Network Working Group
Request for Comments: 4916
Updates: 3261
Category: Standards Track

J. Elwell
Siemens Enterprise Communications Limited

June 2007

Connected Identity in the Session Initiation Protocol (SIP)

Status of This Memo

Copyright Notice

Abstract

This document provides a means for a Session Initiation Protocol (SIP) User Agent (UA) that receives a dialog-forming request to supply its identity to the peer UA by means of a request in the reverse direction, and for that identity to be signed by an Authentication Service. Because of retargeting of a dialog-forming request (changing the value of the Request-URI), the UA that receives it (the User Agent Server, UAS) can have a different identity from that in the To header field. The same mechanism can be used to indicate a change of identity during a dialog, e.g., because of some action in the Public Switched Telephone Network (PSTN) behind a gateway. This document normatively updates RFC 3261 (SIP).

Table of Contents

1. Introduction

The Session Initiation Protocol (SIP) (RFC 3261 [1]) initiates sessions but also provides information on the identities of the parties at both ends of a session. Users need this information to help determine how to deal with communications initiated by a SIP. The identity of the party who answers a call can differ from that of the initial called party for various reasons such as call forwarding, call distribution and call pick-up. Furthermore, once a call has been answered, a party can be replaced by a different party with a different identity for reasons such as call transfer, call park and retrieval, etc. Although in some cases there can be reasons for not disclosing these identities, it is desirable to have a mechanism for providing this information.

This document extends the use of the From header field to allow it to convey what is commonly called "connected identity" information (the identity of the connected user) in either direction within the context of an existing INVITE-initiated dialog. It can be used to convey:

- the callee identity to a caller when a call is answered;
- the identity of a potential callee prior to answer; or
- the identity of a user that replaces the caller or callee following a call rearrangement such as call transfer carried out within the PSTN or within a back-to-back user agent (B2BUA) using third party call control techniques.

  Note that the use of standard SIP call transfer techniques, involving the REFER method, leads to the establishment of a new dialog and hence normal mechanisms for caller and callee identity apply.

The provision of the identity of the responder in a response (commonly called "response identity") is outside the scope of this document.

Note that even if identity were to be conveyed somehow in a response, there would in general be difficulty authenticating the UAS. Providing identity in a separate request allows normal authentication techniques to be used.

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 RFC 2119 [2].

This specification defines the following additional terms:

caller: the user of the UA that issues an INVITE request to initiate a call.

caller identity: the identity (Address of Record) of a caller.

callee: the user of the UA that answers a call by issuing a 2xx response to an INVITE request.

callee identity: the identity (Address of Record) of a callee.

potential callee: the user of any UA to which an INVITE request is targeted resulting in formation of an early dialog, but because of parallel or serial forking of the request, not necessarily the user that answers the call.

connected user: any user involved in an established call, including the caller, the callee or any user that replaces the caller or callee following a call re-arrangement such as call transfer.

connected identity: the identity (Address of Record) of a connected user.

3. Overview of Solution

A mid-dialog request is used to provide connected identity. The User Agent Client (UAC) for that request inserts its identity in the From header field of the request. To provide authentication, the Identity header field (RFC 4474 [3]) is inserted by a suitable Authentication Service on the path of the mid-dialog request. Unless provided at the UAC, the Authentication Service is expected to be at a proxy that record routes and is able to authenticate the UAC.

A request in the opposite direction to the INVITE request prior to or at the time the call is answered can indicate the identity of the potential callee or callee respectively. A request in the same direction as the INVITE request prior to answer can indicate a change of caller. A request in either direction after answering can indicate a change of the connected user. In all cases, a dialog (early or confirmed) has to be established before such a request can be sent.

This solution uses the UPDATE method (RFC 3311 [4]) for the request, or in some circumstances the re-INVITE method. To send the callee identity, the UAS for the INVITE request sends the UPDATE request after sending the 2xx response to the INVITE request and after receiving an ACK request. To send the potential callee identity, RFC 3262 [5] is expected to be supported. In this case, the UAS for the INVITE request sends the UPDATE request after receiving and responding to a PRACK request (which occurs after sending a reliable 1xx response to the INVITE request). The UPDATE request could conceivably be used for other purposes too, e.g., it could be used during an early dialog to send the potential callee identity at the same time as a Session Description Protocol (SDP) offer for early media. To indicate a connected identity change during an established call, either the UPDATE method or the re-INVITE method can be used. The re-INVITE method would be used if required for other purposes (e.g., when a B2BUA performs transfer using Third Party Call Control (3PCC) techniques it has to issue a re-INVITE request without an SDP offer to solicit an SDP offer from the UA).

