Calling Party Category using SAML
draft-schubert-sipping-saml-cpc-00.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

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/ietf/1id-abstracts.txt.

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

This Internet-Draft will expire on July 5, 2006.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

Ability to convey a trait information of caller, such as calling party category which includes things like Law Enforcement, Technical Support, Anonymous Caller from Payphone etc. and type of location where the call initiated which includes things like Police Station, Hotel/Motel, Fire Station, Jail etc. might be useful for receiving
entity of the call to make an authorization decision on its treatment of incoming call. This draft proposes an approach for conveying trait information for caller’s category and call initiating point in SIP using the Security Assertion Markup Language (SAML). It relies on a third party to act as an asserting party to provide information described above. This draft is in a fairly early state and has many details that are missing. This version tries to describe and illustrate what the SAML based solution would look like to aid in evaluating SAML as solution to carry calling party’s category and call initiating location information.

Table of Contents

1. Introduction ............................................. 3
2. Terminology .............................................. 5
3. Use Cases ................................................ 7
   3.1. ACR Override ........................................ 7
   3.2. Call back from Law Enforcement ....................... 7
   3.3. PSTN Interaction .................................... 7
   3.4. Station Type and Privacy Setting ..................... 7
4. Overview of Operation .................................... 8
5. UAC Behavior ............................................ 11
6. Server Behaviors ........................................ 12
   6.1. Home Proxy with request ............................. 12
   6.2. Outbound Proxy with request ......................... 13
   6.3. Server Behavior receiving requests .................. 14
7. Examples Call Flows ..................................... 16
   7.1. Example Flow 1 ...................................... 16
   7.2. Example Flow 2 ...................................... 17
   7.3. Example Flow 3 ...................................... 19
   7.4. Example Flow 4 ...................................... 21
8. Station Type .............................................. 23
9. Calling Party Category ................................... 24
10. XML Schema for Calling Party Category ................. 25
11. XML Schema for Station Type ........................... 26
12. XML Example for Calling Party Category ............... 27
13. XML Example for Station Type .......................... 28
14. Security Considerations ................................ 29
15. Acknowledgement ....................................... 30
16. References .............................................. 31
   16.1. Normative Reference ................................. 31
   16.2. Informative Reference .............................. 31
Authors’ Addresses ......................................... 32
Intellectual Property and Copyright Statements ............ 33
1. Introduction

The Session Initiation Protocol (SIP), RFC 3261[2] is used to establish and maintain a dialog between a pair of User Agents (UA) in order to manage a communications session.

Just as one might set up a white list and black list to prioritize a treatment of incoming calls, prioritizing calls and differentiating the treatments of incoming calls according to traits and meta data of caller might be desirable at time. It is at least proven useful to convey and consume some trait information to differentiate the treatments of incoming calls in PSTN/ISDN, and it might be equally useful in SIP.

SS7 ISUP defines a Calling Party’s Category (CPC) and OLI (Originating Line Information) parameters that characterizes the station used to originate the call and carries other important state that can describe the originating party.

Looking at the semantics of the information carried in CPC and OLI, there are 3 distinctive types/categories of information. Trait information representing the caller or caller’s organization which we call Calling Party’s Category (CPC) in this draft, information representing the station where call is originating, which we call Station Type (ST) in this draft and information describing a type of call which is not considered in this draft as there are likely other ways to describe a call type using pre-existing SIP mechanisms and extensions.

When CPC or OLI carried in ISUP messages are to be carried in SIP, the party responsible for each of this information may differ from when they are carried in ISUP messages. For example, trait information associated with the caller and caller’s organization (CPC) are likely to be managed by the home service provider, on the other hand information characterizing station where call is originating are likely to be provided through the service provider serving the local network where user is connected.

