Independent Submission
Request for Comments: 5379
Category: Informational
ISSN: 2070-1721

M. Munakata
S. Schubert
T. Ohba
NTT

February 2010

Guidelines for Using the Privacy Mechanism for SIP

Abstract

This is an informational document that provides guidelines for using the privacy mechanism for the Session Initiation Protocol (SIP) that is specified in RFC 3323 and subsequently extended in RFCs 3325 and 4244. It is intended to clarify the handling of the target SIP headers/parameters and the Session Description Protocol (SDP) parameters for each of the privacy header values (priv-values).

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This is a contribution to the RFC Series, independently of any other RFC stream. The RFC Editor has chosen to publish this document at its discretion and makes no statement about its value for implementation or deployment. Documents approved for publication by the RFC Editor are not a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5379.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Table of Contents

1. Introduction

This document clarifies the privacy mechanism for the Session Initiation Protocol (SIP) [RFC3261] defined in [RFC3323], which was later extended in [RFC3325] and [RFC4244]. This document describes the practical manner of operations of the privacy mechanism as a guideline and does not change the existing privacy mechanism.

In RFC 3323, the semantics of the basic set of priv-values (header, session, user, none, and critical) is defined, but there are some ambiguities in regards to the target information to be obscured per priv-value, which are not explicitly specified. An ambiguity such as this could result in different interpretations of privacy handling for each of the priv-values defined, both at an entity setting a Privacy header and at an entity processing a Privacy header, which could have an adverse impact on interoperability.

Additional priv-values "id" and "history" are defined in RFCs 3325 and 4244, respectively.

In RFC 4244, the priv-value "history" is defined in order to request privacy for History-Info headers, and the target to be obscured for "history" priv-value is specified as only the History-Info headers. In addition, the RFC clearly describes that History-Info headers are also the target when "header"- and "session"-level privacy are requested.

On the other hand, RFC 3325 defines the P-Asserted-Identity header and a priv-value "id", which is used to request privacy for only the P-Asserted-Identity header, but it does not specify how other priv-values may impact the privacy handling of the P-Asserted-Identity header. Because of this lack of specification, it has been observed that some implementations are suffering from the inability to achieve the intended privacy due to discrepancies in interpretations.

This document tries to clarify the SIP headers and SDP parameters to be obscured for each of the priv-values to alleviate the potential interoperability issues already seen due to a lack of explicit text.

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].

Note: This document is informational; therefore, it does not specify any new normative behaviors of privacy mechanism. All the RFC 2119 language in this document is derived from the normative text in the existing RFCs, such as RFC 3323.

priv-value:
Values registered with IANA to be used in the Privacy header. Registered priv-values are "header", "session", "user", "none", and "critical" defined in [RFC3323]; "id" defined in [RFC3325]; and "history" defined in [RFC4244].

privacy service:
A network entity that executes privacy functions before forwarding messages to the next hop. It is sometimes abbreviated to PS in this document.

user-level privacy:
Privacy for user-inserted information that can be anonymized by the user agent itself.

3. Semantics of Existing priv-values

This section provides the semantics of each priv-value defined in RFCs 3323, 3325, and 4244. The descriptions are taken from the IANA registration.

Privacy Type	Description	Reference
user	Request that privacy services provide a user-level privacy function	[RFC3323]
header	Request that privacy services modify headers that cannot be set arbitrarily by the user (Contact/Via).	[RFC3323]
session	Request that privacy services provide privacy for session media	[RFC3323]
none	Privacy services must not perform any privacy function	[RFC3323]
critical	Privacy service must perform the specified services or fail the request	[RFC3323]
id	Privacy requested for Third-Party Asserted Identity	[RFC3325]

history	Privacy requested for History-Info header(s)	[RFC4244]

4. Target for Each priv-value

Tables in this section show the recommended treatment of SIP headers and SDP parameters per priv-value. SIP headers and SDP parameters not shown in the tables are regarded as non-targets of these priv-values. Some non-target SIP headers/SDP parameters may carry privacy-sensitive information that may need privacy treatment regardless of the privacy level requested. This is further described in 5.3.

The way in which SIP headers and SDP parameters listed here are obscured may depend on the implementation and network policy. This document does not prevent different variations that may exist based on local policy but tries to provide recommendations for how a privacy service treats SIP headers and SDP parameters.

Note: The scope of these tables is SIP headers and related parameters specified in RFCs.

4.1. Target SIP Headers for Each priv-value

Table 1 below shows a recommended treatment of each SIP header for each priv-value. Detailed descriptions of the recommended treatment per SIP header are covered in Section 5.

