Network Working Group
Internet-Draft
Expires: August 13, 2003

R. Sparks
dynamicsoft

February 12, 2003

The SIP Referred-By Mechanism
draft-ietf-sip-referredby-01

Status of this Memo

Copyright Notice

Abstract

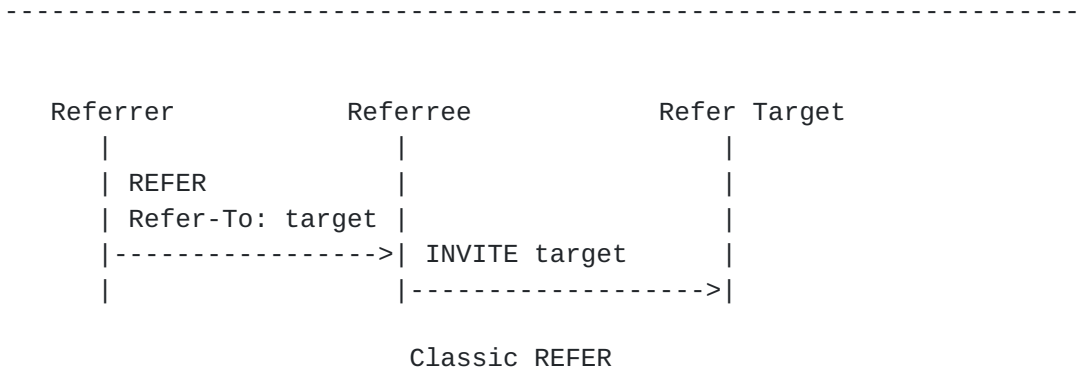
The SIP REFER method [2] provides a mechanism where one party (the referrer) gives a second party (the referree) an arbitrary URI to reference. If that URI is a SIP URI, the referree will send a SIP request, often an INVITE, to that URI (the refer target). This document extends the REFER method allowing the referrer to provide information about the reference to the refer target using the referree as an intermediary. This information includes the identity of the referrer and the URI to which the referrer referred. The mechanism utilizes S/MIME to help protect this information from a malicious intermediary. This protection is optional, but a recipient may refuse to accept a request unless it is present.

Table of Contents

1. Overview 3
2. The Referred-By Mechanism 4
2.1 Referrer behavior 4
2.2 Referree behavior 5
2.3 Refer Target behavior 5
3. The Referred-By Header Field 6
4. The Referred-By Token 7
4.1 Refer target inspection of a Referred-By token 7
5. The 429 Provide Referrer Identity error response 8
6. Security Considerations 8
7. Examples 10
7.1 Basic REFER 10
7.2 Insecure REFER 13
7.3 Requiring Referrer Identity 13
7.4 Nested REFER 17
8. IANA Considerations 21
9. Open Issues 22
10. Changes from -00 22
Normative References 23
Informative References 23
Author's Address 23
Full Copyright Statement 24

1. Overview

The SIP REFER method [2] provides a mechanism where one party (the referrer) provides a second party (the referree) with an arbitrary URI to reference. If that URI is a SIP URI, the referree will send a SIP request, often an INVITE, to that URI (the refer target). Nothing provided in [2] distinguishes this referenced request from any other request the referree might have sent to the refer target.



Classic REFER

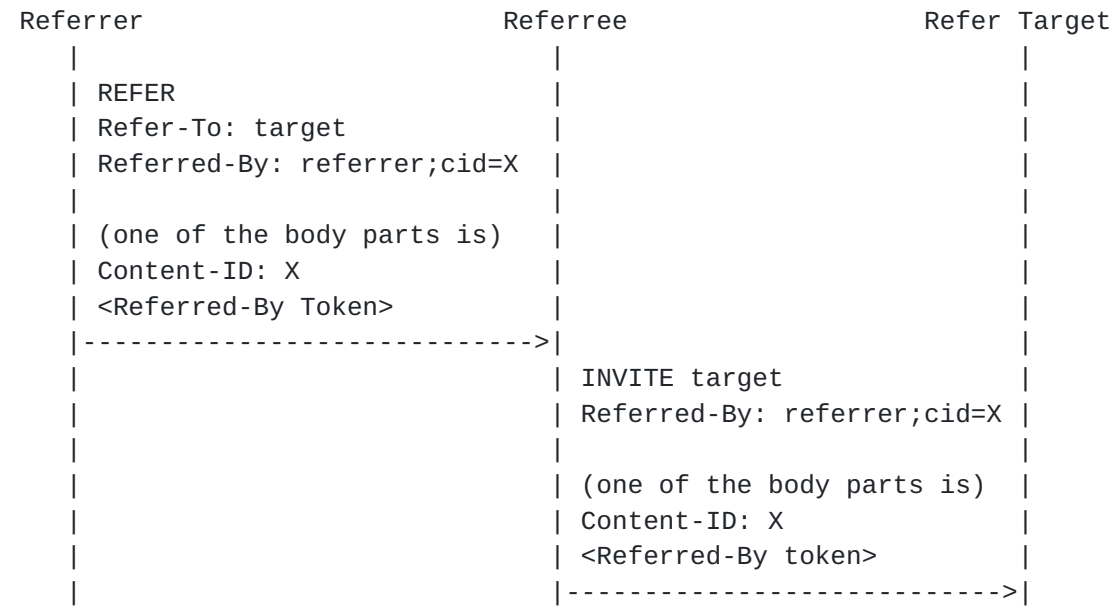
There are applications of REFER, such as call transfer [7], where it is desirable to provide the refer target with certain information about the referrer and the REFER request itself. This information may include, but is not limited to, the referrer's identity, the referred to URI, and the time of the referral. The refer target can use this information when deciding whether to admit the referenced request. This draft defines one set of mechanisms to provide that information.

