

PANA Working Group  
Internet-Draft  
Expires: January 10, 2005

H. Tschofenig  
Siemens  
V. Sankhla  
University of Southern California  
July 12, 2004

Bootstrapping Kerberos  
draft-tschofenig-pana-bootstrap-kerberos-00

Status of this Memo

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, and any of which I become aware will be disclosed, in accordance with [RFC 3668](#).

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/lid-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 January 10, 2005.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

Abstract

This document proposes a mechanism to obtain a Kerberos Ticket Granting Ticket based on a successful EAP authentication and key agreement message exchange. The initial network access authentication procedure based on EAP is ideal for this purpose. This proposal allows Kerberos to be used within a local network without relying on a global Kerberos infrastructure. It should allow an incremental deployment of Kerberos and a wider distribution of Kerberos into roaming environments.

Internet-Draft

Bootstrapping Kerberos

July 2004

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Terminology . . . . .	<a href="#">4</a>
<a href="#">3.</a>	Problem Statement . . . . .	<a href="#">5</a>
<a href="#">4.</a>	Solution Approach . . . . .	<a href="#">6</a>
<a href="#">5.</a>	What are the advantages? . . . . .	<a href="#">11</a>
<a href="#">6.</a>	What are the disadvantages? . . . . .	<a href="#">12</a>
<a href="#">7.</a>	Security Considerations . . . . .	<a href="#">13</a>
<a href="#">8.</a>	Open Issues . . . . .	<a href="#">14</a>
<a href="#">9.</a>	Acknowledgments . . . . .	<a href="#">16</a>
<a href="#">10.</a>	References . . . . .	<a href="#">17</a>
<a href="#">10.1</a>	Normative References . . . . .	<a href="#">17</a>
<a href="#">10.2</a>	Informative References . . . . .	<a href="#">17</a>
	Authors' Addresses . . . . .	<a href="#">19</a>
	Intellectual Property and Copyright Statements . . . . .	<a href="#">20</a>

## 1. Introduction

Kerberos (see [[RFC1510](#)] and [[I-D.ietf-krb-wg-kerberos-clarifications](#)]) is a well-known security protocol which provides authentication, authorization and key distribution and is used to secure a number of protocols - a list too large to mention here. It is widely deployed in enterprise networks where cross-realm authentication is not required at all or only to a certain extent (in a environment with a hierarchical organizational structure). In mobility environments Kerberos is, unfortunately, not widely deployed since AAA protocols (such as RADIUS and DIAMETER), which have different cross-realm (or inter-domain) signaling message exchanges, are heavily used. The security properties of AAA protocols and Kerberos also differ. The EAP key management framework is described in [[I-D.ietf-eap-keying](#)]. This proposal tries to combine the two protocols: Kerberos is used within the local network and the AAA protocol is used as part of the network access authentication and for communication between the visited network and the home network.

## [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 [[RFC2119](#)].

### [3.](#) Problem Statement

RADIUS [[RFC2865](#)] and DIAMETER [[RFC3588](#)] are used in an environment where accounting and charging is an important functionality. Kerberos was never designed to provide these features. Kerberos provides cross-realm functionality in a way which is different to EAP/AAA protocols. Even though the cross-realm authentication approach used by Kerberos might provide better security properties (such as denial of service protection) the EAP/AAA is gaining importance.

By combining the functionality of AAA protocols (cross-realm/inter-domain behavior, accounting functionality and the existing AAA infrastructure) with the benefits of Kerberos (support by a number of existing protocols, authorization capabilities, key distribution and protection of messages) a number of advantages can be achieved.

Section 3.4.4 of [[I-D.iab-research-funding](#)] points to the importance of providing solutions for inter-realm Kerberos deployments: 'The need for scalable inter-domain user authentication is increasingly acute as ad-hoc computing and mobile computing become more widely

deployed. Thus, work on scalable mechanisms for mobile, ad-hoc, and non-hierarchical inter-domain authentication would be very helpful.'

