XEP-0314: Security Labels in PubSub

Ashley Ward
mailto:ashley.ward@surevine.com
xmpp:ashward@jabber.org
http://www.surevine.com/

2012-07-27
Version 0.1

Status	Type	Short Name
Deferred	Standards Track	NOT_YET_ASSIGNED

This specification defines an extension to XEP-0258 (Security Labels) to allow for the use of security labels in XEP-0060 (Publish-Subscribe). This document describes how security label metadata can be applied to the various elements within Publish-Subscribe, including nodes and items.

Legal

Copyright

Permissions

Warranty

Liability

Conformance

Contents

1 Introduction

The use of security labels within XMPP is currently defined in Security Labels in XMPP (XEP-0258) [1]. This, however, does not cover the use of security labels within Publish-Subscribe (XEP-0060) [2]. This XEP defines a method to include security labels into publish-subscribe.
This allows content publishers to limit visibility of any sensitive published items to only those users with appropriate clearance to view them.
This document does not deal with the semantics of a Security Label or how the security policy is applied to decisions regarding Security Labels and Clearances.
This document should be read in conjunction with Publish-Subscribe (XEP-0060) [3] and Security Labels in XMPP (XEP-0258) [4].

2 Requirements

- A publisher MUST be able to apply a Security Label to items within a node.
- A node creator SHOULD be able to apply a Security Label to a node (this controls which entities can access the node).
- A node creator SHOULD be able to apply a Clearance to a node (this controls which Security Labels can be applied to items within the node).
- A node creator MAY be able to apply a default Security Label to a node (this applies to items published to the node without a Security Label).
- Node lists returned by the server SHOULD NOT contain nodes that the requesting entity is not Cleared to view.
- Item lists returned by the server MUST NOT contain items that the requesting entity is not Cleared to view.
- A client SHOULD only publish items to a node that are compatible with the Clearance of the node (if the node has a Clearance), and a server MUST NOT store such items against the node or send any notifications of any such items to subscribers.
- Server responses from a request involving a node that the entity is not Cleared to view SHOULD be identical to a response as if that node did not exist.
- Server responses from a request involving an item that the entity is not Cleared to view MUST be identical to a response as if that item did not exist.
- A server MUST NOT notify or deliver items to an entity that the entity does not have appropriate Clearance to view.

[1] XEP-0258: Security Labels in XMPP <https://xmpp.org/extensions/xep-0258.html>.
[2] XEP-0060: Publish-Subscribe <https://xmpp.org/extensions/xep-0060.html>.
[3] XEP-0060: Publish-Subscribe <https://xmpp.org/extensions/xep-0060.html>.
[4] XEP-0258: Security Labels in XMPP <https://xmpp.org/extensions/xep-0258.html>.

3 Glossary

In addition to the Glossary defined for Publish-Subscribe (XEP-0060) [5] the following terms are used:

Security Label A label that can be applied to content to restrict the visibility of the content to entities with appropriate Clearance. The schema is defined in Security Labels in XMPP (XEP-0258) XEP-0258: Security Labels in XMPP <https://xmpp.org/extensions/xep-0258.html>. with the XML namespace "urn:xmpp:sec-label:0".

Clearance A collection of Security Labels that an entity is authorized to access.

Cleared An entity is Cleared to access content if the Access Control Decision Function (ACDF) of the server yields a Grant given the entity's Clearance, the Security Label of the content and the governing security policy.

4 Entity Use Cases

This section defines the additions and caveats for the use cases and protocols defined in Publish-Subscribe (XEP-0060) [6].

4.1 Discovering Feature Support

A Security Label aware client SHOULD discover support for Security Labels within the Publish-Subscribe (XEP-0060) [7] service domain. If the service domain does not report support for Security Labels then the client SHOULD NOT publish with Security Labels.

