| Section | SubSection | Page | No | Description | Statu |
|---|---|---|---|---|---|
| 4 | 4.1 | 8 | 1 | The first and most obvious step is that user agents **SHOULD NOT** include any optional headers that might divulge personal information; there's certainly no reason for a user seeking privacy to include a Call-Info. | S |
| 4 | 4.1 | 8 | 2 | Secondly, the user **SHOULD** populate URIs throughout the message in accordance with the guidelines given in Section 4.1.1. | S |
| 4 | 4.1 | 8 | 3 | For example, users SHOULD create an anonymous From header field for the request. | S |
| 4 | 4.1 | 8 | 4 | User agents **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). | S |
| 4 | 4.1.1.1 | 9 | 5 | It is **RECOMMENDED** that user agents seeking anonymity use a display-name of "Anonymous". | R |
| 4 | 4.1.1.3 | 10 | 6 | For these reasons, the hostname value 'anonymous.invalid' **SHOULD** be used for anonymous URIs (see [3] for more information about the reserved 'invalid' DNS TLD). | S |
| 4 | 4.1.1.3 | 10 | 7 | The full recommended form of the From header for anonymity is (note that this From header, like all others, **MUST** contain a valid and unique 'tag=' parameter): | M |
| 4 | 4.1.1.3 | 10 | 8 | For headers indicating how further requests in the current dialog should be routed (namely the Contact header, Via header, and session information in the SDP), there seems to be little that a user can do to disguise the existing URI, because users **MUST** provide a value that will allow them to receive further requests. | M |
| 4 | 4.1.1.3 | 10 | 9 | This document thus recommends that the host portion of URIs that are used in the routing of subsequent requests, such as URIs appearing in the Contact header, **SHOULD NOT** be altered by the user agent due to privacy considerations. | S |

| Section | SubSection | Page | No | Description | Statu |
|---|---|---|---|---|---|
| 4 | 4.2 | 11 | 10 | User agents **SHOULD** include a Privacy header when network-provided privacy (as described in Section 3.3) is required. | S |
| 4 | 4.2 | 11 | 11 | However, such intermediaries **SHOULD** only do so if they are operating at a user's behest, for example if a user has an administrative arrangement with the operator of the intermediary that it will add such a Privacy header. | S |
| 4 | 4.2 | 11 | 12 | An intermediary **MUST NOT** modify the Privacy header in any way if the 'none' priv-value is already specified. | M |
| 4 | 4.2 | 11 | 13 | When session privacy is requested, user agents **MUST NOT** encrypt SDP bodies in messages. | M |
| 4 | 4.3 | 12 | 14 | User agents MAY however set this privacy level for REGISTER requests, but **SHOULD NOT** set 'user' level privacy for other requests. | S |
| 4 | 4.3 | 12 | 15 | Intermediaries **MUST NOT** remove or alter a Privacy header whose priv-value is 'none'. | M |
| 4 | 4.3 | 12 | 16 | User agents **MUST NOT** populate any other priv-values (including 'critical') in a Privacy header that contains a value of 'none'. | M |
| 4 | 4.3 | 12 | 17 | When a Privacy header is constructed, it **MUST** consist of either the value 'none', or one or more of the values 'user', 'header' and 'session' (each of which **MUST** appear at most once) which MAY in turn be followed by the 'critical' indicator. | M |
| 4 | 4.3 | 12 | 18 | | M |

| Section | SubSection | Page | No | Description | Statu |
|---|---|---|---|---|---|
| 4 | 4.4 | 13 | 19 | It is **RECOMMENDED** that service providers couple the privacy service function with a local outbound proxy. | R |
| 4 | 4.4 | 13 | 20 | It is highly **RECOMMENDED** that user agents use network or transport layer security, such as TLS, when contacting a privacy service. | R |
| 4 | 4.4 | 13 | 21 | Ideally, users **SHOULD** establish a direct (i.e., single pre-loaded Route header) connection to a privacy service; this will both allow the user to inspect a certificate presented by the privacy service, and it will provide confidentiality for requests that will reduce the chances that the information that the privacy service will obscures is revealed before a message arrives at the privacy service. | S |
| 4 | 4.4 | 13 | 22 | If a direct connection is impossible, users **SHOULD** use a mechanism like SIPS to guarantee the use of lower-layer security all the way to the privacy service. | S |
| 4 | 4.4 | 13 | 23 | If a user agent believes that it is sending a request directly to a privacy service, it **SHOULD** include a Proxy-Require header containing a new option-tag, 'privacy', especially when the 'critical' priv-value is present in the Privacy header. | S |

