NSIS
Internet-Draft
Expires: January 10, 2005

H. Tschofenig
J. Kross
Siemens AG

July 12, 2004

Extended QoS Authorization for the QoS NSLP
draft-tschofenig-nsis-qos-ext-authz-00

Status of this Memo

Copyright Notice

Abstract

Proper authorization is essential for a Quality of Service signaling protocol. Three authorization models have been identified: a two-party model, a token-based three-party model, and a generic three-party model

This document discusses two possible solution for the generic three-party model: a challenge/response based and an EAP-based approach.

Table of Contents

1. Introduction

Three authorization models are described in Section 3.6 of [I-D.ietf-nsis-qos-nslp]:

- Two party approach
- Token based three party approach
- Generic three party approach

The two party approach is sketched in Section 3.6.1 of [I-D.ietf-nsis-qos-nslp], the token based three party approach is described in Section 3.6.2 of [I-D.ietf-nsis-qos-nslp] (based on [RFC3520] and [RFC3521]), and an overview of the generic three party approach is provided with Section 3.6.3 of [I-D.ietf-nsis-qos-nslp].

It is obvious that these authorization approaches offer different security and address different deployment scenarios.

This document focuses on a more detailed discussion of the generic three party approach. Section 3 provides an overview of the generic three party approach. Section 4 lists two possible solution approaches. For completeness, object payloads are described in Section 5. A short conclusion is given in Section 6.

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. Overview

This section offers message flows and protocol-specific details about authorization for QoS reservations for the generic three party approach.

Figure 1 illustrates a case where an entity A (e.g., an end host) sends an NSIS QoS signaling message towards an entity B (e.g, a NSIS aware router). This request cannot be authorized by entity B itself but is rather forwarded to another entity C. The protocol used between entity A and entity B is based on NSIS whereas the protocol used between entity B and entity C is, for example, Diameter. A proposal for a Diameter QoS application is provided with [I-D.alfano-aaa-qosprot].

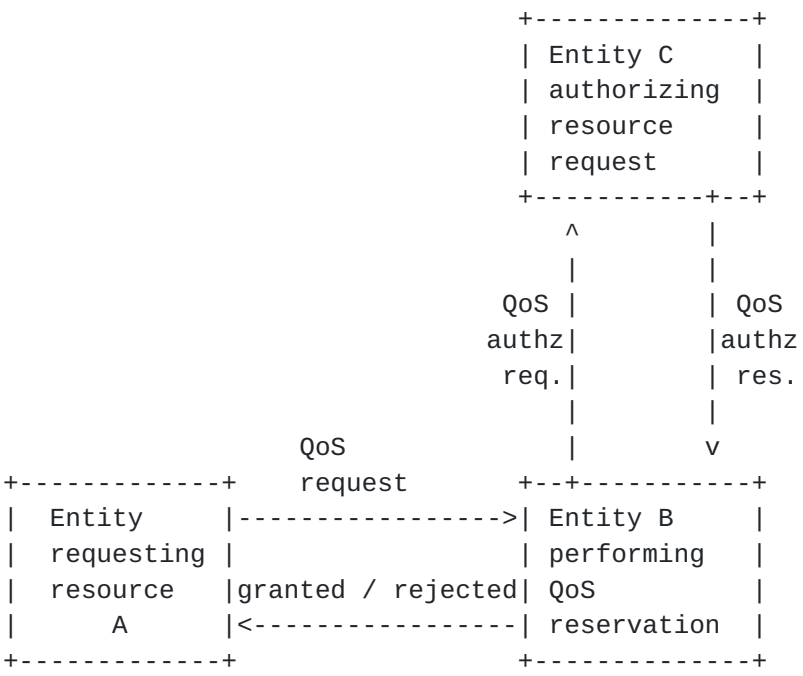


Figure 1: Three party approach

In the following, two alternative solution proposals for this model are shown:

- Challenge/Response-based Authentication and Authorization
- EAP-based Authentication and Authorization

4. Protocol Alternatives

4.1 Challenge/Response-based Authentication/Authorization

Figure 2 shows a message flow for the generic three party approach with a challenge-response mechanism. In this case, after entity B asked entity C for authorization of a QoS request, entity C issues a challenge to entity A, which is passed on by entity B. Entity A resubmits its QoS request, including a response to the challenge. This is again forwarded to entity C, which verifies whether entity A is the one it claims to be, and if so, and after checking for entity A's authorization to use the resources it requests, either grants or denies the request.

