XEP-0258: Security Labels in XMPP

Kurt Zeilenga
mailto:Kurt.Zeilenga@Isode.COM
xmpp:Kurt.Zeilenga@Isode.COM

2018-11-03
Version 1.1.1

Status	Type	Short Name
Draft	Standards Track	sec-label

This document describes the use of security labels in XMPP. The document specifies how security label metadata is carried in XMPP, when this metadata should or should not be provided, and how the metadata is to be processed.

Legal

Copyright

Permissions

Warranty

Liability

Conformance

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 is 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, a message could be labeled as "SECRET", and hence requiring the sender and the receiver to each have a clearance granting access to "SECRET" information. X.841 [1] provides a discussion of security labels, clearances, and security policy.
Sensitivity-based authorization is used in networks which operate under a set of information classification rules, such as in government agency networks. The standardized formats for security labels, clearances, and security policy are generalized and do have application in non-government networks.
This document describes the use of security labels in XMPP [2]. The document specifies how security label metadata is carried in XMPP. It standardizes a mechanism for carrying ESS Security Labels in XMPP, as well as provides for use of other label formats. ESS Security Labels are specified in RFC 2634 [3]. ESS Security Labels are commonly used in conjunction with X.500 [4] clearances and either X.841 or SDN.801c [5] security policies.

Listing 1: Message with ESS Security Label

```
<message to='romeo@example.net' from='juliet@example.com/balcony'>
    <body>This content is classified.</body>
    <securitylabel xmlns='urn:xmpp:sec-label:0'>
        <displaymarking fgcolor='black' bgcolor='red'>SECRET</
            displaymarking>
        <label><esssecuritylabel xmlns='urn:xmpp:sec-label:ess:0'>
            MQYCAQQGASk=
        </esssecuritylabel></label>
    </securitylabel>
</message>
```

Listing 2: Message with IC-ISM Label

```
<message to='romeo@example.net' from='juliet@example.com/balcony'>
    <body>This content is classified.</body>
    <securitylabel xmlns='urn:xmpp:sec-label:0'>
        <displaymarking fgcolor='black' bgcolor='red'>SECRET</
            displaymarking>
```

[1] X.841: Security techniques - Security information objects for access control <http://www.itu.int/rec/T-REC-X.841-200010-I/en>.
[2] Extensible Messaging and Presence Protocol (XMPP) <https://xmpp.org/>.
[3] RFC 2634: Enhanced Security Services for S/MIME <http://tools.ietf.org/html/rfc2634>.
[4] X.500: The Directory: Overview of concepts, models and service <http://www.itu.int/rec/T-REC-X.500-200102-I/en>.
[5] SDN.801c: Access Control Concept and Mechanism, US National Security Agency, Revision C, 12 May 1999.

```
        <label><icismlabel xmlns='http://example.gov/IC-ISM/0'
            classification='S'
             ownerProducer='USA'/></label>
    </securitylabel>
</message>
```

Note: The IC-ISM [6] label example is for *illustrative purposes only*.
The document details when security label metadata should or should not be provided, and how this metadata is to be processed.
This document does not provide:

- any mechanism for a client to discover the security policy in force at its home server, or any other server;
- any mechanism for a client to discover the user's clearance, or the clearance of associated with any resource; nor
- any administrative mechanism for a client to configure configure policy, clearance, and labels of any resource.

Such mechanisms may be introduced in subsequent documents.
This document does not discuss how one might securely bind a security label to a stanza. It is expected a subsequent document will tackle this topic.

2 Discovering Feature Support

An entity (client or server) which supports the XMPP Security Label protocol MUST report that fact by including a service discovery feature of "urn:xmpp:sec-label:0" in response to a Service Discovery (XEP-0030) [7] information request.
Clients wishing to include a XMPP Security Label element in any stanza they generate SHOULD determine if their server supports the XMPP Security Label protocol. If their server does not support XMPP Security Label, the client SHOULD NOT generate XMPP Security Labels as the server not supporting this protocol will generally ignore XMPP Security Labels as they would any other unrecognized element.
As each service domain may have different support for security labels, servers should advertise and clients should perform appropriate discovery lookups on a per service basis.