| Section | SubSecti | Page | No | Description | Statu |
|---|---|---|---|---|---|
| 5 | | 15 | 1 | When a message arrives at a server that can act as a privacy service, the service **SHOULD** evaluate the level of privacy requested in a Privacy header. | S |
| 5 | | 15 | 2 | However, if the Privacy header value of 'none' is specified in a message, privacy services **MUST NOT** perform any privacy function and **MUST NOT** remove or modify the Privacy header. | M |
| 5 | | 15 | 3 | | M |
| 5 | | 15 | 4 | Privacy services **MUST** implement support for the 'none' and 'critical' privacy tokens, and MAY implement any of other privacy levels described in Section 4.2 as well as any extensions that are not detailed in this document. | M |
| 5 | | 15 | 5 | If the 'critical' privacy level is present in the Privacy header of a request, then if the privacy service is incapable of performing all of the levels of privacy specified in the Privacy header then it MUST fail the request with a 500 (Server Error) resp | M |
| 5 | | 15 | 6 | The reason phrase of the status line of the response **SHOULD** contain appropriate text indicating that there has been a privacy failure as well as an enumeration of the priv-value(s) which were not supported by the privacy service (the reason phrase **SHOULD** also respect any Accept-Language header in the request if possible). | S |
| 5 | | 15 | 7 | | S |
| 5 | | 15 | 8 | When a privacy service performs one of the functions corresponding to a privacy level listed in the Privacy header, it **SHOULD** remove the corresponding priv-value from the Privacy header - otherwise, any other privacy service involved with routing this mes | S |
| 5 | | 15 | 9 | When the last priv-value (not counting 'critical') has been removed from the Privacy header, the entire Privacy header **MUST** be removed from a message. | M |

| Section | SubSecti | Page | No | Description | Statu |
|---|---|---|---|---|---|
| 5 | | 15 | 10 | When the privacy service removes the entire Privacy header, if the message is a request, the privacy service **MUST** also remove any 'privacy' option-tag from the Proxy-Require header field of the request. | M |
| 5 | 5.1 | 16 | 11 | Firstly, a request for header privacy entails that the server **SHOULD NOT** add any headers to the message that reveal any identity or personal information, including the following: Call-Info, Server, and Organization. | S |
| 5 | 5.1 | 16 | 12 | Privacy services operating on requests **SHOULD** remove all Via headers that have been added to the request prior to its arrival at the privacy service (a practice referred to as "Via stripping") and then **SHOULD** add a single Via header representing themselve | S |
| 5 | 5.1 | 16 | 13 | | S |
| 5 | 5.1 | 16 | 14 | A privacy service **SHOULD** replace the value of the Contact header in a message with a URI that does not dereference to the originator of the message (such as the anonymous URI described in Section 4.1.1.3). | S |
| 5 | 5.1 | 16 | 15 | The URI that replaces the existing Contact header field value **MUST** dereference to the privacy service. | M |
| 5 | 5.1 | 16 | 16 | In a manner similar to Via stripping, a privacy service SHOULD also strip any Record-Route headers that have been added to a request before it reaches the privacy service - though note that no such headers will be present if there is only one hop between | S |
| 5 | 5.1 | 16 | 17 | When further requests or responses associated with the dialog reach the privacy service, it **MUST** restore values for the Via, Record-Route/Route or Contact headers that it has previously removed in the interests of privacy. | M |
| 5 | 5.2 | 17 | 18 | The following procedures are **RECOMMENDED** for handling the Record-Route header field of requests and responses, which provides specialchallenges to a privacy service: | R |

| Section | SubSecti | Page | No | Description | Statu |
|---|---|---|---|---|---|
| 5 | 5.2 | 17 | 19 | The privacy service logical role MUST therefore act as a back-to-back user agent in order to provide media privacy, effectively terminating and re-originating the messages that initiate a session (although in support of session privacy the privacy service | M |
| 5 | 5.2 | 18 | 20 | For that reason, requesting session-level privacy without resort to some sort of end-to-end security for the session traffic (with RTP [6] media, for example, SRTP [4]) is **NOT RECOMMENDED**. | R |
| 5 | 5.3 | 18 | 21 | Note that the privacy service **MUST** remove any non-essential informational headers that have been added by the user agent, including the Subject, Call-Info, Organization, User-Agent, Reply-To and In-Reply-To. | M |
| 5 | 5.3 | 18 | 22 | Therefore, any time that a privacy service needs to modify any dialog-matching headers for privacy reasons, it **SHOULD** act as a transparent back-to-back user agent, and it **MUST** persist the former values of the dialog-matching headers. | S |
| 5 | 5.3 | 18 | 23 | | M |
| 5 | 5.3 | 18 | 24 | These values **MUST** be restored in any messages that are sent to the originating user agent. | M |