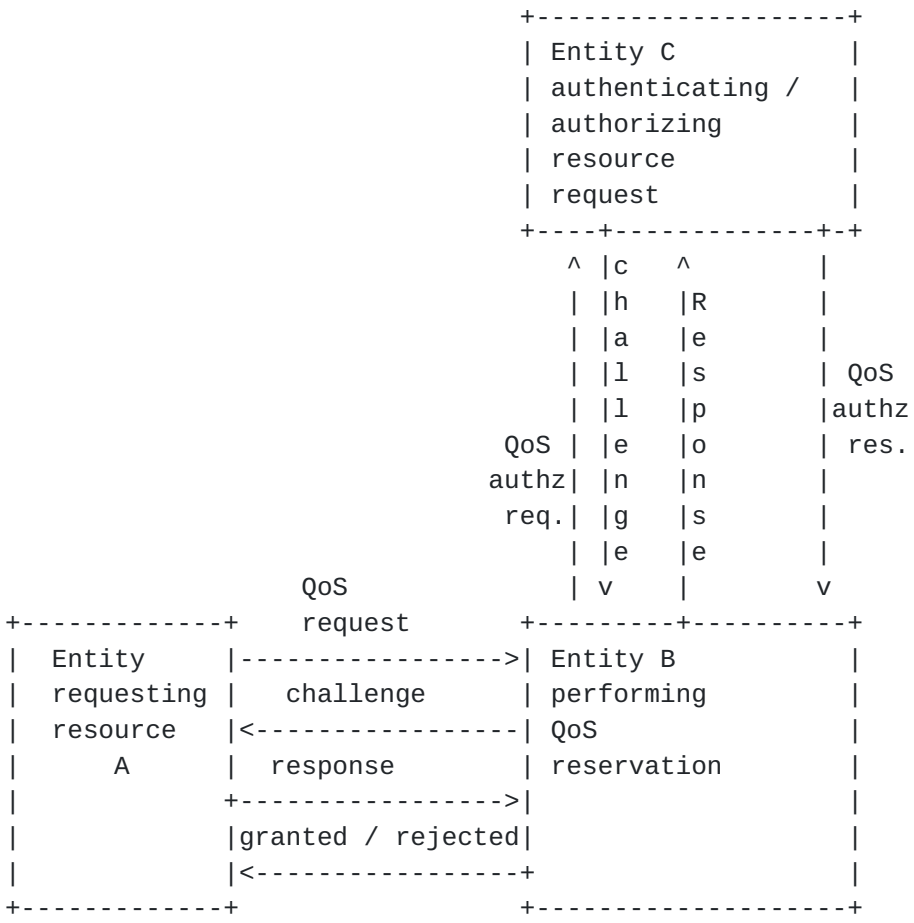


Figure 2: Three party challenge-response based approach

Please note that the QoS NSLP does not explicitly send a successful response message for the challenge/response protocol after a QoS reservation request. Instead the successful outcome of the protocol

run is implicated by the successul commitment of the entire QoS reservation. An unsuccessful outcome of the challenge/response protocol, however, would be indicated explicitly by a reject message returned immediately - the error codes still need to be defined in [I-D.ietf-nsis-qos-nslp].

The properties of this approach are intentionally similar to the digest-authentication used with SIP (see [RFC3261]). This approach provides better security properties than a token-based authorization approach since a stronger liveness check needs to be provided. The QoS request and the result of the challenge/response authentication and authorization need to be associated with each other. Furthermore, it is necessary to bind subsequent refresh messages to the initial authentication and authorization protocol step. This is typically accomplished with the establishment of session keys and the protection of signaling messages between entity A and B.

The necessary steps for the QoS NSLP are the following:

- A challenge/response protocol needs to be defined or selected. A number of protocols can be reused, including the digest-authentication approach listed in [RFC3261]. This authentication and key exchange protocol needs to provide mutual authentication, replay protection and session key establishment. It seems to be reasonable to investigate some of the requirements raised in [I-D.walker-ieee802-req] regarding the selection of such a protocol.

- Integrity protection needs to be applied to signaling messages exchanged between the entity A and entity B once a session key is available.

- Since the authentication and key establishment is executed betwen entity A and entity C, it is necessary to forward the established keying material from entity C to entity B (using AAA protocols).