This solution involves changing the URI (not the tags) in the To and From header fields of mid-dialog requests and their responses, compared with the corresponding values in the dialog forming request and response. Changing the To and From header field URIs was contemplated in Section 12.2.1.1 of RFC 3261 [1], which says:

> "Usage of the URI from the To and From fields in the original request within subsequent requests is done for backwards compatibility with RFC 2543 [6], which used the URI for dialog identification. In this specification, only the tags are used for dialog identification. It is expected that mandatory reflection of the original To and From URI in mid-dialog requests will be deprecated in a subsequent revision of this specification."

This document therefore deprecates mandatory reflection of the original To and From URIs in mid-dialog requests and their responses, which constitutes a change to RFC 3261 [1]. This document makes no provision for proxies that are unable to tolerate a change of URI, since changing the URI has been expected for a considerable time. To cater for any UAs that are not able to tolerate a change of URI, a new option tag "from-change" is introduced for providing a positive indication of support in the Supported header field. By sending a request with a changed From header field URI only to targets that have indicated support for this option, there is no need to send this option tag in a Require header field.

In addition to allowing the From header field URI to change during a dialog to reflect the connected identity, this document also requires a UA that has received a connected identity in the URI of the From

header field of a mid-dialog request to use that URI in the To header field of any subsequent mid-dialog request sent by that UA.

In the absence of a suitable Authentication Service on the path of the mid-dialog request, the UAS will receive an unauthenticated connected identity (i.e., without a corresponding Identity header field). The implications of this are discussed in Section 7

4. Behaviour

4.1. Behaviour of a UA that Issues an INVITE Request Outside the Context of an Existing Dialog

When issuing an INVITE request, a UA compliant with this specification MUST include the "from-change" option tag in the Supported header field.

> Note that sending the "from-change" option tag does not guarantee that connected identity will be received in subsequent requests.

4.2. Behaviour of a UA that Receives an INVITE Request outside the Context of an Existing Dialog

After receiving an INVITE request, a UA compliant with this specification MUST include the "from-change" option tag in the Supported header field of any dialog-forming response.

> Note that sending the "from-change" option tag does not guarantee that connected identity will be received in the event of a change of caller.

After an early dialog has been formed, if the "from-change" option tag has been received in a Supported header field, the UA MAY issue an UPDATE request (RFC 3311 [4]) on the same dialog, subject to having sent a reliable provisional response to the INVITE request and having received and responded to a PRACK request. After a full dialog has been formed (after sending a 2xx final response to the INVITE request), if the "from-change" option tag has been received in a Supported header field and an UPDATE request has not already been sent on the early dialog, the UA MUST issue an UPDATE request on the same dialog. In either case, the UPDATE request MUST contain the callee's (or potential callee's) identity in the URI of the From header field (or an anonymous identity if anonymity is required).

> Note that even if the URI does not differ from that in the To header field URI of the INVITE request, sending a new request allows the Authentication Service to assert authentication of this identity and confirms to the peer UA that the connected identity

is the same as that in the To header field URI of the INVITE request.

4.3. Behaviour of a UA Whose Identity Changes during an Established INVITE-initiated Dialog

If the "from-change" option tag has been received in a Supported header field during an INVITE-initiated dialog and if the identity associated with the UA changes (e.g., due to transfer) compared to the last identity indicated in the From header field of a request sent by that UA, the UA MUST issue a request on the same dialog containing the new identity in the URI of the From header field (or an anonymous identity if anonymity is required). For this purpose the UA MUST use the UPDATE method unless for other reasons the re-INVITE method is being used at the same time.

4.4. General UA Behaviour

4.4.1. Sending a Mid-Dialog Request

When sending a mid-dialog request, a UA MUST observe the requirements of RFC 4474 [3] when populating the From header field URI, including provisions for achieving anonymity.