Putting it into SIP terms, from the caller’s viewpoint, trait information characterizing the caller (CPC) is likely to be provided through the service provider serving the home network and is likely to be bound or linked with the AoR or the domain of the AoR. Trait information characterizing the station where call is initiated (ST) is likely to be provided through service provider serving the local network which can be a network which user had no previous relationship.

It is also important to note that many of the values carried either
in CPC or OLI are meaningless outside of PSTN or can be represented using another existing mechanism or/and extension. For example, the language of an operator can be expressed more richly using the Accept-Language head in SIP, emergency call can be expressed better using the SOS URI and Service URI defined in [5], and priority of the call can be represented using [6].

If these informations are primarily consumed by the gateway that interworks ISUP networks with SIP networks, and information are generally only carried in one way direction from ISUP networks to SIP networks, mechanism in consideration such as SAML might not be necessary.

But as traits information described here alter the callee’s treatments of incoming calls, sometime so much so that other calls in progress might be pre-empted to prioritize the calls with trait information with higher priority, it is important when deployed in SIP, that callee has a way to assure and ascertain that the trait information provided is valid and verifiable.

This draft explores what it would be like to retrieve and carry trait information such as CPC and ST using SAML and SIP to see if it really satisfies the property desired for exchanging these trait information.
2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [1].

This work adopts the terminology from the framework in [4]

Additionally, the following terms are used:

Calling Party Category: Calling Party Category is an attribute of a caller that characterizes caller. It generally represents the kind of organization caller is associated with. (Police, Operator etc.)

Station Type: Station type is an attribute which characterizes the location(facility) used to originate the call.

Asserting Party: An asserting Party is an entity, which by some means authorize and authenticate the target for an assertion and it is an entity that will verify the assertion when recipient of an assertion inquires about the assertion’s validity.

Assertion: An assertion is an XML document that contains authentication statements, attribute statements and authorization decision statements. In an authentication statement, an issuing authority asserts that a certain subject was authenticated by certain means at a certain time. In an attribute statement, an issuing authority asserts that a certain subject is associated with certain attributes which has certain values. In an authorization decision statement, a certain subject with a certain access type to a certain resource has given certain evidence that the identity is correct. The assertion is digitally signed to protect it against unwanted modifications by third parties.

Artifact: An artifact is a base-64 encoded string that is 40 bytes long that serves as a pointer to a server that temporarily stores an assertion. The first 20 bytes provide an indication from which server the assertion needs to be retrieved. The remaining 20 bytes identify a unique assertion.

Application Service Provider(ASP): The organization or entity that provides application-layer services, which may include voice (see "Voice Service Provider"). This entity can be a private individual, an enterprise, a government, or a service provider. An ASP is defined as something more general than a Voice Service Provider, since emergency calls are sometimes likely to use other media, including text and video. Note: For a particular user, the ASP may or may not be the same organization as the IAP and/or ISP.
Voice Service Provider (VSP): A specific type of Application Service Provider which provides voice related services based on IP, such as call routing, a SIP URI, or PSTN termination.

Internet Attachment Provider (IAP): An organization that provides physical network connectivity to its customers or users, e.g. through digital subscriber lines, cable TV plants, Ethernet, leased lines or radio frequencies. Examples of such organizations include telecommunication carriers, municipal utilities, larger enterprises with their own network infrastructure, and government organizations such as the military.
3. Use Cases

Many use cases are likely to be realized as category of information defined in this draft becomes readily available to be consumed by servers, but here are some possible use cases.

3.1. ACR Override

Some User Agent Server (UAS), proxy and other servers might have Anonymous Call Rejection (ACR) service, which rejects call when the incoming call is an anonymous call. The same entity that has ACR service activated might have a local policy, where upon receiving a call with a "calling party category (CPC)" of "police", it would allow the call to go through even when the caller is anonymous by overriding the ACR service.

3.2. Call back from Law Enforcement

VSP/ASP might have a local policy where upon receiving a request with a CPC of "police" asking to obtain an Address of Record (AOR) of caller recently making an anonymous call to the police station, it would override its general privacy policy about withholding the identity of the anonymous caller and return the AOR in question.