- In some circumstances it might be necessary to combine the security protection at the NTLP with the security protection at the NSLP. This can, for example, be accomplished by combining the session keys of both security protocols as suggested in [I-D.puthenkulam-eap-binding]. Such a binding is necessary if the reused challenge/response protocol is also used in other protocols.

4.2 EAP-based Authentication/Authorization

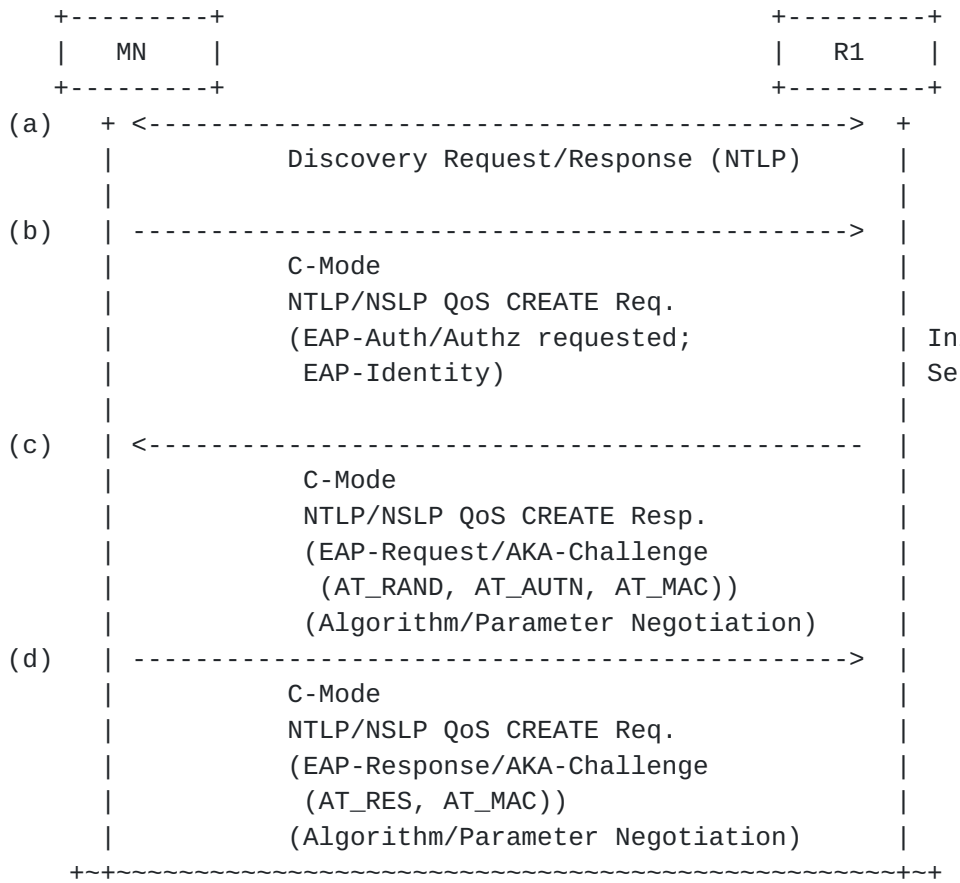
The Extensible Authentication Protocol (EAP) serves as a container

for EAP methods. EAP methods themselves are authentication and key exchange protocols. EAP is agnostic with regard to the underlying protocol carrying the EAP payloads.

The main difference between the EAP-based approach discussed in this section, and the challenge/response based approach discussed in Section 4.1 is related to the flexible choice of authentication and key exchange protocols with EAP on the one hand, and some degree of inefficiency introduced with EAP (such as the EAP-Request/Identity, EAP-Response/Identity and EAP-Success messages) on the other hand.

Due to the usage of EAP in IEEE 802.1X and also in PANA, the security properties have been studied extensively. The discussions in the EAP keying framework (see [I-D.ietf-eap-keying]) are also applicable. Please note that EAP is not necessarily a three party protocol - EAP also supports the two party scenario.

An example message flow is shown in Figure 3 which uses the EAP-AKA method [I-D.arkko-pppext-eap-aka] for authentication and session key establishment. Please note that the AAA messages triggered by this exchange are not shown for editorial reasons.



