

Geopriv
Internet Draft

H. Tschofenig
Siemens
John B. Morris, Jr.
Center for Democracy and Technology
(Eds.)

J. Cuellar
Siemens
James Polk
Cisco
H. Schulzrinne
Columbia U.

Expires: February 2004

August 2003

Location Object Authorization Policies
<[draft-tschofenig-geopriv-authz-00.txt](#)>

Status of this Memo

This document is an Internet-Draft and is subject to all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/lid-abstracts.html>

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>

Abstract

This document describes a set of policy rules to satisfy Element E through L of the "Core Privacy Protections for Geopriv Location

Object" draft. The draft uses XCAP.

Location Object Authorization Policies

August 2003

This draft aims to provide input for discussions at the Geopriv Interim Meeting in Washington (September 2003). This document presents a very preliminary version of design team discussions. Not all listed authors have fully reached consensus on all issues of the proposed language.

Table of Contents

1.	Introduction.....	2
2.	Authorization Policies.....	2
2.1	Element E.....	3
2.2	Element F.....	4
2.3	Element G.....	6
2.4	Element H.....	8
2.5	Element I.....	9
2.6	Element J.....	11
2.7	Element K.....	13
2.8	Element L.....	14
3.	XML Schema.....	16
4.	Security Considerations.....	16
5.	Open Issues.....	16
6.	Normative References.....	16
7.	Informative References.....	16
	Acknowledgments.....	16
	Author's Addresses.....	17
	Full Copyright Statement.....	17

[1.](#) Introduction

The policy rules defined in this document extend the Extensible Markup Language (XML) Configuration Access Protocol (XCAP) [[XCAP](#)] and in particular the XML schema in [[XCAP-USAGE](#)]. Geopriv adds authorization policies beyond what is offered in [[XCAP-USAGE](#)]. The XML schema in [[XCAP-USAGE](#)] is extended with Geopriv specific content as described in this document.

The authorization policies described in this document try to satisfy the Elements E through L defined in [Core].

[Section 2](#) enumerates the Elements E through L with a description of

a possible way to address them. This includes XML schema snippets and examples. [Section 3](#) will (in a future version) provide a full XML schema.

[2.](#) Authorization Policies

This section describes the outcome of the design team working on the authorization policies described in [Core]. Code snippets for XML

schemas, which extend the [[XCAP-USAGE](#)] schema, are provided in addition to some examples that explain the usage of these policies.

Most of the elements do not depend on the geospatial content and thus should be additions to the basic XCAP authorization schema. For instance, the <area> element should be placed in a geopriv-specific namespace.

[2.1](#) Element E

Element E: Permission to disclose only to someone presenting a specified key (for instance, a shared key or the private key corresponding to a particular public key), or a special type of credential (an e-token to be defined).

[XCAP-USAGE] specifies the elements <auth-mechanism> and <anonymous> inside the acceptance permission which allows to refer to SIP specific authentication mechanisms such as:

- None
- TLS
- Digest
- SMIME
- P-Asserted-ID

These mechanisms are sufficient for authorization policies in the context of SIP and SIP Presence (although splitting TLS according to the authentication mechanisms would be more appropriate e.g., public key based authentication, Kerberos-based authentication or SRP based authentication). For a first version of the Geopriv authorization policies these authentication mechanisms and XML elements will be

reused without modification.

Another approach, which aims to be more generic and was also considered, is to reuse a proposal of an (expired) Internet Draft on "Authentication Mechanisms Levels" [Levels]. Instead of enumerating different authentication protocols different authentication levels are defined such as:

- None (no authentication)
- Weak (vulnerable against eavesdroppers)
- Limited (no protection against active attacks)
- Strong (protection against active attacks)

Examples for the different authentication levels are provided in [Levels].

Currently there is no provision in [[XCAP-USAGE](#)] to provide authorization for anonymous access to location information (e.g. by using tokens). A proposal will be described in a separate document.