This will allow an Authentication Service on the path of the mid-dialog request to insert an Identity header field.

When sending a mid-dialog request, a UA MUST populate the To header field URI with the current value of the remote URI for that dialog, where this is subject to update in accordance with the rules of Section 4.4.2 of this document rather than being fixed at the beginning of the dialog in accordance with RFC 3261 [1].

After sending a request with a revised From header field URI (i.e., revised compared to the URI sent in the From header field of the previous request on this dialog or in the To header field of the received dialog-forming INVITE request if no request has been sent), the UA MUST send the same URI in the From header field of any future requests on the same dialog, unless the identity changes again. Also, the UA MUST be prepared to receive the revised URI in the To header field of subsequent mid-dialog requests and MUST also continue to be prepared to receive the old URI at least until a request containing the revised URI in the To header field has been received.

The mid-dialog request can be rejected in accordance with RFC 4474 [3] if the UAS does not accept the connected identity. If the UAC receives a 428, 436, 437, or 438 response to a mid-dialog request it SHOULD regard the dialog as terminated in the case of a dialog-

terminating request and SHOULD take no action in the case of any other request.

Any attempt to repeat the request or send any other mid-dialog request is likely to result in the same response, since the UA has no control over actions of the Authentication Service.

4.4.2. Receiving a Mid-Dialog Request

If a UA receives a mid-dialog request from the peer UA, the UA can make use of the identity in the From header field URI (e.g., by indicating to the user). The UA MAY discriminate between signed and unsigned identities. In the case of a signed identity, the UA SHOULD invoke a Verifier (see Section 4.6) if it cannot rely on the presence of a Verifier on the path of the request.

If a UA receives a mid-dialog request from the peer UA in which the From header field URI differs from that received in the previous request on that dialog or that sent in the To header field of the original INVITE request and if the UA sends a 2xx response, the UA MUST update the remote URI for this dialog, as defined in RFC 3261 [1]. This will cause the new value to be used in the To header field of subsequent requests that the UA sends, in accordance with the rules of Section 4.4.1. If any other final response is sent the UA MUST NOT update the remote URI for this dialog.

4.5. Authentication Service Behaviour

An Authentication Service MUST behave in accordance with RFC 4474 [3] when dealing with mid-dialog requests.

Note that RFC 4474 is silent on how to behave if the identity in the From header field is not one that the UAC is allowed to assert, and therefore it is a matter for local policy whether to reject the request or forward it without an Identity header field. Policy can be different for a mid-dialog request compared with other requests.

Note that when UAs conform with this specification the Authentication Service should (subject to the normal rules for authentication) be able to authenticate the sender of a request as being the entity identified in the From header field and hence will be able provide a signature for this identity. This is in contrast to UAs that do not support this specification, where retargeting and mid-dialog identity changes can render the From header field inaccurate as a means of identifying the sender of the request.

4.6. Verifier Behaviour

When dealing with mid-dialog requests, an Authentication Service MUST behave in accordance with RFC 4474 [3] updated as stated below.

RFC 4474 [3] states that it is a matter of policy whether to reject a request with a 428 (Use Identity Header) response if there is no Identity header field in the request. A UA MAY adopt a different policy for mid-dialog requests compared with other requests.

4.7. Proxy Behaviour

A proxy that receives a mid-dialog request MUST be prepared for the To header field URI and/or the From header field URI to differ from those that appeared in the dialog-forming request and response.

A proxy that is able to provide an Authentication Service for mid-dialog requests MUST record route if Supported: from-change is indicated in the dialog forming request received by the proxy from the UAC.