#### 4. Solution Approach

At its abstract level this proposal suggests to start with a regular AAA communication which might includes the usage of EAP [[I-D.ietf-eap-rfc2284bis](#)]. EAP acts as a container for a number of authentication and key agreement mechanisms. The AAA infrastructure is used to route, to transport and to secure AAA messages and their payloads. As a result of the network access authentication the user is authenticated to its home AAA server (in the subscription based scenario) and the AAA protocol is ready to exchange collected accounting records. In addition to this exchange the visited network (to which the user's device is attached) receives the gurantee through the execution of the AAA protocol and the AAA infrastructure (roaming agreements etc.) that the home network can be hold liable

for the payment for the consumed resources by the end user.

Subsequently to a successful authentication and authorization the AAA protocol does not only transmit a session key to the AAA attendant but also creates a Kerberos Ticket Granting Ticket (TGT). This TGT is only valid for the local network and is sent to the end host. The session key is only sent to the Authenticator and not to the end host whereas the TGT has to be made available to the end host itself. A protocol between the end host and the Authenticator is therefore required to carry the TGT.

Using the obtained TGT the user is able to request further service tickets using a standard Kerberos service ticket request. A user might also request service tickets for various applications, to secure infrastructure services (DHCP, SLP, DNS, etc.), to secure QoS signaling protocols (see [\[RFC3182\]](#) for RSVP security based on Kerberos) or might even request a service ticket to subsequently execute KINK [\[I-D.ietf-kink-kink\]](#) for the purpose of establishing IPsec security associations.

Figure 1 shows a typical message exchange executed when an end host moves to a new network. First, in step (1) some sort of address configuration procedure takes place. If the network access authentication procedure is executed as part of the link layer protocol as for example in IEEE 802.11 then address configuration is executed after step (2). The network access procedure (2) might require many roundtrips depending on the authentication and key exchange protocol used. Finally, after a successful completion of the protocol exchange a TGT is attached to the final message and sent to the end host in step (3). This requires an additional Radius/Diameter attribute to carry the TGT from the local AAA server (if we assume that it is created at the local AAA server), which is assumed to be co-located with the Kerberos Authentication Server (labeled as KDC in Figure 1). Co-locating these two entities is done mainly for

simplicity reasons since an additional protocol would be required for communication rather than an API call. The TGT must, additionally, be sent from the AAA attendant to the end host. Subsequently Kerberos service tickets can be requested using the standard Kerberos message exchange (step (4)).

FOR DISCUSSION: Should we create

- o a Ticket Granting Ticket which is sent to the end host or
- o bootstrap a security association (and in particular a session key) which is then used by the end host to request the Ticket Granting Ticket.

The latter approach would not modify the initial TGT Kerberos exchange. Further issues are discussed in [Section 8](#).

EAP acts as a container for a number of authentication and key exchange protocols. As such some observations have to be made concerning the properties of the used mechanisms: Since the Ticket Granting Ticket has to include the AAA distributed session key (key field in the encrypted part of the ticket) this proposal requires an EAP mechanism which provides session key distribution. This session key is then used by the end host to create an Authenticator for a subsequent service ticket requests.



