

ST AS Identity Presentation Service Management Guide

MTAS

USER GUIDE

Copyright

© Ericsson AB 2016, 2017. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Introduction	1
1.1	Prerequisites	1
2	Overview	3
2.1	Subfunctions	4
2.2	Traffic View	6
2.3	Configuration View	7
2.4	Interaction with Other Services	7
3	ST AS Identity Presentation Service Configuration	9
3.1	Configuration Activities	9
3.2	Identity Presentation Administrative State Configuration	10
3.3	Reason for Lack of Caller Identity Configuration	10
3.4	Service Data Configuration	10
4	Performance Management	15
5	Fault Management	17





1 Introduction

This document describes how to configure the SIP Trunking Application Server (ST AS) Identity Presentation service in MTAS.

It also describes how this service is co-located with other services in the ST AS, for example, ST AS Communication Diversion (CDIV) and ST AS Communication Barring (CB), and describes the interaction between them.

1.1 Prerequisites

It is assumed that the user of this document is familiar with the Operation and Maintenance (O&M) area, in general.

1.1.1 Licenses

To enable the ST AS Identity Presentation feature, the ST AS Base license must be installed.

For more information about the ST AS Base license, refer to *MTAS Licenses*.

1.1.2 Documents

Before starting any procedure in this document, ensure that the following documents are available:

- *Ericsson Command-Line Interface User Guide*
- *Managed Object Model (MOM)*

1.1.3 Conditions

The following condition must apply:

- An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.





2 Overview

The purpose of the ST AS Identity Presentation services and their subfunctions is to enable or restrict presentation of identities in a communication based on the participant preference, information received at the initiation of the communication and information received in each message.

ST AS Identity Presentation service consists of the following:

- Originating Identity Presentation (OIP)
- Originating Identity Restriction (OIR)
- Terminating Identity Presentation (TIP)
- Terminating Identity Restriction (TIR)

The OIP and TIP services enable presentation of the identities of participants in a communication to the other participants and are executed on behalf of the terminating Private Branch Exchange (PBX).

The OIR and TIR services enable a participant to withhold their identity information from the other participants and are executed on behalf of the originating PBX.

The restriction by OIR service can be overridden by the OIP service for participants with the override option. The restriction by TIR service can be overridden by the TIP service for participants with the override option. The purpose of this override option is to serve needs of special categories of users like Law Enforcement Agencies and health sector.

In an IP Multimedia Subsystem (IMS) network, several entities are needed to realize the Identity Presentation services. The main logic is concentrated to the ST AS, but because certain signaling information must be preserved in the IMS network, the ST AS cannot remove all user identities directly. Other nodes, like the Call Session Control Functions (CSCFs), are part of the complete solution and responsible for deleting parts of the user identification elements. The terminals are also part of the complete solution, but since the terminals are not part of the operator trusted domain, the enforcement of identity presentation policies resides in the IMS core network and the ST AS.

For a description of their behavior, refer to the following protocol specifications *3GPP TS 24.607 v8.3.0*.

The ST AS Identity Presentation is based on the Session Initiation Protocol (SIP) `Privacy` header information. Different values of the `Privacy` header specify which type of privacy is requested. The values that are supported by ST AS are listed in Table 1.

*Table 1 Privacy Header Values Supported by ST AS*

Privacy Header Value	Headers
none	No privacy is requested.
id	“Network asserted user identity” privacy. This involves P-Asserted-Identity headers.
user	“Headers added by the user” privacy. This involves From header.
header	“Headers added by the network” privacy. This involves, for example, through and Record Route headers.

Note: Values other than those listed in Table 1 are handled as if no privacy is requested.

If communication to a PBX is diverted, all the Presentation Identity services must be executed on behalf of the diverted PBX. When AS chaining is disabled, OIR is executed directly in the terminating ST AS, which then acts in a transit role. When AS chaining is enabled, the request is returned to Serving CSCF (S-CSCF) after retargeting by the diversion service so that the OIR service can be executed in an appropriate originating AS.

For more information about Originating AS chaining, refer to *MTAS SIP Trunking Management Guide*.

2.1 Subfunctions

This section describes the subfunctions of the ST AS Identity Presentation service.

The different ST AS Identity Presentation subfunctions are started on originating, transit, and terminating MTAS, see Table 2.

Table 2 Invocation of Subfunctions

Subfunction	MTAS Type
OIP	Terminating
OIR	Originating
	Transit (AS chaining disabled)
TIP	Terminating
TIR	Originating
	Transit (AS chaining disabled)



2.1.1 Originating Identity Presentation

The OIP enables for a terminating PBX to see the identity of the Originating User as the result of receiving SIP messages. If identity restriction is indicated in the received messages, several headers are deleted or anonymized. If the override option of OIP is not active, then any requests to restrict the identity is ignored.