All of the mechanisms in this draft involve placing information in the REFER request that the referee copies into the referenced request. This necessarily establishes the referee as an eavesdropper and places the referree in a position to launch man-in-the-middle attacks on that information.

At the simplest level, this draft defines a mechanism for carrying the referrer's identity, expressed as a SIP URI in a new header: Referred-By. The refer target can use that information, even if it has not been protected from the referree, at the perils and with the limitations documented here. The draft proceeds to define an S/MIME based mechanism for expressing the identity of the referrer and capturing other information about the REFER request, allowing the refer target to detect tampering (and other undesirable behaviors) by the referree.

2. The Referred-By Mechanism

The following figure summarizes how Referred-By information is carried to the Refer Target. The Referrer provides a Referred-By header with its SIP address-of-record, optionally associating an S/MIME protected token reflecting the identity of the referrer and details of the REFER request. The Referree copies this header and the token, if provided, into the triggered request (shown here as an INVITE).



REFER with Referred-By

2.1 Referrer behavior

A UA sending a REFER request (a referrer) MAY provide a Referred-By header field value in the request. A REFER request MUST NOT contain more than one Referred-By header field value.

A referrer MAY include a Referred-By token in a REFER request. A REFER request containing a Referred-By token MUST contain a Referred-By header field value with a cid parameter value equal to the Content-ID of the body part containing the token.

The referrer will receive a NOTIFY with a sipfrag indicating a final

response of 429 "Provide Referrer Identity" to the referenced request if the refer target requires a valid Referred-By token to accept the request. The can occur when either no token is provided or a provided token is invalid.

The referrer will receive a 429 "Provide Referrer Identity" response to the REFER if the referee requires a Referred-By token to be present in order to accept the REFER.

2.2 Referree behavior

A UA receiving a REFER request (a referree) to a SIP URI (using either the sip: or sips: scheme) MUST copy any Referred-By header field value and token into the referenced request without modification.

A referree MAY reject a REFER request that does not contain a Referred-By token with a 429 "Provide Referrer Identity" response. A referree SHOULD NOT reject a request that contains a Referred-By token encrypted to a key it does not possess. Note that per [5] the referee should still be able to verify the signature of such an encrypted token.

2.3 Refer Target behavior

A UA receiving a non-REFER SIP request MAY inspect the request for a Referred-By header field and token.

If a Referred-By header field value is not present, this UA can not distinguish this request from any other the UA acting as the referree might have sent. Thus, the UA would apply exactly the admissions policies and processing described in [1] to the request.

If a Referred-By header field value is present, the receiving UA can consider itself a refer target and MAY apply additional admission policies based on the contents of the Referred-By header field and token.

The referee is in a position to modify the contents of the Referred-By header field value, or falsely provide one even if no REFER actually exists. If such behavior could affect admission policy (including influencing the agent's user by rendering misleading content), the refer target SHOULD require that a valid Referred-By token be present.

The refer target MAY reject a request if no Referred-By token is present or if the token is stale using the 429 "Provide Referrer Identity" error response defined in Section 5. The 428 error

response from [4] is not appropriate for this purpose - it is needed for the refer target to request an authentication token from the referee.

If no Referred-By token is present, the refer target MAY proceed with processing the request. If the agent provides any information from the Referred-By header to its user as part of processing the request, it MUST notify the user that the information is suspect.

The refer target MUST reject an otherwise well-formed request with an invalid Referred-By token (see Section 4) with a 429 error response.

3. The Referred-By Header Field

Referred-By is a request header field as defined by [1]. It can appear in any request. It carries a SIP URI representing the identity of the referrer and, optionally, the Content-ID of a body part (the Referred-By token) that provides a more secure statement of that identity.

```
Referred-By  =  ("Referred-By" / "b") HCOLON referrer-uri
                *( SEMI (referredby-id-param / generic-param) )

referrer-uri = ( name-addr / addr-spec )

referredby-id-param = "cid" EQUAL msg-id

msg-id = TO BE INCORPORATED from rfc2822 (at great pain)
```

Referred-By Syntax

The Referred-By header field MAY appear in any SIP request, but is meaningless for ACK and CANCEL. Proxies do not need to be able to read Referred-By header field values and MUST NOT remove or modify them.

The following row should be interpreted as if it appeared in Table 3 of RFC 3261.

Header field	where	proxy	ACK	BYE	CAN	INV	OPT	REG
Referred-By	R	-	o	-	o	o	o	

4. The Referred-By Token

The Referred-By token is an Authenticated Identity Body as defined by [5]. This body part MUST be identified with a MIME [6] Content-ID: field.

In addition to the From, Date, and Call-ID header fields required by [5], the sipfrag inside a Referred-By token MUST contain copies of the Refer-To and Referred-By header fields from the REFER request. As in [5] additional header fields and body parts MAY be included.