Listing 3: Service Discovery information request

```
<iq type='get'
    from='user@example.com/Work'
```

[6] Common Information Sharing Standard for Information Security Marking: XML Implementation, Office of the Director of National Intelligence, Release 2.0.3, 15 February 2006.
[7] XEP-0030: Service Discovery <https://xmpp.org/extensions/xep-0030.html>.

```
    to='example.com'
    id='disco1'>
  <query xmlns='http://jabber.org/protocol/disco#info'/>
</iq>
```

Listing 4: Service Discovery information response

```
<iq type='result'
    from='example.com'
    to='user@example.com/Work'
    id='disco1'>
  <query xmlns='http://jabber.org/protocol/disco#info'>
    ...
    <feature var='urn:xmpp:sec-label:0'/>
    ...
  </query>
</iq>
```

3 Protocol

An element, <securitylabel/>, is defined to carry security label metadata. This metadata includes a security label, zero or more equivalent security labels, and optionally display marking data.

Listing 5: Labeled Message

```
<message to='romeo@example.net' from='juliet@example.com/balcony'>
    <body>This content is classified.</body>
    <securitylabel xmlns='urn:xmpp:sec-label:0'>
        <displaymarking fgcolor='black' bgcolor='red'>SECRET</
           displaymarking>
        <label>
            <esssecuritylabel xmlns='urn:xmpp:sec-label:ess:0'
                >MQYCAQIGASk=</esssecuritylabel>
        </label>
        <equivalentlabel>
            <esssecuritylabel xmlns='urn:xmpp:sec-label:ess:0'
                >MRUCAgD9DA9BcXVhIChvYnNvbGV0ZSk=</esssecuritylabel>
        </equivalentlabel>
    </securitylabel>
</message>
```

The security label metadata is carried in an <securitylabel/> element. The <securitylabel/> element which contains one and only one <label/> element, zero or more <equivalentlabel/> elements, and an optional <displaymarking/> element.
The <label/> provides the primary security label. It is commonly issued by the sender under the security policy of that they and their home server operating under. The <label/> contains

either a single element representing the primary security label or is empty to indicate use of a default.
Each <equivalentlabel/> represents an equivalent security label under other policies. Each <equivalentlabel/> contains a single element representing the equivalent label. This element might be used when a recipient is known to hold a clearance under a different policy than the sender.
The <displaymarking/> element contains a display string for use by implementations which are unable to utilize the applicable security policy to generate display markings. The element may optionally contain two attributes, fgcolor= and bgcolor=, whose values are HTML color strings (e.g., 'red' or '#ff0000'), for use in colorizing the display marking. The fgcolor= default is black. The bgcolor= default is white.

4 Label Catalog Discovery

A client can request a catalog for a particular JID by sending a catalog discovery request to the client's server. Where the JID is hosted by some other server, the client's server is expected to produce a suitable catalog (or fail the request). The client's server may, as needed, query catalogs from other servers in order to fulfill the client's request.
While this specification does not preclude a client from directing a catalog request elsewhere, it is noted that catalog returned by a party other than its server may not be directly usable by the client. For instance, the client's server might require a particular only-locally-known label be used in messages to a particular remote JID.
It is RECOMMENDED the server publish catalogs of security label for use by clients.
Two identical catalog requests may return different results, even for the same requester, as the results may depend on numerous factors. It is suggested that clients request a catalog for use in a short-lived context, such as short-lived 1-to-1 chat session, for all use in stanzas of that session. For use in long-lived context, such as a long-lived Multi-User Chat session, it is suggested the client request the current catalog when the user becomes present after a period of extended absence. Alternatively, a client could simply cache catalog results for a configurable amount of time. With either approach, it is also suggested clients provide a means for the user to request an immediate refresh of all catalogs in all contexts. This is useful where the user made changes to a personal label catalog which the XMPP server uses as input in processing catalog requests. Note: there is no requirement that XMPP servers support 'personal label catalogs' (such details are beyond the scope of this document).
If catalog is restrictive, as indicated by the restrict= attribute with value of true, the client SHOULD restrict the user to choosing one of the items from the catalog and use the label of that item (or no label if the selected item is empty).
One and only one of the items may have a default= attribute with value of true. The client should default the label selection to this item in cases where the user has not selected an item. An item may have no security label. Such an item explicitly offers a choice of sending a stanza without a label. A non-restrictive catalog implicitly offers this choice when it does not contain an empty item.