The identity in the `From` header can be presented in a locally dialable format, unless it has been previously anonymized. This feature is controlled by configuration of the OIP service and requires that the PBX is provisioned with Country Code (CC) and Area Code (AC).

To ensure that the `To` header is identical to the target identity, it is possible to configure the OIP to copy the content of the `Request-URI` to the `To` header.

The OIP can be used to provide the reason indication for restriction of caller identity to the terminating network by mapping the reason indication from the `P-Asserted-Identity` header display-name portion to the `From` header display-name portion. This feature is controlled by configuration of the OIP service.

2.1.2 Originating Identity Restriction

The OIR enables an originating PBX to restrict the presentation of the identity to the terminating user.

The service exists in two modes; permanent and temporary. It further supports two levels of restriction, “asserted identity” and “all private information”.

In the temporary mode, the default OIR action is provisioned for the PBX. The default action can be either to restrict or not restrict the presentation of the PBX identity. The PBX user can override the default action by including a `Privacy` header in SIP messages that it originates. This allows the PBX to either present or restrict the identity on a call by call basis, or message by message basis.

In permanent mode, the OIR action is always set to restrict the presentation of the PBX identity.

If the `From` header screening is enabled on PBX or node level, the OIR overwrites the content of the `P-Asserted-Identity` with the `From` header. The `From` header screening is controlled by a configuration on node level and by provisioning data in HSS for OIR on PBX level. Provisioned data in HSS if present, overrides the node level configuration.

The service can be used to provide the reason for restriction of caller identity for the terminating network by setting the display-name of the `P-Asserted-Identity` header. The reason for restriction of caller identity owing to active OIR is indicated by the `P-Asserted-Identity` header URI display-name portions set to “Anonymous”.



2.1.3 TIP

The TIP makes it possible for an originating PBX to see the identity of the terminating user as the result of receiving SIP messages. If identity restriction is indicated in the received messages, several headers are removed or anonymized. Unless the override option of TIP is active, in which case any requests to restrict the identity are ignored.

When TIP is active and the initial `INVITE` contains the “from-change” option tag in the `Supported` header, the PBX can receive a new `From` header in an `UPDATE` or `INVITE` request.

2.1.4 TIR

The TIR makes it possible for a terminating PBX to restrict the presentation of the identity to the originating user.

The service exists in two modes; permanent and temporary. It further supports one level of restriction; “asserted identity”.

In the temporary mode, the default TIR action is provisioned for the PBX. The default action can be either to restrict or to not restrict the presentation of the PBX identity. The PBX user can override the default action by including a `Privacy` header in SIP messages that it originates. This allows the PBX to either present or restrict the identity on a call by call basis, or message by message basis.

In permanent mode, the TIR action is always set to restrict the presentation of the PBX identity.

When TIR is not in permanent mode, “connected identity support” is enabled and the initial `INVITE` contains the “from-change” option tag in the `Supported` header, the PBX can add the “from-change” option tag in the `Supported` header in a response to the initial `INVITE`. When the response includes the “from-change” tag, the PBX can send an `UPDATE` or `INVITE` with a changed `From` header.

2.2 Traffic View

ST AS Identity Presentation performs the following steps that are the same for all subfunctions:

- Service invocation, an event triggers the execution of Identity Presentation, for example, incoming `INVITE`.
- Service execution, Identity Presentation evaluates the settings of the served PBX, and determines if the identity is to be presented.

The different subfunctions of ST AS Identity Presentation are triggered by SIP events. The service settings are fetched from the Home Subscriber Server



(HSS) through the `Sh` interface, and evaluated together with the received SIP data by the function that determines if the identity is presented.

2.3 Configuration View

There are two categories of configuration, as follows:

- Node level configuration
- PBX subscription configuration

Node level configuration is performed by the operator who can lock and unlock the ST AS Identity Presentation service and modify its default behavior.

The PBX configuration is managed through the XML Document Management Server (XDMS) that provides the Customer Administration Interface Third Generation (CAI3G) interface to the operator. The XDMS uses Session Handler (`Sh`) Diameter to update the HSS. Through the CAI3G interface, the service data can be provisioned individually for each PBX. For the temporary mode, the default OIR action is set through PBX service data. The denormalization of the `From` header depends on the provisioning of country and area code in the PBX operator common data.