> OPEN ISSUE: The Call-ID header from the referrer will not be useful to the refer target. It can even be argued that including it leaks information to the refer target that it should not get to see. Should we require that this field be populated with a minimal, meaningless constant value?

As described in [5], a Referred-By token MAY be encrypted as well as signed.

4.1 Refer target inspection of a Referred-By token

> (Editor's note: This section is new, replacing and modifying text that was removed from sip-identity. Please review it carefully.)

A refer target MUST treat a Referred-By token with an invalid signature as an invalid token. A target SHOULD treat a token with an aged Date header field value as invalid.

A target SHOULD verify that the request it receives matches the reference in the Refer-To header field in the token. Note that the URI in that header field may not match the request URI in the received request due to request retargetting between the referree and the refer target.

The target SHOULD verify that the identity in the From header field in the token exactly matches the SubjectAltName from the signing certificate.

> OPEN ISSUE: [5] suggests this check with a non-normative "should". Can we expect a referrer to always have a certificate that matches whatever From header field value it happened to be using in the middle of a call? Is From even the right field to be looking at?

The referrer may need to provide a different identity to the refer target than it provides to the referee. Should we be basing this on the Referred-By header field instead? If no, then we should remove Referred-By from the token. If yes, is there any value in including real information in the From field, or should we recommend using a minimal, meaningless constant value.

OPEN ISSUE: Can the target make any meaningful use of the To header field in the token? This value could quite reasonably have no relation to the identity that the referree presents to the refer target. Is it appropriate to restrict the referree to reuse the To value from the original dialog (helpdesk@example.com perhaps) as the From in the referenced request? Or do we need a way for the referrer to tell the referree "Use this identity for me in the token you build"? As noted in Section 9, a similar problem may exist in sip-identity and the solution may belong there.

5. The 429 Provide Referrer Identity error response

The 429 client error response code is used by a refer target to indicate that the referree must provide a valid Referred-By token. As discussed in the behavior section, the referree will forward this error response to the referrer in a NOTIFY as the result of the REFER. The suggested text phrase for the 429 error response is "Provide Referrer Identity".

6. Security Considerations

This mechanism defined in this specification relies on an intermediary (the referree) to forward information from the referrer to the refer target. This necessarily establishes the referree as an eavesdropper of that information and positions him perfectly to launch man-in-the-middle attacks using the mechanism.

A SIP proxy is similarly positioned. Protecting SIP messaging from malicious proxy implementations is discussed in [1]. In contrast to a proxy, the referree's agent is an endpoint. Proxies will typically be managed and monitored by service providers. Malicious behavior by a proxy is more likely to be noticed and result in negative repercussions for the provider than malicious behavior by an endpoint would be. The behavior of an endpoint can be entirely under the control of a single user. Thus, it is more feasible for an endpoint acting as referree to behave maliciously than it is for a proxy being operated by a service provider.

This specification uses an S/MIME based mechanism to enable the refer

target to detect manipulation of the Referred-By information by the referree. Use of this protection is optional! The community has asserted that there are systems where trust in the validity of this information is either not important or can be established through other means. Any implementation choosing not to use this optional mechanism needs to provide its own defense to the following risks:

- The Referred-By information is highly likely to influence request admission policy. For instance, it may be displayed to the user of the agent with a "This call was transferred to you by X. Accept?" prompt. A malicious referree can unduly influence that policy decision by providing falsified referred-by information. This includes falsely claiming to have been referred in the first place. (The S/MIME mechanism protects the information with a signature, hampering the referree's ability to inject or modify information without knowing the key used for that signature).

- A referree is by definition an eavesdropper of the referred-by information. Parts of that information may be sensitive. (The S/MIME mechanism allows encryption).

- The referree may store any referred-by information it sees and paste it into future unrelated requests. (The S/MIME mechanism allows detection of stale assertions by covering a timestamp with the signature and allows detection of use in unrelated requests by covering the Refer-To header field with the signature).

The mechanisms in this specification do NOT prevent the referree from deleting ALL referred-by information from the referenced request. A refer target can not detect such deletion. This introduces no new problems since removing all referred-by information from a referenced request transforms it into an ordinary SIP request as described in [1]. Thus the referree gains no new influence over processing logic at the refer target by removing the referred-by information.

Refer targets can protect themselves from the possibility that a malicious referree removed a token (leaving an unsecured identity in the Referred-By header field) by using the 429 error response.

Applications using the mechanisms in this draft may be able to take advantage of pre-existing relationships between the participants to mitigate the risks of its use. In some transfer scenarios, A has the choice of referring B to C or referring C to B. If A and B have a pre-existing trust relationship leading A to have greater confidence that B will not behave maliciously (B is A's administrative assistant for example), referring B to C may make more sense.

This mechanism involves two SIP messages between three endpoints, the

REFER and the referenced request. The content of those messages (including the referred-by information) is subject to the security considerations and protection mechanisms documented in [1].