3.3. PSTN Interaction

CPC and OLI can be mapped to the trait information described here in this draft for interaction between SIP networks and ISUP networks.

3.4. Station Type and Privacy Setting

When roaming, user might use an outbound proxy that are provided through facility that they are visiting such as library, jail etc. If these facilities can be recognized through trait information as a call's originating point, receiving end might behave differently with its treatment of the call.

For example, when receiving end recognizes that the call is coming through jail, callee might assume that call is monitored and warn the user about its possible privacy implication.

When the call is coming through Library, UAS might automatically increases the volume on the microphone of the phone as it assumes that the caller would speak quietly.
4. Overview of Operation

Both CPC and ST would not work unless the asserting parties asserting the assertion and receiving entity verifying the assertion have a mutual trust relationships either directly or through federation. The discovery of this trust relationship and federation is out of scope. There are ideas trying to explore the associated federation using DNS as seen in [7].

Note that asserting party of CPC and ST may differ according to an environment the caller is making a call. Where CPC is an attribute of a caller and generally associated with the caller through caller’s organization (police, fire department etc.), Station Type (ST) is an attribute of a call’s originating point. As one can roam easily in SIP using the same identity, ST may not always stay the same and rather changes frequently if the caller is using a mobile device such as WIFI cellular phone or laptop to make a call.

Although this might be out of scope to discuss, an asserting party for CPC in most cases is likely to be the VSP which caller or caller’s organization subscribes to. Caller or organization which would get assertion to claim some kind of CPC besides "ordinary" generally needs to go through some offline administrative arrangement to claim specific CPC.

ST on the other hand represents an attribute of the call’s originating point, which in many cases is a characteristic describing location and other trait information of an outbound proxy where caller is connected. And therefore asserting party of ST is usually a VSP of the local network.

Process of obtaining the CPC and ST largely depends on who sets the assertion or artifact to the message. It seems desirable for proxies to query the assertion party and attach the CPC or ST in a form of artifact to a message rather than UAC querying the asserting party and attaching the assertion or artifact itself for several reasons. Reasons behind this are mentioned in the section 6.1 and 6.2.

If it is the proxy that attaches the artifact then it will simply authenticate the user and attach the artifact according to its local policy. If the proxy is not an asserting party then, it can retrieve the assertion for its domain prior to handling the request or it can retrieve the assertion upon receiving the request on behalf of the user. If the proxy is an asserting party then it can simply use the local policy to decide whether to attach the artifact or not. The behavior of the receiving entity would be the same for proxy attaching the artifact and UAC attaching the assertion/artifact.
If it is the UAC that attaches the artifact/assertion, process of obtaining the trait information preferably takes place before caller generates a request or even as part of the boot strap process, to minimize the call set-up delay. And this might be reasonable timing to obtain these trait information as both CPC and ST are rather static as long as user is not moving around and changing its outbound proxy.

Location of asserting party for both ST and CPC are likely to be distributed through means such as manual configuration, SIP UA Profile framework[4] or some other proprietary means, if it’s the UAC that queries the asserting parties to retrieve the

If the caller is connected to the Internet from network that’s not served by the home service provider, it is likely for caller to end up with two different location to inquire for assertions, one for CPC and one for ST. (For an example, user subscribed to AT&T but connected through an outbound proxy at your client’s office or Jail served by another service provider..)

UAC would query asserting party for CPC and ST independently, even if the assertion party for both CPC and ST are the same entity.

Asserting party when receiving request would be required to do its best at authorizing and authenticating the SAML request. For CPC this would be accomplished through some form of a user authentication and authorization to see if the user is eligible to claim CPC. To minimize the configuration burden on UA, home proxy might query and obtain assertion on behalf of the caller and insert the assertion to the message on UAC’s behalf.