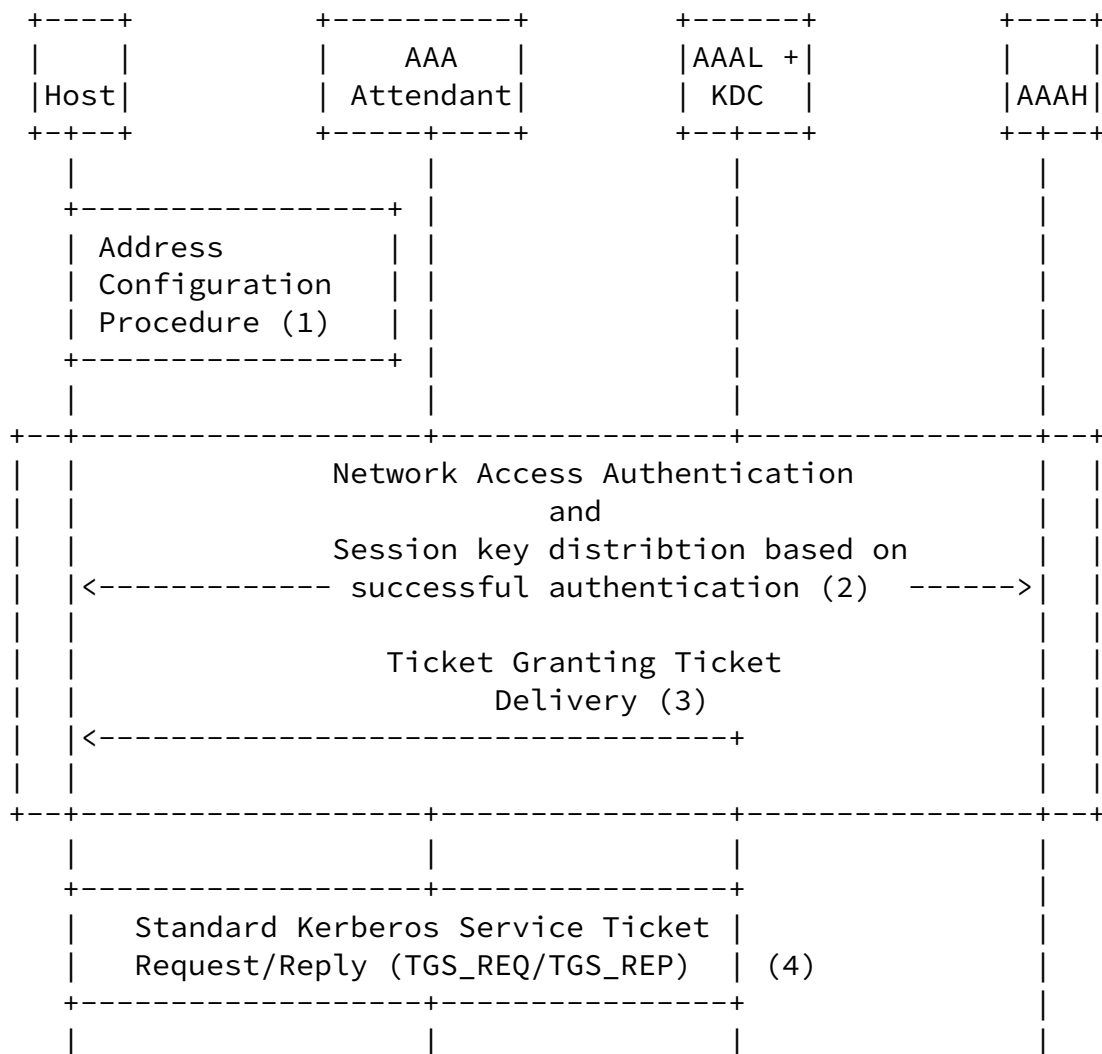


Figure 1: Message Flow

Figure 2 shows a Ticket Granting Ticket with the relevant fields. The ticket consists of two parts - one unencrypted and an encrypted part. The unencrypted part contains only information for the recipient (in our case for the Ticket Granting Server) to be able to recognize a ticket for which a key to decrypt the ticket is available. In the described case these fields contain the ticket version number, the realm name of the visited network and the principal name of the Ticket Granting Server (TGS). The remaining fields of the ticket are encrypted with the key known only to the TGS and the Authentication Server (AS). Note that the AS is co-located with the local AAA server in our scenario. The encrypted part of the ticket contains information about the user's realm and its identity which are obtained from the initial authentication procedure. The flags field contains a flag which provides an indication of this Kerberos bootstrapping procedure to differentiate it to a regular AS\_REQ/AS\_REP exchange. The key field is important since it contains the session key distributed during the initial authentication

Note that a protocol is required to carry the EAP messages and the TGT from the AAA attendant to the end host. Such a protocol is required to exchange the necessary parameters. This document does not mandate a particular protocol. However, PANA [[I-D.ietf-pana-pana](#)] is suitable for this purpose since it is a flexible and extensible protocol and allows the secure exchange of parameters between the end host and the network.

