



Cisco BTS 10200 Softswitch SIP Privacy Header Feature Module

Revised: July 31, 2008

This document describes the Session Initiation Protocol (SIP) Privacy Header feature for Release 6.0 of the Cisco BTS 10200 Softswitch. It includes the following topics:

- [Understanding the SIP Privacy Header Feature](#)
- [Feature Considerations](#)
- [Provisioning](#)

Understanding the SIP Privacy Header Feature

The SIP Privacy Header feature provides privacy services to the caller to withhold personal information (caller details) from the parties involved in a call. This feature enables the user to request privacy functions from the Cisco BTS 10200 operating as a SIP network-based privacy service.

This feature allows the Cisco BTS 10200 SIP interface to apply privacy services using the Privacy header (as defined in RFC 3323). The Privacy header is received by Cisco BTS 10200 from an originator requesting privacy or from a SIP proxy on the originator's behalf. If privacy services are requested, they are applied to an initial INVITE message sent out on a SIP trunk or sent towards a terminating SIP subscriber.

This feature does the following:

- Applies privacy services exclusively to initial INVITE requests sent from a Cisco BTS 10200 SIP interface
- Provides support for privacy by interpreting the set of services requested in the Privacy header
- Allows to set the calling number restriction when the Cisco BTS 10200 SIP interface receives the initial INVITE requests



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2008 Cisco Systems, Inc. All rights reserved.

When privacy is requested and applied, Cisco BTS 10200 adds privacy information to the initial outbound INVITE request. It assigns anonymous entries to the user, the display name, and host field of the From header and the user field of the Contact header. A single VIA header is set with the host name of this local Cisco BTS 10200 (this follows normal back-to-back user agent behavior).

When privacy is applied, Cisco BTS 10200 provides anonymous entries to the Form header and the User field of the Contact header, as shown here:

```
FROM: "Anonymous" sip:Anonymous@Anonymous.invalid;tag=AParty
Via: <single VIA with local BTS host>
Contact: sip:Anonymous@localhost:5060
```

SIP Signaling Details

In SS7-to-SIP calls on Cisco BTS 10200, the user and header privacy services are applied to the outbound SIP INVITE message, if restrictions are applied to the calling name and number fields.

For SIP-to-SIP calls on Cisco BTS 10200, the header level privacy is always applied to initial outbound SIP INVITE messages. If header level privacy is requested, the header privacy token is handled in the following way:

- The privacy services are enabled. It is assumed that the header level privacy is applied. The token is removed from the Privacy header.
- If the privacy services are not enabled, the Cisco BTS 10200 indicates that header level privacy was not applied, even though the back-to-back user agent (UA) operations implicitly provided that level of privacy. The token remains on the privacy header.



Note

This feature does not support a session level privacy service because Cisco BTS 10200 does not terminate or manage the media path. In case of SIP-to-SIP trunk calls, Cisco BTS 10200 passes the privacy token and any of the privacy services to the Cisco BTS 10200 SIP interface (which does not render).

The Cisco BTS 10200 SIP interface applies the user level privacy to the outbound SIP INVITE request if any privacy services are requested, even if the user privacy was applied previously by the originator. Privacy services are not applied under the following conditions:

- If the ID privacy service is requested, the P-Asserted-ID (PAID) header (as defined in RFC 3325) is not sent to local SIP subscribers. The Cisco BTS 10200 SIP trunks are assumed to be pointing towards trusted SIP devices. Therefore, the PAID header is always sent out to the SIP trunks (assuming that the SIP trunk is provisioned to allow sending the PAID header).
- If the NONE privacy service is requested, Cisco BTS 10200 does not apply privacy services. In this case, if the call is routed out a SIP trunk, the Privacy header passes the NONE token outbound without modification.
- The Cisco BTS 10200 ignores the Proxy-Require header that requests the privacy service for incoming messages. This header is not passed through in a SIP-to-SIP call through the Cisco BTS 10200.
- For an outbound SIP trunk call, privacy services requested from the originator which are not rendered by the Cisco BTS 10200 SIP interface are represented in the Privacy header as remaining tokens and forwarded to the next SIP device. For an outbound SIP subscriber call, the Privacy header is not sent under any condition.

In general, the Cisco BTS 10200 does not add privacy services to initial outbound INVITE messages. However, if a SIP trunk is provisioned to send the PAID header, and the calling number presentations are restricted, then the Privacy header with ID token is sent in the INVITE request. This was Cisco BTS 10200 behavior maintained prior to this feature.

PRIVACY Token

The PRIVACY token is in the SUBSCRIBER table. NONE is a value that can be set for the PRIVACY token. When the user requests that no privacy services be applied, the PRIVACY token with a NONE value is applied in the originating device, regardless of provisioning or defaults.