For ST, outbound proxy might need to query the asserting party at all time on behalf of the caller as there is generally no prior relationship between the caller and an asserting party of the local network if the caller is connected through network not served by its home service provider.

After authenticating and authorizing the caller or the proxy, asserting party responsible for CPC would set an appropriate CPC for the caller and assertion party responsible for ST would do the same for ST and return the response in forms of either an artifact or an assertion as described in "Using SAML for SIP"[3].

After obtaining assertion containing CPC and/or ST or an artifact pointing to them, UAC would set them to its message following the convention described in [3] and send it to the callee.

Proxy or UAS receiving either an artifact or assertion that
understand this specification and interested in consuming the information would verify the validity of an assertion if desired following the convention described in [3].

If the asserting party of the information provided is not acknowledged by the receiving end, the information provided by the asserting party unknown to the receiving end SHOULD be considered invalid and no special treatment of incoming call SHOULD take place on that particular trait information.

If the information is considered valid, and receiving end recognizes the asserting party, UAS or Proxy MAY reflect the given information to help make a better informative authorization decision for treatments of an incoming call.
5. UAC Behavior

We assume that UAC is either configured manually or configured through means such as SIP UA Profile Framework[4] with an assertion parties to inquire for an assertion. And how UAC would be configured is out of scope of this document.

If [4] is to be used, asserting party for CPC is likely to be realized through use of "user" profile type and that of ST is likely to be realized through "local-network" profile type.

UAC supporting this specification SHOULD query using the SAML request, the asserting party responsible for CPC if it’s configured with its location, following the convention described in [3].

UAC supporting this specification SHOULD query using the SAML request, the asserting party responsible for ST if it’s configured with its location, following the convention described in [3].

If UAC receives an error in SAML response, UAC may receive a reason why it failed but it is NOT RECOMMENDED retry with the same request.

If UAC receives an assertion in SAML response, it SHOULD set it to the outgoing message following the convention described in [3] for each assertion it receives.

If UAC receives an artifact it SHOULD set it to its outgoing message following the convention described in [3] for each artifact it receives.

If possible, UAC SHOULD cache the artifact/assertion it obtained for future communication and reuse them as long as the client is connected through the same outbound proxy or is communicating with the same AOR.

UAC SHOULD indicate that it can accept the application/cpc and application/station MIME type in SIP requests it sends out.

If UAC desires proxies on its request path to handle the CPC or ST, it is RECOMMENDED to either set the artifact in the SIP header or not to encrypt the message if the assertion is used.

If it’s the proxy that attaches the artifact, UAC does not need to be aware of this specification.
6. Server Behaviors

6.1. Home Proxy with request

Home proxy might query the asserting party on behalf of caller for the following reasons.

CPC such as "police" is generally assigned to an organization, and not to an individual. Therefore it might be more sensible for home proxy representing the organization to query the asserting party on behalf of an individual belonging to that organization.

It enables call initiated from device not supporting this specification to carry an artifact.

It minimizes the configuration needed on UAC for obtaining the CPC or ST.

When home proxy supporting this specification receives a request and it is set up to query an asserting party or it is an asserting party, it MAY check to see if the message already contains an assertion or an artifacts by searching within message’s body for MIME type of application/cpc and application/station.

NOTE: How do we distinguish the trait type if it’s set as a header? Are we going to have a separate header for each artifact (SAML extension) defined? Also, do we want to define new MIME type for every SAML extensions? If not, we need to define a way to address the type of information contained in SAML, possibly using cid etc.

If it finds neither or just one the following process should take place, otherwise it would behave as any other proxy normally would, and transfer the call.

If the request only contains CPC, Proxy SHOULD verify that the request is going out through the processing proxy as an outbound proxy and it MAY query an asserting party responsible for ST to obtain an artifact if it’s not an asserting party or it MAY attach the artifact if it is an asserting party responsible for ST following the convention described in [3]. Proxy would be assumed to be pre-configured with asserting parties to query.