Unencrypted part of the ticket	Ticket Version Number	
	Realm that issued a ticket	
	Server's Principal Name (sname)	
(with a key known to the TGS)		
	Flags	
	Key	
	Realm in which the client is registered (crealm)	
	Client's principal identifier (cname)	
	Transited Realms	
	Time of initial authentication (authtime)	
	Starttime	
	Endtime	
	Renew-till	
Hostaddress(es) (caddr)		
Authorization-data		

It is important to highlight that the proposal described in this document makes an assumption which has to be satisfied in order for this bootstrapping mechanism to work:

The authentication and key exchange protocol shown in Figure 1 (step 2) assumes that a session key is distributed and after a successful protocol execution established between the end host and the AAA attendant. The session key distribution with the help of AAA also

allows the local AAA server to learn the session key. Since the Ticket Granting Ticket requires a session key to be placed in the Key field as shown in Figure 2. Hence authentication and key exchange protocol which do not establish a session key between the end host and the local network (AAA attendant/local AAA server) cannot be used

for bootstrapping a Kerberos Ticket Granting Ticket.

Additionally it should be noted that the proposed bootstrapping protocol does not necessarily require the execution of a EAP protocol. Protocols such as described in [[I-D.perkins-aaav6](#)], in [[I-D.mun-aaa-dbu-mobileipv6](#)] and in [[I-D.le-aaa-diameter-mobileipv6](#)] would also provide the desired functionality without relying on EAP methods for authentication. Instead a custom authentication and key exchange protocol is defined. Even the protocols developed in the SACRED working group would provide the necessary pre-requisity to return a Ticket Granting Ticket and to use this proposal. To focus on an increasingly common deployment environment we have focused on EAP.

## 5. What are the advantages?

The authors think that this proposal has the following advantages:

- o A large number of protocols support Kerberos as an authentication and key distribution protocol. Enabling Kerberos to be used for these environments would also enable these protocols to be secured with Kerberos.
- o Initial cross-realm/inter-domain authentication can be done using an arbitrary protocol (in case of EAP).
- o Kerberos relies on symmetric keys (ignoring PKINIT [[I-D.ietf-cat-kerberos-pk-init](#)] and PKCROSS [[I-D.ietf-cat-kerberos-pk-cross](#)]) for authentication and key distribution. The usage of symmetric keys is highly efficient and the risk of denial of service attacks often found in public key based protocols is reduced.
- o Kerberos tickets are designed to allow authorization information to be added to the ticket itself. Authorization information can be added by the KDC and allows services to base their access control policies not only on the identity of the principal.
- o When passwords are used with Kerberos (without PKINIT or other mechanisms) then there might be a vulnerability to dictionary attacks. Replacing the AS exchange with an EAP authentication this vulnerability can be prevented. Note that this assumes that the chosen EAP method is not vulnerable to dictionary attacks.

- o Some EAP methods provide user identity confidentiality of the EAP peer against either active or passive adversaries. If a Kerberos Ticket Granting Ticket is created with the help of the EAP derived key and the user identity is not copied to the Ticket Granting Ticket then there is no indication for an eavesdropper about the identity of a user. This approach therefore adds user identity confidentiality to Kerberos.

## 6. What are the disadvantages?

Despite the advantages listed in the previous section there are some disadvantages or constraints with the following proposal:

- o A Kerberos implementation has to be supported by end hosts.
- o Kerberos heavily relies on timestamps. If the clocks of the end host and the various servers in the access network suffer from a clock-drift then some procedure is required for clock-synchronization. Such procedures are for example described in[I-D.ietf-krb-wg-kerberos-clarifications]. It requires further investigation whether a secure time distribution mechanism should be included in this proposal.

## [7.](#) Security Considerations

The security of the proposed mechanism relies on the selected EAP mechanism, on Kerberos and on the AAA key distribution mechanism. A security analysis of different EAP methods is outside the scope of this document. It is assumed that the AAA key distribution mechanism, the selected EAP method and Kerberos is secure.

Hence this section can only describe threats related to the proposed distribution of the TGT.

