Confidential Access Levels for the Session Initiation Protocol (SIP)  
draft-hewett-sipping-cal-00

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on August 27, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

This specification defines a header for indicating the confidentiality level established between the involved parties.
1. Introduction

When sensitive and confidential communications are required in SIP [RFC3261], a mechanism is needed by which each participant can be assured of the confidentiality level established between the involved parties. The notion of confidentiality presented here refers to both the user agent (UA) devices and all transited network connections between them. By establishing a level of trust in the session, participants are free to communicate at a level that is appropriate for the sensitivity of the information being shared. There are numerous examples for the need of such a mechanism including the protection of sensitive information by corporate executives, financial institutions, national security and military organizations.

We note that the level of trust discussed here is orthogonal to what is normally associated with channel encryption and authentication schemes like Transport Layer Security (TLS). While TLS encrypts the stream and provides authentication indication of the connected peer, it does not indicate the level of authorization of the connected party; i.e., is the connected party someone with an executive privilege, or does the connected party possess top-secret clearance, for instance.

There are two areas of trust to consider for the establishment of session confidentiality. The first is the UA itself and the authorization of that device for a particular individual. Although no mechanism is specified in this document, some type of user authentication to a device is assumed. Many methods can be used, ranging from physical access restrictions in which the devices themselves are under lock and key to identity management systems that use elements such as biometric authentication to enable the device at the appropriate confidentiality level.

The second aspect of trust is the interconnecting facilities between the caller and callee. Both the signaling and media planes are considered with respect to trusted facilities. The signaling session may transit SIP proxies and interconnecting network components before terminating to the callee. Each proxy must consider the level of trust associated with the next signaling hop.

This document deals only with format and exchange of a header to the SIP signaling messages that indicates the confidentiality level established between the involved parties. It assumes that the user has been authorized to use a device, and furthermore, that a proxy is configured with appropriate confidentiality levels to allow it to service an incoming request appropriately.
2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Overview

There are two modes of operation for establishing the confidentiality level: fixed mode and variable mode. Fixed mode enforces a specific level of confidentiality whereas variable mode resolves to a specific access level based on the values offered by participating entities. When a specific confidentiality level must be established, fixed mode is the preferred method. When a level of confidentiality is desired but call completion is more essential, variable mode is used.

Each UA uses an assigned Confidential Access Level (CAL) mode and value while a proxy has a CAL mode and value associated with the chosen network domain for routing. This means that a proxy or UA may receive a mode that is different than what they are configured for. This is permissible and resolution of the access level will be handled as described later in this section.

CAL is processed in both the request path and the response path by updating two separate access level values. For example, an INVITE will contain a CAL whose access level is updated as it is processed in the forward direction and a 200 OK to the INVITE will contain a CAL with the second access level being updated in the backwards direction. The 200 OK for the INVITE will transport the value originated by the UAS and resolved in the response path as well as the "reflected" access level. The reflected access level is the value that was resolved in the forward direction and indicates the final resolved level at the UAS. By having both access level values returned to the caller, the UAC has the answer to the offered access level returned in the reflected-access-level as well as an offer of what can be supported by the UAS. The reflected-access-level received by the UAC determines the access level presented to the caller. However, an implementation MAY use the local-access-level returned by the UAS in conjunction with the reflected-access level to make its' final determination. It is beneficial for the UAC to understand what can be supported by the UAS, particularly in scenarios such as adhoc conferences where the access level may need to be renegotiated due to callers joining or leaving a call. Providing the local-access-level in the response message provides this benefit.

The access level value of 0 SHALL be reserved to indicate that no
confidentiality has been established and is only valid when using variable mode. This is useful for cases where the access levels could not be resolved to any confidential level but it is still desirable to complete the call.