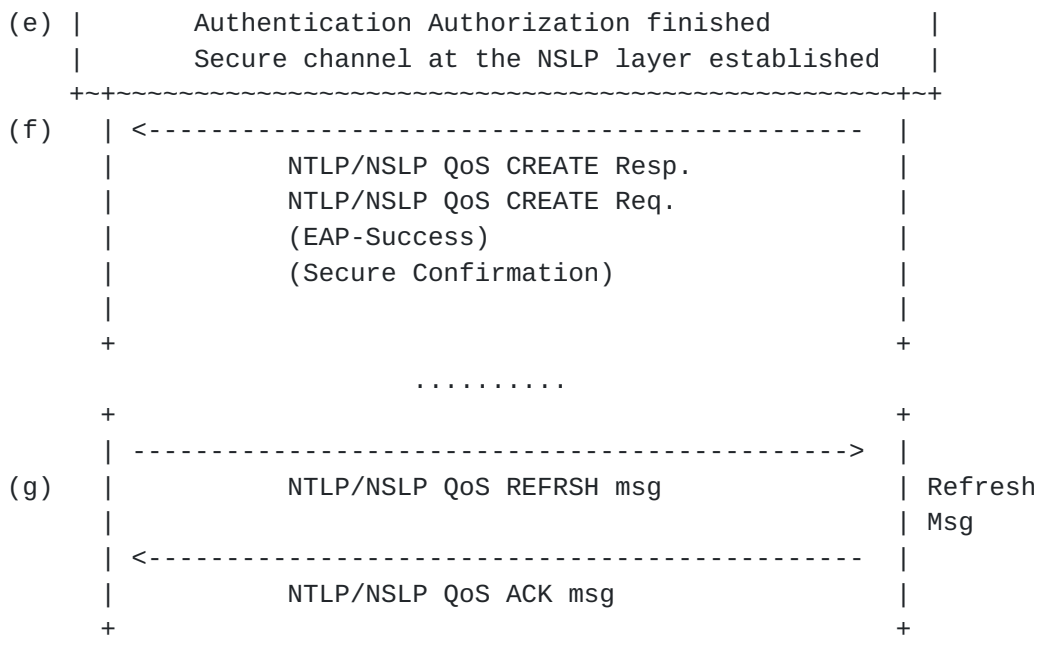


Figure 3: EAP based Auth/Authz exchange using EAP-AKA

The message exchange shown in Figure 3 starts with the optional discovery of the next QoS NSLP aware node (messages (a)). The first QoS NSLP message with a resource request is sent with the Network Access Identity and a request to perform EAP-based authentication (message (b)). Note that this exchange assumes that the EAP-Request/ Identity and the EAP-Response/Identity exchange is omitted. This exchange is optional in EAP if the identity can be provided by other means. Router 1 contacts the AAA infrastructure, and the EAP server starts the message exchange. The AAA message communication is not shown. Subsequently, two messages (messages (c) and (d)) are exchanged between the EAP peer and the EAP server which contain EAP-AKA specific information. After successful authentication and authorization, session keys are derived and provided to R1 via AAA mechanisms (see [I-D.ietf-aaa-eap] and [RFC3579]). These session keys can then be used to protect subsequent NSLP messages as indicated by (e). The EAP-Success message can already experience such a protection (see message (f)). Furthermore, it is useful to repeat the previously sent objects. Subsequent refresh messages (g) are protected with the previously established session keys and are therefore associated with the previous authentication and authorization protocol execution.

5. Payload Formats

5.1 Challenge/Response-based Authentication/Authorization

For carrying the credentials for the challenge/response-based authentication and authorization approach within the QoS NSLP, it is proposed to use a new Policy Element, called CR policy element. Its format is shown in Figure 4.

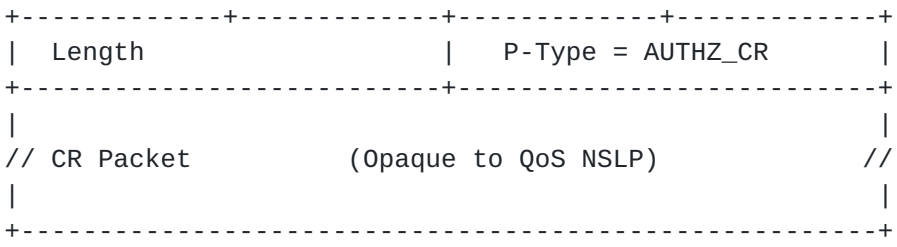


Figure 4: Format of CR Policy Element

CR Packet: The CR Packet contains the information required for the Challenge/Response handshake. Further details will be described in a future version of this document.

