Extensible Authentication Protocol
Internet-Draft
Expires: August 9, 2004

B. Aboba
Microsoft
M. Beadles
WorldCom Advanced Networks
J. Arkko
Ericsson
P. Eronen
Nokia

February 9, 2004

The Network Access Identifier
draft-arkko-roamops-rfc2486bis-00

Status of this Memo

Copyright Notice

Abstract

In order to provide roaming services, it is necessary to have a standardized method for identifying users. This document defines the syntax for the Network Access Identifier (NAI), the user identity submitted by the client during, for instance, PPP and wireless LAN authentication. "Roaming" may be loosely defined as the ability to use any one of multiple Internet service providers (ISPs), while

maintaining a formal, customer-vendor relationship with only one. Examples of where roaming capabilities might be required include ISP "confederations" and ISP-provided corporate network access support. This document is a revised version of RFC 2486 which originally defined NAIs. Enhancements include international character set and privacy support, as well as a number of corrections to the original RFC.

Table of Contents

1. Introduction

Considerable interest exists for a set of features that fit within the general category of "roaming capability" for dialup Internet users, wireless LAN authentication, and other applications. Interested parties have included:

- Regional Internet Service Providers (ISPs) operating within a particular state or province, looking to combine their efforts with those of other regional providers to offer dialup service over a wider area.

- National ISPs wishing to combine their operations with those of one or more ISPs in another nation to offer more comprehensive dialup service in a group of countries or on a continent.

- Wireless LAN hotspots providing service to one or more ISPs.

- Businesses desiring to offer their employees a comprehensive package of dialup services on a global basis. Those services may include Internet access as well as secure access to corporate intranets via a Virtual Private Network (VPN), enabled by tunneling protocols such as PPTP, L2F, L2TP, and IPSEC tunnel mode.

In order to enhance the interoperability of roaming services, it is necessary to have a standardized method for identifying users. This document defines syntax for the Network Access Identifier (NAI). Examples of implementations that use the NAI, and descriptions of its semantics, can be found in [8].

This document is a revised version of RFC 2486 which originally defined NAIs. Differences and enhancements compared to RFC 2486 are listed in Appendix A.

1.1 Terminology

This document frequently uses the following terms:

Network Access Identifier

The Network Access Identifier (NAI) is the userID submitted by the client during PPP authentication. In roaming, the purpose of the NAI is to identify the user as well as to assist in the routing of the authentication request. Please note that the NAI may not necessarily be the same as the user's e-mail address or the userID submitted in an application layer authentication.

Network Access Server

The Network Access Server (NAS) is the device that clients dial in order to get access to the network. In PPTP terminology this is referred to as the PPTP Access Concentrator (PAC), and in L2TP terminology, it is referred to as the L2TP Access Concentrator (LAC).

Roaming Capability

Roaming capability can be loosely defined as the ability to use any one of multiple Internet service providers (ISPs), while maintaining a formal, customer-vendor relationship with only one. Examples of cases where roaming capability might be required include ISP "confederations" and ISP- provided corporate network access support.

Tunneling Service

A tunneling service is any network service enabled by tunneling protocols such as PPTP, L2F, L2TP, and IPSEC tunnel mode. One example of a tunneling service is secure access to corporate intranets via a Virtual Private Network (VPN).

1.2 Requirements language

In this document, the key words "MAY", "MUST, "MUST NOT", "optional",

"recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [3].

1.3 Purpose

As described in [8], there are a number of services implementing dialup roaming, and the number of Internet Service Providers involved in roaming consortia is increasing rapidly.

In order to be able to offer roaming capability, one of the requirements is to be able to identify the user's home authentication server. For use in roaming, this function is accomplished via the Network Access Identifier (NAI) submitted by the user to the NAS in the initial PPP authentication. It is also expected that NASes will use the NAI as part of the process of opening a new tunnel, in order to determine the tunnel endpoint.

2. NAI Definition

2.1 Formal Syntax

The grammar for the NAI is given below, described in ABNF as documented in [4]. The grammar for the username is based on [7], and the grammar for the realm is an updated version of [1].

```
nai         = username / ( username "@" realm ) / ( "@" realm" )

username    = dot-istring

realm       = [ realm "." ] ilabel

ilabel      = let-dig * (ldh-str)

ldh-str     = *( Alpha / Digit / "-" ) let-dig

dot-istring = istring / ( dot-istring "." istring )

istring     = ichar / ( string ichar )
```

```
ichar       = c / ( "\" x )

let-dig     = Alpha / Digit

Alpha       = %x41-5A / %x61-7A   ; A-Z / a-z

Digit       = %x30-39  ;0-9

c           = < a character as specified in
Section 2.4
 >

x           = %x00-7F
              ; all 128 ASCII characters, no exception

SP          = %x20 ; Space character

special     = "<" / ">" / "(" / ")" / "[" / "]" / "\" / "."
               / "," / ";" / ":" / "@" / %x22  / Ctl
               ; %x22 is '"'

Ctl         = %x00-1F / %x7F
              ; the control characters (ASCII codes 0 through 31
              ; inclusive and 127)
```


