Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 5, 2015

K. Zeilenga
A. Melnikov
Isode Limited
July 4, 2014

# Security Labels in Internet Email
# draft-zeilenga-email-seclabel-08

## Abstract

This document describes a header field, SIO-Label, for use in Internet Mail to convey the sensitivity of the message. This header field which may carry a textual representation (a display marking) and/or a structural representation (a security label) of the sensitivity of the message. This document also describes a header field, SIO-Label-History, for recording changes in the message's label.

## 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."

This Internet-Draft will expire on January 5, 2015.

Table of Contents



## 1. Introduction

A security label, sometimes referred to as a confidentiality label, is a structured representation of the sensitivity of a piece of information. A security label can be used in conjunction with a clearance, a structured representation of what information sensitivities a person (or other entity) is authorized to access, and a security policy to control access to each piece of information. For instance, an email message could have a EXAMPLE CONFIDENTIAL label, and hence requiring the sender and the receiver to have a clearance granting access to EXAMPLE CONFIDENTIAL labeled information. X.841 [X.841] provides a discussion of security labels, clearances, and security policy.

A display marking is a textual representation of the sensitivity of a piece of information. For instance, "EXAMPLE CONFIDENTIAL" is a textual representation of the sensitivity. A security policy can be used to generate display markings from security labels. Display markings are generally expected to be prominently displayed whenever the content is displayed.

Sensitivity-based authorization is used in networks which operate under a set of information classification rules, such as in government military agency networks. The standardized formats for security labels, clearances, and security policy and associated authorization models are generalized and can be used in non-government deployments where appropriate.

Security labels may also be used for purposes other than authorization. In particular, they may be used simply to convey the sensitivity of a piece information. The security label could be used, for instance, to organize content in a content store.

This document describes a protocol for conveying the sensitivity of a electronic mail message [RFC5322], as a whole. In particular, this document describes a header field, SIO-Label, to carry a security label, a display marking, and display colors. This document also describes a header field, SIO-Label-History, to record changes in the message's security label.

This protocol is based in part upon Security Labels in XMPP [XEP258] protocol.

### 1.1. Relationship to Inline Sensitivity Markings

In environments requiring messages to be marked with an indication of their sensitivity, it is common to place a textual representation of the sensitivity, a display marking, within the body to the message and/or in the Subject header field. For instance, the authors often receives messages of the form:

```
To: author <author@example.com>;
From: Some One <someone@example.net>;
Subject: the subject (UNCLASSIFIED)

UNCLASSIFIED

Text of the message.

UNCLASSIFIED
```

Typically, when placed in the body of the message, the marking is inserted into the content such that it appears as the first line(s) of text of the body of the message. This is known as a FLOT (First Line(s) of Text) marking. The marking may or may not be surrounded by other text indicating the marking denotes the sensitivity of the message. A FLOT may also accompanied by a LLOT (Last Line(s) of Text) marking. The message above contains a two-line FLOT and a two-line LLOT (in both cases, a line providing the marking and a empty line between the marking and the original content).

Typically, when placed in the Subject of the message, the marking is inserted before or after the original subject field contents surrounded with by parentheses or the like, and/or separated from the content by white space.

The particulars syntax and semantics of inline sensitivity markings is generally a local matter. This hinders interoperability within an organization wanting to take actions based upon these markings, and hinders interoperability between cooperating organizations wanting to usefully share sensitivity information

The authors expect such markings to be continued to widely used, especially in absence of ubiquitous support for a standardized header field indicating the sensitivity of the message.

The authors hope that through the use of standardized header field, interoperability within organizations and between organizations can be improved.

## 1.2. Relationship to preexisting Security Label Header Fields

A number of non-standard header fields, such as the X-X411 field, are used to carry a representation of the sensitivity of the message, whether a structured representation or textual representation.

The authors hope the use of non-standard header fields will be replaced, over time, with use of the header field described in this document.

## 1.3. Relationship to Enhanced Security Services for S/MIME

Enhanced Security Services for S/MIME (ESS) [RFC2634] provides, amongst other services, signature services "for content integrity, non-repudiation with the proof of origin, and [securely] binding attributes (such as a security label) to the original content.