3.1. Fixed Mode

Fixed mode is a more restrictive and simpler means of establishing calls. It is used when communication must occur at a particular level of confidentiality. When a call is attempted at the specified access level, each proxy as well as the destination UA must be able to support that level of confidentiality. A comparison is made of the access level being offered in the SIP request to the access level that the proxy or UA processing the request is able to grant. If the proxy or UA cannot provide the requested level of confidentiality, a response code of 418 MUST be returned.

3.2. Variable Mode

Variable mode allows the caller to offer a desired CAL, which may get modified by each proxy and the called UA to a level that can be supported by each processing entity. Each proxy or UA must provide a mechanism to resolve a new CAL value when using variable mode.

3.3. Resolving Access Levels

Access level values are used programatically by each UA or proxy involved in the session to provide a resolved value based on the combination of the incoming access level value and a locally configured value. For fixed mode, a simple equality comparison is made between the received value and the locally configured value. Variable access levels are not intended to be compared numerically to determine if one value is higher than another.

When variable mode is used, an incoming access level must be resolved against a locally configured value to provide a result. An example implementation might render this in the form of an x-y matrix vector where the x value is taken from the incoming header, the y value is taken from the locally configured value for the destination resource and the vector is the resolved value. The actual implementation may be done in different ways but should allow the flexibility of having programmable results based on the intersection of incoming access level and configured access level.

For example, an incoming CAL header using variable may contain a value of 2 and the receiving proxy or UA may have a locally configured value of 6. The resolved value could by any valid agreed upon access level. The administrator may choose a value of 2 if...
using ascending priority values since 2 is the highest common denominator. However, the actual values are left to the discretion of the administrator rather than specified by this document. The use of resolution vectors rather simple numerical ordering mandates agreement between SIP processing entities on configured resolution values.

Refer to section 3.4 for resolving access levels where the access mode being requested does not match the mode configured,

3.4. Resolving Mixed Mode Access Levels

A proxy or UA may receive a CAL header with a mode that is different than the locally configured mode. When a different mode is received, the resulting mode must always be "fixed" since a fixed mode value cannot be changed. For example, consider a UA that is configured as variable and the received CAL mode is a fixed access level of 10. The resolved value must be a fixed value of 10 to match the incoming fixed value of 10 in order for the session to be successfully established.

The same negotiation rules extend to scenarios involving supplementary services such as transfer and conferencing. For example, when a conference is established, each new participant joining the conference MUST go through access resolution to determine if the participant is allowed to join. If the existing conference or the new participant uses fixed mode access, it is necessary to resolve to fixed mode along with the predetermined access level in order to establish the session.

4. Protocol Details

We now specify the related headers and response code.

4.1. Confidential Access Level Header

The CAL header may appear in a SIP request or response, and indicates the need for secure and confidential communications. The CAL header is a new SIP header that conveys the mode and level of confidentiality that is desired for the session being established.

The syntax of the CAL header is defined as follows.
Confidential-Access-Level: 4;mode=variable;ref=2;rmode=fixed
Confidential-Access-Level: 50;mode=variable;ref=40;rmode=variable

Confidential Access Level Header

The access-level indicates the confidentiality level of the session. The access-mode indicates whether the fixed or variable method is used. The local-access-level is used to indicate CAL for the path over which the header is being transported. The reflected-access-level provides to the UAC the final value resolved in the request path to UAS. The reflected-mode indicates to the UAC the mode being using by the UAS.

The Confidential-Access-Level header is supported in the following request messages: INVITE [RFC3261], UPDATE [RFC3311].

The Confidential-Access-Level header is to be supported in the following response messages: 200 (OK), 418 (Incompatible CAL). The local-access-level of the CAL header in a 418 response contains the CAL value of the routing domain at the proxy or the CAL value of the device at the UAS, depending on where the 418 is generated.

The following table extends the values in table 2 of [RFC3261].