2.2 NAI Length Considerations

Devices handling NAIs MUST support an NAI length of at least 253 octets. However, the following interoperability considerations should be noted:

- RFC 2486 required the support of NAIs only up to the length of 72 octets. As a result, it can generally not be assumed that all devices can support 253 octets.

- NAIs are often transported in the User-Name attribute of RADIUS [10]. Unfortunately, RADIUS requires devices to support content lengths of only 63 octets for this attribute. As a result, it may not be possible to transfer NAIs beyond 63 octets through all

devices. In addition, due to its message structure, RADIUS is unable to support content lengths beyond 253 octets

- o NAIs can also be transported in the User-Name attribute of Diameter [13], which supports content lengths up to 2^24 - 9 octets. As a result, NAIs processed only by Diameter nodes can be very long. Unfortunately, a NAI transported over Diameter may eventually be translated to RADIUS, in which case the above limitations apply.

2.3 Support for Username Privacy

Interpretation of the "username" part of the NAI depends on the realm in question. Therefore, the "username" part SHOULD be treated as opaque data when processed by nodes that are not authoritative (in some sense) for that realm.

Where privacy is a concern, NAIs MAY be provided in an abbreviated form by omitting the username portion. This is possible only when NAIs are used in connection with a separate authentication method that can transfer the username in a secure manner.

For roaming purposes it is typically necessary to locate the appropriate backend authentication server for the given NAI before the authentication conversation can proceed. As a result, realm portion is typically required in order for the authentication exchange to be routed to the appropriate server.

2.4 International Character Sets

Characters of the username portion in a NAI MUST fulfill the requirements specified in [6]. In addition, the use of the SP character is prohibited as well in order to retain compatibility with

the previous version of this RFC.

The realm name is an "IDN-unaware domain name slot" as defined in [5]. That is, it can contain only ASCII characters. An implementation MAY support internationalized domain names (IDNs) using the ToASCII operation; see [5] for more information.

2.5 Compatibility with E-Mail Usernames

As proposed in this document, the Network Access Identifier is of the form user@realm. Please note that while the user portion of the NAI is based on the BNF described in [7], it has been extended for internationalization support as well as for purposes of Section 2.7, and is not necessarily compatible with the usernames used in e-mail. Note also that the internationalization requirements for NAIs and e-mail addresses are different, since the former need to be typed in only by the user himself and his own operator, not by others.

2.6 Compatibility with DNS

The BNF of the realm portion allows the realm to begin with a digit, which is not permitted by the BNF described in [1]. This change was made to reflect current practice; although not permitted by the BNF described in [1], FQDNs such as 3com.com are commonly used, and accepted by current software.

2.7 Realm Construction

NAIs are used, among other purposes, for routing AAA transactions to the user's home realm. Usually, the home realm appears in the realm portion of the NAI, but in some cases a different realm can be used. This may be useful, for instance, when the home realm is only reachable via another mediating realm.

Such usage may prevent interoperability unless the parties involved have a mutual agreement that the usage is allowed. In particular, NAIs MUST NOT use a different realm than the home realm unless the sender has explicit knowledge that (a) the specified other realm is available and (b) the other realm supports such usage. The sender may determine the fulfillment of these conditions through a database, dynamic discovery, or other means not specified here. Note that the first condition is affected by roaming, as the availability of the other realm may depend on the user's location or the desired application. The use of the home realm MUST be the default unless otherwise configured.

Where these conditions are fulfilled, a NAI "user@homerealm" MAY be represented as "homerealm!user@otherrealm". When receiving such NAI,

the other realm MUST convert the format back to "user@homerealm" when passing the NAI onwards, as well as apply necessary AAA routing for the transaction.

2.8 Examples

Examples of valid Network Access Identifiers include:

```
fred@3com.com
fred@foo-9.com
fred_smith@big-co.com
fred=?#$&*+-/^smith@bigco.com
fred@bigco.com
nancy@eng.bigu.edu
eng!nancy@bigu.edu
```

Examples of invalid Network Access Identifiers include:

```
fred@foo
fred@foo_9.com
@howard.edu
fred@bigco.com@smallco.com
eng:nancy@bigu.edu
eng;nancy@bigu.edu
<nancy>@bigu.edu
```

3. Security Considerations

Since an NAI reveals the home affiliation of a user, it may assist an attacker in further probing the username space. Typically this problem is of most concern in protocols which transmit the user name in clear-text across the Internet, such as in RADIUS, described in [10] and [11]. In order to prevent snooping of the user name, protocols may use confidentiality services provided by protocols transporting them, such RADIUS protected by IPsec [12] or Diameter protected by TLS [13].