Stealing of the TGT:

An adversary might eavesdrop on the wireless link between the end host and the AAA attendant to learn the exchanged TGT. Without

confidentiality protection of the TGT an adversary might be able to retrieve the TGT. Since the TGT is encrypted with the key of the ticket granting server (TGS). It is assumed that this key has sufficient length. This assures that an adversary is able to learn the encrypted content of the ticket. Hence we can conclude that an adversary might not be able to request further service tickets only based on the knowledge of the ticket granting ticket. This is inline with the basic principles of Kerberos.

#### Modification of the TGT:

An adversary might want to modify the content of the TGT. A TGS would immediately detect such a modification because most parts of the ticket are encrypted. The unencrypted parts only contain information about the TGS and its realm and are useless for an adversary.

#### Replay of the TGT:

An adversary (malicious end host) might want to reuse a TGT of a previous message exchange. Since the TGT contains a lifetime field it is not possible to use TGTs with an expired lifetime. In order to request a service ticket the end host has to know the session key to build an Authenticator.

## [8.](#) Open Issues

This section lists some open issues which have been identified during the work on this approach:

- o Packet formats (e.g., AAA AVP, PANA AVPs, etc.) are missing.
- o As an alternative to provide the end host (i.e., user) with a TGT

it would be possible to create a tentative user account at the KDC. This allows the end host to request a TGT and subsequently service tickets. This approach would not require a TGT to be transferred to the end host with the initial AAA exchange.

- o In order to provide a service ticket to run KINK for achieving secure network access an additional roundtrip is required. Solutions are possible which allow the establishment of an IPsec security association with a fewer number of roundtrips.
- o Should it be possible to request more than a TGT (for example a service ticket for secure network access) with the help of this proposal?
- o It might be helpful to have a flag inside the ticket to indicate that the ticket presented to a server was not obtained by a regular AS exchange but rather with this bootstrapping mechanism.
- o It would also be possible to provide the client with a secure network time by protecting the timestamp as part of a PANA exchange.
- o Should the proposed extension return a full AS\_REP instead of only the TGT? This would allow the end host to learn the current time based on the information inside the ticket. The TGT also contains time information but it is not accessible for the end host (i.e. it is included in the encrypted part).
- o In this proposal the TGT is created at the local AAA server. Therefore the local AAA server needs to wait until a successful network access authentication indication is available. The EAP-Success message indicates a successful EAP method protocol run. Hence, it is necessary for the AAA server to bind the EAP run to the TGT. Furthermore, the local AAA server needs to inspect the session key transferred with the AAA attribute in order to create the TGT. More details need to be provided. It might be possible to create the TGT at the Authenticator itself rather than in the local AAA server. This would, however, cause an increase in the number of entities which need to be trusted by the KDC.

- o Finally, it might be possible to replace this entire bootstrapping



mechanism with a new AS\_REQ/AS\_REP protocol exchange which uses EAP. This exchange could use EAP and the KDC would act as the Authenticator in the EAP architecture. The main advantage of this approach is achieved by protocol separation. A full EAP roundtrip might not be required since the local AAA server might have stored the session key of the previous protocol run already.

- o Some discussions with regard to the EAP keying framework should go in [Section 7](#). A future version of this document will contain a formal verification of the proposed approach.
- o The relationship with the work done in the 3GPP Bootstrapping architecture and the SACRED work needs to be described.

## [9.](#) Acknowledgments

We would like to thank Guenther Horn, Dirk Kroeselberg and Wolfgang Buecker for their comments to this draft.

Furthermore, Hannes Tschofenig would like to thank Derek Atkins for discussions with an older version of this draft (more than a year ago).

Jorge Cuellar encourage us to publish this document.

## [10.](#) References

### [10.1](#) Normative References

[I-D.ietf-eap-rfc2284bis]

Blunk, L., Carlson, J. and B. Aboba, "Extensible Authentication Protocol (EAP)", [draft-ietf-eap-rfc2284bis-09](#) (work in progress), February 2004, <reference.I-D.ietf-eap-rfc2284bis.xml>.

[I-D.ietf-pana-pana]

Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H. and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", [draft-ietf-pana-pana-04](#) (work in progress), May 2004, <reference.I-D.ietf-pana-pana.xml>.