[2.2](#) Element F

Element F: Requirement that the granularity/precision of location information be reduced

In Section 4.2.2.3 of [[XCAP-USAGE](#)] content permissions are defined. These permissions allow to restrict access to certain XML elements. In particular, the use of the <show-element> seems to be useful to support the concept of location information reduction. By listing only those elements of the location object to which access is allowed by a specific individual the granularity can be reduced. This approach is similar to <include> statement proposed in [[Sch03](#)] but the functionality of the <exclude> statement is not provided. Adding field exclusion primarily offers efficiency advantages, rather than new capabilities and thus can be safely omitted.

The following three approaches can be used to specify access to certain location information elements. Please note that the text-values inside the <element-name> </element-name> elements are artificial since the format of the location object (civil and geospatial) is not yet defined. Hence it should only be treated as a hint for the reader what the future content will be.

a) Leave the XCAP schema unmodified and to repeat the <show-element> element (if required)

As an example, the following authorization policy will be the result.

```
<?xml version="1.0" encoding="UTF-8"?>
<permission-statements
  xmlns:pidf="urn:ietf:params:xml:ns:pidf"
  xmlns:rpids="urn:ietf:params:xml:ns:sip-rpids"
  xmlns:lo="urn:ietf:params:xml:ns:geopriv-lo">
  <statement id="as8f">
    <applies-to>
      <uri>sip:mankin@psg.com</uri>
    </applies-to>

    <permissions>
      <accept/>
      <show-namespace>urn:ietf:params:xml:ns:pidf
        </show-namespace>
      <show-element>
        <element-name>rpids:placetype</element-name>
```

```
</show-element>
<show-element>
  <element-name>lo:civil/c</element-name>
</show-element>
<show-element>
  <element-name>lo:civil/a1</element-name>
</show-element>
<show-element>
  <element-name>lo:gml/Point</element-name>
</show-element>
<any-event/>
</permissions>

</statement>
</permission-statements>
```

b) Extend the XCAP schema to allow the <element-name> element to appear arbitrarily often

In the above-mentioned example the modifications would lead to:

```
<show-element>
  <element-name>rpids:placetype</element-name>
  <element-name>lo:civil/c</element-name>
  <element-name>lo:civil/a1</element-name>
  <element-name>lo:gml/Point</element-name>
</show-element>
```

The same result is achieved with approach (c). The difference between (b) and (c) is only a technical detail and some alignment with the [\[XCAP-USAGE\]](#) XML schema. The second option offers a more space-efficient encoding of these rules. We strive to make the rule set be space-efficient since it may be transported across bandwidth-constrained links and since the number of rules may be large if they are automatically generated from external information such as address books and calendars.

c) Enhance the <element-name> element of the XCAP schema itself to appear arbitrarily often

```
<xs:annotation>
  <xs:documentation>Content Permissions</xs:documentation>
</xs:annotation>
<xs:element name="all-content" minOccurs="0"/>
  <xs:sequence>
    <xs:element name="show-contact-element" minOccurs="0"/>
    <xs:element name="show-note" minOccurs="0"/>
    <xs:element name="show-tuple" type="xs:string" minOccurs="0"
      maxOccurs="unbounded"/>
```

```
<xs:element name="show-element" minOccurs="0"
  maxOccurs="unbounded">
  <xs:complexType>
    <xs:choice>
      <xs:element name="element-name" type="xs:string"
        maxOccurs="unbounded" />
    </xs:choice>
  </xs:complexType>
<!--
  ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
  This statement allows a number of <element-name>
  elements to be used.
-->
```

```

        <xs:element name="element-path" type="xs:string"/>
      </xs:choice>
    </xs:complexType>
  </xs:element>
  <xs:element name="show-namespace" type="xs:string"
    minOccurs="0" maxOccurs="unbounded"/>
  <xs:element name="show-values" minOccurs="0"
    maxOccurs="unbounded">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="element-name"
          type="xs:string"/>
        <xs:element name="value" type="xs:string"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="encrypt" minOccurs="0"/>
</xs:sequence>
</xs:sequence>

```

It seems to be easiest to use approach (a). More information on the attributes provided by the location object is required to illustrate useful and complete examples.