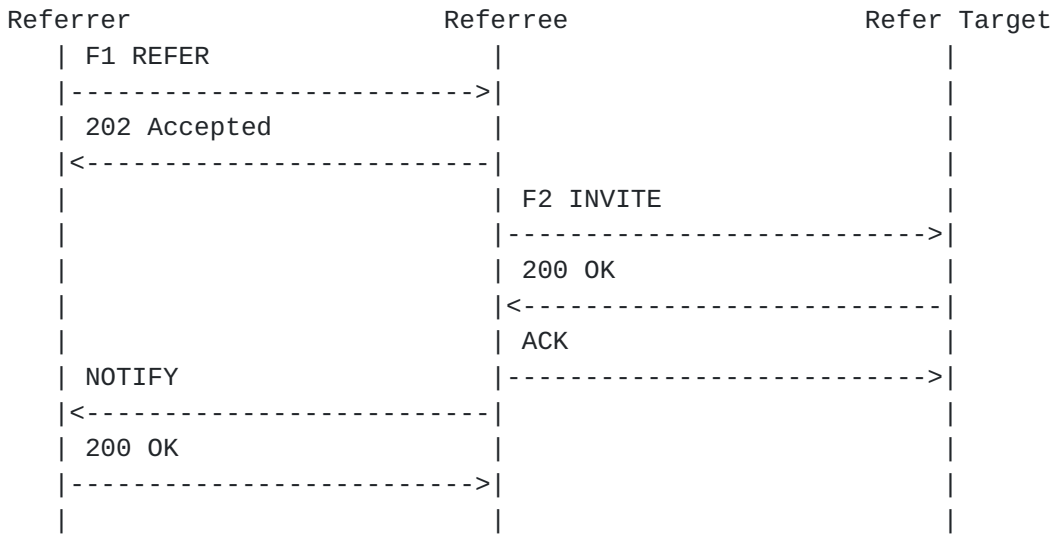
Proxies between the participants may collect referred-by information and reinsert it in future request or make them available to hostile endpoints. The end-to-end confidentiality capabilities discussed in [1] can help reduce risk of exposing sensitive referred-by information to these proxies. The abuse possibilities in subsequent requests by proxies (or endpoints that they may leak information to) between the referree and the refer target are identical to abuse by the referree and the considerations discussed for malicious referree applies. The abuse possibilities in subsequent requests by proxies (or endpoints that they may leak information to) between the referrer and the referree are identical to those discussed for the presentation of Authenticated Identity Bodies in [4].

7. Examples

7.1 Basic REFER

This example shows the secured Referred-By mechanism applied to a REFER to an SIP INVITE URI.

Details are shown only for those messages involved in exercising the mechanism defined in this document.




```
F1 REFER sip:referree@referree.example SIP/2.0
   Via: SIP/2.0/UDP referrer.example;branch=z9hG4bK392039842
   To: sip:referree@referree.example
   From: sip:referror@referror.example;tag=39092342
```

```
      Call-ID: 2203900ef0299349d9209f023a
      CSeq: 1239930 REFER
      Max-Forwards: 70
      Contact: <sip:referrer.example>
      Refer-To: sip:refertarget@target.example
      Referred-By: sip:referror@referror.example
         ;cid=%3C20398823.2UWQFN309shb3@referror.example%3E
      Content-Type: multipart/mixed; boundary=unique-boundary-1
      Content-Length: (appropriate value)

      --unique-boundary-1

      Content-Type: multipart/signed;
        protocol="application/pkcs7-signature";
        micalg=sha1; boundary=dragons39
      Content-ID: <20398823.2UWQFN309shb3@referror.example>
      Content-Length: (appropriate value)

      --dragons39
      Content-Type: message/sipfrag
      Content-Disposition: auth-id; handling=optional

      From: sip:referror@referror.example
      Date: Thu, 21 Feb 2002 13:02:03 GMT
      Call-ID: 2203900ef0299349d9209f023a
      Refer-To: sip:refertarget@target.example
      Referred-By: sip:referror@referror.example
         ;cid=%3C20398823.2UWQFN309shb3@referror.example%3E

      --dragons39
      Content-Type: application/pkcs7-signature; name=smime.p7s
      Content-Transfer-Encoding: base64
      Content-Disposition: attachment; filename=smime.p7s;
         handling=required

      (appropriate signature goes here)

      --dragons39--

      --unique-boundary-1--

   F2 INVITE sip:refertarget@target.example SIP/2.0
      Via: SIP/2.0/UDP referree.example;branch=z9hG4bKffe209934aac
      To: sip:refertarget@target.example
      From: sip:referree@referree.example;tag=2909034023
      Call-ID: fe9023940-a3465@referree.example
      CSeq: 889823409 INVITE
      Max-Forwards: 70
```

```
Contact: <sip:referree@referee.example>
Referred-By: sip:referror@referror.example
   ;cid=%3C20398823.2UWQFN309shb3@referror.example%3E
Content-Type: multipart/mixed; boundary=my-boundary-9
Content-Length: (appropriate value)

--my-boundary-9

Content-Type: application/sdp
Content-Length: (appropriate value)

v=0
o=referree 2890844526 2890844526 IN IP4 referree.example
s=Session SDP
c=IN IP4 referree.example
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000

--my-boundary-9

Content-Type: multipart/signed;
  protocol="application/pkcs7-signature";
  micalg=sha1; boundary=dragons39
Content-ID: <20398823.2UWQFN309shb3@referror.example>
Content-Length: (appropriate value)

--dragons39
Content-Type: message/sipfrag
Content-Disposition: auth-id; handling=optional

From: sip:referror@referror.example
Date: Thu, 21 Feb 2002 13:02:03 GMT
Call-ID: 2203900ef0299349d9209f023a
Refer-To: sip:refertarget@target.example
Referred-By: sip:referror@referror.example
   ;cid=%3C20398823.2UWQFN309shb3@referror.example%3E

--dragons39
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s;
   handling=required

(appropriate signature goes here)

--dragons39--
--my-boundary-9--
```