[RFC1510] Kohl, J. and B. Neuman, "The Kerberos Network Authentication Service (V5)", [RFC 1510](#), September 1993, <reference.RFC.1510.xml>.

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

[RFC2865] Rigney, C., Willens, S., Rubens, A. and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", [RFC 2865](#), June 2000.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G. and J. Arkko, "Diameter Base Protocol", [RFC 3588](#), September 2003, <reference.RFC.3588.xml>.

### [10.2](#) Informative References

[I-D.iab-research-funding]

Atkinson, R. and S. Floyd, "IAB Concerns & Recommendations Regarding Internet Research & Evolution", [draft-iab-research-funding-03](#) (work in progress), May 2004, <reference.I-D.iab-research-funding.xml>.

[I-D.ietf-cat-kerberos-pk-cross]

Tsudik, G., Neuman, C., Sommerfeld, B., Tung, B., Hur, M., Ryutov, T. and A. Medvinsky, "Public Key Cryptography for Cross-Realm Authentication in Kerberos", [draft-ietf-cat-kerberos-pk-cross-08](#) (work in progress), November 2001, <reference.I-D.ietf-cat-kerberos-pk-cross.xml>.

[I-D.ietf-cat-kerberos-pk-init]

Tung, B., Neuman, C., Hur, M., Medvinsky, A., Medvinsky, S., Wray, J. and J. Trostle, "Public Key Cryptography for Initial Authentication in Kerberos", [draft-ietf-cat-kerberos-pk-init-19](#) (work in progress), April 2004, <reference.I-D.ietf-cat-kerberos-pk-init.xml>.

[I-D.ietf-eap-keying]

Aboba, B., "EAP Key Management Framework", [draft-ietf-eap-keying-01](#) (work in progress), October 2003, <reference.I-D.ietf-eap-keying.xml>.

[I-D.ietf-kink-kink]

Thomas, M. and J. Vilhuber, "Kerberized Internet Negotiation of Keys (KINK)", [draft-ietf-kink-kink-05](#) (work in progress), January 2003, <reference.I-D.ietf-kink-kink.xml>.

[I-D.ietf-krb-wg-kerberos-clarifications]

Neuman, C., "The Kerberos Network Authentication Service (V5)", [draft-ietf-krb-wg-kerberos-clarifications-05](#) (work in progress), February 2004, <reference.I-D.ietf-krb-wg-kerberos-clarifications.xml>.

[I-D.le-aaa-diameter-mobileipv6]

Faccin, S., "Diameter Mobile IPv6 Application", [draft-le-aaa-diameter-mobileipv6-03](#) (work in progress), April 2003, <reference.I-D.le-aaa-diameter-mobileipv6.xml>.

[I-D.mun-aaa-dbu-mobileipv6]

Kim, M. and Y. Mun, "Dynamic Binding Update using AAA", [draft-mun-aaa-dbu-mobileipv6-00](#) (work in progress),

December 2002, <reference.I-D.mun-aaa-dbu-mobileipv6.xml>.

[I-D.perkins-aaav6]

Perkins, C., Flykt, P. and T. Eklund, "AAA for IPv6 Network Access", [draft-perkins-aaav6-06](#) (work in progress), May 2003, <reference.I-D.perkins-aaav6.xml>.

[RFC3182] Yadav, S., Yavatkar, R., Pabbati, R., Ford, P., Moore, T., Herzog, S. and R. Hess, "Identity Representation for RSVP", [RFC 3182](#), October 2001, <reference.RFC.3182.xml>.

Tschofenig & Sankhla

Expires January 10, 2005

[Page 18]

---

Internet-Draft

Bootstrapping Kerberos

July 2004

#### Authors' Addresses

Hannes Tschofenig  
Siemens  
Otto-Hahn-Ring 6  
Munich, Bayern 81739  
Germany

EMail: [Hannes.Tschofenig@siemens.com](mailto:Hannes.Tschofenig@siemens.com)

Vishal Sankhla  
University of Southern California  
1860N, Fuller Avenue, Apt 117  
Los Angeles, California 90046  
USA

EMail: [sankhla@usc.edu](mailto:sankhla@usc.edu)

#### 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](mailto: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 (2004). 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.