5. Examples

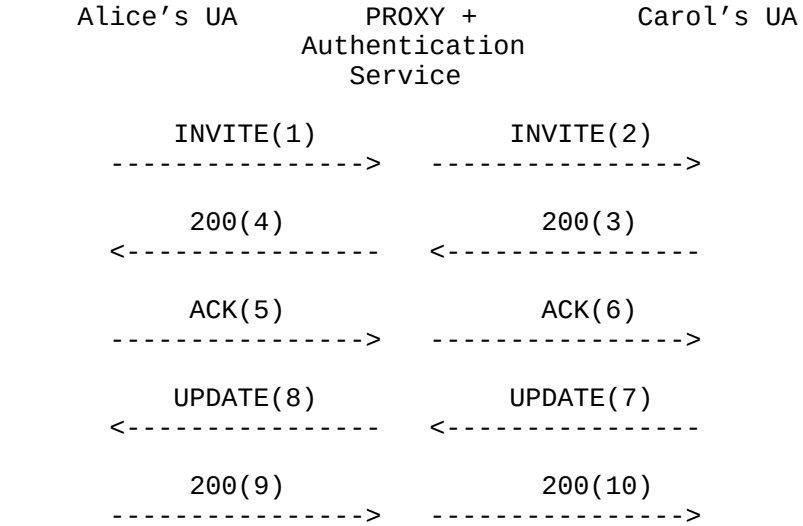
In the examples below, several messages contain unfolded lines longer than 72 characters. These are captured between tags. The single unfolded line is reconstructed by directly concatenating all lines appearing between the tags (discarding any line-feeds or carriage returns).

In the examples, the domain example.com is assumed to have the following private key (rendered in PEM format). The private key is used by the Authentication Service for generating the signature in the Identity header field.

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDPPMBtHVoPkXV+Z6jq1LsgfTELVWpy2BVUffJMPH06LL0cJSQO
aIeVzIojzWtpauB7IylZKlAjB5f429tRuoUiedCwMLKblWAqZt6eHWpCNZJ7lONc
IEwnmh2nAccKk83Lp/VH3tgAS/43DQoX2sndnYh+g8522Pzwg7EGWspzzwIDAQAB
AoGBAK0W3tnEFD7AjVQAnJNXDtx59Aa1Vu2JEXe6oi+OrkFysJjbZJwsLmKtrgtt
PXOU8t2mZpi0wK4hX4tZhntiwGKkUPC3h9Bjp+GerifP341RMyMO+6fPgjqOzUDw
+rPjjMpwD7AkcEcqDgbTrZnWv/QnCSaaF3xkUGfFkLx5OKcRAkEA7UxnsE8XaT30
tP/UUc51gNk2KGKgxQQTHopBcew9yfeCRFhvdL7jpaGatEi5iZwGGQQDVOVHUN1H
0YLpHQjRowJBAN+R2bvA/Nimq464ZgnelEDPqaEAZWaD3kOfhS9+vL7oqES+u5E0
J7kXb7ZkiSVUg9XU/8PxMKx/DAz0dUmOL+UCQH8C9ETUMI2uEbqHbBdVUGNk364C
DFcndSxVh+34KqJdjiYSx6VPPv26X9m7S0OydTkSgs3/4ooPxo8HaMqXm80CQB+r
xbB3UlpOohcBwFK9mTrlMB6Cs9ql66KgwnlL9ukEhHHYozGatdXeoBCyhUsogdSU
6/aSAFcvWEGtj7/vyJECQQCCS1lKgEXoNQPqONalvYhyyMZRXFLdD4gbwRPK1uXK
Ypk3CkfFzOyfjeLcGPxXzq2qzuHzGTDxZ9PAepwX4RSk
-----END RSA PRIVATE KEY-----
```

5.1. Sending Connected Identity after Answering a Call

In this example, Carol's UA has been reached by retargeting at the proxy and thus her identity (AoR) is not equal to that in the To header field of the received INVITE request (Bob). Carol's UA conveys Carol's identity in the From header field of an UPDATE request. The proxy also provides an Authentication Service and therefore adds Identity and Identity-Info header fields to the UPDATE request.



INVITE (1):

```
INVITE sip:Bob@example.com SIP/2.0
Via: SIP/2.0/TLS ua1.example.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@example.com>
From: Alice <sip:alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 1 INVITE
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:02:03 GMT
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, UPDATE
Supported: from-change
Contact: <sip:alice@ua1.example.com>
Content-Type: application/sdp
Content-Length: 154

v=0
o=UserA 2890844526 2890844526 IN IP4 ua1.example.com
s=Session SDP
c=IN IP4 ua1.example.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