[2.3](#) Element G

Element G: The ability to provide additional Privacy Rules for specific requestors or groups of requestors

Using the schema extension described below the <permission-statements> element of [[XCAP-USAGE](#)] is enhanced with an element (<additionalGRF>) pointing to additional privacy rules.

It must be ensured that an implementation prevents infinite loops by limiting the inclusion depth. If it is not possible to resolve or

retrieve the policies at the indicated URL then the location object is not returned.

An alternative approach would be to have the external rule set only provide additional permissions, but not allow it to restrict

permissions granted in the base document. In that case, the rule engine may not have to retrieve the additional rules in all cases, e.g., if only a particular request needs to be evaluated against a rule set rather than generating a set of notifications for all recipients. External rule sets add a number of complications, such as privacy concerns (retrieval indicates access to the information), reliability and bandwidth issues.

Schema snippet:

```
<xs:schema ....
xmlns:ps="urn:ietf:params:xml:ns:permission-statements" ...>

<xs:element name="permission-statements"
  type="gp:permission-statements-type">
<xs:complexType name="permission-statements-type">
  <xs:complexContent>
    <xs:extension base="ps:permission-statements">
      <xs:sequence>
        <xs:element name="additionalGRF" type="xs:string"
          minOccurs="0" />
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
  ...
</xs:complexType>
</xs:schema>
```

Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<permission-statements>

  <statement id="as8f">
    <applies-to>
      <uri>sip:mankin@psg.com</uri>
    </applies-to>

    <permissions>
      <!-- permissions for Allison -->
    </permissions>

  </statement>
```



```

<additionalGRF>
  http://example.com/policies.xml
</additionalGRF>

</permission-statements>

```

In this example additional privacy rules are available at "http://example.com/policies.xml".

2.4 Element H

Element H: The ability to define a time until which a permission is valid

To specify a time period until which a permission is valid two attributes ("from" and "until") are added to the <permission-statements> element. Both, the "from" and the "until" attribute are optional. If the "from" attribute is missing then the policies are valid immediately. If the "to" attribute is missing then the policies have no restricted lifetime. Both attributes use the data type dateTime.

Schema snippet:

```

<xs:schema ....
  xmlns:ps="urn:ietf:params:xml:ns:permission-statements" ...>

  <xs:element name="permission-statements" type="gp:permission-
statements-type">
    <xs:complexType name="permission-statements-type">
      <xs:complexContent>
        <xs:extension base="ps:permission-statements">
          <xs:attribute name="from" type="xs:dateTime" use="optional">
            <xs:attribute name="until" type="xs:dateTime" use="optional">
          </xs:extension>
        </xs:complexContent>
      </xs:complexType>
    </xs:element>
  </xs:schema>

```

Example:

```

<?xml version="1.0" encoding="UTF-8"?>
<permission-statements
  from="2003-09-04T09:00:00" until="2003-09-05T18:00:00">

  <statement id="as8f">
    <applies-to>
      <uri>sip:mankin@psg.com</uri>
    </applies-to>
  </statement>
</permission-statements>

```

Location Object Authorization Policies

August 2003