Listing 1: Service discovery information request

```
<iq from='francisco@denmark.lit/barracks'
    id='disco1'
    to='pubsub.shakespeare.lit'
    type='get'>
  <query xmlns='http://jabber.org/protocol/disco#info'/>
</iq>
```

Listing 2: Service discovery information response

```
<iq from='pubsub.shakespeare.lit'
    id='disco1'
    to='francisco@denmark.lit/barracks'
```

[5] XEP-0060: Publish-Subscribe <https://xmpp.org/extensions/xep-0060.html>.
[6] XEP-0060: Publish-Subscribe <https://xmpp.org/extensions/xep-0060.html>.
[7] XEP-0060: Publish-Subscribe <https://xmpp.org/extensions/xep-0060.html>.

```
    type='result'>
  <query xmlns='http://jabber.org/protocol/disco#info'>
    ...
    <feature var='urn:xmpp:sec-label:0'/>
    ...
  </query>
</iq>
```

A server SHOULD provide label feature and information discovery for each node.
Clients SHOULD discover label feature and information on a per-node basis.

Listing 3: Label feature discovery request for a node

```
<iq from='francisco@denmark.lit/barracks'
    id='disco2'
    to='pubsub.shakespeare.lit'
    type='get'>
  <query node='princely_musings' xmlns='http://jabber.org/protocol/
    disco#info'/>
</iq>
```

Listing 4: Label feature discovery response for a node

```
<iq from='pubsub.shakespeare.lit'
    id='disco2'
    to='francisco@denmark.lit/barracks'
    type='result'>
  <query node='princely_musings' xmlns='http://jabber.org/protocol/
    disco#info'>
    ...
    <feature var='urn:xmpp:sec-label:catalog:2'/>
    ...
  </query>
</iq>
```

A server SHOULD provide Security Label catalog discovery for each node.
Clients SHOULD discover the Security Label catalog on a per-node basis.
The server SHOULD limit the catalog for a node to those labels that are compatible with any Clearance associated with the node.

Listing 5: The client requests the catalog for a node

```
<iq id='cat1'
    to='pubsub.shakespeare.lit'
    type='get'>
  <catalog xmlns='urn:xmpp:sec-label:catalog:2'
           to='pubsub.shakespeare.lit'
           node='princely_musings'/>
</iq>
```

Listing 6: The server responds with the catalog for the node

```
<iq from='pubsub.shakespeare.lit'
    id='cat1'
    to='francisco@denmark.lit/barracks'
    type='result'>
  <catalog xmlns='urn:xmpp:sec-label:catalog:2'
      to='example.com'
      name='Default'
      desc='The␣set␣of␣labels␣applicable␣to␣the␣&quot;princely_musings
          &quot;␣node'
      restrict='false'
      node='princely_musings'>
    <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>
```

4.2 Discover Nodes

The server SHOULD NOT return any nodes that have a Security Label that the entity is not Cleared to view.

Listing 7: Entity request list of top-level nodes

```
<iq from='francisco@denmark.lit/barracks'
    id='nodes1'
    to='pubsub.shakespeare.lit'
    type='get'>
  <query xmlns='http://jabber.org/protocol/disco#items'/>
</iq>
```

Listing 8: Server responds with list of nodes with Security Labels

```
<iq type='result'
    from='pubsub.shakespeare.lit'
    to='francisco@denmark.lit/barracks'
    id='nodes1'
    xmlns:slps='urn:xmpp:sec-label:pubsub:0'>
  <query xmlns='http://jabber.org/protocol/disco#items'>
    <item jid='pubsub.shakespeare.lit'
          node='blogs'
          name='Weblog updates'
          slps:label='seclabel-1'/>
    <item jid='pubsub.shakespeare.lit'
          node='news'
          name='News and announcements'
          slps:label='seclabel-2'/>
    <securitylabel xmlns='urn:xmpp:sec-label:0' slps:id='seclabel-1'>
      <displaymarking fgcolor='black' bgcolor='green'>UNCLASSIFIED</
          displaymarking>
      <label>
        <esssecuritylabel xmlns='urn:xmpp:sec-label:ess:0'>MQMGASk=</
            esssecuritylabel>
      </label>
    </securitylabel>
    <securitylabel xmlns='urn:xmpp:sec-label:0' slps:id='seclabel-2'>
      <displaymarking fgcolor='black' bgcolor='red'>SECRET</
          displaymarking>
      <label>
        <esssecuritylabel xmlns='urn:xmpp:sec-label:ess:0'>MQYCAQIGASk
            =</esssecuritylabel>
      </label>
    </securitylabel>
  </query>
</iq>
```

4.3 Discover Items for a Node

The item list MUST NOT contain items that the entity is not Cleared to view.
The server SHOULD return an <item-not-found/> error if the entity is not Cleared to view the node.
See Subscriber Use Cases: Retrieve Items from a Node for more details of how Security Labels are respresented in the server response.