The "where" column describes the request and response types in which the header needs the treatment to maintain privacy. Values in this column are:

R: The header needs the treatment when it appears in a request.

r: The header needs the treatment when it appears in a response.

The next five columns show the recommended treatment for each priv-value:

delete: The header is recommended to be deleted at a privacy service.

not add: The header is recommended not to be added at a privacy service.

anonymize: The header is recommended to be anonymized at a privacy service. How to anonymize the header depends on the header. Details are given in Section 5.

anonymize*: An asterisk indicates that the involvement of a privacy service and treatment of the relevant header depend on the circumstance. Details are given in Section 5.

Target headers	where	user	header	session	id	history
Call-ID (Note)	R	anonymize	-	-	-	-
Call-Info	Rr	delete	not add	-	-	-
Contact	R	-	anonymize	-	-	-
From	R	anonymize	-	-	-	-
History-Info	Rr	-	delete	delete	-	delete
In-Reply-To	R	delete	-	-	-	-
Organization	Rr	delete	not add	-	-	-
P-Asserted-Identity	Rr	-	delete	-	delete	-
Record-Route	Rr	-	anonymize	-	-	-
Referred-By	R	anonymize*	-	-	-	-
Reply-To	Rr	delete	-	-	-	-
Server	r	delete	not add	-	-	-
Subject	R	delete	-	-	-	-
User-Agent	R	delete	-	-	-	-
Via	R	-	anonymize	-	-	-
Warning	r	anonymize	-	-	-	-

Table 1: Recommended PS behavior for each SIP header

Note: Any time a privacy service modifies a Call-ID, it MUST retain the former and modified values as indicated in Section 5.3 in RFC 3323. It MUST then restore the former value in a Call-ID header and other corresponding headers and parameters (such as In-Reply-To, Replaces, and Target-Dialog) in any messages that are sent using the modified Call-ID to the originating user agent. It should also modify a Call-ID header and other corresponding headers/parameters (such as Target-Dialog and "replaces" parameter) in any further relevant messages that are sent by the originating user agent. Refer to Section 5.1.1 (Call-ID) for the detailed behavior.

Identity/Identity-Info, Path, Replaces, Route, Service-Route, and Target-Dialog headers are not targets of these priv-values (and should not be anonymized or modified by a privacy service based on a priv-value in a Privacy header). Refer to Section 5.3 for details.

4.2. Target SDP Parameters for Each priv-value

The recommended PS behaviors for each SDP parameters are simple. The c, m, o, i, u, e, and p lines in SIP request/response are recommended to be anonymized when user privacy is requested with Privacy:session.

4.3. Treatment of priv-value Not Supported by the Privacy Service

As specified in RFC 3323, if the priv-value of "critical" is present in the Privacy header of a request, and if the privacy service is incapable of performing all of the levels of privacy specified in the Privacy header, it MUST fail the request with a 500 (Server Error) response code as indicated in Section 5 in RFC 3323.

Since the protection of privacy is important, even if the priv-value "critical" is not present in the Privacy header, the privacy service should fail the request with a 500 response code when it is incapable of performing all of the levels of privacy specified in the Privacy header.

5. Recommended Treatment of User-Privacy-Sensitive Information

The following SIP headers and related parameters may concern privacy. This section describes what kind of user-privacy-sensitive information may be included in each SIP header/parameter, and how to maintain privacy for such information at a user agent or a privacy service when the information is indeed privacy-sensitive.

5.1. Target SIP Headers

This section describes privacy considerations and recommended treatment for each SIP header that may reveal user-privacy-sensitive information. This section goes into details about how each header affects privacy, the desired treatment of the value by the user agent and privacy service, and other instructions/additional notes necessary to provide privacy.

5.1.1. Call-ID

This field frequently contains an IP address or hostname of a UAC (User Agent Client) appended to the Call-ID value.

A user agent executing a user-level privacy function on its own SHOULD substitute for the IP address or hostname that is frequently appended to the Call-ID value a suitably long random value (the value used as the 'tag' for the From header of the request might even be reused) as indicated in Section 4.1 in RFC 3323.

A privacy service MAY anonymize the Call-ID header when the request contains Privacy:user by substituting for the IP address or hostname in the Call-ID a suitably long random value (such as a From tag value) so that it is sufficiently unique as indicated in Section 5.3 in RFC 3323.

