MTAS Identity Presentation Management Guide

MTAS

USER GUIDE

38/1553-AVA 901 29/9 Uen B

Contents

1 Introduction

This document describes how to configure the Identity Presentation service in the MTAS.

1.1 Prerequisites

It is assumed that the user of this document is familiar with the O&M area, in general.

1.1.1 Licenses

To enable the Calling Name Identity Presentation (CNIP) service and the Originating Calling Name Identity Presentation (OCNIP), the CNIP license must be installed.

For more information about the CNIP 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 MTAS offers the following Identity Presentation services to its subscribers:

- Flexible Identity Presentation (FIP)
- Originating Identity Presentation (OIP)
- Originating Identity Restriction (OIR)
- Terminating Identity Presentation (TIP)
- Terminating Identity Restriction (TIR)
- Calling Name Identity Presentation (CNIP)
- Originating Calling Name Identity Presentation (OCNIP)

The services enable presentation of the identities of participants in a communication to the other participants and for a participant to withhold the identity information from the other participants. The restriction may be overridden by the OIP and TIP function for participants with the override option.

The “Dynamic ad-hoc Identity Presentation” only switches on/off the OIR function for one call attempt.

The CNIP service replaces the display name portion of the identity information of the originating participant with information retrieved from an external database.

The OCNIP service is similar to the CNIP service. One main difference is that the display name can be retrieved from the subscriber data.

The purpose of the Identity Presentation function and its subfunctions is to enable or restrict presentation of identities in a communication based on the participant’s preferences, information received at the initiation of the communication, and information received in each message.

In an IP Multimedia Subsystem (IMS) network several entities are needed to realize this function. The MTAS is the application server realizing this function. Other nodes, like the Call Session Control Functions (CSCFs), are also part of the complete solution of this function. Since some information is required in the IMS network, it cannot be removed by an application server. It is the IMS core network’s responsibility to remove the information. The terminals are also part of the complete solution, but since the terminal behavior cannot be trusted, this is to be ensured by the network. For a description of their behavior, refer to the following protocol specifications:

- 3GPP TS 24.607 v8.3.0
- 3GPP TS 24.608 v8.2.0

The different subfunctions are either functions executing on behalf of the originating user or executing on behalf of the terminating user. The OIR, TIP, and OCNIP functions are originating services and OIP, CNIP, and TIR are terminating services. The functions can be executed on different Application Servers (ASs), one serving the originating user and another one serving the terminating user. The override functionality is part of the OIP and TIP functions.

The OIR in temporary mode can be initiated on a per call basis (dynamic ad-hoc) by using Supplementary Service Codes (SSCs). The support includes `Invocation` or `Disabling` of Identity Presentation.

The Identity Presentation is based on the Session Initiation Protocol (SIP) privacy header information. The header can have several values. Different values on the `Privacy` header specify for what headers that privacy is requested. The values that are of interest for the MTAS are listed in Table 1.

Table 1 Privacy Header Value

Privacy Header Value	**Headers**
none	No privacy is requested.
id	"Network asserted user identity" privacy requested, for example, `P-Asserted-Identity`.
user	"Headers added by the user" privacy, for example, `From` header.
header	"Headers added by the network" privacy, for example, `via`, `Record Route`.

Values other than those listed in Table 1 are handled transparently.

When communication is diverted and AS chaining is disabled, originating services like OIR are executed directly in terminating MTAS.

When communication is diverted and AS chaining is enabled, the `INVITE` is returned to S-CSCF after retargeting. Invocation of originating services like OIR is triggered by S-CSCF by sending the `INVITE` to the terminating MTAS (or other AS) for the originating session case.

The terminating AS becomes a transit AS, the OIR, and TIR services act differently for this AS compared to originating or terminating AS.

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

2.1 Subfunctions

The Identity Presentation function consists of a number of subfunctions described in the following sections.

The different Identity Presentation subfunctions are started on originating, transit, and terminating MTAS, for both registered and unregistered users, see Table 2.

Table 2 Invocation of Subfunctions

Subfunction	MTAS Type	User	
		Registered	Unregistered
OIP	Terminating	X	
OIR	Originating	X	X
OIR	Transit	X	X
OIR permanent	Originating	X	
OIR permanent	Transit	X	X
OIR Dynamic ad-hoc Identity Presentation	Originating	X	
TIP	Originating	X	
TIR	Terminating	X	X
TIR	Transit	X	X
CNIP	Terminating	X	
FIP	Originating	X	X
FIP	Transit	X	X
OCNIP	Originating	X	X

2.1.1 Originating Identity Presentation

The Originating Identity Presentation subfunction makes it possible for a Terminating User to see the identity of the Originating User as the result of receiving SIP messages. If identity restriction is requested, then a number of headers are removed or anonymized.