**Note**

For SIP-to-SIP calls, the PRIVACY token is passed through if the call is routed out a SIP trunk on the Cisco BTS 10200.

Privacy services are not applied on the terminating SIP side when the PRIVACY token with a NONE value is received, regardless of any provisioning settings or privacy indications.

When the Cisco BTS 10200 receives the PRIVACY token with a NONE value, the following conditions hold true:

- The PRIVACY token does not affect the Cisco BTS 10200 SIP interface configuration that involves the selection of FROM or PAID SIP headers for deriving call information when a SIP call is received.
- If a Cisco BTS 10200 SIP interface is provisioned to interpret the calling party using the PAID header when an initial INVITE is received, the calling name and number presentations are set to Allowed.
- If a Cisco BTS 10200 SIP interface is provisioned to interpret the calling party using the FROM header when an initial INVITE is received, the PRIVACY token does not affect how the calling name and number are mapped by the FROM header.
- When the user terminates the SIP calls from the Cisco BTS 10200 SIP interface, the PRIVACY token does not affect how the calling name and number presentations are applied in the FROM or PAID headers towards that terminated calls.

**Note**

For more information on calling name and number mapping on the Cisco BTS 10200 SIP interface, check with technical support.

Feature Interactions

The SIP Privacy Header feature interacts with the Cisco BTS 10200 and SIP features. The TGID draft (R5) applies the TGID user information parameters in the contact header for outbound SIP trunks. When the privacy services are applied, the personal information of the user is removed because the user part of the contact header is anonymous.

Prerequisites

The user should have knowledge of RFC 3323 and RFC 3325 before using this feature.

Limitations

The SIP Privacy Header feature for Release 6.0 of the Cisco BTS 10200 Softswitch has the following limitations:

- The Cisco BTS 10200 does not support session level privacy because it does not terminate or manage the media path.
- All outbound SIP trunks are expected to be provisioned within the trusted domain. Therefore, Cisco BTS 10200 SIP trunks do not apply privacy services to the callers who are on different domains (as per RFC 3325).

Feature Considerations

The user has to consider the following points before using the SIP Privacy Header feature:

- In RFC 3323, the NONE token in the Privacy header is sent or received as a single token. It is invalid to send or receive the Privacy CRITICAL token as a single token.
- It is invalid to receive an anonymous or non-existent user information field in the PAID header, as the purpose of the PAID header is to assert an identity.
- The Cisco BTS 10200 SIP interface (in keeping with PacketCable 1.5) supports an anonymous name display field in the PAID header that indicates the restricted name.
- If the Privacy tokens "session" and "critical" are received and the call is routed towards a SIP subscriber, the call fails. This occurs because the Cisco BTS 10200 cannot apply the session privacy service, and there no intermediary switch that can route the call.

Provisioning

Use the following flags to provision the privacy services:

- [USE_PAI_HDR_FOR_ANI](#)
- [APPLY_USER_PRIVACY](#)
- [SIA_SUB_SEND_PAID_HDR](#)

USE_PAI_HDR_FOR_ANI

The USE_PAI_HDR_FOR_ANI flag is in the SOFTSW-TG_PROFILE table. If the customer wants the Privacy header feature to handle the privacy ID token on SIP trunks, the USE_PAI_HDR_FOR_ANI flag on the SIP trunk profile must be enabled. In the USE_PAI_HDR_FOR_ANI flag, the disable privacy service has the following conditions:

- When this flag is disabled, the ID token in the Privacy header and the entire PAID header are ignored if received, and they are not sent under any condition.
- When this flag is disabled, the ID token is not sent, regardless of the Privacy header feature enabled for outbound SIP trunks.

APPLY_USER_PRIVACY

The APPLY_USER_PRIVACY flag is in the SOFTSW-TG_PROFILE table. The APPLY_USER_PRIVACY SIP trunk profile flag can enable or disable privacy services on the terminating SIP trunk. If the originator requests a privacy service, the calling party information in the initial outbound SIP INVITE is set to anonymous, in order to hide the caller identity. Privacy is requested when the calling party name and/or number indicate presentation restrictions. Privacy is also requested when the Cisco BTS 10200 SIP interface receives a SIP call with a Privacy header containing privacy service requests. Regardless of what privacy function is requested, the Cisco BTS 10200 SIP interface provides only User and Header level privacy.

SIA_SUB_SEND_PAID_HDR

A new flag SIA_SUB_SEND_PAID_HDR is added to the CA-CONFIG table. This flag can have a Yes (Y) or No (N) value. The default value is N (default disabled). Use this flag to determine if the PAID header is sent to SIP subscribers. If the flag is enabled, the PAID header is sent if the calling party screening indicator is set to “network provided”, and the Privacy: ID token did not exist in the originating message. This flag applies only to terminating SIP subscribers.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

Copyright © 2008 Cisco Systems, Inc. All rights reserved.