Each catalog provided should only contain labels for which the client is allowed to use (based upon the user's authorization) in a particular context (such as in chat room). A catalog may not include the complete set of labels available for the use by the client in the context.
Note: the single catalog per context approach used here is likely inadequate in environments where there are a large number of labels in use. It is expected that a more sophisticated approach will be introduced in a subsequent revision of this specification.
As each service domain may have different support for security labels, servers should advertise and clients should perform appropriate discovery lookups on a per service basis.
To indicate the support for label catalog discovery, a server advertises the urn:xmpp:sec-label:catalog:2 feature. The following pair of examples illustrates this feature discovery.
Items in the catalog may contain a selector= attribute. The value of this attribute represents the item's placement in a hierarchical organization of the items. If one item has a selector= attribute, all items should have a selector= attribute. The value of the selector= attribute conforms to the selector-value ABNF production:

```
selector-value = (<item>"|")*<item>
```

where <item/> is a sequence of characters not including "|".
A value of "X|Y|Z" indicates that this item is "Z" in the the "Y" subset of the "X" subset of items. This information may be used, for instance, in generating label selection menus in graphical user interfaces.
Note: use of unnecessarily deep hierarchies should be avoided.

Listing 6: Label Catalog Feature Discovery request

```
<iq type='get'
    to='example.com'
    from='user@example.com/Work'
    id='disco1'>
  <query xmlns='http://jabber.org/protocol/disco#info'/>
</iq>
```

Listing 7: Label Information Feature Discovery response

```
<iq type='result'
    from='example.com'
    to='user@example.com/Work'
    id='disco1'>
  <query xmlns='http://jabber.org/protocol/disco#info'>
    ...
    <feature var='urn:xmpp:sec-label:catalog:2'/>
    ...
  </query>
</iq>
```

The following example pair illustrates catalog discovery. The client directs the <iq/> to its server regardless of which catalog it requests via the to= attribute of in <catalog/> element.

The client SHOULD NOT provide a from= attribute in the <catalog/> element.

Listing 8: Label Catalog request

```
<iq to='example.com' type='get' id='cat1'>
  <catalog xmlns='urn:xmpp:sec-label:catalog:2' to='example.com'/>
</iq>
```

Listing 9: Label Catalog Get response

```
<iq type='result' to='user@example.com/Work' id='cat1'>
  <catalog xmlns='urn:xmpp:sec-label:catalog:2'
      to='example.com' name='Default'
      desc='an example set of labels'
          restrict='false'>
        <item selector="Classified|SECRET">
            <securitylabel xmlns='urn:xmpp:sec-label:0'>
                <displaymarking fgcolor='black' bgcolor='red'>SECRET</
                    displaymarking>
                <label>
                    <esssecuritylabel xmlns='urn:xmpp:sec-label:ess:0'
                        >MQYCAQQGASk=</esssecuritylabel>
                </label>
            </securitylabel>
        </item>
        <item selector="Classified|CONFIDENTIAL">
            <securitylabel xmlns='urn:xmpp:sec-label:0'>
                <displaymarking fgcolor='black' bgcolor='navy'>
                    CONFIDENTIAL</displaymarking>
                <label>
                    <esssecuritylabel xmlns='urn:xmpp:sec-label:ess:0'
                        >MQYCAQMGASk</esssecuritylabel>
                </label>
            </securitylabel>
        </item>
        <item selector="Classified|RESTRICTED">
            <securitylabel xmlns='urn:xmpp:sec-label:0'>
                <displaymarking fgcolor='black' bgcolor='aqua'>
                    RESTRICTED</displaymarking>
                <label>
                    <esssecuritylabel xmlns='urn:xmpp:sec-label:ess:0'
                        >MQYCAQIGASk=</esssecuritylabel>
                </label>
            </securitylabel>
        </item>
        <item selector="UNCLASSIFIED" default="true"/>
  </catalog>
</iq>
```

Where the server needs to obtain a catalog from another server in order to respond to its client, it can send an <iq/> to that server requesting that catalog. The requesting server provides the bare JID of the requesting user in the from= attribute in the <catalog/> element when it desires a catalog to be prepared specifically for the user. Otherwise the from= attribute in the <catalog/> element is absent.

5 Use in XMPP

The sensitivity-based access control decisions discussed herein are to be made independently of other access control decisions or other facilities. That is, the sensitivity-based access control decisions are not conditional on other factors.