```
</applies-to>

<permissions>
  <!-- permissions for Allison -->
</permissions>

</statement>

<additionalGRF>
  http://example.com/policies.xml
</additionalGRF>

</permission-statements>
```

This example shows that the described policy is valid from the 4th of September (9am) to the 5th of September (6pm).

Note that in order for this extension to work it is necessary to specify the `<permission-statements>` element in [[XCAP-USAGE](#)] as global (and not as local).

[2.5](#) Element I

Element I: The ability to define a geographical area for which the permission is valid ("if I am in area x then you can tell y my location")

As part of the discussion regarding Element I it was decided to support functionality like:

- a) "Within z km of point x,y, assuming a spherical earth."
- OR
- b) "An equality match on country or state or city (civil location)."

The assumption about spherical earth provides a good simplification and the error is said to be fairly low. Going beyond this, as in "as long as I'm within three streets of my home" or "as long as I'm in the area bounded by 112 and 120th Street and Amsterdam Avenue and Broadway" (which describes the Morningside Heights campus of Columbia University) is likely to get messy.

The details on the location object (for both civil and geospatial

coordinates) will be provided as soon as the discussions on the location object are finished. Hence a placeholder is used for illustrative purposes below.

The <permissions> element is extended to support an element <area> which either contains civil location or spherical area (based on GML most likely).

Schema snippet:

```
<xs:schema ....
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:ps="urn:ietf:params:xml:ns:permissions"
xmlns:lo="urn:ietf:params:xml:ns:geopriv-lo" ...>

<xs:element name="permissions" type="gp:permissions-type">
  <xs:complexType name="permissions-type">
    <xs:complexContent>
      <xs:extension base="ps:permissionsType">
        <xs:sequence>
          <xs:element name="area" type="gp:area-type"
            minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="area-type">
    <xs:choice>
      <xs:element ref="lo:civil-area"/>
      <xs:element ref="lo:spherical-area"/>
    <!--
      These two elements are defined as part
      of the geopriv location object. It is assumed
      that the namespace for these objects is lo
      as defined above.
    -->
    </xs:choice>
    <xs:attribute name="name" type="xs:string" use="required"/>
  </xs:complexType>

</xs:schema>
```

Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<permission-statements
  xmlns:lo="urn:ietf:params:xml:ns:geopriv-lo">

  <statement id="as8f">
    <applies-to>
      <uri>sip:mankin@psg.com</uri>
    </applies-to>

    <permissions>
      <accept-if>
```

```
      <auth-mechanism>digest</auth-mechanism>
    </accept-if>
    <area name="bergen">
      <civil-area>
        <lo:a1>US</a1>
        <lo:a2>NJ</a2>
        <lo:a3>Bergen</a3>
      </civil-area>
    </area>
  </permissions>

</statement>
</permission-statements>
```

In this example location information is provided to Allison only if the target is within the indicated area labeled as "bergen" (in addition to the other policies).

[2.6](#) Element J

Element J: The ability to define a repeatable time window (such as weekdays during office hours) during which a permission is valid

Various approaches have been investigated to support a repeatable time window such as the flexible approach suggested in [[Sch03](#)]: "The time recurrence rules are specified using the iCal notation in [RFC 2445](#) [[RFC2445](#)], translated into XML schema format, roughly

following the (expired) Internet draft [draft-ietf-calsch-many-xcal-00](#). 'exdate' 4.8.5.2, 'rdate' 4.8.5.3, 'rrule', 4.8.5.4.0" ([Section 4.3](#)). It was decided to consider this approach in future version of Geopriv authorization policies.

Other suggestions reused flags for each weekday, included exceptions or reused the format of the Unix CRON command.

Finally it was decided to address a repeatable time window with a list of "from"/"until" XML dateTime values. Particularly for non-human written authorization policies (which is likely to be case) this approach seems to provide sufficient flexibility.

The following schema snippet extends the <permissions> element and adds another child element <recurrence>. The <recurrence> element may appear arbitrarily often whereby each element has two sub-elements <from> and <until> of data type dateTime. It may be unnecessary to have both <from>/<until> and recurrence, since the latter is a generalization of the former, but this redundancy may be use-friendly.