Listing 9: Entity requests all of the items for a node

```
<iq from='francisco@denmark.lit/barracks'
    id='items1'
    to='pubsub.shakespeare.lit'
    type='get'>
  <query xmlns='http://jabber.org/protocol/disco#items'
         node='princely_musings'/>
</iq>
```

Listing 10: Server responds with items in the node

```
<iq from='pubsub.shakespeare.lit'
    id='items1'
    to='francisco@denmark.lit/barracks'
    type='result'
    xmlns:slps='urn:xmpp:sec-label:pubsub:0'>
  <query xmlns='http://jabber.org/protocol/disco#items'
         node='princely_musings'>
    <item
      jid='pubsub.shakespeare.lit'
      name='368866411b877c30064a5f62b917cffe'
      slps:label='seclabel-1'/>
    <item
      jid='pubsub.shakespeare.lit'
      name='3300659945416e274474e469a1f0154c'
      slps:label='seclabel-1'/>
    <item
      jid='pubsub.shakespeare.lit'
      name='4e30f35051b7b8b42abe083742187228'
      slps:label='seclabel-2'/>
    <item
      jid='pubsub.shakespeare.lit'
      name='ae890ac52d0df67ed7cfdf51b644e901'
      slps:label='seclabel-1'/>
    <securitylabel xmlns='urn:xmpp:sec-label:0' slps:id='seclabel-1'>
      <displaymarking fgcolor='black' bgcolor='green'>UNCLASSIFIED</
          displaymarking>
      <label>
        <esssecuritylabel xmlns='urn:xmpp:sec-label:ess:0'>MQMGASk=</
            esssecuritylabel>
```

```
      </label>
    </securitylabel>
    <securitylabel xmlns='urn:xmpp:sec-label:0' slps:id='seclabel-2'>
      <displaymarking fgcolor='black' bgcolor='red'>SECRET</
          displaymarking>
      <label>
        <esssecuritylabel xmlns='urn:xmpp:sec-label:ess:0'>MQYCAQIGASk
            =</esssecuritylabel>
      </label>
    </securitylabel>
  </query>
</iq>
```

5 Subscriber Use Cases

5.1 Subscribe to a Node

The server SHOULD return an <item-not-found/> error if the subscriber is not Cleared to view the node.

5.2 Retrieve Items from a Node

The server SHOULD return an <item-not-found/> error if the subscriber is not Cleared to view the node.
The item list MUST NOT contain items that the subscriber is not Cleared to view.
The server MUST attach relevant <securitylabel/> child elements to the <items/> element.
Each of these <securitylabel/> elements MUST posess an 'id' attribute (from the urn:xmpp:sec-label:pubsub:0 namespace) which is unique within the stanza.
The server SHOULD normalise the elements so that multiple <item/> elements with the same Security Label reference the same <securitylabel/> element; However, the server might instead include a <securitylabel/> element for each <item/> element regardless of whether there are duplicates.
Each <item/> that has a Security Label MUST posess a 'label' attribute (from the urn:xmpp:sec-label:pubsub:0 namespace) that references the id of the relevant <securitylabel/>.
The server SHOULD NOT include <securitylabel/> elements which are not referenced within the stanza.