If the request only contains ST, it MAY query an asserting party responsible for CPC if it’s not an asserting party or it MAY attach an artifact if it is an asserting party responsible for CPC following the convention described in [3].

If the request carries neither ST nor CPC, it MAY query two asserting
parties, one responsible for CPC and one responsible for ST using SAML request if it’s not an asserting party or it MAY attach an artifact for ST and CPC if it is an asserting party for CPC and ST following the convention described in [3]. In case of ST, proxy should verify that the request is going out through the processing proxy as an outbound proxy.

If the response from the asserting party contains an error, it MAY log the error but it SHOULD NOT stop processing the requests it receives. And it SHOULD NOT retry to get an artifact with the same requests. It SHOULD process the request without the artifact.

If proxy is not an asserting party and it receives an artifact, it SHOULD set it to the header of an outgoing message following the convention described in [3] for each artifact it receives.

NOTE: As proxy is unable to modify the body, proxy MUST only accept an artifact, and base spec[3] is going to enable the inclusion of an artifact in the header for this to work.

After attaching the artifact, proxy SHOULD forward the request.

6.2. Outbound Proxy with request

Outbound proxy might query the asserting party on behalf of the caller for following reasons.

Caller when roaming or using visiting network, generally has no prior relationship to an outbound proxy or with an asserting party which is responsible for a ST of the connecting outbound proxy. This can be problematic as an asserting party for ST has no way to authenticate and authorize the caller. Allowing issuing an assertion without any authentication or authorization is not desirable.

It enables call initiated from device not supporting this specification to carry an artifact.

It minimizes the configuration needed on UAC for obtaining the ST.

When outbound proxy supporting this specification receives a request and it is set up to query an asserting party, it would check to see if the message already contains an assertion or artifacts by searching within message’s body for MIME type of application/station.

If it finds none it would do the followings, otherwise it would behave as it normally would as a proxy and forward the message
If the request contains no ST, proxy should verify that the request is going out through the processing proxy as an outbound proxy, if so it MAY query an asserting party responsible for ST to obtain an artifact if it’s not an asserting party or it MAY attach an artifact if it’s an asserting party following the convention described in [3].

If the response from the asserting party is an error, it MAY log the error but it SHOULD NOT stop processing the requests. And it SHOULD NOT retry to get an artifact with the same requests. And it MUST forward the message without the artifact.

If proxy receives an artifact it SHOULD set it to the header of an outgoing message following the convention described in [3].

After attaching the artifact, proxy SHOULD forward the request.

6.3. Server Behavior receiving requests

UAS and/or Proxy servers supporting this specification, when receiving a request indicating the support for application/cpc and application/station MIME type SHOULD look into the message body for these MIME types.

Upon finding the MIME body, UAS and/or Proxy server SHOULD check to see if the asserting party is one that it recognizes by checking the URI within the artifact if it’s an artifact, and check the servingURL within the assertion if it’s an assertion.

If the asserting party is unknown, it SHOULD stop processing the assertion or artifact with an unknown asserting party and process the next assertion or artifact if there is more than one.

If the asserting party is known but not trusted, it SHOULD stop processing the assertion or artifact and process the next assertion or artifact if there is more than one.

If the asserting party is known to the processing party and it is an artifact, it SHOULD obtain the actual assertion following the convention described in [3].

NOTE: The matching process and list of assertion parties that are to be used for verifying the trusted assertion parties might be obtained through SIP UA Profile Framework[4] or some other mechanisms such as one described in [7].