Schema snippet:

```
<xs:schema ....
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:ps="urn:ietf:params:xml:ns:permissions"...>

<xs:element name="permissions" type="gp:permissions-type">
  <xs:complexType name="permissions-type">
    <xs:complexContent>
      <xs:extension base="ps:permissionsType">
        <xs:sequence>
          <xs:element name="recurrence"
            type="gp:recurrence-type" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="recurrence-type">
```

```

        <xs:sequence>
            <xs:element name="from" type="xs:dateTime" />
            <xs:element name="until" type="xs:dateTime" />
        </xs:sequence>
    </xs:complexType>

</xs:schema>

```

Example:

```

<?xml version="1.0" encoding="UTF-8"?>
<permission-statements
  xmlns:lo="urn:ietf:params:xml:ns:geopriv-lo">

  <statement id="as8f">
    <applies-to>
      <uri>sip:jon.peterson@neustar.biz</uri>
    </applies-to>

    <permissions>
      <!-- additional permissions go in here.... -->
      <recurrence>
        <from>2003-09-04T09:00:00-05:00</from>
        <until>2003-09-04T18:00:00-05:00</until>
      </recurrence>
      <recurrence>
        <from>2003-09-05T09:00:00-05:00</from>
        <until>2003-09-05T18:00:00-05:00</until>
      </recurrence>
    </permissions>
  </statement>
</permission-statements>

```

```

    </recurrence>
  </permissions>

</statement>
</permission-statements>

```

This example shows two recurrence elements which approximately capture the timeframe of the Geopriv interim meeting. In the example Jon Peterson will be able to request the location information of target (e.g. Jorge) only during the interim meeting hours.

[2.7](#) Element K

Element K: The ability to require that express consent of the

Target/Rule Maker be obtained prior to disclosing location

The mechanism used to enforce consent requires enhancing the <permission> element with a sub-child <consent-required>. The data type of this element is anyURI.

Schema snippet:

```
<xs:schema ....
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:ps="urn:ietf:params:xml:ns:permissions"...>

<xs:element name="permissions" type="gp:permissions-type">
  <xs:complexType name="permissions-type">
    <xs:complexContent>
      <xs:extension base="ps:permissionsType">
        <xs:sequence>
          <xs:element name="consent-required"
            type="xs:anyURI " minOccurs="0"
            maxOccurs="1"/>
        </xs:sequence>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>
</xs:schema>
```

Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<permission-statements
  xmlns:lo="urn:ietf:params:xml:ns:geopriv-lo">

  <statement id="as8f">
```

```
<applies-to>
  <uri>sip:jon.peterson@neustar.biz</uri>
</applies-to>

<permissions>
<!-- permissions go in here.... -->
  <consent-required>sip:hgs@cs.columbia.edu</consent-required>
```

```
</permissions>

</statement>
</permission-statements>
```

This example shows the policy which requires to contact Henning (hgs@cs.columbia.edu) if Jon asks for location information. There currently is no protocol mechanism for inquiring about permissions from users. In order to define an interoperable protocol, the design team will strive to provide a protocol mechanism first, if that proves feasible, or may remove the feature otherwise.

[2.8](#) Element L

Element L: The ability to require that notice be provided to the Target if location is provided

The mechanism used for Element L is similar to the one used for Element K. Again the <permissions> element is extended with a <notify> element.

Schema snippet:

```
<xs:schema ....
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:ps="urn:ietf:params:xml:ns:permissions"...>

<xs:element name="permissions" type="gp:permissions-type">
  <xs:complexType name="permissions-type">
    <xs:complexContent>
      <xs:extension base="ps:permissionsType">
        <xs:sequence>
          <xs:element name="notify" type="xs:anyURI"
            minOccurs="0" maxOccurs="1"/>
        </xs:sequence>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>
</xs:schema>
```


Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<permission-statements
  xmlns:lo="urn:ietf:params:xml:ns:geopriv-lo">

  <statement id="as8f">
    <applies-to>
      <uri>sip:mankin@psg.com</uri>
    </applies-to>

    <permissions>
      <!-- permissions go in here.... -->
      <notify>sip:anewton@ecotroph.net</notify>
    </permissions>

  </statement>
</permission-statements>
```

Andrew Newton (anewton@ecotroph.net) is the rule maker and is notified if Allison Mankin (mankin@psg.com) requests access to Andrew's location information.