INVITE (2):

```
INVITE sip:Carol@ua2.example.com SIP/2.0
Via: SIP/2.0/TLS proxy.example.com;branch=z9hG4bK776asdhds
<allOneLine>
Via: SIP/2.0/TLS ua1.example.com;branch=z9hG4bKnashds8;received=192.0.2.
1
</allOneLine>
To: Bob <sip:bob@example.com>
From: Alice <sip:alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 1 INVITE
Max-Forwards: 69
Date: Thu, 21 Feb 2002 13:02:03 GMT
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, UPDATE
Supported: from-change
Contact: <sip:alice@ua1.example.com>
Record-Route: <sip:proxy.example.com;lr>
<allOneLine>
Identity: "xN6gCHR6KxGM+nyiEM13LcWgAFQD3lkni1DPkwgadxh4BB7G+VwY1
3uRv5hbCI2VSvKuZ4LYN0JNoe7v8VAzruKMyi4Bi4nUghR/fFGBrpBSjztmfffLT
p6SFLxo9XQSVrkm1O4c/4UrKn2ejRz+5BULu9n9kWswzKDNjlYlmmc="
</allOneLine>
Identity-Info: <https://example.com/example.cer>;alg=rsa-sha1
Content-Type: application/sdp
Content-Length: 154

v=0
o=UserA 2890844526 2890844526 IN IP4 ua1.example.com
s=Session SDP
c=IN IP4 ua1.example.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

200 (3):

```
SIP/2.0 200 OK
<allOneLine>
Via: SIP/2.0/TLS proxy.example.com;branch=z9hG4bK776asdhds;received=192.
0.2.2
</allOneLine>
<allOneLine>
Via: SIP/2.0/TLS ua1.example.com;branch=z9hG4bKnashds8;received=192.0.2.
1
<allOneLine>
To: Bob <sip:bob@example.com>;tag=2ge46ab5
From: Alice <sip:alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, UPDATE
Supported: from-change
Contact: <sip:carol@ua2.example.com>
Record-Route: <sip:proxy.example.com;lr>
Content-Type: application/sdp
Content-Length: 154

v=0
o=UserB 2890844536 2890844536 IN IP4 ua2.example.com
s=Session SDP
c=IN IP4 ua2.example.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

200 (4):

```
SIP/2.0 200 OK
<allOneLine>
Via: SIP/2.0/TLS ua1.example.com;branch=z9hG4bKnashds8;received=192.0.2.
1
</allOneLine>
To: Bob <sip:bob@example.com>;tag=2ge46ab5
From: Alice <sip:alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, UPDATE
Supported: from-change
Contact: <sip:carol@ua2.example.com>
Record-Route: <sip:proxy.example.com;lr>
Content-Type: application/sdp
Content-Length: 154
```

```
v=0
o=UserB 2890844536 2890844536 IN IP4 ua2.example.com
s=Session SDP
c=IN IP4 ua2.example.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

ACK (5):

```
ACK sip:carol@ua2.example.com SIP/2.0
Via: SIP/2.0/TLS ua1.example.com;branch=z9hG4bKnashds9
From: Alice <sip:Alice@example.com>;tag=13adc987
To: Bob <sip:Bob@example.com>;tag=2ge46ab5
Call-ID: 12345600@ua1.example.com
CSeq: 1 ACK
Max-Forwards: 70
Route: <sip:proxy.example.com;lr>
Content-Length: 0
```

ACK (6):

```
ACK sip:carol@ua2.example.com SIP/2.0
Via: SIP/2.0/TLS proxy.example.com;branch=z9hG4bK776asdhdt
<allOneLine>
Via: SIP/2.0/TLS ua1.example.com;branch=z9hG4bKnashds9;received=192.0.2.
1
</allOneLine>
From: Alice <sip:Alice@example.com>;tag=13adc987
To: Bob <sip:Bob@example.com>;tag=2ge46ab5
Call-ID: 12345600@ua1.example.com
CSeq: 1 ACK
Max-Forwards: 69
Content-Length: 0
```

UPDATE (7):

