

## The Roaming Relationship (REL) Resource Record in the DNS

### [1.](#) Status of this Memo

This document is an Internet-Draft. 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.''

To learn the current status of any Internet-Draft, please check the ``[1id-abstracts.txt](#)'' listing contained in the Internet-Drafts Shadow Directories on [ds.internic.net](#) (US East Coast), [nic.nordu.net](#) (Europe), [ftp.isi.edu](#) (US West Coast), or [munnari.oz.au](#) (Pacific Rim).

The distribution of this memo is unlimited. It is filed as <[draft-ietf-roamops-dnsrr-03.txt](#)>, and expires September 15, 1997. Please send comments to the authors.

### [2.](#) Abstract

This document describes the use of the Roaming Relationship (REL) record in the DNS for the description of roaming relationships. REL resource records may be used for determining the existence of a roaming relationship path between the local ISP and the user's home domain, as well as the location of an appropriate accounting agent. However, unless the roaming relationship path is authenticated by some method (such as via tokens or certificates returned by the home authentication server), hierarchical authentication routing must be used in order to validate the path.

### [3.](#) Introduction

Considerable interest has arisen recently in a set of features that fit within the general category of "roaming capability" for dialup Internet users. 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.

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, or L2TP.

This document describes the use of the Roaming Relationship (REL) record in the DNS for the description of roaming relationships. REL resource records may be used for determining the existence of a roaming relationship path between the local ISP and the user's home domain, as well as the location of an appropriate accounting agent. However, unless the roaming relationship path is authenticated by some method (such as via tokens or certificates returned by the home authentication server), hierarchical authentication routing must be used in order to validate the path.

### [3.1.](#) Terminology

This document frequently uses the following terms:

#### roaming relationship path

The roaming relationship path is the series of roaming relationships that link together a local ISP and user's home domain. The roaming relationship path may or may not be the same as the authentication route, depending on whether the local proxy is able to directly contact the home authentication server.

#### authentication route

The route that an authentication will take in traveling between the local ISP's authentication proxy and the home authentication server. Where RADIUS proxy authentication is

used, the authentication route follows the roaming relationship path.

#### Network Access Server

The Network Access Server (NAS) is the device that clients dial in order to get access to the network.

#### RADIUS server

This is a server which provides for authentication/authorization via the protocol described in [3], and for accounting as described in [4].

#### RADIUS proxy

In order to provide for the routing of RADIUS authentication and accounting requests, a RADIUS proxy may be employed. To the NAS, the RADIUS proxy appears to act as a RADIUS server, and to the RADIUS server, the proxy appears to act as a RADIUS

client.

#### RADIUS domain

In order to provide for the routing of RADIUS authentication and accounting requests, the userID field used in PPP and in the subsequent RADIUS authentication and accounting requests, may contain structure. This structure provides a means by which the RADIUS proxy will locate the RADIUS server that is to receive the request.

### [3.2.](#) Requirements language

This specification uses the same words as [14] for defining the significance of each particular requirement. These words are:

**MUST** This word, or the adjectives "REQUIRED" or "SHALL", means that the definition is an absolute requirement of the specification.

**MUST NOT** This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.

SHOULD This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

SHOULD NOT

This phrase means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

MAY

This word, or the adjective "OPTIONAL", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option.(except, of course, for the feature the option provides)

An implementation is not compliant if it fails to satisfy one or more of the must or must not requirements for the protocols it implements. An implementation that satisfies all the must, must not, should and should not requirements for its protocols is said to be

"unconditionally compliant"; one that satisfies all the must and must not requirements but not all the should or should not requirements for its protocols is said to be "conditionally compliant."

#### [4.](#) The Roaming Relationship (REL) Record

In order to enable roaming, it is necessary for a local provider to be able to determine whether a roaming relationship path exists between itself and the user's home domain, so as to enable the local provider to be paid for the use of its resources. These roaming relationships

are typically of two types: the relationship between a firm and a provider, in which the firm delegates roaming authority to the provider; or the relationship between a provider and a roaming association, in which the provider agrees to allow members of the consortium to access its network resources, in exchange for compensation. However, it is also possible for a company or even an individual to form a direct relationship with a roaming consortia, or for consortia to form a relationship with another consortia.