Listing 11: The server returns a list of items with Security Labels

```
<iq from='pubsub.shakespeare.lit'
    id='items1'
    to='francisco@denmark.lit/barracks'
    type='result'
    xmlns:slps='urn:xmpp:sec-label:pubsub:0'>
```

```
  <pubsub xmlns='http://jabber.org/protocol/pubsub'>
    <items node='princely_musings'>
      <item id='368866411b877c30064a5f62b917cffe' slps:label='seclabel
          -1'>
        <entry xmlns='http://www.w3.org/2005/Atom'>
          <title>The Uses of This World</title>
          <summary>
O, that this too too solid flesh would melt
Thaw and resolve itself into a dew!
          </summary>
          <link rel='alternate' type='text/html'
                href='http://denmark.lit/2003/12/13/atom03'/>
          <id>tag:denmark.lit,2003:entry-32396</id>
          <published>2003-12-12T17:47:23Z</published>
          <updated>2003-12-12T17:47:23Z</updated>
        </entry>
      </item>
      <item id='3300659945416e274474e469a1f0154c' slps:label='seclabel
          -1'>
        <entry xmlns='http://www.w3.org/2005/Atom'>
          <title>Ghostly Encounters</title>
          <summary>
O all you host of heaven! O earth! what else?
And shall I couple hell? O, fie! Hold, hold, my heart;
And you, my sinews, grow not instant old,
But bear me stiffly up. Remember thee!
          </summary>
          <link rel='alternate' type='text/html'
                href='http://denmark.lit/2003/12/13/atom03'/>
          <id>tag:denmark.lit,2003:entry-32396</id>
          <published>2003-12-12T23:21:34Z</published>
          <updated>2003-12-12T23:21:34Z</updated>
        </entry>
      </item>
      <item id='4e30f35051b7b8b42abe083742187228' slps:label='seclabel
          -2'>
        <entry xmlns='http://www.w3.org/2005/Atom'>
          <title>Alone</title>
          <summary>
Now I am alone.
O, what a rogue and peasant slave am I!
          </summary>
          <link rel='alternate' type='text/html'
                href='http://denmark.lit/2003/12/13/atom03'/>
          <id>tag:denmark.lit,2003:entry-32396</id>
          <published>2003-12-13T11:09:53Z</published>
          <updated>2003-12-13T11:09:53Z</updated>
        </entry>
      </item>
```

```
      <item id='ae890ac52d0df67ed7cfdf51b644e901' slps:label='seclabel
         -1'>
        <entry xmlns='http://www.w3.org/2005/Atom'>
          <title>Soliloquy</title>
          <summary>
To be, or not to be: that is the question:
Whether 'tis␣nobler␣in␣the␣mind␣to␣suffer
The␣slings␣and␣arrows␣of␣outrageous␣fortune,
Or␣to␣take␣arms␣against␣a␣sea␣of␣troubles,
And␣by␣opposing␣end␣them?
␣␣␣␣␣␣␣␣␣␣</summary>
␣␣␣␣␣␣␣␣␣␣<link␣rel='alternate'␣type='text/html'
␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣href='http://denmark.lit/2003/12/13/atom03'/>
␣␣␣␣␣␣␣␣␣␣<id>tag:denmark.lit,2003:entry-32397</id>
␣␣␣␣␣␣␣␣␣␣<published>2003-12-13T18:30:02Z</published>
␣␣␣␣␣␣␣␣␣␣<updated>2003-12-13T18:30:02Z</updated>
␣␣␣␣␣␣␣␣</entry>
␣␣␣␣␣␣</item>
␣␣␣␣␣␣<securitylabel␣xmlns='urn:xmpp:sec-label:0'␣slps:id='seclabel-1'
    >
␣␣␣␣␣␣␣␣<displaymarking␣fgcolor='black'␣bgcolor='green'>UNCLASSIFIED</
    displaymarking>
␣␣␣␣␣␣␣␣<label>
␣␣␣␣␣␣␣␣␣␣<esssecuritylabel␣xmlns='urn:xmpp:sec-label:ess:0'>MQMGASk
    =</esssecuritylabel>
␣␣␣␣␣␣␣␣</label>
␣␣␣␣␣␣</securitylabel>
␣␣␣␣␣␣<securitylabel␣xmlns='urn:xmpp:sec-label:0'␣slps:id='seclabel-2'
    >
␣␣␣␣␣␣␣␣<displaymarking␣fgcolor='black'␣bgcolor='red'>SECRET</
    displaymarking>
␣␣␣␣␣␣␣␣<label>
␣␣␣␣␣␣␣␣␣␣<esssecuritylabel␣xmlns='urn:xmpp:sec-label:ess:0'>
    MQYCAQIGASk=</esssecuritylabel>
␣␣␣␣␣␣␣␣</label>
␣␣␣␣␣␣</securitylabel>
␣␣␣␣</items>
␣␣</pubsub>
</iq>
```

6 Publisher Use Cases

6.1 Publish an Item to a Node

A <publish/> element MAY contain a <securitylabel/> which the service must apply to all the items within the <publish/>.
If a publisher wishes to publish multiple items with different Security Labels, they MUST send

multiple <iq/> stanzas - one for each Security Label.
The server SHOULD apply the default label for the node to any items within a <publish/> which does not contain a <securitylabel/>.
Any <securitylabel/> within a <publish/> should be compatible with any Clearance associated with the node, else the service MUST return an <insufficient-clearance/> error.
If a publisher attempts to publish to a node which the publisher is not Cleared to view, the service SHOULD return an <item-not-found/> error.
A publisher SHOULD not attempt to publish an item with a Security Label which is not suitable to the Clearance of the node.
Any <publish/> with a <securitylabel/> should be compatible with the Clearance of the publishing entity, else the server MUST return an <insufficient-clearance/> error.