5.2 EAP-based Authentication/Authorization

Figure 3 illustrates an example message flow for EAP-based authentication and authorization. This section proposes how to integrate the data required for the EAP exchange into the QoS NSLP message format.

[I-D.ietf-nsis-qos-nslp] describes the generic format for Policy Elements. It is proposed that the EAP data is carried within a new Policy Element, called EAP Policy Element. It follows the generic format of Policy elements as defined in Appendix A.7.3 of [I-D.ietf-nsis-qos-nslp]. Figure 5 illustrates the specific format.

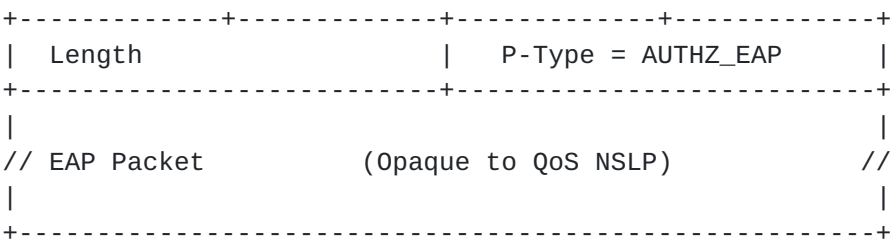


Figure 5: Format of EAP Policy Element

EAP Packet: The EAP Packet contains an EAP packet in the format of [RFC3748], section 4.

5.3 Integrity Object

A future version of this document will describe the payload format of an Integrity Object.

6. Conclusion

The QoS NSLP has to be provided for the generic three party case in order to be complete. This document discusses two possible solutions: the challenge/response and the EAP-based approach

The working group needs to make the following two decisions:

- Should a challenge/response or an EAP-based scheme be developed?
- Should this work be included in the main QoS NSLP [I-D.ietf-nsis-qos-nslp] document?

There are some technical aspects that need to be addressed, as explained throughout the text. Hence, the enhancement is more complex than just adding one new payload to the NSLP. Some security issues and also non-security issues need to be solved. For example, EAP itself is only a container and does not provide fragmentation and reliable transmission of EAP payloads. Carrying EAP within the QoS NSLP requires further investigations since different transport protocols have to be supported by GIMPS (see [I-D.schulzrinne-nsis-ntlp]). These issues have already been discussed in, for example, PANA [I-D.ietf-pana-pana].

7. Security considerations

Selected security aspects with the challenge/response based approach have been mentioned in Section 4.1 and with respect to EAP in Section 4.2.

If security protection is provided by GIMPS (which is an instantiation of the NTLP) and also at the NSLP with the mechanisms discussed in this document, then the two phases should be combined since security vulnerabilities are introduced otherwise. For example, running EAP over TLS for client-side authentication could be one possibility but it raises issues with the discovered man-in-the-middle attack problems for tunneled authentication (see [I-D.puthenkulam-eap-binding]).

There is certainly a tradeoff between the flexibility of EAP and the simplicity of a challenge/response protocol.

In some scenarios, it is necessary to cope with the 'lying NAS' problem. With the usage of EAP, it is necessary to provide the EAP server with enough information to perform the authorization steps. However, EAP methods themselves are independent of the environment in which they are executed. Hence, an adversary (acting as an NSIS NSLP node) could misuse an EAP exchange to create the illusion for the EAP server that the context is different (e.g., wireless LAN access). The work in the area [I-D.arkko-eap-service-identity-auth] and [I-D.mariblanca-aaa-eap-lla] is applicable in this context. The goal is to give both, the EAP peer and the EAP server, enough assurance that the Authenticator (i.e., QoS NSLP in this context) is not lying.

It might be worth mentioning that the introduction of COPS in RSVP (see [RFC2749]) and the usage of POLICY_OBJECT [RFC3182] already provided a first attempt in offering a generic three party authorization model. Hence, the problem is not artifical. Unfortunately, the multiple-roundtrip communication and the AAA infrastructure was not fully worked out at that time. The deficiencies in a roaming environment have first been mentioned with [I-D.thomas-nsis-rsvp-analysis]. A more detailed treatment of the security properties are provided with [I-D.ietf-nsis-rsvp-sec-properties].