Inter-domain roaming relationships may extend to several levels. For example, BIGCO may delegate roaming authority to ISPA, who may in turn join roaming association ISPGROUP. When Fred dials into ISPB and attempts to authenticate as fred@bigco.com, it is necessary for ISPB to determine whether it has a means for being paid for the resources consumed by Fred. This is accomplished by tracing the web of roaming relationships backwards from the bigco.com domain, in order to determine whether a path of roaming relationships exists between ISPB and BIGCO.

Please note that the task of determining the path of roaming relationships is orthogonal to the issue of authentication routing. Where authentication proxy chaining is used, authentication routing is required in order to improve scalability. However, when public key authentication is available, it is possible for an authentication proxy to directly contact a home authentication server. However, regardless of how the authentication is routed, it is still necessary for the local ISP to determine the path of roaming relationships so that it can determine whether it can be paid for the transaction.

The purpose of the Roaming Relationship (REL) resource record is to document inter-domain roaming relationships. When hierarchical authentication routing is being used, REL resource records are typically retrieved by the local ISP's authentication proxy, and used both for determination of the roaming relationship path as well as for use in authentication routing. If public key authentication technology is available, it may be possible for the local ISP's authentication proxy to contact the home domain's authentication server directly. In this case, hierarchical authentication routing will not be required, and the home authentication server may return tokens or certificates in order to validate the roaming relationship path. If this is done, then the local ISP's authentication proxy may not need to look up any REL resource records itself, and as a result, the total time required for the authentication will be decreased. This will lessen the probability

of a timeout.

#### [4.1.](#) REL resource record RDATA format

The RDATA for a REL resource record is as follows:

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                               Preference                               |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
/                                                                                               /
/                                                                                               /
/                                                                                               /
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

##### [4.1.1.](#) Preference

The Preference field, which is two octets, specifies the preference given to this record versus other records of the same type and owner. Lower values are preferred.

##### [4.1.2.](#) Flags

The flags field, which is two octets, is as follows:

```

0                               1
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|U P C A I F H R R R R R R R R R|
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

U = User. If U=1, then the REL resource record represents an individual user or account. The user name is represented the same way as in the SOA or RP resource records. As a result, fred@bigco.com will be represented as fred.bigco.com. Since the DNS was not intended for use as a user database, it is expected that this flag will only be set on rare occasions.

P = Provider. If P=1, then the REL resource record represents delegation of roaming authority from a non-ISP to an ISP or a roaming consortia.

C = Consortia. If C=1, then the REL resource record represents delegation of roaming authority from an ISP to a roaming consortia.

A = Accounting agent. If A=1, then a accounting agent exists within

the domain.

I = Internet access. If I=1, then the REL resource record may be used for provisioning of Internet access. In roaming applications this bit MUST be set.

Aboba

[Page 5]

---

INTERNET-DRAFT

7 March 1997

F = Fax. If F=1, then the REL resource record may be used for provisioning of Internet fax.

H = H.323. If H=1, then the REL resource record may be used for provisioning of H.323 conferencing.

R = Reserved.

#### [4.1.3.](#) Domain

The domain field represents the domain name to which roaming authority has been delegated by the owner name.

#### [4.2.](#) Use of the Roaming Relationship (REL) Resource Record

The Roaming Relationship (REL) resource record uses semantics similar to that of the Mail Exchange (MX) record, in that it includes a priority as well as the domain to which roaming authority has been delegated. The REL resource record is of the form:

```
bigco.com.  IN REL 10 (; priority
                ispa.com.  ;domain with roaming authority
                P I        ;flags. P = Provider, I = Internet Access
                )
```

Here 10 refers to the priority of the REL resource record, and ispa.com is the domain to which BIGCO has delegated roaming responsibilities. The use of a priority field allows multiple relationships to be represented, with authenticating ISPs checking the relationships in ascending order of priority. Thus, an REL resource record of priority [10](#) would be checked before a REL resource record of priority 20. As described in the previous section, letters are used to denote flag bits.

Routes for a given domain SHOULD be given different priorities, so as to allow for predictable behavior. Since routes at the same priority will be round-robin, this will result in alternation of routes. Unless there is a good reason for balancing the load this way, this approach SHOULD NOT be used.

## [5.](#) Examples

### [5.1.](#) Example One

Let us assume that Fred is an employee of BIGCO, who has established roaming relationships with ISPA and ISPC, both of which are members of roaming consortia ISPGROUP1. BIGCO also has a relationship with clearing houses ISPGROUP2 and ISPGROUP3. ISPB is a member of the ISPGROUP1 roaming consortia.

The REL resource records for BIGCO appear as follows:

```
bigco.com. IN REL 10 ispa.com.      P I
bigco.com. IN REL 20 ispc.com.      P I
bigco.com. IN REL 30 ispgroup3.com. P I
bigco.com. IN REL 40 ispgroup2.com. P I
```

The REL resource records for ISPA, ISPB, ISPC, ISPGROUP1, ISPGROUP2 and ISPGROUP3 appear as follows:

```
ispa.com. IN REL 10 ispgroup1.com.  C I
ispb.com. IN REL 10 ispgroup1.com.  C I
ispc.com. IN REL 10 ispgroup1.com.  C I
ispgroup1.com. IN REL 10 ispgroup1.com. C I A
ispgroup2.com. IN REL 10 ispgroup2.com. C I A
ispgroup3.com. IN REL 10 ispgroup3.com. C I A
```



#### 5.1.1. Sequence of events

Fred logs into ISPB as fred@bigco.com; as a result the ISPB authentication proxy receives this NAI. ISPB's authentication proxy first checks for the presence of a user record for fred.bigco.com. If so, then it retrieves the REL resource records for the domain to whom Fred has delegated roaming authority. If there is no user record, then it checks its configuration files to see whether bigco.com is one of the domains with whom it has a direct roaming relationship. This check will fail since BIGCO has no direct roaming relationship with ISPB. As a result, ISPB's authentication proxy will need to retrieve REL resource records either from its own cache or from the bigco.com zone.

Assuming that ISPB's authentication proxy does not support public key authentication, then hierarchical authentication routing will be used. In this case, ISPB's authentication proxy will need to retrieve REL resource records from the bigco.com zone. If ISPB's authentication proxy supports public key authentication and ISPEC, then rather than immediately retrieving REL resource records, it will retrieve the SRV, KEY and SIG resource records for the bigco.com zone. Using the SRV resource record, ISPB's authentication proxy can locate the authentication proxy for the bigco.com domain. The SIG resource records for the bigco.com zone can then be retrieved in order to determine whether the bigco.com authentication server supports public key authentication. If so, then ISPB's authentication proxy may contact the bigco.com authentication server directly. In its authentication reply, the bigco.com authentication server may return the REL resource records for its zone as well as those of the zones to which it has delegated roaming authority, in the form of attributes within the Access-Reply. If so, then ISPB's authentication proxy will be saved the work of having to retrieve these resource records itself prior to

forwarding the authentication reply on to the NAS.

Once the REL resource records have been retrieved by one mechanism or another, a depth first search is performed in order to select the roaming relationship path. In this case, ISPB determines whether it has a direct roaming relationship with ISPA (priority 10 record from the bigco.com zone). If not, then it looks at the REL resource records for the ispa.com domain, and determines whether it has a direct roaming relationship with any of the domains to whom ISPA has delegated roaming responsibility. In this case, ISPB determines that it has a

direct roaming relationship with ISPGROUP1 (priority 10 record from the ispa.com zone). As a result, the roaming relationship path bigco.com/ispa.com/ispgroup1.com/ispb.com is selected. Since ISPGROUP1 operates an accounting agent within its domain, accounting records for the transaction will be sent to ISPGROUP1's accounting agent.

If ISPA had not been a member of the ISPGROUP1 roaming consortia, then the depth-first search would have terminated, and ISPB would proceed to check for a business relationship on the branch represented by the priority 20 REL resource record in the bigco.com zone (ispc.com). In this case the roaming relationship path bigco.com/ispc.com/ispgroup1.com/ispb.com would have been selected.

If ISPB were a member of the ISPGROUP3 roaming consortia, and not a member of the ISPGROUP1 or ISPGROUP2 consortia, then the breadth-first search would fail on both the priority 10 and 20 branches of the bigco.com tree. In this case, the business relationship path bigco.com/ispgroup3.com/ispb.com would have been selected.

## 5.2. Example Two

Let us assume that BIGCO has branch offices in multiple locations. The BIGCO branch office in Illinois has a contract with ISPA, which is a member of ISPGROUP1. However, ISPGROUP1 does not have coverage in Israel. As a result, the branch office in Israel has a contract with ISPC, which is a member of ISPGROUP2, which does have coverage in Israel. It is desired that Fred be able to login either from Illinois or from Israel, with the authentication being done by the appropriate ISP. When logging in from Illinois, Fred uses the POPs of ISPB, while in Israel, he uses the POPs of ISPD. It should be noted that ISPA and ISPC can be located anywhere; they need not necessarily reside in Illinois or Israel.

In this case, the REL records for BIGCO will appear as follows:

```
bigco.com. IN REL 10 ispa.com.          P I
bigco.com. IN REL 20 ispc.com.          P I
```

The records for ISPA, ISPB, ISPC, ISPD, ISPGROUP1 and ISPGROUP2 appear as follows:

```
ispa.com.  IN REL 10 ispgroup1.com.      C I
```

```
ispb.com.  IN REL 10 ispgroup1.com.      C I
ispc.com.  IN REL 10 ispgroup2.com.      C I
ispd.com.  IN REL 10 ispgroup2.com.      C I
ispgroup1.com.  IN REL 10 ispgroup1.com.  C I A
ispgroup2.com.  IN REL 10 ispgroup2.com.  C I A
```

#### 5.2.1. Sequence of events

While in the United States, Fred logs into ISPB as fred@bigco.com; as a result the ISPB authentication proxy receives this NAI. ISPB's authentication proxy first checks for the presence of a user record for fred.bigco.com. If so, then it retrieves the REL resource records for the domain to whom Fred has delegated roaming authority. If there is no user record, then it checks its configuration files to see whether bigco.com is one of the domains with whom it has a direct roaming relationship. This check will fail since BIGCO has no direct roaming relationship with ISPB. As a result, ISPB's authentication proxy will need to retrieve resource records either from its own cache or from the bigco.com zone.

Once the REL resource records have been retrieved by one mechanism or another, a depth first search is performed in order to select the roaming relationship path. In this case, ISPB determines whether it has a direct roaming relationship with ISPA (priority 10 record from the bigco.com zone). If not, then it looks at the REL resource records for the ispa.com domain, and determines whether it has a direct roaming relationship with any of the domains to whom ISPA has delegated roaming responsibility. In this case, ISPB determines that it has a direct roaming relationship with ISPGROUP1 (priority 10 record from the ispa.com zone). As a result, the roaming relationship path bigco.com/ispa.com/ispgroup1.com/ispb.com is selected. Since ISPGROUP1 operates a accounting agent within its domain, accounting records for the transaction will be sent to ISPGROUP1's accounting agent.

While in Israel, Fred logs into ISPD as fred@bigco.com; as a result, the ISPD authentication proxy receives this NAI. ISPD's authentication proxy then checks its configuration files to see whether bigco.com is one of the domains with whom it has a direct roaming relationship. This check will fail since BIGCO has no direct roaming relationship with ISPD. As a result, ISPD's authentication proxy will need to retrieve REL resource records either from its own cache or from the bigco.com zone.

Once the REL resource records have been retrieved by one mechanism or another, a depth first search is performed in order to select the roaming relationship path. In this case, ISPD determines whether it has a direct roaming relationship with ISPA (priority 10 record from the bigco.com zone). If not, then it looks at the REL resource records for the ispa.com domain, and determines whether it has a direct

---

INTERNET-DRAFT

7 March 1997

roaming relationship with any of the domains to whom ISPA has delegated roaming responsibility. In this case, ISPD determines that no roaming relationship path exists passing through ISPA.

As a result, ISPD checks for a roaming relationship path on the ISPC branch (priority 20 REL resource record from the bigco.com zone). First, it determines whether there is a direct roaming relationship between ISPD and ISPC (there is not). Then it looks at the REL records for the ispc.com domain, and determines whether it has a direct roaming relationship with any of the domains to whom ISPC has delegated roaming responsibility. In this case, ISPD determines that it has a direct roaming relationship with ISPGROUP2 (priority 10 REL resource record from the ispc.com zone). As a result, the roaming relationship path bigco.com/ispc.com/ispgroup2.com/ispd.com is selected. Since ISPGROUP2 operates an accounting agent within its domain, accounting records for the transaction will be sent to ISPGROUP2's accounting agent.

### [5.3.](#) Example Three

Let us assume that Fred wishes to travel to a country which is not served by the roaming consortia that BIGCO's provider ISPA has joined. In this case, Fred will wish to make use of the user REL resource record.

In this case, the REL resource records for BIGCO will appear as follows:

```
bigco.com.      IN REL 10 ispa.com.    P I
fred.bigco.com. IN REL 10 ispe.com.    U I
```

The records for ISPA, ISPB, ISPD, ISPGROUP1 and ISPGROUP2 appear as

follows:

```
ispa.com.  IN REL 10 ispgroup1.com.      C I
ispb.com.  IN REL 10 ispgroup1.com.      C I
ispb.com.  IN REL 10 ispgroup2.com.      C I

ispe.com.  IN REL 10 ispgroup2.com.      C I

ispgroup1.com.  IN REL 10 ispgroup1.com.  C I A
ispgroup2.com.  IN REL 10 ispgroup2.com.  C I A
```

#### [5.3.1.](#) Sequence of events

While traveling, Fred logs into ISPB as fred@bigco.com; as a result the ISPB authentication proxy receives this NAI. ISPB's authentication proxy first checks for the presence of a user record for fred.bigco.com. If so, then it retrieves the REL resource records for

the domain to whom Fred has delegated roaming authority. In this case, a user record exists for fred@bigco.com, so that the authentication proxy determines whether it has a direct roaming relationship with ISPE (priority 10 REL resource record from the fred.bigco.com zone). If not, then it looks at the REL resource records for the ispe.com domain, and determines whether it has a direct roaming relationship with any of the domains to whom ISPE has delegated roaming responsibility. In this case, ISPB determines that it has a direct roaming relationship with ISPGR0UP2 (priority 10 REL resource record from the ispe.com zone). As a result, the roaming relationship path fred.bigco.com/ispe.com/ispgroup2.com/ispb.com is selected. Since ISPGR0UP2 operates a accounting agent within its domain, accounting records for the transaction will be sent to ISPGR0UP2's accounting agent.

Please note that even though Fred has a user REL resource record, the authentication conversation will still be conducted between ISPB's authentication proxy and BIGCO's authentication server.

## [6.](#) Prevention of looping topologies

Since it is possible to create looping topologies using REL resource records, a mechanism must be provided to prevent endless loops. As a result, it is recommended that authentication proxies be configured with a default maximum of four hops. This would support the scenario of an authentication passing from a NAS to an authentication proxy, from the proxy to ISPGROUP, from ISPGROUP to ISPA, and from ISPA to BIGCO.

## 7. Use of the REL RR

When REL resource records are utilized, no assurance can be provided as to the authenticity of the roaming relationships represented by these records. As a result, it is necessary to verify the validity of the roaming relationship path by another means. This can be accomplished by causing the authentication to be routed along the roaming relationship path, or by verifying the authenticity of a certificate or token returned by the home authentication server.

As an example, let us assume that the roaming relationship path bigco.com/ispc.com/ispgroup2.com/ispd.com is selected. If this path has not been authenticated, then ISPD's authentication proxy will forward it's authentication request to ISPGROUP2, including the roaming relationship path as a source route. ISPGROUP2 will then in turn forward the authentication to ISPC, who will forward it to BIGCO. At each step of the way, a pre-existing relationship will need to exist between hops in order for this authentication forwarding to proceed. As a result, the act of authenticating Fred via the roaming relationship path acts to validate the roaming relationship as determined from the REL resource records.