Section 4.3 of [[Sch03](#)] addresses some security considerations with this mechanisms and in particular with third-party notifications:

"This clearly has security implications, since a malicious target could use this mechanism to cause messages to be sent to third parties, introducing a new form of 'open proxy' spamming. Thus, such notification is only appropriate if the notifying party can convince itself that the address indeed belongs to the presentity. Unfortunately, there is no fool-proof way of ensuring that, but a recipient of this information may compare the non-schema part of the notification URI with the presentity and only allow notification on equality. Given these constraints and the inherent unreliability and delays in most current notification mechanisms, a target cannot rely on receiving notification."

Third-party notifications must be ruled out. Related to some scenarios presented in this context it might also be possible to use some sort of logging statement to provide similar functionality.

There currently is no protocol mechanism for conveying semantically meaningful information about location transmission about permissions from users. In order to define an interoperable protocol, the design team will strive to provide a protocol mechanism first, if that proves feasible, or may remove the feature otherwise.

[3.](#) XML Schema

Once full consensus is reached on the authorization policies and on how to implement them a full XML schema will be provided.

[4.](#) Security Considerations

This document raises and addresses some security issues which are described in [DM+03]. Some additional security concerns (e.g. denial of service attacks) are expressed in [[Sch03](#)].

A future version of this document will structure these threats in the appropriate manner once the discussions on the individual mechanisms are finished.

[5.](#) Open Issues/Future Work

- Combining this draft with [Core] draft.
- How the authorization policies can be used with other using protocols such as HTTP.
- XML Schema
- More examples

[6.](#) Normative References

[DM+03] M. Danley, D. Mulligan, J. Morris and J. Peterson: "Threat Analysis of the Geopriv Protocol", Internet Draft, Internet Engineering Task Force, (work in progress), February 2003.

[XCAP] Rosenberg, J., "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)", Internet Draft, Internet Engineering Task Force, (work in progress), May 2003.

[XCAP-USAGE] J. Rosenberg: "Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Usages for Setting Presence Authorization", Internet Draft, Internet Engineering Task Force, (work in progress), June, 2003.

[7.](#) Informative References

[Level] K. Zeilenga: "Authentication Mechanisms Levels" Internet Draft, Internet Engineering Task Force, (expired), April, 2001.

[Sch03] H. Schulzrinne: "Location Objects and Location Privacy Information for Presence Information", June, 2003.

We would like to thank Christian Guenther for his input on the XML schema snippets in this draft.

Author's Addresses

Hannes Tschofenig
Siemens AG
Otto-Hahn-Ring 6
81739 Munich
Germany
EMail: Hannes.Tschofenig@siemens.com

Jorge R Cuellar
Siemens AG
Corporate Technology
CT IC 3
81730 Munich
Germany
EMail: Jorge.Cuellar@siemens.com

John B. Morris, Jr.
Director, Internet Standards, Technology & Policy Project
Center for Democracy and Technology
1634 I Street NW, Suite 1100
Washington, DC 20006
USA

Email: jmorris@cdt.org
<http://www.cdt.org>

Henning Schulzrinne
Columbia University
Department of Computer Science
450 Computer Science Building
New York, NY 10027
US

Phone: +1 212 939 7042
EMail: hgs+nsis@cs.columbia.edu
URI: <http://www.cs.columbia.edu>

James M. Polk

Cisco Systems
2200 East President George Bush Turnpike
Richardson, Texas 75082 USA

Email: jmpolk@cisco.com

Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.

Tschofenig, Morris

Expires - February 2004

[Page 17]

Location Object Authorization Policies

August 2003

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

Tschofenig, Morris

Expires - February 2004

[Page 18]