Listing 12: Publisher publishes an item with a Security Label

```
<iq from='hamlet@denmark.lit/blogbot'
    id='pub1'
    to='pubsub.shakespeare.lit'
    type='set'>
  <pubsub xmlns='http://jabber.org/protocol/pubsub'>
    <publish node='princely_musings'>
      <item>
        <entry xmlns='http://www.w3.org/2005/Atom'>
          <title>Soliloquy</title>
          <summary>
To be, or not to be: that is the question:
Whether 'tis␣nobler␣in␣the␣mind␣to␣suffer
The␣slings␣and␣arrows␣of␣outrageous␣fortune,
Or␣to␣take␣arms␣against␣a␣sea␣of␣troubles,
And␣by␣opposing␣end␣them?
␣␣␣␣␣␣␣␣␣␣</summary>
␣␣␣␣␣␣␣␣␣␣<link␣rel='alternate'␣type='text/html'
␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣href='http://denmark.lit/2003/12/13/atom03'/>
␣␣␣␣␣␣␣␣␣␣<id>tag:denmark.lit,2003:entry-32397</id>
␣␣␣␣␣␣␣␣␣␣<published>2003-12-13T18:30:02Z</published>
␣␣␣␣␣␣␣␣␣␣<updated>2003-12-13T18:30:02Z</updated>
␣␣␣␣␣␣␣␣</entry>
␣␣␣␣␣␣</item>
␣␣␣␣␣␣<securitylabel␣xmlns='urn:xmpp:sec-label:0'>
␣␣␣␣␣␣␣␣<displaymarking␣fgcolor='black'␣bgcolor='green'>UNCLASSIFIED</
    displaymarking>
␣␣␣␣␣␣␣␣<label>
␣␣␣␣␣␣␣␣␣␣<esssecuritylabel␣xmlns='urn:xmpp:sec-label:ess:0'>MQMGASk
    =</esssecuritylabel>
␣␣␣␣␣␣␣␣</label>
␣␣␣␣␣␣</securitylabel>
␣␣␣␣</publish>
␣␣</pubsub>
</iq>
```

The service then notifies appropriately Cleared subscribers. The server MUST NOT notify subscribers that do not have appropriate Clearance to view the item.
The server MUST include the <securitylabel/> element as a child of the <message/> stanza.
The server MUST NOT include the <securitylabel/> element within the <items/> element.
The Security Label applies to the entire message (including all the items within the <items/> element and any <body/> if the entity's subscription is so configured).

Listing 13: Subscriber receives event notification with payload

```
<message from='pubsub.shakespeare.lit' id='foo' to='francisco@denmark.
    lit'>
  <event xmlns='http://jabber.org/protocol/pubsub#event'>
    <items node=princely_musings'>
      <item id='ae890ac52d0df67ed7cfdf51b644e901'>
        <entry xmlns='http://www.w3.org/2005/Atom'>
          <title>Soliloquy</title>
          <summary>
To be, or not to be: that is the question:
Whether 'tis nobler in the mind to suffer
The slings and arrows of outrageous fortune,
Or to take arms against a sea of troubles,
And by opposing end them?
          </summary>
          <link rel='alternate' type='text/html'
                href='http://denmark.lit/2003/12/13/atom03'/>
          <id>tag:denmark.lit,2003:entry-32397</id>
          <published>2003-12-13T18:30:02Z</published>
          <updated>2003-12-13T18:30:02Z</updated>
        </entry>
      </item>
    </items>
  </event>
  <securitylabel xmlns='urn:xmpp:sec-label:0'>
    <displaymarking fgcolor='black' bgcolor='green'>UNCLASSIFIED</
       displaymarking>
    <label>
      <esssecuritylabel xmlns='urn:xmpp:sec-label:ess:0'>MQMGASk=</
         esssecuritylabel>
    </label>
  </securitylabel>
</message>
```