As part of a verification process, UAS and/or Proxy SHOULD check the URI of the party which requested the assertion for ST, and compare it with an entity in a VIA header in case it is different from the value

found in From header. If none of the entry in the VIA header matches
the value represented in the assertion, it should be considered
invalid. (If the outbound proxy in non-home network attaches the
assertion on behalf of the UAC, it is)

UAS and/or Proxy server MAY use ST or CPC that are validated to alter
its treatment of incoming call.
7. Examples Call Flows

7.1. Example Flow 1

The following call flow shows a basic attachment of an assertion/artifact by UAC’s home proxy. This is likely the architecture for individual users subscribing to VSP such as Vonage etc. (VSP is part of the federation and proxy from this VSP is an asserting party.)

As you can see Alice does not need to be aware of the asserting party.
7.2. Example Flow 2

The following call flow shows a basic attachment of an assertion/artifact by UAC’s company proxy. This is likely the architecture for corporate environment where organization/company subscribes to VSP such as Vonage etc. (VSP is part of the federation and proxy from this VSP is an asserting party.) and organization/company is assigned a single CPC value such as "police".

As you can see Alice does not need to be aware of the asserting party.
Figure 2: Corporate architecture
7.3. Example Flow 3

The following call flow shows a basic retrieval of an assertion/artifact from a single source of asserting party by UAC. It is assumed that UA is configured with information for assertion parties.

As you can see Alice query the assertion twice, once for CPC and once for ST.
<table>
<thead>
<tr>
<th>Alice’s phone</th>
<th>proxy.atlanta.com</th>
<th>Asserting Party</th>
<th>proxy.biloxi.com</th>
<th>Bob’s phone</th>
</tr>
</thead>
</table>

**Figure 3:** UA querying the asserting parties
7.4. Example Flow 4

Following is an example call flow for Alice initiating a call to Bob’s phone from starbucks.com. Home proxy and outbound proxy are both querying an asserting party on behalf of the caller. It is assumed that Alice’s UAC is pre-configured with the route set which makes the request route through outbound proxy and home proxy, which allows each proxy to query the assertion party and attach the artifact received in response to the outgoing message that it proxies. Note due to the space, proxy on Bob’s side and bob is not shown.
Figure 4: Roaming scenario.
8. Station Type

Predefined Values for station type is taken from CPC/OLI defined in ISUP:

- **payphone**: The calling station is a payphone.
- **prison**: The calling station is in a prison.
- **hotel**: The calling station is in a hotel or motel.
- **hospital**: The calling station is in a medical facility.
- **police**: The calling station is associated with a branch of law enforcement.
- **cellular**: The calling station is a radio-telephone operating in its home network.
- **cellular-roaming**: The calling station is a radio-telephone roaming in another network.
9. Calling Party Category

Predefined Values for calling party category is taken from CPC/OLI defined in ISUP:

payphone: The caller has been identified as a payphone user.

ordinary: The caller has been identified, and has no special features.

operator: The call was generated by an operator position.
10. XML Schema for Calling Party Category

TBD
11. XML Schema for Station Type

TBD
12. XML Example for Calling Party Category

TBD
13. XML Example for Station Type

TBD
14. Security Considerations

As the information carried in both CPC and ST may alter the treatment of the call by the recipient, it is important that the information carried is securely transferred. Usage of TLS and preferably direction connection with the assertion party when fetching and requesting the SAML document is recommended.
I like to thank Erick Sasaki and Christian Schmidt for providing constructive feedbacks.
16. References

16.1. Normative Reference


16.2. Informative Reference


Authors’ Addresses

Hannes Tshofenig
NTT Corporation
1549 W15th Ave
Vancouver, BC  V6H 1R6
Canada

Phone: +1 604 762 5606
URI: http://www.ntt.co.jp

Hannes Tshofenig
Siemens
Otto-Hahn-Ring 6
Munich, Bavaria  81739
Germany

Phone:
Email: Hannes.Tschofenig@siemens.com
URI:  http://www.siemens.com/

Martin Dolly
AT&T
San Francisco, CA  94110
US

Phone:
Email: dolly@att.com
URI:  http://www.att.com/
Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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.

Copyright Statement

Copyright (C) The Internet Society (2006). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

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