Call-ID is essential to dialog matching, so any time a privacy service modifies this field, it MUST retain the former value and restore it in a Call-ID header in any messages that are sent to/by the originating user agent inside the dialog as indicated in Section 5.3 in RFC 3323. A privacy service should be prepared to receive a request outside the dialog containing the value of the Call-ID set by the PS in other SIP headers (e.g., In-Reply-To/Replaces/ Target-Dialog), at least while the dialog state is active for the dialog whose Call-ID was modified by that PS. When such a request is received, the Call-ID value contained in the relevant headers indicated above should be replaced by the retained value.

Note: This is possible only if the privacy service maintains the state and retains all the information it modified to provide privacy. Some PSs are known to encrypt information prior to obfuscation in the Via header, etc. In this case, the PS cannot correlate the modified Call-ID value with the original Call-ID. Further challenges are imposed when the PS needs to stay on a signaling path to ensure that it receives all the messages targeted towards the caller for which a PS provides privacy, especially when the request is out-of-dialog.

Refer to the corresponding sections, 5.1.6 (In-Reply-To), 5.3.3 (Replaces Header/Parameter), and 5.3.6 (Target-Dialog), for detailed discussion.

5.1.2. Call-Info

This field contains additional information about the user.

A user agent executing a user-level privacy function on its own SHOULD NOT add a Call-Info header as indicated in Section 4.1 in RFC 3323.

A privacy service MUST delete a Call-Info header if one exists when user privacy is requested with Privacy:user as indicated in Section 5.3 in RFC 3323. A privacy service SHOULD NOT add a Call-Info header when user privacy is requested with Privacy:header as indicated in Section 5.1 in RFC 3323.

5.1.3. Contact

This field contains a URI used to reach the user agent for mid-dialog requests and possibly out-of-dialog requests, such as REFER [RFC3315]. Since the Contact header is essential for routing further requests to the user agent, it must include a functional URI even when it is anonymized.

A user agent MUST NOT anonymize a Contact header, unless it can obtain an IP address or contact address that is functional yet has a characteristic of anonymity as indicated in Section 4.1.1.3 in RFC 3323.

Since RFC 3323 was published, there have been proposals that allow UAs to obtain an IP address or contact address with a characteristic of anonymity.

The mechanisms that are discussed at the time of this writing are Globally Routable User Agent URIs (GRUU) [SIPGRUU], which provides a functional Contact address with a short life span, making it ideal for privacy sensitive calls, and Traversal Using Relays around NAT (TURN) [TURN], through which an IP address of a relay can be obtained for use in a Contact header.

A privacy service SHOULD anonymize a Contact header by replacing the existing Contact header field value with the URI that dereferences to the privacy service when user privacy is requested with Privacy:header, as indicated in Section 5.1 in RFC 3323. This is generally done by replacing the IP address or hostname with that of the privacy service.

5.1.4. From

This field contains the identity of the user, such as display-name and URI.

A user agent executing a user-level privacy function on its own SHOULD anonymize a From header using an anonymous display-name and an anonymous URI as indicated in Section 4.1 in RFC 3323.

A privacy service should anonymize a From header when user privacy is requested with Privacy:user.

Note: This does not prevent a privacy service from anonymizing the From header based on local policy.

The anonymous display-name and anonymous URI mentioned in this section use display-name "Anonymous", a URI with "anonymous" in the user portion of the From header, and the hostname value "anonymous.invalid" as indicated in Section 4.1.1.3 in RFC 3323.

The recommended form of the From header for anonymity is:

```
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=1928301774
```

The tag value varies from dialog to dialog, but the rest of this header form is recommended as shown.

5.1.5. History-Info

History-Info [RFC4244] header URIs to which the request was forwarded or retargeted can reveal general routing information.

A user agent executing a user-level privacy function on its own SHOULD NOT add a History-Info header as indicated in Section 3.3 in RFC 4244.

A privacy service SHOULD delete the History-Info headers when user privacy is requested with Privacy:header, Privacy:session, or Privacy:history as indicated in Section 3.3 in RFC 4244.

The privacy could be also expressed for a specific History-Info entry by inserting "privacy=history" in the History-Info header. In such a case, a privacy service SHOULD delete the History-Info entry as indicated in Section 4.3.3.1.1 in RFC 4244.

Refer to [RFC4244] for detailed behavior for dealing with History-Info headers.

5.1.6. In-Reply-To

The In-Reply-To header contains a Call-ID of the referenced dialog. The replying user may be identified by the Call-ID in an In-Reply-To header.

```
Alice > INV(Call-ID:C1) > Bob
Bob   > INV(In-Reply-To:C1) > Alice
```

In this case, unless the In-Reply-To header is deleted, Alice might notice that the replying user is Bob because Alice’s UA knows that the Call-ID relates to Bob.