While it may be possible to utilize the protocol described in this document concurrently with ESS, this protocol should generally be viewed as an alternative to ESS.

It is noted that in ESS, the security label applies to MIME [RFC2045] content, where in this protocol the label applies to the message as a whole.

It is also noted that in ESS, security labels are securely bound to the MIME content through the use of digital signatures. This protocol does not provide message signing services, and hence does not provide securely binding the label to the message, or for content integrity, or for non-repudiation of the proof of origin.

This protocol is designed for situations/environments where message signing is not necessary to provide sufficient security.

## 2. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

The formal syntax specifications in this document use the Augmented Backus-Naur Form (ABNF) as described in [RFC5234].

The term "base64 encoding" is used to refer to the Base 64 encoding defined in Section 4 of [RFC4648]. The term "BER encoding" is used to refer to encoding per the Basic Encoding Rules (BER) as defined in [X.690].

## 3. Overview

A Mail User Agent (MUAs) originating a message can, if so configured, offer the user with a menu of sensitivities to choose from and, upon selection, insert the display marking, foreground and background colors, and security label parameters associated with that selection into the SIO-Label header field of the message.

Mail Submission Agents (MSAs), Mail Transfer Agents (MTAs), and Mail Delivery Agents (MDAs) then can, if so configured, use the provided (or lack thereof) sensitivity information in determining whether to accept, forward, or otherwise act on the message as submitted. These agents, here after referred to as Service Agents (SAs), can, if so configured, modify the sensitivity information of the message, such as replacing the security label and/or display marking with an equivalent representations of the sensitivity of the message. SAs which add or modify or delete the SIO-Label header field SHOULD add an SIO-Label-History header.

Receiving MUAs which implement this extension SHALL, when displaying the message, also prominently display the marking, if any, conveyed in the SIO-Label header field or, if policy aware and configured to display locally generated markings, a marking generated by the conveyed label and the governing policy. It is also desirable to display this marking in listings of messages. In the case the conveyed marking is displayed, marking SHOULD be displayed using the foreground and background colors conveyed in the header field. In the case the marking was generated from conveyed label and the governing policy, the marking SHOULD be displayed using the foreground and background colors conveyed by the governing policy.

While MUAs are not expected to make authorization decisions based upon values of the SIO-Label header field, MUAs can otherwise use the provided (or lack thereof) sensitivity information in determining how

to act on the message. For instance, the MUA may organize messages in its store of messages based upon the content of this header field.

## 4. The SIO-Label header field

The header field name is "SIO-Label" and its content is a set of key/value pairs, each referred to as a parameter.

Formal header field syntax:

```
sio-label = "SIO-Label:" [FWS] sio-label-parm-seq [FWS] CRLF

sio-label-parm-seq = sio-label-parm
    [ [FWS] ";" [FWS] sio-label-parm-seq ]

sio-label-parm = parameter
```

where the parameter production is defined in [RFC2231], the FWS production are defined in [RFC5322], and the CRLF production is defined in [RFC5234]. It is noted that the RFC 2231 productions rely on [RFC0822] ABNF which implicitly allows for white space in certain cases. In particular, white space is implicitly allowed in the parameter production immediately before and after the "=". It is also noted that RFC 2231 allows for quoted-string values (of the parameter production) of substantial length and for string characters outside of US-ASCII, or other such cases. Implementors should consult the referenced specifications for specifics.

The "marking" parameter is a display string for use by implementations which are unable or unwilling to utilize the governing security policy to generate display markings. The "marking" parameter SHOULD generally be provided in SIO-Label header fields. It ought only be absent where an SA relies on other SA to generate the marking.

The "fgcolor" and "bgcolor" parameters are tokens restricted to color production representing the foreground and background colors, respectively, for use in colorizing the display marking string. Their values are RGB colors in hexadecimal format (e.g., "#ff0000"), or one of the CSS color names (e.g., "red") given in named-color type below (the 16 HTML4 colors + "orange") [CSS3-Color]. The default foreground color is black. The default background is white. The "fgcolor" and "bgcolor" parameters SHALL be absent if the marking parameter is absent. The HEXDIG production below is defined in [RFC5234]