Listing 14: Subscriber receives event notification without payload

```
<message from='pubsub.shakespeare.lit' id='foo' to='francisco@denmark.
    lit'>
  <event xmlns='http://jabber.org/protocol/pubsub#event'>
    <items node=princely_musings'>
      <item id='ae890ac52d0df67ed7cfdf51b644e901' />
```

```
␣␣␣␣</items>
␣␣</event>
␣␣<securitylabel␣xmlns='urn:xmpp:sec-label:0'>
␣␣␣␣<displaymarking␣fgcolor='black'␣bgcolor='green'>UNCLASSIFIED</
    displaymarking>
␣␣␣␣<label>
␣␣␣␣␣␣<esssecuritylabel␣xmlns='urn:xmpp:sec-label:ess:0'>MQMGASk=</
    esssecuritylabel>
␣␣␣␣</label>
␣␣</securitylabel>
</message>
```

6.1.1 Error Cases

If a publisher attempts to publish to a node with a Security Label that is incompatible with the Clearance of the node then the server MUST return an <insufficient-clearance/> error.

Listing 15: Publishing to a node with insufficient node Clearance

```
<iq from='pubsub.shakespeare.lit'
    id='sub1'
    to='francisco@denmark.lit/barracks'
    type='error'>
  <error type='modify'>
    <bad-request xmlns='urn:ietf:params:xml:ns:xmpp-stanzas'/>
    <insufficient-clearance xmlns='urn:xmpp:sec-label:pubsub:errors:0'
        />
  </error>
</iq>
```

If a publisher attempts to publish to a node with a Security Label that is incompatible with the Clearance of the publisher then the server MUST return an <insufficient-clearance/> error.

Listing 16: Publishing to a node with insufficient publisher Clearance

```
<iq from='pubsub.shakespeare.lit'
    id='sub1'
    to='francisco@denmark.lit/barracks'
    type='error'>
  <error type='auth'>
    <insufficient-clearance xmlns='urn:xmpp:sec-label:pubsub:errors:0'
        />
  </error>
</iq>
```

6.2 Delete an item from a node

The server SHOULD return an <item-not-found/> error if the subscriber is not Cleared to view the node or item.
The server MUST NOT send retract requests to subscribers who are not Cleared to view the item.

7 Owner Use Cases

7.1 Node Configuration

The server SHOULD allow for configuration of Security Label parameters for a node via node configuration mechanisms. This approach is intended to be ad-hoc and so this section is intended to be illustrative of one possible approach. Implementations are free to utilize other approaches.
The server MUST disallow a node being created that has a default Security Label that is not within the clearance of the node.

Listing 17: Node configuration form

```
<iq from='pubsub.shakespeare.lit'
    id='config1'
    to='hamlet@denmark.lit/elsinore'
    type='result'>
  <pubsub xmlns='http://jabber.org/protocol/pubsub#owner'>
    <configure node='princely_musings'>
      <x xmlns='jabber:x:data' type='form'>
        ...
        <field label='Node 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='UNCLASSIFIED'><value>Catalog:UNCLASSIFIED</
              value></option>
          <option label='Custom'><value>Custom</value></option>
        </field>
        <field label='Custom Node Label' type='text-single'
            var='sec-label#custom-label'/>

        <field label='Node Clearance' 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='UNCLASSIFIED'><value>Catalog:UNCLASSIFIED</
              value></option>
          <option label='Custom'><value>Custom</value></option>
        </field>
        <field label='Custom Node Clearance' type='text-single'
            var='sec-label#custom-clearance'/>
      </x>
    </configure>
  </pubsub>
</iq>
```

7.1.1 Updating an Existing Node Configuration

Changing the Security Label or Clearance of an existing node is problematic for a number of reasons:

- Subscribers may no longer be Cleared to view a node to which they are already subscribed
- Existing items persisted within a node may be of a higher Security Label than the new node clearance allows