It is intended that <securitylabel/> elements are only used as prescribed by this document, documents extending this document, or other formal specifications. Any other use of <securitylabel/> SHOULD be viewed as a protocol violation. The stanza SHOULD be discarded with, if appropriate, an error response. Such error responses SHOULD NOT include content from the violating stanza, excepting that necessary to well-formed error responses. Error responses MUST NOT contain a <securitylabel/> element. Any such error response violates this protocol and MUST be discarded by servers implementing this specification. Error responses MUST NOT be subjected to security label authorization checks. However, this prohibition does not preclude a server from taking appropriate action to prevent the disclosure of sensitive information, such as closing the stream.

When use of a <securitylabel/> element is prescribed, that use is RECOMMENDED. Absence of a <securitylabel/> element implies the stanza has the default label as specified in the governing security policy. Given that the governing policy may not specify a default label, hence denying access to the stanza, supporting clients SHOULD provide a <securitylabel/> element where prescribed.

Typically, a client would allow the user to choose populate the <securitylabel/> from one of from a small set of security labels selections known to it (through configuration and/or discovery and/or other means), such as from a pull-down menu. That selection would include appropriate values for the <label/>, <displaymarking/>, and <equivalentlabel/> elements.

A policy-aware client may provide the user with an interface allowing the user to produce custom labeling data for inclusion in this set. A policy-aware client SHOULD preclude the user from producing <label/> values which the user's own clearance does not grant access to, and SHOULD preclude sending any label which the user's own clearance does not grant access to. Each <equivalentlabel/> value, if any, MUST be equivalent under an equivalent policy to the <label/>. The <displaymarking/> element SHOULD be set the display marking prescribed for the <label/> under the governing policy, or, if the governing policy prescribes no display marking for the <label/>, absent.

A client which receives a stanza with <securitylabel/> element is to prominently display the <displaymarking/> value. A policy-aware client may alternatively prominently display the marking for the <label/> prescribed by the governing policy.

Each server is expected to make a number of sensitivity-based authorization decisions. Each

decision is made by evaluating an Access Control Decision Function (ACDF) with a governing policy, a clearance, and a security label. The ACDF yields either *Grant* or *Deny*.
If the user holds a valid clearance (known to the server) under the governing policy, the clearance input is the user's clearance. Otherwise, if the governing policy provides a default clearance, the clearance input is the default clearance. Otherwise, the clearance input is the nil clearance. The nil clearance is a clearance for which the ACDF always returns Deny when given as the clearance input.
If the stanza contains a <securitylabel/> element and the either the <label/> element or one of the <equivalentlabel/> elements contain an appropriate label, that label input is that label. Otherwise, the label input is the default label provided the governing policy or, if no default label is provided, the nil label. The nil label is a label for which the ACDF always returns Deny when given as the label input.
The term "effective clearance" and "effective label" refer, respectively, to the clearance and label provided as input to the ACDF.
Not all sensitivity-based authorization decisions an XMPP server might make involve a user clearance and/or stanza label. A server may only provide service to users which hold an appropriate clearance as determined by calling the ACDF with the user's clearance and a label associated with the service. A clearance might also be associated with the service to restrict the set of labels may be used in labeling stanzas. Labels and clearances can also be associated with network interfaces, remote servers, and chat rooms.

5.1 Use in Instant Messaging

A client may provide a <securitylabel/> element in any <message/> it sends.

5.2 Use in Group Chat and Multi-User Chat

A client may provide a <securitylabel/> element in <message/> stanzas.

5.2.1 Discovery

A server SHOULD provide a label feature and information discovery for the room.
Clients SHOULD discover label feature and information on a per room basis.

5.2.2 Sending Messages

Sending groupchat messages is similar to sending normal messages, however their are a few differences.
Groupchat messages are addressed to the room. The room clearance must be suitable for the message label, else it should be rejected.
The room's clearance may allow a variety of labels to be used. Not all participants may

be cleared for all labels allowed in the room. The server MUST only deliver messages to participants for which they are cleared to receive.

5.2.3 Room History

The server MUST only deliver messages to participants for which they are cleared to receive.

5.2.4 Private Messages

Private messages SHOULD be handled much like groupchat messages, including rejection of messages for a label not suitable for the room. The server MUST NOT deliver messages to participants for which they are cleared to receive.

5.2.5 Invitations

Invitations may be labeled.

5.2.6 Room Subject

A stanza intended to change the room subject SHOULD not carry a security label and SHOULD NOT be subject to security-label authorization checks. Such a stanza does not have any impact on the security-label parameters associated with the room.