Formal color syntax:

```
color = hex-color / named-color

hex-color = "#" 6HEXDIG    ; Hex encoded RGB

named-color =
           "aqua" /
           "black" /
           "blue" /
           "fuschia" /
           "gray" /
           "green" /
           "lime" /
           "maroon" /
           "navy" /
           "olive" /
           "purple" /
           "red" /
           "silver" /
           "teal" /
           "white" /
           "yellow" /
           "orange" ; named colors
```

The "type" parameter is a quoted-string containing the string ":ess" or the string ":x411" or the string ":xml" or a URI [RFC3986] denoting the type and encoding of "label" parameter. The "label" parameter value is a quoted string. The "type" parameter SHALL be present if the "label" parameter is present. The "label" parameter SHALL be present if the "type" parameter is present. The absence of the "type" and "label" parameters indicates the message is handled, where sensitivity-based authorization is performed, under default handling rules (e.g., as if no SIO-Label was present).

The string ":ess" indicates the "label" parameter value is the base64 encoding of the BER encoding of an ESS security label [RFC2634].

ESS Label Example:

```
SIO-Label: marking="EXAMPLE CONFIDENTIAL";
    fgcolor=black; bgcolor=red;
    type=":ess"; label="MQYGASkCAQM="
```

The string ":x411" indicates the "label" parameter value is the base64 encoding of the BER encoding of an X.411 security label [X.411].

X.411 Label Example:

```
SIO-Label: marking="EXAMPLE CONFIDENTIAL";
    fgcolor=black; bgcolor=red;
    type=":x411"; label="MQYGASkCAQM="
```

The string ":xml" indicates the "label" parameter value is the base64 encoding of a security label represented using [XML]. The XML prolog SHOULD be absent unless specifically required (such as when the character encoding is not UTF-8). The particular flavor of security label representation is indicated by the root element name and its name space.

The ":ess" and ":x411" formats SHOULD be used represent ESS or X.411 security labels, respectively, instead of any direct XML representation of these formats.

XML Label Example:

```
SIO-Label: marking="EXAMPLE CONFIDENTIAL";
    fgcolor=black; bgcolor=red;
    type=":xml";
    label*0="PFNlY0xhYmVsIHhtbG5zPSJodHRwOi8vZXhhbX";
    label*1="BsZS5jb20vc2VjLWxhYmVsLzAiPjxQb2xpY3lJ";
    label*2="ZGVudGlmaWVyIFVSST0idXJuOm9pZDoxLjEiLz";
    label*3="48Q2xhc3NpZmljYXRpb24+MzwvQ2xhc3NpZmlj";
    label*4="YXRpb24+PC9TZWNMYWJlbD4=";
```

The header field SHALL minimally contain a "marking" parameter or contain both the "type" and "label" parameters.

This header field may be extended to include additional parameters by future document formally updating (or replacing) this document. Implementations SHOULD ignore additional parameters they do not recognize. This recommendation is not a mandate so as to allow agents to process a message with an SIO-header field with unrecognized header fields differently than a message less those unrecognized header fields.

Each message SHALL contain zero or one SIO-Label header field.

Extended Example:

```
SIO-Label: marking*=us-ascii'en'EXAMPLE%20CONFIDENTIAL;
    fgcolor = black ; bgcolor = red ;
    type=":ess"; label*0="MQYG";
    label*1="ASkCAQM="
```

The Extended Example is equivalent to the ESS Label Example above.

## 5. The SIO-Label-History header field

Any service agent MAY record label changes in an SIO-Label-History header. This header field is intended to provide trace information (and only trace information). For instance, it can be used to record the label change when an SIO-Label header is added, modify, or deleted by an service agent. This field use can be used in other sitations as well. For instance, an X.400 to Internet messagging gateway can use this header field to record labeling changes made while translating a message.

The formal syntax of the SIO-Label-History header is the same as the SIO-Label, but with parameters as discussed here

change - one of "add", "replace", "delete".

changed-by - contains a string identify the agent, commonly the agent's fully qualified domain name.

changed-at - contains a date-time production, as specified in [RFC5322] representing the date and time the header was rewritten.

changed-comment - contains a string containing a comment.

marking, fgcolor, bgcolor, type, label - records the message's label information prior to add, modify, delete of SIO-Label, using same parameter syntax used of SIO-Label. These parameters are absent when the change action is add.

new-marking, new-fgcolor, new-bgcolor, new-type, new-label - records the message's label information after add, modify, delete of SIO-Label, using same parameter syntax used for corresponding SIO-Label parameters. These parameters are absent when the change type is delete.