<table>
<thead>
<tr>
<th>Header Field</th>
<th>Where</th>
<th>Proxy</th>
<th>INV</th>
<th>UPD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidential Access Level</td>
<td>R</td>
<td>mr</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>Confidential Access Level</td>
<td>200</td>
<td>mr</td>
<td>o</td>
<td>o</td>
</tr>
</tbody>
</table>

Summary of header fields
4.2. The secure-access-level Option Tag

This document defines the confidential-access-level option-tag. The confidential-access-level option-tag MUST be included in the Require header and in the Proxy-Require header when CAL is required for a session.

4.3. 418 Response Code

If a proxy or UAS cannot resolve to a valid CAL value in a request and determines that the call should not continue, a 418 response code MUST be returned to the requestor. This response code indicates that when the offered CAL value and the locally configured CAL value were resolved, a decision was made to not allow the session to be established. The decision to reject a call is based on the locally administered policy, which is not specified by this document.

The 418 response SHOULD contain the CAL header with the reflected-access-level set to the last successfully resolved value in the request path. The local-access-level SHOULD be set to the access-level supported by the UAS or to the access-level supported for the routing domain that failed resolution at a proxy.

5. UAC Procedures

While CAL is generally established at call setup, a change in the media path may require the access level to be upgraded or downgraded. A re-INVITE or UPDATE may be used to convey a different access level for the new media path.

5.1. Processing a Request

The level of confidentiality assigned to a device is communicated via the CAL header. This does not preclude different classifications from being assigned to a device when the appropriate authorization level has been granted for using the device at that level. The header is included in an outgoing INVITE at initial call setup to communicate the desired level at which the session should be established. The inclusion of the ‘confidential-access-level’ option tag MUST be included in both the Require and Proxy-require headers. This is the only way to ensure that every segment of the session is established at the appropriate access level.

5.2. Processing a Response

The CAL MUST be received from the UAS in a 200 response if the request contained a CAL header. The CAL header will include two
access values. The reflected-access-level should be indicated to the caller. Again, displaying the name of the callee is recommended. The reflected CAL value indicates what has been presented to the UAS as the access level. The local-access-level in the response indicates the initial value sent by the UAS, updated appropriately by each proxy in the response path. The local-access-level received by the UAC represents the level that can be supported by the UAS using the path between the UAS and UAC. The form in which the name and CAL level are presented to the user is not specified but left up to the implementor’s discretion. If a 418 response is received, an appropriate indication should be given to the caller.

6. Proxy Procedures

Proxies must be able to recognize and process the CAL header. Otherwise, integrity of the complete path cannot be guaranteed. Each proxy MUST determine the trust level of the domain to which the message is being sent.

6.1. Processing a Request

The CAL local-access-level in the incoming header is resolved against the locally configured routing domain. The local-access-level value and mode of the CAL header are updated based on the results. Refer to section 3 for details on resolving access levels.

For fixed mode, if the access level being requested cannot be met, a 418 response MUST be returned. For variable mode, if the access level can be resolved to an acceptable level, the local-access-level of the CAL header is updated with the new value. The proxy MAY return a 418 response if the CAL value cannot be resolved to an acceptable value. If local policy determines that the call should continue even though an acceptable access level could not be resolved, the local-access-level value MUST be set to 0 in the CAL header.

In variable mode, a forking proxy MAY use the same or different CAL levels for each fork. In fixed mode, a forking proxy MUST use the same CAL level as the incoming request for all branches.

6.2. Processing a Response

The local-access-level in the incoming CAL header of a 200 response is resolved against the locally configured routing domain. The local-access-level value and mode of the CAL header are updated based on the results. Refer to section 3 for details on resolving access levels. If the local-access-level cannot be resolved to an
acceptable level in the response path, the proxy MUST set the local-access-level to 0. A local-access-level of 0 in the response indicates to the UAC that CAL could not be resolved to an acceptable level in the response path.

When a forking proxy receives multiple responses from different branches, it is responsible for aggregating the responses and providing a single final response. When at least one branch is successful, the forking proxy would normally forward the successful response, as mandated by RFC3261.