For these reasons an implementation MAY wish to disallow changes to the Security Label of an existing node with subscribers, disallow changes to the Clearance of a node with items, or limit the options within the node configuration to those which do not cause a conflict.
If an implementation chooses to allow a change to the clearance of a node that conflicts with the Security Label of existing items within the node then the server MUST purge the node of all items which are no longer within the updated clearance of the node, with or without notifying subscribers.
If an implementation chooses to allow a change to the Security Label of the node that causes conflicts with existing subscribers to the node then the server MUST remove all subscriptions from subscribers that are no longer Cleared to view the node. The server MUST notify these subscribers. The server SHOULD send a Node Deletion notification, but might instead send a Subscription Cancellation notification if entities are to be aware of the existence of nodes they do not have Clearance to view.
The server MUST prevent a change to the Security Label of the node which would prevent a node owner from accessing the node.

Listing 18: Node Deletion Notification

```
<message from='pubsub.shakespeare.lit' id='deletenotify1' to='
    francisco@denmark.lit'>
  <event xmlns='http://jabber.org/protocol/pubsub#event'>
```

```
    <delete node='princely_musings' />
  </event>
</message>
```

Listing 19: Subscription Cancellation Notification

```
<message from='pubsub.shakespeare.lit' id='unsubnotify1' to='
    horatio@denmark.lit'>
  <event xmlns='http://jabber.org/protocol/pubsub#event'>
    <subscription jid='horatio@denmark.lit' node='princely_musings'
        subscription='none'/>
  </event>
</message>
```

8 Business Rules

1. An entity SHOULD NOT be aware of the existance of nodes or items that they do not have appropriate Clearance to view (But see Implementation Notes: Access to items for which the entity is not Cleared)
2. Items MUST only be accessible by entities with the appropriate Clearance
3. If a node has an associated Clearance then the node MUST only deal with (i.e. persist or notify) items which are compatible with the Clearance

9 Implementation Notes

9.1 Access to Items for which the Entity is not Cleared

The protocol defined has the intention that, as far as possible, an entity should be unaware of the existence of any nodes or items which they are not Cleared to view. Therefore server responses to a request for a node which the entity is not Cleared to view SHOULD be identical to a response as if that node did not exist (See BR1), i.e. an <item-not-found/> error is returned

Listing 20: Request for a node that the entity is not Cleared to view

```
<iq from='pubsub.shakespeare.lit'
    id='sub1'
    to='francisco@denmark.lit/barracks'
    type='error'>
  <error type='cancel'>
    <item-not-found xmlns='urn:ietf:params:xml:ns:xmpp-stanzas'/>
  </error>
</iq>
```

It is worth noting that there are certain situations where this is impossible, for example if an entity wishes to create a node with the same NodeID as an existing node that they are not Cleared to view.
Alternatively, an implementation might wish to relax this rule and allow entities to become aware of nodes they do not have Clearance to view. In this case an <insufficient-clearance/> error MAY be returned instead.

9.2 Collection Nodes

If a service implements PubSub Collection Nodes (XEP-0248) [8] then there will need to be some consideration of node and item visibility within the node hierarchy.
Due to the complexity of the access control policies involved, an implementation MAY choose to do one or more of the following to simplify the implementation:

- Prevent the use of Security Labels and/or Clearances on collection nodes.
- Prevent publishing items with Security Labels to non-orphan leaf nodes (i.e. leaf nodes with an association to a collection node).
- Prevent the association of leaf nodes containing Security Labelled items with collection nodes.
- Prevent the association of Security Labelled nodes with collection nodes.

The rules and protocols defined elsewhere in this document are generally applicable to collection nodes with the following additions:

9.2.1 Notifications

A collection node MUST NOT forward a publish notification with a Security Label that is incompatible with the Clearance of the collection node.
A collection node SHOULD NOT forward a node change notification (create/update/delete/associate) where the Security Label of the affected node is incompatible with the Clearance of the collection node.
The server SHOULD NOT send node change notifications to any entity where the Security Label of the affected node is incompatible with the Clearance of the entity.

9.2.2 Retrieving Items on Collection Nodes

The server MUST NOT return any items from leaf nodes where the individual Security Label of the item is incompatible with the Clearance of the requesting entity.

[8] XEP-0248: PubSub Collection Nodes <https://xmpp.org/extensions/xep-0248.html>.

The server SHOULD NOT return any items from any associated nodes where the Security Label of the leaf node, or any intermediate collection node on the node graph, is incompatible with the Clearance of the requesting entity.