8. References

8.1 Normative References

[I-D.ietf-nsis-qos-nslp]
Bosch, S., Karagiannis, G. and A. McDonald, "NSLP for Quality-of-Service signaling", draft-ietf-nsis-qos-nslp-03 (work in progress), May 2004.

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

[RFC3579] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J. and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

8.2 Informative References

[I-D.alfano-aaa-qosprot]
Alfano, F., McCann, P. and H. Tschofenig, "Diameter Quality of Service Application", draft-alfano-aaa-qosprot-00 (work in progress), July 2004, <reference.I-D.alfano-aaa-qosprot.xml>.

[I-D.arkko-eap-service-identity-auth]
Arkko, J. and P. Eronen, "Authenticated Service Identities for the Extensible Authentication Protocol (EAP)", draft-arkko-eap-service-identity-auth-00 (work in progress), April 2004, <reference.I-D.arkko-eap-service-identity-auth.xml>.

[I-D.arkko-pppext-eap-aka]
Arkko, J. and H. Haverinen, "EAP AKA Authentication", draft-arkko-pppext-eap-aka-12 (work in progress), April 2004, <reference.I-D.arkko-pppext-eap-aka.xml>.

[I-D.ietf-aaa-eap]
Eronen, P., Hiller, T. and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", draft-ietf-aaa-eap-08 (work in progress), June 2004, <reference.I-D.ietf-aaa-eap.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-nsis-nslp-natfw]
Stiemerling, M., Tschofenig, H., Martin, M. and C. Aoun, "A NAT/Firewall NSIS Signaling Layer Protocol (NSLP)", draft-ietf-nsis-nslp-natfw-02 (work in progress), May 2004.

[I-D.ietf-nsis-ntlp]
Schulzrinne, H. and R. Hancock, "GIMPS: General Internet Messaging Protocol for Signaling", draft-ietf-nsis-ntlp-02 (work in progress), May 2004.

[I-D.ietf-nsis-rsvp-sec-properties]
Tschofenig, H. and R. Graveman, "RSVP Security Properties", draft-ietf-nsis-rsvp-sec-properties-04 (work in progress), February 2004, <reference.I-D.ietf-nsis-rsvp-sec-properties.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>.

[I-D.mariblanca-aaa-eap-lla]
Mariblanca, D., "EAP lower layer attributes for AAA protocols", draft-mariblanca-aaa-eap-lla-01 (work in progress), June 2004, <reference.I-D.mariblanca-aaa-eap-lla.xml>.

[I-D.puthenkulam-eap-binding]
Puthenkulam, J., "The Compound Authentication Binding Problem", draft-puthenkulam-eap-binding-04 (work in progress), October 2003, <reference.I-D.puthenkulam-eap-binding.xml>.

[I-D.schulzrinne-nsis-ntlp]
Schulzrinne, H., "GIMPS: General Internet Messaging Protocol for Signaling", draft-schulzrinne-nsis-ntlp-00 (work in progress), June 2003, <reference.I-D.schulzrinne-nsis-ntlp.xml>.

[I-D.thomas-nsis-rsvp-analysis]
Thomas, M., "Analysis of Mobile IP and RSVP Interactions", draft-thomas-nsis-rsvp-analysis-00 (work in progress), November 2002,

<reference.I-D.thomas-nsis-rsvp-analysis.xml>.

[I-D.walker-ieee802-req]
Stanley, D., "EAP Method Requirements for Wireless LANs", draft-walker-ieee802-req-01 (work in progress), May 2004, <reference.I-D.walker-ieee802-req.xml>.

[RFC2749] Herzog, S., Boyle, J., Cohen, R., Durham, D., Rajan, R. and A. Sastry, "COPS usage for RSVP", RFC 2749, January 2000, <reference.RFC.2749.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>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002, <reference.RFC.3261.xml>.

[RFC3520] Hamer, L., Gage, B., Kosinski, B. and H. Shieh, "Session Authorization Policy Element", RFC 3520, April 2003.

[RFC3521] Hamer, L-N., Gage, B. and H. Shieh, "Framework for Session Set-up with Media Authorization", RFC 3521, April 2003.

Authors' Addresses

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

EMail: Hannes.Tschofenig@siemens.com

Joachim Kross
Siemens AG
Otto-Hahn-Ring 6
Munich, Bayern 81739
Germany

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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