The header field SHALL minimally contain the "change", "changed-by", and "changed-at" parameters.

This header field can be extended to include additional parameters by future document formally updating (or replacing) this document.

Each message can contain zero or more SIO-Label-History header fields. All SIO-Label-History header fields should immediately follow the the SIO-Label header field, if any, and be grouped together. Additional SIO-Label-History header fields should be added immediately preceeding any existing SIO-Label-History header fields.

SIO Label History add, modify, delete example:

```
SIO-Label-History: marking="EXAMPLE CONFIDENTIAL";
    fgcolor=black; bgcolor=red;
    type=":xml";
    label*0="PFNlY0xhYmVsIHhtbG5zPSJodHRwOi8vZXhhbX";
    label*1="BsZS5jb20vc2VjLWxhYmVsLzAiPjxQb2xpY3lJ";
    label*2="ZGVudGlmaWVyIFVSST0idXJuOm9pZDoxLjEiLz";
    label*3="48Q2xhc3NpZmljYXRpb24+MzwvQ2xhc3NpZmlj";
    label*4="YXRpb24+PC9TZWNMYWJlbD4=";
    change=delete;
    changed-by="delete.example.com";
    changed-at="18 Feb 2013 9:24 PDT";
    changed-comment="delete"
SIO-Label-History: marking="EXAMPLE CONFIDENTIAL";
    fgcolor=black; bgcolor=red;
    type=":ess"; label="MQYGASkCAQM=";
    new-marking="EXAMPLE CONFIDENTIAL";
    new-fgcolor=black; new-bgcolor=red;
    new-type=":xml";
    new-label*0="PFNlY0xhYmVsIHhtbG5zPSJodHRwOi8vZXhhbX";
    new-label*1="BsZS5jb20vc2VjLWxhYmVsLzAiPjxQb2xpY3lJ";
    new-label*2="ZGVudGlmaWVyIFVSST0idXJuOm9pZDoxLjEiLz";
    new-label*3="48Q2xhc3NpZmljYXRpb24+MzwvQ2xhc3NpZmlj";
    new-label*4="YXRpb24+PC9TZWNMYWJlbD4=";
    change=replace;
    changed-by="modify.example.net";
    changed-at="18 Feb 2013 8:24 PDT";
    changed-comment="replaced with XML variant"
SIO-Label-History: new-marking="EXAMPLE CONFIDENTIAL";
    new-fgcolor=black; new-bgcolor=red;
    new-type=":ess"; new-label="MQYGASkCAQM=";
    change=add;
    changed-by="add.example.net";
    changed-at="18 Feb 2013 7:24 PDT";
    changed-comment="added label"
```

## 6. IANA Considerations

Registration of the the SIO-Label and SIO-Label-History header fields in the "Provisional Message Header Field Registry" is requested in accordance with [RFC3864].

Header field name: SIO-Label
Applicable protocol: mail [RFC5322]
Status: provisional
Author/change controller: Kurt Zeilenga (kurt.zeilenga@isode.com)
Specification document(s): this document

Header field name: SIO-Label-History

Applicable protocol: mail [RFC5322]
Status: provisional
Author/change controller: Kurt Zeilenga (kurt.zeilenga@isode.com)
Specification document(s): this document

## 7. Security Considerations

Sensitive information should be appropriately protected (whether labeled or not). For email messages, it is generally appropriate for the sending entity to authenticate the receiving entity and to establish transport level security, including both data integrity and data confidential protective services. Where a receiving entity to make authorization decisions based upon assertions of the sending entity, including assertions of identity, it is generally appropriate for the receiving entity to authenticate the sending entity.

This document provides a facility for expressing the sensitivity of an email message. The mere expression of actual sensitivity of a generally does not elevate the sensitivity of the message, however expressions of sensitivities can themselves be regarded as sensitive information. For instance, a marking of "BLACK PROJECT RESTRICTED" could disclose the existence of a sensitivity project.