A user agent executing a user-level privacy function on its own should not add an In-Reply-To header as implied in Section 4.1 in RFC 3323.

A privacy service MUST delete the In-Reply-To header when user privacy is requested with Privacy:user as indicated in Section 5.3 in RFC 3323.

In addition, since an In-Reply-To header contains the Call-ID of the dialog to which it is replying, special attention is required, as described in Section 5.1.1 (Call-ID), regardless of the priv-value or

presence of a Privacy header. Once a privacy service modifies a Call-ID in the request, a privacy service should restore the former value in an In-Reply-To header, if present in the INVITE request replying to the original request, as long as the privacy service maintains the dialog state.

Example:
Alice > INV(Call-ID:C1, Privacy:user) > PS > INV(Call-ID:C2) > Bob
Bob > INV(In-Reply-To:C2, Privacy:none) > PS >
INV(In-Reply-To:C1) > Alice

Note: This is possible only if the privacy service maintains the state and retains all the information that it modified to provide privacy even after the dialog has been terminated, which is unlikely. Call-back is difficult to achieve when a privacy service is involved in forming the dialog to be referenced.

5.1.7. Organization

This field contains additional information about the user.

A user agent executing a user-level privacy function on its own should not add an Organization header as implied in Section 4.1 in RFC 3323.

A privacy service MUST delete the Organization header if one exists when user privacy is requested with Privacy:user as indicated in Section 5.3 in RFC 3323. A privacy service SHOULD NOT add an Organization header when user privacy is requested with Privacy: header as indicated in Section 5.1 in RFC 3323.

5.1.8. P-Asserted-Identity

This header contains a network-verified and network-asserted identity of the user sending a SIP message.

A privacy service MUST delete the P-Asserted-Identity headers when user privacy is requested with Privacy:id as indicated in Section 7 in RFC 3325 and should delete the P-Asserted-Identity headers when user privacy is requested with Privacy:header before it forwards the message to an entity that is not trusted.

It is recommended for a privacy service to remove the P-Asserted-Identity header if user privacy is requested with Privacy:id or Privacy:header even when forwarding to a trusted entity, unless it can be confident that the message will not be routed to an untrusted entity without going through another privacy service.

5.1.9. Record-Route

This field may reveal information about the administrative domain of the user.

In order to hide Record-Route headers while keeping routability to the sender, privacy services can execute a practice referred to as "stripping". Stripping means removing all the Record-Route headers that have been added to the request prior to its arrival at the privacy service and then adding a single Record-Route header representing itself. In this case, the privacy service needs to retain the removed headers and restore them in a response.

Alternatively, privacy services can remove the Record-Route headers and encrypt them into a single Record-Route header field. In this case, the privacy service needs to decrypt the header and restore the former values in a response.

A privacy service SHOULD strip or encrypt any Record-Route headers that have been added to a message before it reaches the privacy service when user privacy is requested with Privacy:header as indicated in Section 5.1 in RFC 3323.

As in the case of a Call-ID, if a privacy service modifies the Record-Route headers, it MUST be able to restore Route headers with retained values as indicated in Section 5.1 in RFC 3323. Some examples where the restoration of the Route headers is necessary and unnecessary are given below.

When a UAC (Alice) requires privacy for a request, a privacy service does not have to restore the Route headers in the subsequent request (see Example 1).

On the other hand, when a UAS (User Agent Server) (Bob) requires privacy for a response, a privacy service has to restore the Route headers in the subsequent request (see Example 2).

Example 1:
Restoration of Route header is UNNECESSARY when UAC requires privacy

```
Alice > INV(Privacy:header) > P1 >
        INV(Record-Route:P1, Privacy:header) > PS >
        INV(Record-Route:PS) > P2 >
        INV(Record-Route:P2,PS) > Bob
Bob   > 200(Record-Route:P2,PS) > P2 > PS >
        200(Record-Route:P2,PS,P1) > P1 > Alice
Alice > re-INV(Route:P2,PS,P1, Privacy:header) > P1 >
        re-INV(Route:P2,PS, Privacy:header) > PS >
        re-INV(Route:P2) > P2 > re-INV > Bob
```