5.2.7 Room Configuration

The server may allow for configuration of security label parameters via room configuration mechanisms. The approach is intended to be ad-hoc. Hence this section is intended to be illustrative of one possible approach. Implementations are free to utilize other approaches.

Listing 10: Room Configuration Form

```
<iq from='room@muc.example.com'
    id='create1'
    to='user@example.com/Work'
    type='result'>
<query xmlns='http://jabber.org/protocol/muc#owner'>
    <x xmlns='jabber:x:data' type='form'>
       <title>"darkcave" room configuration</title>
       ...
       <field label='Room␣Label' type='list-single' var='sec-label#
           label'>
```

```
        <value>Catalog:UNCLASSIFIED</value>
        <option label='SECRET'><value>Catalog:SECRET</value></option>
        <option label='CONFIDENTIAL'><value>Catalog:CONFIDENTIAL</value
            ></option>
        <option label='UNCLASSIFED'><value>Catalog:UNCLASSIFIED</value>
            </option>
        <option label='Custom'><value>Custom</value></option>
        </field>
        <field label='Custom␣Room␣Label' type='text-single'
             var='sec-label#custom-label'/>

        <field label='Room␣Allowed␣Markings' type='list-multi' var='sec
            -label#clearance'>
        <value>Catalog:UNCLASSIFIED</value>
        <option label='SECRET'><value>Catalog:SECRET</value></option>
        <option label='CONFIDENTIAL'><value>Catalog:CONFIDENTIAL</value
            ></option>
        <option label='UNCLASSIFED'><value>Catalog:UNCLASSIFIED</value>
            </option>
        <option label='Custom'><value>Custom</value></option>
        </field>
        <field label='Custom␣Room␣Clearance' type='text-single'
             var='sec-label#custom-clearance'/>
    </x>
</query>
</iq>
```

In the above example, the server allows the room label to be set to one of to a subset of labels from the label catalog (see below), using the display name for selection, as well as custom label support. For custom label choice support, the server offers an single text box for entry of an appropriate text string indicating the label to use. Likewise for the room clearance and default room clearance.
Though offering choices from the label catalog is often desirable, a server could only offer custom label and/or clearance support.

Listing 11: Room Configuration Form

```
<iq from='room@muc.example.com'
    id='create1'
    to='user@example.com/Work'
    type='result'>
<query xmlns='http://jabber.org/protocol/muc#owner'>
    <x xmlns='jabber:x:data' type='form'>
        <title>"darkcave" room configuration</title>
        ...
        <field label='Room␣Label' type='text-single'
             var='sec-label#custom-label'/>
        <field label='Room␣Clearance' type='text-single'
             var='sec-label#custom-clearance'/>
```

```
    </x>
</query>
</iq>
```

5.3 Use in Presence

<securitylabel/> elements are not to appear in <presence/> stanzas. Server SHALL treat any <presence/> stanza that contains a <securitylabel/> as a protocol violation.
Presence information is subject to sensitivity-base authorization decisions, however these decisions are made are made using a label associated with the presence resource, such as a chat room's label.

6 Extension Considerations

This extension is itself extensible. In particular, the <label/> and <equivalentlabel/> elements are designed to hold a range of security labels formats. XML name spaces SHOULD be used to avoid name clashes.
Future documents may specify how security-labels are used in other areas of XMPP, such as PubSub.

7 Security Considerations

This document is all about authorization, a key aspect of security. Hence, security considerations are discussed through this document.
Nothing in this document ensures appropriate labeling the sensitivity of a piece of information. Addressing inappropriate labeling of information is beyond the scope of this document.
Certain XMPP stanzas, such as <presence/> stanzas, are not themselves subject to any sensitivity-based authorization decisions, and may be forwarded throughout the XMPP network. The content of these stanzas should not contain information requiring sensitivity-based dissemination controls.
It is desirable to securely bind the security label to the object it labels. This may be accomplished through use of digital signatures. Specification of such is left to a future document.

8 IANA Considerations

This document requires no interaction with the Internet Assigned Numbers Authority (IANA) [8].

[8] The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols, such as port numbers and URI schemes. For further information, see

9 XMPP Registrar Considerations

9.1 Protocol Namespaces

This specification defines the following XML namespaces:

- urn:xmpp:sec-label:0
- urn:xmpp:sec-label:catalog:2
- urn:xmpp:sec-label:ess:0

The XMPP Registrar [9] includes the foregoing namespaces in the registry located at <https://xmpp.org/registrar/namespaces.html>, as described in Section 4 of XMPP Registrar Function (XEP-0053) [10].