9.2.3 Associating a Node to a Collection

A server SHOULD NOT allow an entity to associate, either through configuration or through an <associate/> statement, a child node to a collection node if the Security Label of the child node is incompatible with the Clearance of the collection node.

9.3 Implementation Specific Structuring within Items

An implementation might choose to impose some kind of structure on items within a node. For example: items may include a list of blog posts, but may also include comments relating to specific blog posts from other users.
An implementation MAY apply different logic to the visibility of items in this case, perhaps by disallowing access to comment items if the requester is not Cleared to view the associated blog post item, even if the individual Security Label on the comment item would not normally prevent access.
However, the server MUST NOT allow access to an item if the requester is not Cleared to view the Security Label for the item (i.e. this mechanism must only be used to further restrict access to items and must not be used to widen access).

9.4 Limiting Notifications to a Certain Clearance

An implementation may wish to allow a subscriber to limit the sensitivity of items which are delivered for a certain subscription. For example: a subscriber may wish to only receive notifications of items which are unclassified, even if the node has a higher clearance.
One way this could be implemented is by expanding the Data Form for the subscription options.

Listing 21: Form with ability to limit subscription clearance

```
<iq from='pubsub.shakespeare.lit'
    id='options1'
    to='francisco@denmark.lit/barracks'
    type='result'>
  <pubsub xmlns='http://jabber.org/protocol/pubsub'>
    <options node='princely_musings' jid='francisco@denmark.lit'>
      <x xmlns='jabber:x:data' type='form'>
        ...
        <field label='Limit␣Clearance' 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='UNCLASSIFIED'><value>Catalog:UNCLASSIFIED</
              value></option>
          <option label='Custom'><value>Custom</value></option>
        </field>
        ...
      </x>
    </options>
  </pubsub>
</iq>
```

10 Security Considerations

This document is an extension to Security Labels in XMPP (XEP-0258) [9] and therefore any security considerations noted in that document will also apply to this document.

11 IANA Considerations

This document requires no interaction with the the Internet Assigned Numbers Authority (IANA) [10]

12 XMPP Registrar Considerations

12.1 Protocol Namespaces

This specification defines the following XML namespaces:

- urn:xmpp:sec-label:pubsub:0
- urn:xmpp:sec-label:pubsub:errors:0

12.2 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

[9] XEP-0258: Security Labels in XMPP <https://xmpp.org/extensions/xep-0258.html>.

[10] 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 <http://www.iana.org/>.

number found at the end of the XML namespaces defined herein, as described in Section 4 of XEP-0053.

13 XML Schema

13.1 urn:xmpp:sec-label:pubsub:0

```
<?xml version="1.0" encoding="utf-8" ?>

<xs:schema
    elementFormDefault='qualified'
    targetNamespace='urn:xmpp:sec-label:pubsub:0'
    xmlns='urn:xmpp:sec-label:pubsub:0'
    xmlns:xs='http://www.w3.org/2001/XMLSchema'>

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

  <xs:attribute name='label' type='xs:IDREF'>
    <xs:annotation>
      <xs:documentation>
        References an &quot;id&quot; value in a &lt;securitylabel&gt;
            element. The referenced
        Security Label MUST then be applied to the element content.
      </xs:documentation>
    </xs:annotation>
  </xs:attribute>

  <xs:attribute name='id' type='xs:ID'>
    <xs:annotation>
      <xs:documentation>
        Defines a unique (across the document) id for a &lt;
            securitylabel&gt; element that can be
        referenced from a &quot;label&quot; attribute.
      </xs:documentation>
    </xs:annotation>
  </xs:attribute>

</xs:schema>
```

13.2 urn:xmpp:sec-label:pubsub:errors:0

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

  <xs:annotation>
    <xs:documentation>
      This namespace is used for error reporting only, as
      defined in XEP-xxxx:

      http://xmpp.org/extensions/xep-xxxx.html
    </xs:documentation>
  </xs:annotation>

  <xs:element name='insufficient-clearance' type='empty'/>

</xs:schema>
```

14 Acknowledgements

Thanks to Dave Cridland, John Atherton, Kurt Zeilenga, Lloyd Watkin, Ralph Meijer and Stephen Welch for their contributions.