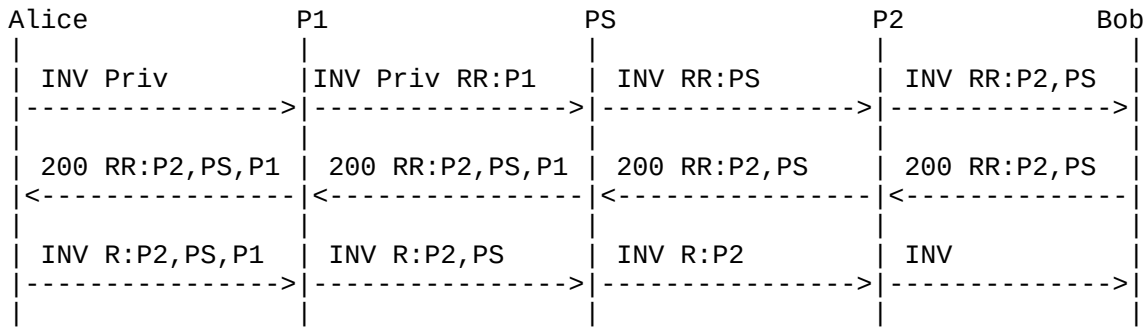

Figure 1: Example when restoration of Route header is UNNECESSARY

Example 2:
Restoration of Route header is NECESSARY when UAS requires privacy
Alice > INV > P1 > INV(Record-Route:P1) > P2 >
INV(Record-Route:P2,P1) > Bob
Bob > 200(Record-Route:P2,P1, Privacy:header) > P2 > PS' >
200(Record-Route:PS',P1) > P1 > Alice
Alice > re-INV(Route:PS',P1) > P1 > re-INV(Route:PS') > PS' >
re-INV(Route:P2) > P2 > Bob

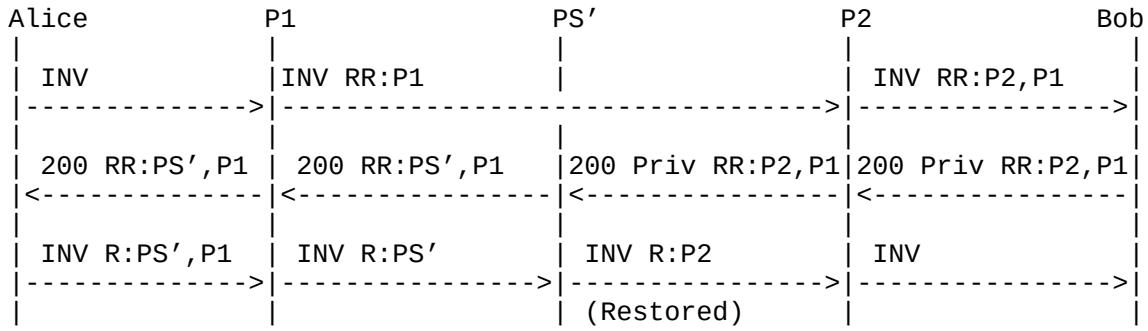

Figure 2: Example when restoration of Route header is NECESSARY

Note: In Figures 1 and 2, Priv means Privacy:header, RR means Record-Route header, and R means Route header.

5.1.10. Referred-By

The Referred-By [RFC3892] header carries a SIP URI representing the identity of the referrer.

The Referred-By header is an anonymization target when the REFER request with the Referred-By header is sent by the user (referrer) whose privacy is requested to be processed in the privacy service.

A user agent that constructs REFER requests executing a user-level privacy function on its own should anonymize a Referred-By header by using an anonymous URI.

A privacy service should anonymize a Referred-By header in a REFER request by using an anonymous URI when user privacy is requested with Privacy:user.

On the other hand, the Referred-By header is not an anonymization target when it appears in a request other than REFER (e.g., INVITE) because the URI in the Referred-By header does not represent the sender of the request.

Example 1:
Referrer requests no privacy and referee requests privacy

```
Alice > REF(Referred-By:Alice) > Bob
Bob   > INV(Referred-By:Alice, Privacy:user) > PS >
        INV(Referred-By:Alice) > Carol
```

Example 2:
Referrer requests privacy and referee requests privacy

```
Alice > REF(Referred-By:Alice, Privacy:user) > PS >
        REF(Referred-By:X) > Bob
Bob   > INV(Referred-By:X, Privacy:user) > PS >
        INV(Referred-By:X) > Carol
```

5.1.11. Reply-To

This field contains a URI that can be used to reach the user on subsequent call-backs.

A user agent executing a user-level privacy function on its own should not add a Reply-To header in the message as implied in Section 4.1 in RFC 3323.

A privacy service MUST delete a Reply-To header when user privacy is requested with Privacy:user as indicated in Section 5.3 in RFC 3323.

5.1.12. Server

This field contains information about the software used by the UAS to handle the request.