```
UPDATE sip:Alice@ua1.example.com SIP/2.0
Via: SIP/2.0/TLS ua2.example.com;branch=z9hG4bKnashdt1
From: Carol <sip:Carol@example.com>;tag=2ge46ab5
To: Alice <sip:Alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 2 UPDATE
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:02:15 GMT
Route: <sip:proxy.example.com;lr>
Contact: <sip:Carol@ua2.example.com>
Content-Length: 0
```

Note that the URI in the From header field differs from that in the To header field in the INVITE request/response. However, the tag is the same as that in the INVITE response.

UPDATE (8):

```
UPDATE sip:Alice@ua1.example.com SIP/2.0
Via: SIP/2.0/TLS proxy.example.com;branch=z9hG4bK776asdhdu
<allOneLine>
Via: SIP/2.0/TLS ua2.example.com;branch=z9hG4bKnashdt1;received=192.0.2.
3
</allOneLine>
From: Carol <sip:Carol@example.com>;tag=2ge46ab5
To: Alice <sip:Alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 2 UPDATE
Max-Forwards: 69
Date: Thu, 21 Feb 2002 13:02:15 GMT
Contact: <sip:Carol@ua2.example.com>
<allOneLine>
Identity: "g8WJiVEzrbYum+z2lnS3pL+MIhuI439gDiMCHm01fwX5D8Ft5Ib9t
ewLfBT9mDOUSn6wkPSWVQfqdMF/QBPkpsIIROIi2sJOYBEMXZpNrhJd8/uboXMl9
KRujDFQefZlmXV8dwD6XsPnMgcH8jAcaZ5aS04NyfWadIwTnGeuxko="
</allOneLine>
Identity-Info: <https://example.com/cert>;alg=rsa-sha1
Content-Length: 0
```

200 (9):

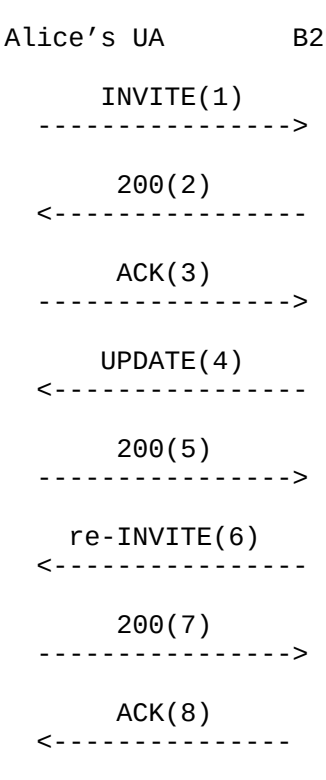
```
SIP/2.0 200 OK
<allOneLine>
Via: SIP/2.0/TLS proxy.example.com;branch=z9hG4bK776asdhdu;received=192.
0.2.2
</allOneLine>
<allOneLine>
Via: SIP/2.0/TLS ua2.example.com;branch=z9hG4bKnashdt1;received=192.0.2.
3
</allOneLine>
From: Carol <sip:Carol@example.com>;tag=2ge46ab5
To: Alice <sip:Alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 2 UPDATE
Contact: <sip:Alice@ua1.example.com>
Content-Length: 0
```

200 (10):

```
SIP/2.0 200 OK
<allOneLine>
Via: SIP/2.0/TLS ua2.example.com;branch=z9hG4bKnashdt1;received=192.0.2.
3
</allOneLine>
From: Carol <sip:Carol@example.com>;tag=2ge46ab5
To: Alice <sip:Alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 2 UPDATE
Contact: <sip:Alice@ua1.example.com>
Content-Length: 0
```

5.2. Sending Revised Connected Identity during a Call

In this example, a call is established between Alice and Bob, where Bob (not shown) lies behind a B2BUA. Bob's identity is conveyed by an UPDATE request. Then the B2BUA executes call transfer using third party call control (3PCC) techniques as described in RFC 3725 [7] (e.g., under the control of a click-to-dial application). As a result, Alice becomes connected to Carol (also not shown), and a re-INVITE request is issued allowing the session to be renegotiated. The B2BUA provides the Authentication Service and thus generates the Identity header field in the re-INVITE request to provide authentication of Carol's identity.



INVITE (1):