7.2 Insecure REFER

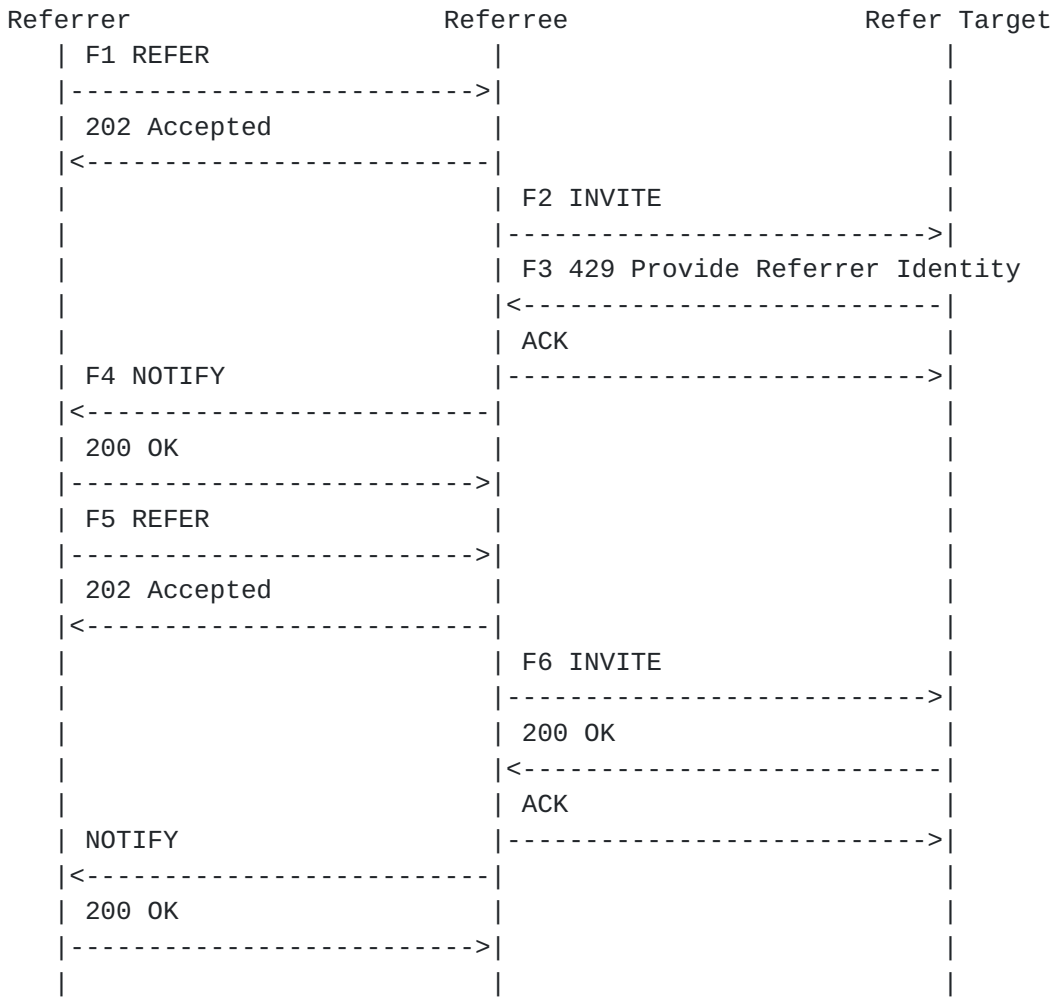
The flow for this example is the same as that of Section 7.1. Here, the referrer has opted to not include a Referred-By token, and the refer target is willing to accept the referenced request without one.

```
 F1 REFER sip:referree@referree.example SIP/2.0
    Via: SIP/2.0/UDP referrer.example;branch=z9hG4bK392039842
    To: sip:referree@referree.example
    From: sip:referror@referror.example;tag=39092342
    Call-ID: 2203900ef0299349d9209f023a
    CSeq: 1239930 REFER
    Max-Forwards: 70
    Contact: <sip:referrer.example>
    Refer-To: sip:refertarget@target.example
    Referred-By: sip:referror@referror.example
    Content-Length: 0

 F2 INVITE sip:refertarget@target.example SIP/2.0
    Via: SIP/2.0/UDP referree.example;branch=z9hG4bKffe209934aac
    To: sip:refertarget@target.example
    From: sip:referree@referree.example;tag=2909034023
    Call-ID: fe9023940-a3465@referree.example
    CSeq: 889823409 INVITE
    Max-Forwards: 70
    Contact: <sip:referree@referee.example>
    Referred-By: sip:referror@referror.example
    Content-Type: application/sdp
    Content-Length: (appropriate value)

    v=0
    o=referree 2890844526 2890844526 IN IP4 referree.example
    s=Session SDP
    c=IN IP4 referree.example
    t=0 0
    m=audio 49172 RTP/AVP 0
    a=rtpmap:0 PCMU/8000
```

7.3 Requiring Referrer Identity

In contrast to the example in Section 7.2, the refer target requires a Referred-By token to accept the referenced request. The referrer choses to provide an encrypted token (note that the block surrounded by asterisks represents encrypted content). F1 and F2 are identical

to the messages detailed in Section 7.2.