A user agent executing a user-level privacy function on its own should not add a Server header in the response as implied in Section 4.1 in RFC 3323.

A privacy service must delete a Server header in a response when user privacy is requested with Privacy:user. A privacy service SHOULD NOT add a Server header in a response when user privacy is requested with Privacy:header as indicated in Section 5.1 in RFC 3323.

5.1.13. Subject

This field contains free-form text about the subject of the call. It may include text describing something about the user.

A user agent executing a user-level privacy function on its own should not include any information identifying the caller in a Subject header.

A privacy service MUST delete a Subject header when user privacy is requested with Privacy:user as indicated in Section 5.3 in RFC 3323.

5.1.14. User-Agent

This field contains the UAC’s information.

A user agent executing a user-level privacy function on its own should not add a User-Agent header as implied in Section 4.1 in RFC 3323.

A privacy service MUST delete a User-Agent header when user privacy is requested with Privacy:user as indicated in Section 5.3 in RFC 3323.

5.1.15. Via

The bottommost Via header added by a user agent contains the IP address and port or hostname that are used to reach the user agent for responses. Via headers added by proxies may reveal information about the administrative domain of the user.

A user agent MUST NOT anonymize a Via header as indicated in Section 4.1.1.3 in RFC 3323, unless it can obtain an IP address that is functional yet has a characteristic of anonymity. This may be possible by obtaining an IP address specifically for this purpose either from the service provider or through features such as TURN.

A privacy service SHOULD strip or encrypt any Via headers that have been added prior to reaching the privacy service when user privacy is requested with Privacy:header as indicated in Section 5.1 in RFC 3323. Refer to Section 5.1.9 (Record-Route) for details of stripping and encryption.

A privacy service MUST restore the original values of Via headers when handling a response in order to route the response to the originator as indicated in Section 5.1 in RFC 3323.

No Via stripping is required when handling responses.

5.1.16. Warning

This field may contain the hostname of the UAS.

A user agent executing a user-level privacy function on its own should not include the hostname representing its identity in a Warning header.

A privacy service should anonymize a Warning header by deleting the hostname portion (if it represents a UAS's identity) from the header when user privacy is requested with Privacy:user.

5.2. Target SDP Parameters

This section describes privacy considerations for each SDP [RFC4566] parameter that may reveal information about the user.

When privacy functions for user-inserted information are requested to be executed at a privacy service, user agents MUST NOT encrypt SDP bodies in messages as indicated in Section 4.2 in RFC 3323.

5.2.1. c/m Lines

The c and m lines in the SDP body convey the IP address and port for receiving media.

A user agent must not anonymize the IP address and port in the c and m lines, unless it can obtain an IP address that is functional yet has a characteristic of anonymity as implied in Section 4.1.1.3 in RFC 3323. This may be possible by obtaining an IP address specifically for this purpose either from the service provider or through features such as TURN.

A privacy service must anonymize the IP address and port in c and m lines using a functional anonymous IP address and port when user privacy is requested with Privacy:session. This is generally done by replacing the IP address and port present in the SDP with that of a relay server.

5.2.2. o Line

The username and IP address in this parameter may reveal information about the user.

A user agent may anonymize the username in an o line by setting username to "-" and anonymize the IP address in the o line by replacing it with a value so that it is sufficiently unique.

A privacy service must anonymize the username and IP address in the o line by setting the username to "-" and replacing the IP address with a value so that it is sufficiently unique when user privacy is requested with Privacy:session.

5.2.3. i/u/e/p Lines

These lines may contain information about the user.

A user agent executing a session-level privacy function on its own should not include user's information in the i, u, e, and p lines.

A privacy service should modify the i, u, e, and p lines to delete the user's identity information when user privacy is requested with Privacy:session.

5.3. Considerations for Non-Target SIP Headers/Parameters

5.3.1. Identity/Identity-Info

The Identity [RFC4474] header field contains a signature used for validating the identity. The Identity-Info header field contains a reference to the certificate of the signer of Identity headers. An Identity-Info header may reveal information about the administrative domain of the user.

The signature in an Identity header provides integrity protection over the From, To, Call-ID, Cseq, Date, and Contact headers and over the message body. The integrity protection is violated if a privacy service modifies these headers and/or the message body for the purpose of user privacy protection.

Once those integrity-protected headers (such as From and Call-ID) are modified, the Identity/Identity-Info header fields are not valid any more. Thus, a privacy service acting on a request for Privacy:user, Privacy:header, or Privacy:session can invalidate integrity protection provided by an upstream authentication service that has inserted Identity/Identity-Info header fields. The use of such a privacy service should be avoided if integrity protect needs to be

retained. Otherwise, if the privacy service invalidates the integrity protection, it should remove the Identity/Identity-Info header fields.