If the ST AS Identity Presentation function is locked on node level or disabled per PBX, all identity information is passed unchanged and the OIR requests are ignored.

2.4 Interaction with Other Services

This section describes the ST AS Identity Presentation service interaction with other ST AS services.

2.4.1 Charging

The OIR service in the originating ST AS node updates the “Calling Party Address Presentation Status” and “`From` Header Presentation Status” attributes used to generate charging records.

The TIR service at the terminating ST AS node updates the “Called Asserted Identity Presentation Status” stored attributes used to generate charging records.

For more information about the Charging service, refer to *Diameter Offline Charging in MTAS* and *Diameter Online Charging in MTAS*.



2.4.2 ST AS Communication Barring

The OIR Override service takes precedence over the ACR service. If the served user has the OIR Override service, no incoming request is treated as anonymous, even if `mtasStAcrGlobal` is enabled. For more information, see *ST AS Communication Barring Service Management Guide*.

2.4.3 ST AS Communication Diversion

The ST AS Communication Diversion (CDIV) interactions between the ST AS Identity Presentation and the ST AS CDIV services are described in *ST AS Communication Diversion Management Guide*.

2.4.4 ST AS Malicious Communication Identification

When an initial `INVITE` is received that matches the Global Identity Presentation Restriction List, and the served user has the OIP service active, and override is not active, the information stored for use by an ST AS Malicious Communication Identification (MCID) invocation is marked as “Anonymous”.

For more information about the ST AS MCID service, refer to *ST AS Malicious Communication Identity Service Management Guide*.



3 ST AS Identity Presentation Service Configuration

The ST AS Identity Presentation service is controlled by the *MtasStIdPres* Managed Object (MO). An overview of the ST AS Identity Presentation MO structure is shown in Figure 1.

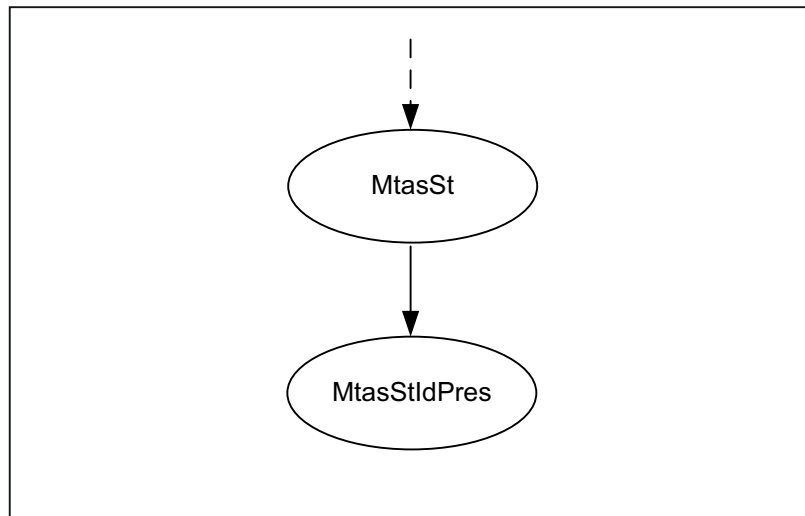


Figure 1 ST AS Identity Presentation MO Structure

Configurable MOs and attributes related to the ST AS Identity Presentation services are defined in *Managed Object Model (MOM)*.

3.1 Configuration Activities

More configuration activities are listed in Table 3.

Table 3 More Configuration Activities

Activity	Attribute
Specifying if screening of the <code>From</code> header is enabled or disabled.	<code>mtasStIdPresFromHeaderScreening</code>
Specifying if denormalization of the <code>From</code> header is enabled or disabled	<code>mtasStIdPresFromHeaderDenorm</code>
Specifying if copying of the Request URI to the <code>To</code> header is enabled or disabled.	<code>mtasStIdPresCopyUriToToHeader</code>

For more information about the ST AS Identity Presentation attributes, refer to *Managed Object Model (MOM)*.



3.2 Identity Presentation Administrative State Configuration

The ST AS Identity Presentation service is enabled by setting the `mtasStIdPresAdministrativeState` attribute in the `MtasStIdPres` MO to 1 (Unlocked). If the `mtasStIdPresAdministrativeState` is set to 0 (Locked), no ST AS Identity Presentation service is provided by the MTAS.

3.3 Reason for Lack of Caller Identity Configuration

Indication of Reason for Lack of Caller Identity can be enabled by setting `mtasStIdPresReasonIndication` attribute in `MtasStIdPres` MO to 1 (Enabled). If `mtasStIdPresReasonIndication` is set to 0 (Disabled), then no reason indication is included in display-name of P-Asserted-Identity.