F3 SIP/2.0 429 Provide Referrer Identity
Via: SIP/2.0/UDP referree.example;branch=z9hG4bKffe209934aac
To: sip:refertarget@target.example;tag=392093422302334
From: sip:referree@referree.example;tag=2909034023
Call-ID: fe9023940-a3465@referree.example
CSeq: 889823409 INVITE
Content-Length: 0

F4 NOTIFY sip:referror@referror.example SIP/2.0
Via: SIP/2.0/UDP referree.example;branch=z9hG4bK2934209da390
To: sip:referror@referror.example;tag=39092342
From: sip:referree@referree.example;tag=199949923
Call-ID: 2203900ef0299349d9209f023a
CSeq: 3920390 NOTIFY
Event: refer;id=1239930
Subscription-State: terminated

```
      Content-Type: message/sipfrag
      Content-Length: (appropriate value)

      SIP/2.0 429 Provide Referrer Identity

   F5 REFER sip:referree@referree.example SIP/2.0
      Via: SIP/2.0/UDP referrer.example;branch=z9hG4bK98823423
      To: sip:referree@referree.example
      From: sip:referror@referror.example;tag=39092342
      Call-ID: 2203900ef0299349d9209f023a
      CSeq: 1239931 REFER
      Max-Forwards: 70
      Contact: <sip:referrer.example>
      Refer-To: sip:refertarget@target.example
      Referred-By: sip:referror@referror.example
         ;cid=%3C20342EFXEI.390sdefn2@referror.example%3E
      Content-Type: multipart/mixed; boundary=unique-boundary-1
      Content-Length: (appropriate value)

      --unique-boundary-1

      Content-Type: multipart/signed;
        protocol="application/pkcs7-signature";
        micalg=sha1; boundary=boundary42
      Content-ID: <20342EFXEI.390sdefn2@referror.example>
      Content-Length: (appropriate value)

      --boundary42

      Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
        name=smime.p7m
      Content-Transfer-Encoding: base64
      Content-Disposition: attachment; filename=smime.p7m
        handling=required
      Content-Length: (appropriate value)

      ***********************************************************
      * Content-Type: message/sipfrag                           *
      * Content-Disposition: auth-id; handling=optional         *
      *                                                         *
      * From: sip:referror@referror.example                     *
      * Call-ID: 2203900ef0299349d9209f023a                     *
      * Date: Thu, 21 Feb 2002 13:02:03 GMT                     *
      * Refer-To: sip:refertarget@target.example                *
      * Referred-By: sip:referror@referror.example              *
      *    ;cid=%3C20342EFXEI.390sdefn2@referror.example%3E     *
      ***********************************************************
```

```
      --boundary42

      Content-Type: application/pkcs7-signature; name=smime.p7s
      Content-Transfer-Encoding: base64
      Content-Disposition: attachment; filename=smime.p7s;
         handling=required

      (appropriate signature)

      --boundary42--

   F6 INVITE sip:refertarget@target.example SIP/2.0
      Via: SIP/2.0/UDP referree.example;branch=z9hG4bK3920390423
      To: sip:refertarget@target.example
      From: sip:referree@referree.example;tag=1342093482342
      Call-ID: 23499234-9239842993@referree.example
      CSeq: 19309423 INVITE
      Max-Forwards: 70
      Referred-By: sip:referror@referror.example
         ;cid=%3C20342EFXEI.390sdefn2@referror.example%3E
      Contact: <sip:referree@referee.example>
      Content-Type: multipart/mixed; boundary=my-boundary-9
      Content-Length: (appropriate value)

      --my-boundary-9

      Content-Type: application/sdp
      Content-Length: (appropriate value)

      v=0
      o=referree 2890844526 2890844526 IN IP4 referree.example
      s=Session SDP
      c=IN IP4 referree.example
      t=0 0
      m=audio 49172 RTP/AVP 0
      a=rtpmap:0 PCMU/8000

      --my-boundary-9

      Content-Type: multipart/signed;
        protocol="application/pkcs7-signature";
        micalg=sha1; boundary=boundary42
      Content-ID: <20342EFXEI.390sdefn2@referror.example>
      Content-Length: (appropriate value)

      --boundary42

      Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
```

```
  name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m
  handling=required
Content-Length: (appropriate value)

************************************************************
* Content-Type: message/sipfrag                            *
* Content-Disposition: auth-id; handling=optional          *
*                                                          *
* From: sip:referror@referror.example                      *
* Call-ID: 2203900ef0299349d9209f023a                      *
* Date: Thu, 21 Feb 2002 13:02:03 GMT                      *
* Refer-To: sip:refertarget@target.example                 *
* Referred-By: sip:referror@referror.example               *
*    ;cid=%3C20342EFXEI.390sdefn2@referror.example%3E      *
************************************************************

--boundary42

Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s;
   handling=required

(appropriate signature)

--boundary42--
--my-boundary-9--
```