An authentication service downstream of the privacy service may add Identity/Identity-Info header fields if the domain name of the From header field URI has not been anonymized (e.g., 'sip:anonymous@example.com'), which makes it possible for the service to authenticate the UAC. This authenticated yet anonymous From header means "this is a known user in my domain that I have authenticated, but I am keeping its identity private" as indicated in Section 12 in RFC 4474.

The desired deployment will have a privacy service located before or co-located with the identity service; thus, integrity and privacy can both be provided seamlessly.

5.3.2. Path

This field may contain information about the administrative domain and/or the visited domain of the user agent. However, the Path header is not the target of any priv-values.

Given that the Path header [RFC3327] only appears in REGISTER requests/responses and is essential for a call to reach the registered UA in the visited domain, it serves no purpose to withhold or hide the information contained in the Path header; rather, it is harmful.

The only reason privacy may be considered desirable is if the visited domain wants to withhold its topology from the home domain of the user. In doing so, the domain withholding the topology needs to ensure that it provides sufficient information so that the home domain can route the call to the visited domain, thus reaching the UA.

However, anonymization of network-privacy-sensitive information is out of scope.

5.3.3. Replaces Header/Parameter

The Replaces [RFC3891] header and the "replaces" parameter contain identifiers of a dialog to be replaced, which are composed of Call-ID, local tag, and remote tag.

The sender of the INVITE with a Replaces header is usually not the originating user agent or terminating user agent of the target dialog to be replaced. Therefore, the Call-ID within the Replaces header is unlikely to be generated by the sender, and thus this header is outside the anonymization target per priv-value.

The "replaces" parameter, which appears in a Refer-To header in a REFER request, is not the target of any particular priv-values either. As described in Section 5.1.1 (Call-ID), regardless of the priv-value or the presence of a Privacy header, once a privacy service modifies a Call-ID in the request, it should monitor headers that may contain Call-ID and restore the portion of the value representing the modified Call-ID to the original Call-ID value in a Replaces header received.

The main challenge for this to function properly is that a privacy service has to be on a signaling path to the originator for every dialog. This is generally not possible and results in REFER requests not functioning at all times. This is a trade-off that is anticipated when privacy is imposed.

The privacy requirements mentioned in Section 5.1.1 will cause the Replaces header and "replaces" parameter to contain values that will fail the resulting dialog establishment in some situations. This loss of functionality is allowed and/or intended as illustrated above (i.e., it is not the responsibility of a privacy service to ensure that these features always work).

The functionality of the Replaces header/parameter when anonymized depends on the circumstances in which it is used. REFER may work or may not work depending on the following three criteria.

1. Who generated the Call-ID.
2. Where the privacy service is on the signaling path.
3. Who initiates the REFER with the "replaces" parameter.

A few examples that explore when the Replaces header/parameter works or fails are given below.

Example 1:
Transfer initiated by the originator, PS added for first INV and REF

```
Alice > INV(Call-ID:C1, Privacy:user) > PS > INV(Call-ID:C2) > Bob
Alice > REF(Refer-To:Bob?Replaces=C1, Privacy:user) > PS >
        REF(Refer-To:Bob?Replaces=C2) > Carol
Carol > INV(Replaces:C2) > Bob (SUCCEED)
```

Example 2:
Transfer initiated by the originator, PS added only for first INV
Alice > INV(Call-ID:C1, Privacy:user) > PS > INV(Call-ID:C2) > Bob
Alice > REF(Refer-To:Bob?Replaces=C1) > Carol
Carol > INV(Replaces:C1) > Bob (FAIL)

Note: Example 2 would succeed if the same PS (that modifies the Call-ID in the INVITE from Alice) is also added for REFER and modifies the value in the "replaces" parameter from C1 to C2 even if there is no Privacy header in the REFER.

Example 3:
Transfer initiated by the originator, PS added only for REF
Alice > INV(Call-ID:C1) > INV(Call-ID:C1) > Bob
Alice > REF(Refer-To:Bob?Replaces=C1, Privacy:user) > PS >
REF(Refer-To:Bob?Replaces=C1) > Carol
Carol > INV(Replaces:C1, Privacy:user) > PS' >
INV(Replaces:C1) > Bob (SUCCEED)

Example 4:
Transfer initiated by the terminating party, PS added for both INV
Alice > INV(Call-ID:C1, Privacy:user) > PS > INV(Call-ID:C2) > Bob
Bob > REF(Refer-To:Alice?Replaces=C2) > Carol
Carol > INV(Replaces:C2) > PS > INV(Replaces:C1) > Alice (SUCCEED)

Note: Example 4 succeeds because the same PS (that modifies the Call-ID in the INVITE from Alice) checks the incoming requests and modifies the value in a Replaces header in the INVITE from Carol to the former value of Call-ID (C1).