4. IANA Considerations

In order to to avoid creating any new administrative procedures, administration of the NAI realm namespace piggybacks on the administration of the DNS namespace.

NAI realm names are required to be unique and the rights to use a given NAI realm for roaming purposes are obtained coincident with acquiring the rights to use a particular fully qualified domain name (FQDN). Those wishing to use an NAI realm name should first acquire the rights to use the corresponding FQDN. Using an NAI realm without ownership of the corresponding FQDN creates the possibility of conflict and therefore is to be discouraged.

Note that the use of an FQDN as the realm name does not imply use of the DNS for location of the authentication server or for authentication routing. Since to date roaming has been implemented on a relatively small scale, existing implementations typically handle location of authentication servers within a domain and perform authentication routing based on local knowledge expressed in proxy configuration files. The implementations described in [8] have not found a need for use of DNS for location of the authentication server within a domain, although this can be accomplished via use of the DNS SRV record, described in [2]. Similarly, existing implementations have not found a need for dynamic routing protocols, or propagation of global routing information. Note also that there is no requirement that the NAI represent a valid email address.

Normative References

[1] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[2] Gulbrandsen, A. and P. Vixie, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2052, October 1996.

[3] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[4] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997.

[5] Faltstrom, P., Hoffman, P. and A. Costello, "Internationalizing Domain Names in Applications (IDNA)", RFC 3490, March 2003.

[6] Zeilenga, K., "SASLprep: Stringprep profile for user names and passwords", draft-ietf-sasl-saslprep-04 (work in progress), October 2003.

Informative References

[7] Postel, J., "Simple Mail Transfer Protocol", STD 10, RFC 821, August 1982.

[8] Aboba, B., Lu, J., Alsop, J., Ding, J. and W. Wang, "Review of Roaming Implementations", RFC 2194, September 1997.

[9] Aboba, B. and M. Beadles, "The Network Access Identifier", RFC 2486, January 1999.

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

[11] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

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

[13] Calhoun, P., Loughney, J., Guttman, E., Zorn, G. and J. Arkko,

"Diameter Base Protocol", RFC 3588, September 2003.

[14] Arkko, J. and B. Aboba, "Network Discovery and Selection within the EAP Framework", draft-ietf-eap-netsel-problem-00 (work in progress), January 2004.

[15] Adrangi, F., "Network Discovery and Selection within the EAP Framework", draft-adrangi-eap-network-discovery-and-selection-00 (work in progress), October 2003.

Authors' Addresses

Bernard Aboba
Microsoft
One Microsoft Way
Redmond, WA 98052
USA

EMail: aboba@internaut.com

Mark A. Beadles
WorldCom Advanced Networks
5000 Britton Rd.
Hilliard, OH 43026
USA

EMail: mbeadles@wcom.net

Jari Arkko
Ericsson

Jorvas 02420
Finland

EMail: jari.arkko@ericsson.com

Pasi Eronen
Nokia Research Center
P.O. Box 407
FIN-00045 Nokia Group
Finland

EMail: pasi.eronen@nokia.com

Appendix A. Changes from RFC 2486

This draft contains the following updates with respect to the original NAI definition in RFC 2486:

- International character set support has been added for both usernames and realms.

- Username privacy support has been added.

- A requirement to support NAI length of at least 253 octets has been added, and compatibility considerations among NAI lengths in this specification and various AAA protocols are discussed.

- The mediating network syntax and its implications have been fully described and not given only as an example. Note that this syntax is not intended to be a full solution to network discovery and selection needs as defined in [14]. Rather, it is intended as a clarification of RFC 2486. It could also be used as a component in approaches such as [15].

- The realm BNF entry definition has been changed to avoid an error (infinite recursion) in the original specification.

- The x and special BNF entries have been clarified.

Appendix B. Acknowledgements

Thanks to Glen Zorn for many useful discussions of this problem space, and for Farid Adrangi and others for suggesting mediating network representation in NAIs. Jonathan Rosenberg reported the BNF error. Dale Worley suggested clarifications of the x and special BNF entries. Arne Norefors reported the length differences between RFC 2486 and RFC 2865.

Intellectual Property Statement

Full Copyright Statement

Acknowledgement

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