9.2 Protocol Versioning

If the protocol defined in this specification undergoes a revision that is not fully backwards-compatible with an older version, the XMPP Registrar shall increment the protocol version number found at the end of the XML namespaces defined herein, as described in Section 4 of XEP-0053.

10 XML Schemas

10.1 Extension Schema

```
<?xml version='1.0' encoding='UTF-8'?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" targetNamespace
    ="urn:xmpp:sec-label:0"
    xmlns="urn:xmpp:sec-label:0" elementFormDefault="qualified">

    <xs:annotation>
      <xs:documentation>
        The protocol documented by this schema is defined in
        XEP-0258: http://xmpp.org/extensions/xep-0258.html
```

<http://www.iana.org/>.

[9] The XMPP Registrar maintains a list of reserved protocol namespaces as well as registries of parameters used in the context of XMPP extension protocols approved by the XMPP Standards Foundation. For further information, see <https://xmpp.org/registrar/>.

[10] XEP-0053: XMPP Registrar Function <https://xmpp.org/extensions/xep-0053.html>.

```
    </xs:documentation>
  </xs:annotation>

  <xs:simpleType name="colorCSS">
    <xs:annotation>
      <xs:documentation>CSS colors (W3C colors + "orange")</
          xs:documentation>
    </xs:annotation>
    <xs:restriction base="xs:string">
      <xs:enumeration value="aqua"/>
      <xs:enumeration value="black"/>
      <xs:enumeration value="blue"/>
      <xs:enumeration value="fuschia"/>
      <xs:enumeration value="gray"/>
      <xs:enumeration value="green"/>
      <xs:enumeration value="lime"/>
      <xs:enumeration value="maroon"/>
      <xs:enumeration value="navy"/>
      <xs:enumeration value="olive"/>
      <xs:enumeration value="purple"/>
      <xs:enumeration value="red"/>
      <xs:enumeration value="silver"/>
      <xs:enumeration value="teal"/>
      <xs:enumeration value="white"/>
      <xs:enumeration value="yellow"/>
      <xs:enumeration value="orange"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="colorRGB">
    <xs:annotation>
      <xs:documentation>Hex encoded RGB</xs:documentation>
    </xs:annotation>
    <xs:restriction base="xs:string">
      <xs:pattern value="#[0-9A-Fa-f]{6}"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="color">
    <xs:annotation>
      <xs:documentation>Color</xs:documentation>
    </xs:annotation>
    <xs:union memberTypes="colorCSS colorRGB"/>
  </xs:simpleType>

  <xs:complexType name="displaymarking">
    <xs:annotation>
      <xs:documentation>Display Marking</xs:documentation>
```

```
            <xs:documentation>String to be prominently displayed along
                with labeled
                object.</xs:documentation>
        </xs:annotation>
        <xs:simpleContent>
            <xs:extension base="xs:string">
                <xs:attribute name="bgcolor" type="color" use="
                    optional" default="white"/>
                <xs:attribute name="fgcolor" type="color" use="
                    optional" default="black"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>

    <xs:complexType name="label">
        <xs:choice minOccurs="0">
            <xs:any namespace="##other" processContents="lax"/>
        </xs:choice>
    </xs:complexType>

    <xs:element name="securitylabel">
        <xs:annotation>
            <xs:documentation>A Security Label</xs:documentation>
        </xs:annotation>
        <xs:complexType>
            <xs:sequence>
                <xs:element name="displaymarking" type="displaymarking
                    ">
                    <xs:annotation>
                        <xs:documentation>A Display Marking</
                            xs:documentation>
                        <xs:documentation>To be prominently displayed<
                            /xs:documentation>
                    </xs:annotation>
                </xs:element>
                <xs:element name="label" type="label">
                    <xs:annotation>
                        <xs:documentation>The Primary Label</
                            xs:documentation>
                    </xs:annotation>
                </xs:element>
                <xs:element name="equivalentlabel" type="label"
                    minOccurs="0" maxOccurs="unbounded">
                    <xs:annotation>
                        <xs:documentation>An Equivalent Label</
                            xs:documentation>
                    </xs:annotation>
                </xs:element>
            </xs:sequence>
```

```
        </xs:complexType>
    </xs:element>
</xs:schema>
```

A copy of this schema is available at http://xmpp.org/schemas/sec-label.xsd.