Example 5:
Hold, PS added only for first INV
Alice > INV(Call-ID:C1, Privacy:user) > PS > INV(Call-ID:C2) > Bob
Alice > REF(Refer-To:Bob?Replaces=C1) > Music-Server
Music-Server > INV(Replaces:C1) > Bob (FAIL)

Note: Example 5 would succeed if the same PS (that modifies the Call-ID in the INVITE from Alice) is added for the INVITE from the Music-Server and modifies the value in a Replaces header from C1 to C2.

As the above examples show, in some scenarios, information carried in the Replaces header/parameter would result in failure of the REFER. This will not happen if the Call-ID is not modified at a privacy service.

5.3.4. Route

This field may contain information about the administrative domain of the user agent, but the Route header is not the target of any priv-values.

Route headers appear only in SIP requests to force routing through the listed set of proxies. If a privacy service anonymizes the Route header, the routing does not function. Furthermore, there is no risk in revealing the information in the Route headers to further network entities, including the terminating user agent, because a proxy removes the value from the Route header when it replaces the value in the Request-URI as defined in RFC 3261.

A privacy service that modifies Record-Route headers may need to restore the values in Route headers as necessary. As indicated in Section 5.1 in RFC 3323, if a privacy service modifies the Record-Route headers, it MUST be able to restore Route headers with retained values. Please refer to Section 5.1.9 (Record-Route) for further detail and examples.

5.3.5. Service-Route

Service-Route headers [RFC3608] appear only in 200 OK responses to REGISTER requests and contain information about the registrar. The purpose of the privacy mechanism defined in RFC 3323 is to secure the user's privacy, so the case where a registrar sets a Privacy header is not considered here. Therefore, the Service-Route header is not the target of any priv-values.

5.3.6. Target-Dialog

The Target-Dialog [RFC4538] header faces exactly the same issues as seen for the Replaces header. Please refer to Section 5.3.3 (Replaces Header/Parameter) for why this is not a target for any particular priv-values and how a privacy service still needs to evaluate and modify the value contained, even if no privacy is requested.

6. Security Considerations

This guideline document adds no new security considerations to those discussed in [RFC3323], [RFC3325], and [RFC4244].

7. Acknowledgements

The authors would like to thank John Elwell, Jon Peterson, Jonathan Rosenberg, Mary Barnes, Paul Kyzivat, and Roland Jesske for their reviews and comments.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3261] 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.

[RFC3323] Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)", RFC 3323, November 2002.

[RFC3325] Jennings, C., Peterson, J., and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", RFC 3325, November 2002.

[RFC4244] Barnes, M., Ed., "An Extension to the Session Initiation Protocol (SIP) for Request History Information", RFC 4244, November 2005.

8.2. Informative References

[TURN] Rosenberg, J., Mahy, R., and P. Matthews, "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)", Work in Progress, July 2008.

[SIPGRUU] Rosenberg, J., "Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP)", RFC 5627, October 2009.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3327] Willis, D. and B. Hoeneisen, "Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts", RFC 3327, December 2002.

[RFC3608] Willis, D. and B. Hoeneisen, "Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration", RFC 3608, October 2003.

[RFC3891] Mahy, R., Biggs, B., and R. Dean, "The Session Initiation Protocol (SIP) "Replaces" Header", RFC 3891, September 2004.

[RFC3892] Sparks, R., "The Session Initiation Protocol (SIP) Referred-By Mechanism", RFC 3892, September 2004.

[RFC4474] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 4474, August 2006.

[RFC4538] Rosenberg, J., "Request Authorization through Dialog Identification in the Session Initiation Protocol (SIP)", RFC 4538, June 2006.

[RFC4566] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol", RFC 4566, July 2006.

Authors' Addresses

Mayumi Munakata
NTT Corporation

Phone: +81 422 36 7502
EMail: munakata.mayumi@lab.ntt.co.jp

Shida Schubert
NTT Corporation

EMail: shida@ntt-at.com

Takumi Ohba
NTT Corporation
9-11, Midori-cho 3-Chome
Musashino-shi, Tokyo 180-8585
Japan

Phone: +81 422 59 7748
EMail: ohba.takumi@lab.ntt.co.jp