7.4 Nested REFER

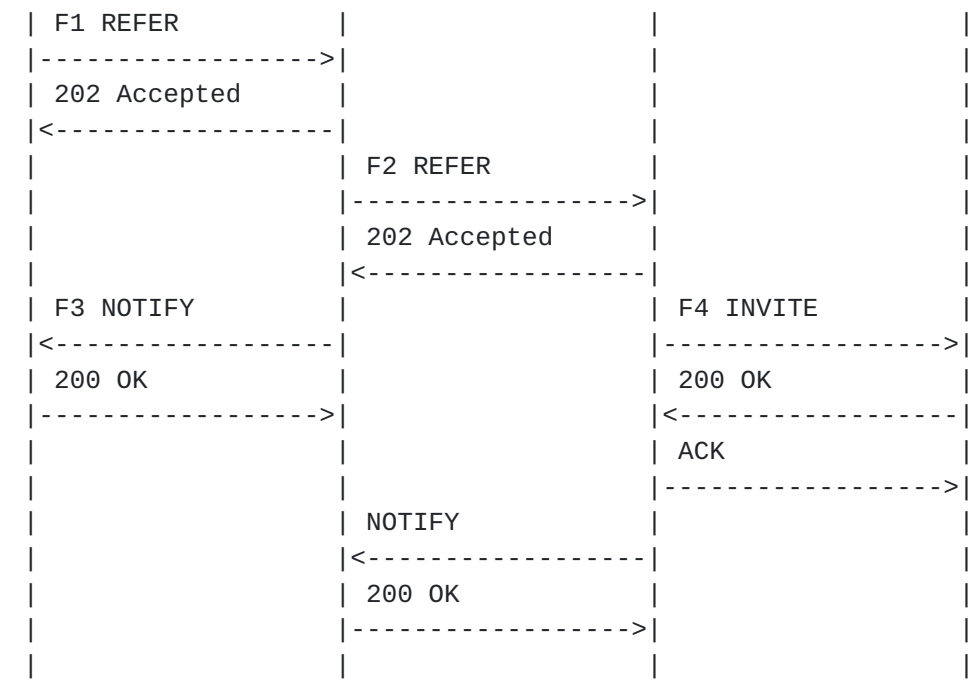
The Refer-To URI may be a SIP URI indicating the REFER method. Consider The following URI which A uses to refer B to send a REFER request to C which refers C to send an INVITE to D.

Note that A provides a Referred-By token which gets passed through B and C to D. In particular, B does not provide its own Referred-By token to C. Also note that A is notified of the outcome of the request it triggered at B (the REFER), not at C (the INVITE).

```
Refer-To: <sip:C;method=REFER?Refer-To=%3Csip:D%3E>
```

This reference would result in the following flow:

```
 A                  B                  C                  D
```




```
F1 REFER sip:B SIP/2.0
   Via: SIP/2.0/UDP A;branch=z9hG4bK3802394232
   To: sip:B
   From: sip:A;tag=23490234
   Call-ID: 2304098023@A
   CSeq: 2342093 REFER
   Max-Forwards: 70
   Contact: <sip:A>
   Refer-To: <sip:C;method=REFER?Refer-To=%3Csip:D%3E>
   Referred-By: <sip:A>;cid=%3C23094202342.10123091233@A%3E
   Content-Type: multipart/mixed; boundary=unique-boundary-1
   Content-Length: (appropriate value)

   --unique-boundary-1

   Content-Type: multipart/signed;
     protocol="application/pkcs7-signature";
     micalg=sha1; boundary=dragons39
   Content-ID: <23094202342.10123091233@A>
   Content-Length: (appropriate value)

   --dragons39
   Content-Type: message/sipfrag
   Content-Disposition: auth-id; handling=optional

   From: sip:A
   Call-ID: 2304098023@A
   Date: Thu, 21 Feb 2002 13:02:03 GMT
```

```
      Refer-To: <sip:C;method=REFER?Refer-To=%3Csip:D%3E>
      Referred-By: <sip:A>;cid=%3C23094202342.101230912342A%3E

      --dragons39
      Content-Type: application/pkcs7-signature; name=smime.p7s
      Content-Transfer-Encoding: base64
      Content-Disposition: attachment; filename=smime.p7s;
         handling=required

      (appropriate signature goes here)

      --dragons39--

      --unique-boundary-1--

   F2 REFER sip:C SIP/2.0
      Via: SIP/2.0/UDP B;branch=z9hG4bK00239842
      To: sip:C
      From: sip:B;tag=2934u23
      Call-ID: 203942834@B
      CSeq: 8321039 REFER
      Max-Forwards: 70
      Contact: <sip:B>
      Refer-To: <sip:D>
      Referred-By: <sip:A>;cid=%3C23094202342.10123091233@A%3E
      Content-Type: multipart/mixed; boundary=unique-boundary-1
      Content-Length: (appropriate value)

      --unique-boundary-1

      Content-Type: multipart/signed;
        protocol="application/pkcs7-signature";
        micalg=sha1; boundary=dragons39
      Content-ID: <23094202342.10123091233@A>
      Content-Length: (appropriate value)

      --dragons39
      Content-Type: message/sipfrag
      Content-Disposition: auth-id; handling=optional

      From: sip:A
      Call-ID: 2304098023@A
      Date: Thu, 21 Feb 2002 13:02:03 GMT
      Refer-To: <sip:C;method=REFER?Refer-To=%3Csip:D%3E>
      Referred-By: <sip:A>;cid=%3C23094202342.101230912342A%3E

      --dragons39
      Content-Type: application/pkcs7-signature; name=smime.p7s
```

```
      Content-Transfer-Encoding: base64
      Content-Disposition: attachment; filename=smime.p7s;
         handling=required

      (appropriate signature goes here)

      --dragons39--

      --unique-boundary-1--

   F3 NOTIFY sip:A SIP/2.0
      Via: SIP/2.0/UDP A;branch=z9hG4bK3802394232
      To: sip:A;tag=23490234
      From: sip:B;tag=5923020
      Call-ID: 2304098023@A
      CSeq: 29420342 NOTIFY
      Event: refer;id=2342093
      Subscription-State: terminated
      Max-Forwards: 70
      Contact: <sip:B>
      Content-Type: message/sipfrag
      Content-Length: (appropriate value)

      SIP/2.0 202 Accepted

   F4 INVITE sip:D SIP/2.0
      Via: SIP/2.0/UDP C;branch=z9hG4bK29348234
      To: sip:D
      From: sip:C;tag=023942334
      Call-ID: 23489020352@C
      CSeq: 1230934 INVITE
      Max-Forwards: 70
      Contact: <sip:C>
      Referred-By: <sip:A>;cid=%3C23094202342.10123091233@A%3E
      Content-Type: multipart/mixed; boundary=unique-boundary-1
      Content-Length: (appropriate value)

      --unique-boundary-1

      Content-Type: application/sdp
      Content-Length: (appropriate value)

      v=0
      o=C 2890844526 2890844526 IN IP4 C
      s=Session SDP
      c=IN IP4 C
      t=0 0
      m=audio 49172 RTP/AVP 0
```

```
a=rtpmap:0 PCMU/8000

--unique-boundary-1

Content-Type: multipart/signed;
  protocol="application/pkcs7-signature";
  micalg=sha1; boundary=dragons39
Content-ID: <23094202342.10123091233@A>
Content-Length: (appropriate value)

--dragons39
Content-Type: message/sipfrag
Content-Disposition: auth-id; handling=optional

From: sip:A
Call-ID: 2304098023@A
Date: Thu, 21 Feb 2002 13:02:03 GMT
Refer-To: <sip:C;method=REFER?Refer-To=%3Csip:D%3E>
Referred-By: <sip:A>;cid=%3C23094202342.101230912342A%3E

--dragons39
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s;
   handling=required

(appropriate signature goes here)

--dragons39--

--unique-boundary-1--
```