3.4 Service Data Configuration

This section describes how to configure the service data.

3.4.1 Operator Subscription Level Service Configuration

Configuration specified in this section is managed by the CAI3G interface by the operator. For more information, refer to *MTAS CAI3G Interface for ST AS*.

Note: If an option is not present and it has a default value, then the default value applies.

3.4.1.1 OIP

The OIP subscription options are listed in Table 4.

Table 4 OIP Subscription Option

Subscription Option	Value	Description
Activated	True False	The Activated option specifies if the service is activated by the operator.
OIR override	Override No override (default)	The OIR override option allows information requested to be restricted, or, to be presented to the Terminating User.

3.4.1.2 OIR

The OIR subscription options are listed in Table 5.



Table 5 OIR Subscription Option

Subscription Option	Value	Description
Activated	True False	The Activated option specifies if the service is activated by the operator.
Mode	Permanent mode Temporary mode	The Mode option decides if the default action can be overridden by the PBX.
Restriction	Restrict asserted identity Restrict all private information (default)	The Restriction option specifies the required level of restriction. The restrict asserted identity is the same as “id” and “user” level privacy and restrict all private information is the same as “header”, “id”, and “user” level privacy.
From header screening	enabled disabled	<p>The From header screening subscription option specifies if the execution of From header screening in the requests sent by the originating PBX take place or not.</p> <p>By default, this option is not available. If available, the From header screening is controlled by this subscription option regardless of if the subscription option “Activated” is set to True or False. If not available, the From header screening is controlled by the <code>mtasStFromHeaderScreening</code> node parameter.</p>

3.4.1.3

TIP

The TIP subscription options are listed in Table 6.



Table 6 TIP Operator Subscription Option

Subscription Option	Value	Description
Activated	True False	The Activated option specifies if the service is activated by the operator.
TIR override	Override No override (default)	The TIR override option allows information requested to be restricted for presentation to the Terminating User.

3.4.1.4 TIR

The TIR subscription options are listed in Table 7.

Table 7 TIR Operator Subscription Option

Subscription Option	Value	Description
Activated	True False	The Activated option specifies if the service is activated by the operator.
Mode	Permanent mode Temporary mode	The Mode option decides if the default action can be overridden by the PBX.
Restriction	Restrict asserted identity Restrict all private information (default)	The Restriction option specifies the required level of restriction. The restrict asserted identity is the same as “id” and “user” level privacy and restrict all private information is the same as “header”, “id”, and “user” level privacy.
Connected-Identity-Support	enabled disabled	The Connected-Identity-Support controls if signaling of connected identity from the PBX is enabled. It can be set to enabled or disabled. If the element is not present, the default setting is disabled. When connected identity is not supported, the From-Change feature is removed from the Supported header of the initial request sent to the PBX.



3.4.2 User Subscription Level Service Configuration

The PBX data is configured by the operator through the CAI3G interface using the XDMS on behalf of the PBX.

3.4.2.1 OIP

The OIP subscription options are listed in Table 8.

Table 8 OIP User Subscription Option

Subscription Option	Value	Description
Active	True	The Active option specifies if the service is activated or deactivated.
	False	

3.4.2.2 OIR

The OIR subscription options are listed in Table 9.

Table 9 OIR User Subscription Option

Subscription Option	Value	Description
Active	True	The Active option specifies if the service is activated or deactivated.
	False	
default-behaviour	presentation-restricted presentation-not-restricted	The “default-behavior” is used to specify the default behavior for temporary mode, presentation restricted, or presentation not restricted.

3.4.2.3 TIP

The TIP subscription options are listed in Table 10.

Table 10 TIP User Subscription Option

Subscription Option	Value	Description
Active	True	The Active option specifies if the service is activated or deactivated.
	False	



3.4.2.4 TIR

The TIR subscription options are listed in Table 11.

Table 11 TIR User Subscription Option

Subscription Option	Value	Description
Active	True False	The Active option specifies if the service is activated or deactivated.
default-behaviour	presentation-restricted presentation-not-restricted	The “default-behavior” is used to specify the default behavior for temporary mode, presentation restricted, or presentation not restricted.

3.4.2.5 Checks of Subscriber Data Performed at XDMS

The XDMS rejects an update if the update does not comply with the schema.



4 Performance Management

For information on measurements related to the ST AS Identity Presentation service, refer to *MTAS Performance Measurements*.





5 Fault Management

There are no alarms related to the ST AS Identity Presentation service.