10.2 <catalog/> schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:sl="
    urn:xmpp:sec-label:0"
    xmlns="urn:xmpp:sec-label:catalog:2" targetNamespace="urn:xmpp:sec
        -label:catalog:2"
    elementFormDefault="qualified">

    <xs:annotation>
      <xs:documentation>
        The protocol documented by this schema is defined in
        XEP-0258: http://xmpp.org/extensions/xep-0258.html
      </xs:documentation>
    </xs:annotation>

    <xs:import schemaLocation="sec-label.xsd" namespace="urn:xmpp:sec-
        label:0"/>

    <xs:attribute name="to" type="xs:string">
        <xs:annotation>
            <xs:documentation>Target JabberId</xs:documentation>
        </xs:annotation>
    </xs:attribute>

    <xs:attribute name="from" type="xs:string">
        <xs:annotation>
            <xs:documentation>Target JabberId</xs:documentation>
        </xs:annotation>
    </xs:attribute>

    <xs:attribute name="name" type="xs:string">
        <xs:annotation>
            <xs:documentation>Name</xs:documentation>
        </xs:annotation>
    </xs:attribute>

    <xs:attribute name="desc" type="xs:string">
        <xs:annotation>
            <xs:documentation>Description</xs:documentation>
        </xs:annotation>
    </xs:attribute>
```

```
<xs:attribute name="id" type="xs:string">
    <xs:annotation>
        <xs:documentation>Identifer for current revision, commonly
            a hash</xs:documentation>
    </xs:annotation>
</xs:attribute>

<xs:attribute name="size" type="xs:integer">
    <xs:annotation>
        <xs:documentation>Number of items</xs:documentation>
    </xs:annotation>
</xs:attribute>

<xs:attribute name="restrict" type="xs:boolean">
    <xs:annotation>
        <xs:documentation>Restrictive</xs:documentation>
    </xs:annotation>
</xs:attribute>

<xs:attribute name="selector" type="xs:string">
    <xs:annotation>
        <xs:documentation>User input selector</xs:documentation>
    </xs:annotation>
</xs:attribute>

<xs:attribute name="default" type="xs:boolean">
    <xs:annotation>
        <xs:documentation>default selection</xs:documentation>
    </xs:annotation>
</xs:attribute>

<xs:element name="catalog">
    <xs:annotation>
        <xs:documentation>A Catalog of Labels</xs:documentation>
    </xs:annotation>

    <xs:complexType>
        <xs:sequence>
            <xs:element name="item" minOccurs="0" maxOccurs="
               unbounded">
                <xs:complexType>
                    <xs:sequence minOccurs="0">
                        <xs:element ref="sl:securitylabel"/>
                    </xs:sequence>
                    <xs:attribute ref="selector" use="optional"/>
                    <xs:attribute ref="default" use="optional"/>
                </xs:complexType>
            </xs:element>
```

```
            </xs:sequence>
            <xs:attribute ref="to" use="optional"/>
            <xs:attribute ref="from" use="optional"/>
            <xs:attribute ref="name" use="optional"/>
            <xs:attribute ref="desc" use="optional"/>
            <xs:attribute ref="id" use="optional"/>
            <xs:attribute ref="size" use="optional"/>
            <xs:attribute ref="restrict" use="optional"/>
        </xs:complexType>
    </xs:element>
</xs:schema>
```

A copy of this schema is available at http://xmpp.org/schemas/sec-label-catalog.xsd.

10.3 <esssecuritylabel/> schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" targetNamespace
    ="urn:xmpp:sec-label:ess:0"
    xmlns="urn:xmpp:sec-label:ess:0" elementFormDefault="qualified">

    <xs:annotation>
      <xs:documentation>
        The protocol documented by this schema is defined in
        XEP-0258: http://xmpp.org/extensions/xep-0258.html
      </xs:documentation>
    </xs:annotation>

    <xs:element name="esssecuritylabel" type="xs:base64Binary">
        <xs:annotation>
            <xs:documentation>An S/MIME ESS SecurityLabel [RFC2634]</
                xs:documentation>
            <xs:documentation>Value is the base64 encoding of the BER/
                DER encoding of an ASN.1
                 ESSSecurityLabel type as defined in RFC 2634. </
                    xs:documentation>
        </xs:annotation>
    </xs:element>
</xs:schema>
```

A copy of this schema is available at http://xmpp.org/schemas/sec-label-ess.xsd.