The SIO-Label header field expresses the sensitivity of the whole message, including the header and body. This document does not provide a means to express the sensitivity of portions of an email message, such as the possibly different sensitivities of various MIME parts that the message may be composed of. This approach used in this favors simplicity and ease of use of a single expression of sensitivity over the complexity and difficultly of use of portion marking and labeling.

The expressed sensitivity can be used in determining how to handle a message. For instance, the value of the SIO-Label header (or lack thereof) field can be used to determine if it appropriate to be forwarded to a particular entity and, if so, what the minimum security services are that which ought to be used in the forwarding exchange. The mechanism for determining how to handle a message based expressed sensitivity is beyond the scope of this document.

The actual content may be more or less sensitivity than indicated by the security label. Agents should avoid lowering security requirements for message exchange with a particular entity based upon conveyed sensitivity.

This protocol does not itself provide message signing services, such a used in providing message integrity protection, non-repudiation, and binding of attributes, such the security label to the message.

While it possible that this protocol could be used with a general message signing service, this document does not detail such use.

While security label and display marking parameters are expected to express the same sensitivity, nothing in this specification ensures that the security label and display marking values express the same sensitivity. For instance, an MUA could submit a message which contains security label which expresses one sensitivity and a display marking a different sensitivity, and by doing so, possibly cause an SA to inappropriately handle the message. It is generally appropriate for each SA making use of the SIO-Label values to determine if the security label and display marking values express the same sensitivity and, if not, take appropriate action (such as rejecting the message).

This document also provides a facility for expressing changes to the label of a message. This is intended to be used for trace purposes only. It is noted that this SIO-Label-History header field can include sensitive information and, as such, can be removed from the message where its inclusion would result in an inapprorpriate information disclosure.

## 8. References

### 8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2231] Freed, N. and K. Moore, "MIME Parameter Value and Encoded Word Extensions:
Character Sets, Languages, and Continuations", RFC 2231, November 1997.

[RFC2634] Hoffman, P., "Enhanced Security Services for S/MIME", RFC 2634, June 1999.

[RFC3864] Klyne, G., Nottingham, M., and J. Mogul, "Registration Procedures for Message Header Fields", BCP 90, RFC 3864, September 2004.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, October 2006.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, October 2008.

[RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

[XML] Paoli, J., Maler, E., Sperberg-McQueen, C., Yergeau, F., and T. Bray, "Extensible Markup Language (XML) 1.0 (Fifth Edition)", World Wide Web Consortium Recommendation REC-xml-20081126, November 2008, <http://www.w3.org/TR/2008/REC-xml-20081126>.

[X.411] International Telephone and Telegraph Consultative Committee, "Message Handling Systems (MHS) - Message Transfer System: Abstract Service Definition and Procedures", CCITT Recommendation X.411, June 1999.

[X.690] International Telephone and Telegraph Consultative Committee, "ASN.1 encoding rules: Specification of basic encoding Rules (BER), Canonical encoding rules (CER) and Distinguished encoding rules (DER)", CCITT Recommendation X.690, July 2002.

[CSS3-Color] Celik, T. and C. Lilley, "CSS3 Color Module", World Wide Web Consortium CR CR-css3-color-20030514, May 2003, <http://www.w3.org/TR/2003/CR-css3-color-20030514>.

## 8.2. Informative References

[RFC0822] Crocker, D., "Standard for the format of ARPA Internet text messages", STD 11, RFC 822, August 1982.

[RFC2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996.

[X.841] International Telephone and Telegraph Consultative Committee, "Security information objects for access control", CCITT Recommendation X.841, October 2000.

[XEP258] Zeilenga, K., "XEP-0258: Security Labels in XMPP", XEP XMPP Extension Protocols, August 2011.

## Appendix A. Acknowledgements

The authors appreciate the review, comment, and text provided by community members, including Dave Cridland, Brad Hards, Russ Housley, Steve Kille, Graeme Lunt, Alan Ross, Jim Schaad, and David Wilson.

## Authors' Addresses

Kurt Zeilenga
Isode Limited

EMail: Kurt.Zeilenga@isode.com

Alexey Melnikov
Isode Limited
14 Castle Mews
Hampton, Middlesex TW12 2NP
UK

EMail: Alexey.Melnikov@isode.com