-id+secret) be used, where HMAC is outlined in [HMAC], message-id is the message-id of the article and secret is a secret key held locally.

This method removes the need for a per-article database containing the cancel-lock used with every article.

## 5. Security Issues

General security issues with hash functions are discussed elsewhere, see
the references in [HMAC] for some pointers. The method outlined in Section 4 is also vulnerable to the secret key being compromised or guessed.

## 6. Examples

The following are Cancel-Lock headers along with a Cancel-Key header that matches them:

```
Cancel-Lock: sha1:bNXHc6ohSmeHaRHHW56BIWZJt+4=
Cancel-Key: sha1:aaaBBBcccDDDeeeFFF

Cancel-Lock: SHA1:H7/zsCUemvbvSDyARDaMs6AQu5s=
Cancel-Key: sha1:chW8hNeDx3iNUsGBU6/ezDk88P4=  sha1:4srkWaRIzvK51ArAP

Cancel-Lock: sha1:JyEBL4w9/abCBuzCxMIE/E73GM4=
       sha1:2Bmg+zWaY1noRiCdy8k3IapwSDU=
Cancel-Key: sha1:K4rkWRjRcXmIzvK51ArAP
```

## 7. References

[ARTICLE] News Article Format. D Ritter. Internet Draft
draft-ietf-usefor-article-01 . 1998.

[HMAC] Keyed-Hashing for Message Authentication. H. Krawczyk, M. Bellare, R. Canetti. February 1997. RFC 2104.

[SHA1] NIST, FIPS PUB 180-1: Secure Hash Standard, Apr 1995.

[RFC-2045] MIME, part 1 Freed, Ned; Borenstein, Nathaniel S.: Multipurpose Internet mail extensions (MIME), part 1: format of Internet message bodies. RFC 2045, Nov 1996.

## 8. Changes from previous draft.

- References to SHA-160 changed to SHA1

- "scheme" is now a case insensitive token and the number "1" has been changed to "sha1".

- Added some examples and fixed the section numbering.

- Updated 2nd paragraph on section 2.2 to make clear what exactly is being hashed and how.

- Changed paragraph 2 of 3.1 to discourage injection-agents from adding the header.

- Removed the Clue-string as this complicated the scheme without adding realistic functionality

- moderators can now add these headers under the same conditions as injection-agents.

## 9. Author's Address

Simon Lyall
PO Box 6616,
Auckland,
New Zealand.

Phone: +64 9 358 5067 ext 701
Email: simon@darkmere.gen.nz