```
INVITE sip:Bob@example.com SIP/2.0
Via: SIP/2.0/TLS ua1.example.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@example.com>
From: Alice <sip:alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 1 INVITE
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:02:03 GMT
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, UPDATE
Supported: from-change
Contact: <sip:alice@ua1.example.com>
Content-Type: application/sdp
Content-Length: 154
```

```
v=0
o=UserA 2890844526 2890844526 IN IP4 ua1.example.com
s=Session SDP
c=IN IP4 ua1.example.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

200 (2)

```
SIP/2.0 200 OK
<allOneLine>
Via: SIP/2.0/TLS ua1.example.com;branch=z9hG4bKnashds8;received=192.0.2.
1
</allOneLine>
To: Bob <sip:bob@example.com>;tag=2ge46ab5
From: Alice <sip:alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, UPDATE
Supported: from-change
Contact: <sip:xyz@b2bua.example.com>
Content-Type: application/sdp
Content-Length: 154

v=0
o=UserB 2890844536 2890844536 IN IP4 ua2.example.com
s=Session SDP
c=IN IP4 ua2.example.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

ACK (3)

```
ACK sip:xyz@b2bua.example.com SIP/2.0
Via: SIP/2.0/TLS ua1.example.com;branch=z9hG4bKnashds9
From: Alice <sip:Alice@example.com>;tag=13adc987
To: Bob <sip:Bob@example.com>;tag=2ge46ab5
Call-ID: 12345600@ua1.example.com
CSeq: 1 ACK
Max-Forwards: 70
Content-Length: 0
```

UPDATE (4)

```
UPDATE sip:alice@ua1.example.com SIP/2.0
Via: SIP/2.0/TLS b2bua.example.com;branch=z9hG4bKnashdt1
From: Bob <sip:Bob@example.com>;tag=2ge46ab5
To: Alice <sip:Alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 2 UPDATE
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:02:12 GMT
Contact: <sip:xyz@b2bua.example.com>
<allOneLine>
Identity: "AQFLSjCDRhO2eXlWmTajk99612hkJii9giDMWki5uT6qc4BrekywO
UuObcwZI3qhJReZCN7ybMBNYFZ5yFXWdyet4j3zLNCONU9ma+rs8ZOv0+z/Q3Z5c
D26HrmitU+OCKWPLObaxbkGQry9hQxOmwRmlUgSjkeCEjgnc1iQc3E="
</allOneLine>
Identity-Info: <https://example.com/cert>;alg=rsa-sha1
Content-Length: 0
```

200 (5)

```
SIP/2.0 200 OK
<allOneLine>
Via: SIP/2.0/TLS b2bua.example.com;branch=z9hG4bKnashdt1;received=192.0.
2.2
</allOneLine>
From: Bob <sip:Bob@example.com>;tag=2ge46ab5
To: Alice <sip:Alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 2 UPDATE
Contact: <sip:Alice@ua1.example.com>
Content-Length: 0
```

re-INVITE (6)

```
INVITE sip:alice@ua1.example.com SIP/2.0
Via: SIP/2.0/TLS b2bua.example.com;branch=z9hG4bKnashdxy
From: Carol <sip:Carol@example.com>;tag=2ge46ab5
To: Alice <sip:Alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 3 INVITE
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:03:20 GMT
Contact: <sip:xyz@b2bua.example.com>
<allOneLine>
Identity: "KCd3YLQHj51SlCQhFMnpQjmP6wHh7JGRO8LsB4v5SGEr/Mwu7j6Gp
al8ckVM2vd1zqH/F4WJXYDlB525uuJm/fN3O1A2xsZ9BxRkh4N4U19TL9I2Tok3U
3kGg8To/6w1mEXpUQjo3OgNYqOBtawHuZI5nrOVaV3IrbQh1b2KgLo="
</allOneLine>
Identity-Info: <https://example.com/cert>;alg=rsa-sha1
Content-Length: 0
```

200 (7)

```
SIP/2.0 200 OK
<allOneLine>
Via: SIP/2.0/TLS b2bua.example.com;branch=z9hG4bKnashdxy;received=192.0.
2.2
</allOneLine>
From: Carol <sip:Carol@example.com>;tag=2ge46ab5
To: Alice <sip:Alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 3 INVITE
Contact: <sip:Alice@ua1.example.com>
Content-Length: 154

v=0
o=UserA 2890844526 2890844526 IN IP4 ua1.example.com
s=Session SDP
c=IN IP4 ua1.example.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