Note that such hop by hop forwarding may be required even if public key authentication is available for use between the local ISP's authentication proxy and the home authentication server. As long as the roaming relationship path has not been authenticated, the local ISP will still need to validate the roaming relationship path. This can be accomplished by forcing the authentication to follow the roaming relationship path, validating the relationships between the proxies at each hop.

Please also note that public key authentication will also typically be used in order to enable signed receipts to be returned by the accounting agent in response to receipt of digitally signed accounting record bundles. DNS security can assist in determining what security features are implemented at a given home authentication server or accounting agent. Accounting agent support for MIME Security Multiparts is indicated via use of the Email bit within the KEY resource record flag field. DNS security may also be used to indicate that a home authentication server supports IPSEC. This is indicated via use of the IPSEC bit within the KEY resource record flag field.

## 8. Acknowledgements

Thanks to Glen Zorn of Microsoft, Pat Calhoun of USR, and Michael Robinson of Global One for many useful discussions of this problem space.

## 9. References

- [1] B. Aboba, J. Lu, J. Alsop, J. Ding. "Review of Roaming Implementations." [draft-ietf-roamops-imprev-01.txt](#), Microsoft, Aimnet, i-Pass Alliance, Asiainfo, January, 1997.
- [2] B. Aboba, G. Zorn. "Dialing Roaming Requirements." [draft-ietf-roamops-roamreq-02.txt](#), Microsoft, January, 1997.
- [3] C. Rigney, A. Rubens, W. Simpson, S. Willens. "Remote Authentication Dial In User Service (RADIUS)." [RFC 2058](#), Livingston, Merit, Daydreamer, January, 1997.
- [4] C. Rigney. "RADIUS Accounting." [RFC 2059](#), Livingston, January, 1997.
- [5] R. Fajman. "An Extensible Message Format for Message Disposition Notifications." [draft-ietf-receipt-mdn-02.txt](#), National Institute of Health, November, 1996.
- [6] M. Elkins. "MIME Security with Pretty Good Privacy (PGP)." RFC 2015, The Aerospace Corporation, October, 1996.
- [7] G. Vaudreuil. "The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages." [RFC 1892](#), Octel Network Services, January, 1996.

- [8] J. Galvin., et al. "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted." [RFC 1847](#), Trusted Information Systems, October, 1995.
- [9] D. Crocker. "MIME Encapsulation of EDI Objects." RFC 1767, Brandenburg Consulting, March, 1995.
- [10] M. Jansson, C. Shih, N. Turaj, R. Drummond. "MIME-based Secure EDI." [draft-ietf-ediint-as1-02.txt](#), LiNK, Actra, Mitre Corp, Drummond Group, November, 1996.
- [11] C. Shih, M. Jansson, R. Drummond, L. Yarbrough. "Requirements for Inter-operable Internet EDI." [draft-ietf-ediint-req-01.txt](#), Actra, LiNK, Drummond Group, May, 1995.
- [12] A. Gulbrandsen, P. Vixie. "A DNS RR for specifying the location of services (DNS SRV)." [RFC 2052](#), Troll Technologies, Vixie Enterprises, October 1996.
- [13] D. Eastlake, 3rd, C. W. Kaufman. "Domain Name System Security Extensions." [Draft-ietf-dnnsec-secext-10.txt](#), CyberCash, Iris, August, 1996.
- [14] S. Bradner. "Key words for use in RFCs to Indicate Requirement Levels." [draft-bradner-key-words-02.txt](#), Harvard University, August, 1996.
- [15] C. Malmud, M. Rose. "Principles of Operation for the TPC.INT Subdomain: General Principles and Policy." [RFC 1530](#), Internet Multicasting Service, Dover Beach Consulting, Inc., October, 1993.

## [10.](#) Authors' Addresses

Bernard Aboba  
Microsoft Corporation  
One Microsoft Way  
Redmond, WA 98052

Phone: 206-936-6605  
EMail: [bernarda@microsoft.com](mailto:bernarda@microsoft.com)