8. IANA Considerations

(Note to RFC Editor: Please fill in all occurrences of XXXX in this section with the RFC number of this specification).

This document defines a new SIP header field name with a compact form (Referred-By and b respectively). It also defines an new SIP client error response code (429).

The following changes should be made to http:///www.iana.org/assignments/sip-parameters

The following row should be added to the header field section (replacing any existing row for Referred-By).

Header Name	Compact Form	Reference
Referred-By	b	[RFCXXXX]

The following row should be added to the response code section under the Request Failure 4xx heading

429 Provide Referrer Identity	[RFCXXXX]

9. Open Issues

1. This mechanism proves to the target that the referrer sent a REFER with this particular Refer-To and Referred-By header field values. It DOES NOT prove to the target that the referrer sent that REFER to this particular referree (which may enable an intercept/cut-paste attack). Including the REFER start line (the Request-URI in particular) is not sufficient to tighten this up - location services may arbitrarily retarget the REFER and the target will generally have no way to reconcile the REFER Request-URI with the actual identity of the referree. Do we need to tighten this? If so, I believe the solution needs to lie in the identity service mechanism. The same attack applies to that mechanism in general, resulting in theft of identity.

2. Is Call-ID in a token a security leak? Is it even useful? See Section 4.

3. Should the identity expressed by the token reflect From or Referred-By? See Section 4.

4. Is the To field in the token useful to the target? See Section 4

10. Changes from -00

- Resolved open issue: A referree is not allowed to change the content-id for the body part containing a token while copying the header and body part into the referenced request. A copy of the Referred-By header is in the token. Allowing the referree to change the copy outside the token adds complexity to the acceptance logic at a refer target.

- Updated to reflect the current identity drafts

- Identified open issues with using the token on reciept

- Added SIP to the draft title

- Updated References

Normative References

[1] 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.

[2] Sparks, R., "The SIP Refer Method", draft-ietf-sip-refer-07 (work in progress), December 2002.

[3] Sparks, R., "Internet Media Type message/sipfrag", RFC 3420, November 2002.

[4] Peterson, J., "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", draft-ietf-sip-identity-00 (work in progress), October 2002.

[5] Peterson, J., "SIP Authenticated Identity Body (AIB) Format", draft-ietf-sip-authid-body-00 (work in progress), October 2002.

[6] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996.

Informative References

[7] Sparks, R. and A. Johnston, "Session Initiation Protocol Call Control - Transfer", draft-ietf-sipping-cc-transfer-00 (work in progress), October 2002.

Author's Address

Robert J. Sparks
dynamicsoft
5100 Tennyson Parkway
Suite 1200
Plano, TX 75024

EMail: rsparks@dynamicsoft.com

Full Copyright Statement

Acknowledgement

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