When all the branches fail, the forking proxy is responsible for aggregating the responses and providing a single final response. If the responses are heterogeneous (i.e., not all response codes are the same), the proxy will use the rules of RFC3261 to choose the best response. Implementations confirming to this specification MUST choose a response code of 418 if at least one of the forked branches contained such a response code. This is to allow the recipient to resubmit the request using a different CAL header value, if it so wants to.

7. UAS Procedures

When a SIP request message is received with a Confidential-Access-Level header, the UAS should first determine whether the received access-mode is fixed or negotiable. If the mode is fixed, the UA should determine if the local-access-level matches the configured CAL value. If the CAL values do not match, this constitutes a CAL incompatibility and a 418 response MUST be returned.

When a SIP request message is received with a Confidential-Access-Level header and the access-mode is variable, the UAS MUST resolve the access level by evaluating the value within the header and the locally configured value. The resolved value will be placed in the reflected-access-level of the CAL header to be sent in the response message. The UAS MUST also resolve its’ locally established CAL for the device against the routing domain of the response path. If an acceptable resolution is made, the resolved value is placed in the local-access-level of the CAL header. If the UAS deems the two values to be incompatible, it MAY send a 418 response code if local policy determines that the call should not continue. If local policy determines that the call should continue, the local-access-level value MUST be set to 0 in the CAL header of the 200 response.

An indication of the access level should be given to the callee and it is recommended that the calling name be provided as well.
The CAL header must be returned in the final response to an INVITE sent with a CAL header. If the offered mode was variable, the returned mode may be changed to fixed mode. However, an initial fixed mode cannot be changed. The access level is changed only if the mode of the UAS is variable. Otherwise, the access level remains the same since it cannot be changed for fixed mode.

8. Examples

8.1. Successful CAL Session Establishment

This example shows a session being initiated by a@a with a CAL of 50 in variable mode. Proxy A forwards the request after changing the CAL to 40. Proxy B forwards the request after changing the CAL to 35. UA b@B responds with CAL 60. Proxy B forwards the response with CAL 40. Proxy A forwards the response unchanged. The call is established with a CAL of 35.
8.2. CAL Rejection

This example shows a session being initiated by a@A with a CAL of 40 in fixed mode. The request is accepted by proxy A and forwarded to proxy B. Proxy B rejects the request with 418 because it cannot support the requested CAL.
9. IANA Considerations

This section defines one new SIP header, one new SIP response code and one new SIP option tag.

Header name: Confidential-Access-Level
Compact form: none

Option tag: 'confidential-access-level'
Descriptive text: Indicates support for the Confidential Access Level.

Response code: 418
Default reason phrase: Confidential Access Level Rejected

10. Security Considerations

Confidentiality, as asserted by the use of CAL depends on the concept of trusted domains. A trusted domain is the collection of proxies, user agents and access network components that provide a complete path from the calling UA to the called UA. When that path lies completely within a private network, there is high degree of confidence in the ability of the network to prevent access to sensitive information communicated over a session. At the other end
of the spectrum, transmission over the public internet provides a much lower degree of confidence. Between these two extremes lie interconnecting network agreements where service providers assure a specified level of security in transit over their network.

When a request or response are sent with the CAL header, each SIP UA or proxy must determine the trust level of the next SIP entity to which they are sending to assess the confidentiality level.

11. Acknowledgments

Thanks to Gary Kelly, Jack Klecha, John Rutledge, Bill Maloid and Cullen Jennings for their help in defining the solution and writing this document.

12. References

12.1. Normative References


12.2. Informative References


Authors’ Addresses

Jeff Hewett
Cisco Systems
7025-2 Kit Creek Rd
Mailstop RTP2H/2/4
Research Triangle Park, NC 27709-4987
USA

Phone +1 919 392 2409
Email: jhewett@cisco.com