ACK (8)

```
ACK sip:alice@ua1.example.com SIP/2.0
Via: SIP/2.0/TLS b2bua.example.com;branch=z9hG4bKnashdxz
From: Carol <sip:Carol@example.com>;tag=2ge46ab5
To: Alice <sip:Alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 3 ACK
Max-Forwards: 70
Content-Length: 154

v=0
o=UserC 2890844546 2890844546 IN IP4 ua3.example.com
s=Session SDP
c=IN IP4 ua3.example.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

6. IANA Considerations

This specification registers a new SIP option tag, as per the guidelines in Section 27.1 of RFC 3261 [1].

This document defines the SIP option tag "from-change".

The following row has been added to the "Option Tags" section of the SIP Parameter Registry:

Name	Description	Reference
from-change	This option tag is used to indicate that a UA supports changes to URIs in From and To header fields during a dialog.	[RFC4916]

7. Security considerations

RFC 4474 [3] discusses security considerations relating to the Identity header field in some detail. Those same considerations apply when using the Identity header field to authenticate a connected identity in the From header field URI of a mid-dialog request.

A received From header field URI in a mid-dialog request for which no valid Identity header field (or other means of authentication) has been received either in this request or in an earlier request on this

dialog cannot be trusted (except in very closed environments) and is expected to be treated in a similar way to a From header field in a dialog-initiating request that is not backed up by a valid Identity header field. However, it is recommended not to reject a mid-dialog request on the grounds that the Identity header field is missing (since this would interfere with ongoing operation of the call). The absence of a valid Identity header field can influence the information given to the user. A UA can clear the call if policy or user preference dictates.

A signed connected identity in a mid-dialog request (URI in the From header field accompanied by a valid Identity header field) provides information about the peer UA in a dialog. In the case of the UA that was the UAS in the dialog-forming request, this identity is not necessarily the same as that in the To header field of the dialog-forming request. This is because of retargeting during the routing of the dialog-forming request. A signed connected identity says nothing about the legitimacy of such retargeting, but merely reflects the result of that retargeting. History information (RFC 4244 [8]) can provide additional hints as to how the connected user has been reached.

Likewise, when a signed connected identity indicates a change of identity during a dialog, it conveys no information about the reason for such a change of identity or its legitimacy.

Use of the sips URI scheme can minimize the chances of attacks in which inappropriate connected identity information is sent, either at call establishment time or during a call.

Anonymity can be required by the user of a connected UA. For anonymity the UA is expected to populate the URI in the From header field of a mid-dialog request in the way described in RFC 4474 [3].

8. Acknowledgments

Thanks to Francois Audet, Frank Derks, Steffen Fries, Vijay Gurbani, Cullen Jennings, Paul Kyzivat, Hans Persson, Jon Peterson, Eric Rescorla, Jonathan Rosenberg, Shida Schubert, Ya-Ching Tan, and Dan Wing for providing valuable comments.

9. References

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

[3] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 4474, August 2006.

[4] Rosenberg, J., "The Session Initiation Protocol (SIP) UPDATE Method", RFC 3311, September 2002.

[5] Rosenberg, J. and H. Schulzrinne, "Reliability of Provisional Responses in the Session Initiation Protocol (SIP)", RFC 3262, June 2002.

9.2. Informative References

[6] Handley, M., Schulzrinne, H., Schooler, E., and J. Rosenberg, "SIP: Session Initiation Protocol", RFC 2543, March 1999.

[7] Rosenberg, J., Peterson, J., Schulzrinne, H., and G. Camarillo, "Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)", RFC 3725, June 2002.

[8] Barnes, M., "An Extension to the Session Initiation Protocol (SIP) for Request History Information", RFC 4244, November 2005.

Author’s Address

John Elwell
Siemens Enterprise Communications Limited
Technology Drive
Beeston, Nottingham NG9 1LA
UK

Phone: +44 115 943 4989
EMail: john.elwell@siemens.com

Full Copyright Statement

Intellectual Property

Acknowledgement

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