It is possible for the user to activate and deactivate this feature by changing the default settings in the user's data and to interrogate the feature status.

If the override option is active, see Table 4, any requests to restrict the identity are ignored.

The identity in the `From` header can be presented in a locally dialable format. This is controlled by configuration and applies if the Administrative State is unlocked and if the `From` header has not been anonymized.

It is a prerequisite that the `user=phone` parameter is present for the SIP embedded Tel URIs.

For a description on how to configure MTAS number normalization, refer to *MTAS Number Normalization Management Guide*.

To make sure that the `To` header is always the target identity, it is possible for this subfunction to copy the content of the Request-URI to the `To` header. This is controlled by configuration and applies if the Administrative State is unlocked and header copying is enabled.

The service can provide the reason indication for lack of caller identity to the terminating network by mapping the reason indication from the `P-Asserted Identity` header's display-name portion to the `From` header's display-name portion.

2.1.2 Originating Identity Restriction

The Originating Identity Restriction subfunction makes it possible for an Originating User to restrict the presentation of the identity to the Terminating User.

The service exists in two modes; permanent and temporary, see Table 5.

In the temporary mode, it is possible for the service default setting to be configured to either restrict or present the user's identity. It is possible for the user to modify this setting by changing the default setting in the user's data. It is also possible to interrogate the service status. In temporary mode the originating function, OIR, Identity Presentation default setting can be overridden on a per call basis using SSCs, that is, ''Dynamic ad-hoc Identity Presentation'' or by a `Privacy` header included in SIP messages from the originating User Agent (UA). This allows the user to either present or restrict the identity on a call by call basis, or message by message basis.

In permanent mode none of these operations are possible and the service is always set to restrict presentation of the user's identity.

There are two possible levels of restriction, ''asserted identity'' and ''all private information'', see Table 5.

If the `From` header screening is to be applied, the `P-Asserted-Identity` is copied into the `From` header. The `From` header screening is controlled by configuration and is applied if the Administrative State is unlocked and `From` header screening is enabled.

The service can provide the reason for lack of caller identity for the terminating network when the caller requested the anonymity.

Display name part of PAI header indicates the reason for lack of caller's identity. The value of CM attribute `mtasIdPresPrivacyDisplayName` (if defined) is set as Display name; otherwise ''Anonymous'' is used.

2.1.2.1 Dynamic ad-hoc Identity Presentation

The ‘‘Dynamic ad-hoc Identity Presentation’’ is tied to the subfunction OIR in temporary mode and can on a per call basis indicate ‘‘present’’ or ‘‘restrict’’.

2.1.3 Terminating Identity Presentation

The Terminating Identity Presentation subfunction makes it possible for an Originating User to see the identity of the Terminating User as the result of receiving SIP messages. If identity restriction is requested, then a number of headers are removed or anonymized.

It is possible for the user to activate and deactivate this feature by changing the default settings in the user’s data and to interrogate the feature status.

If the override option is active, see Table 6, then any requests to restrict the identity are ignored.

2.1.4 Terminating Identity Restriction

The Terminating Identity Restriction subfunction makes it possible for a Terminating User to restrict the presentation of the identity to the Originating User

The service exists in two modes; permanent and temporary, see Table 7. In the temporary mode, it is possible for the user to activate and deactivate this feature by changing the default settings in the user’s data and to interrogate the feature status. It is possible to override the configured setting in temporary mode by inclusion of a `Privacy` header in SIP messages sent from the terminating UA.

In permanent mode these actions are not possible and the service is always set to restrict presentation of the user’s identity. There is one level of restriction, ‘‘asserted identity’’.

2.1.5 Calling Name Identity Presentation

The Calling Name Identity Presentation subfunction makes it possible for a Terminating User to see the display name of the Originating User as provided by an external Calling Name Server. If the CNIP function is requested, the display-name portion of the `P-Asserted-Identity` and `From` headers can be changed.

The service exists in two modes; ‘‘always’’ and ‘‘interrogate-on-unavailability’’. In ‘‘interrogate-on-unavailability’’ mode, the display name is only retrieved if the display name is missing from identity provided in the SIP request from the Originating User in both the `P-Asserted-Identity` and `From` headers. In ‘‘always’’ mode, the display name is always retrieved and the display name in the request is overwritten if it is already present on the Originating User’s request.

The CNIP uses the `NameDb` interface over SOAP, for details, refer to *NameDb*.

2.1.6 Flexible Identity Presentation

The Flexible Identity Presentation subfunction makes it possible for an Originating User to replace its own identity with a different identity assigned to the user by the operator. Alternatively the FIP subfunction also makes it possible to hide the originating user's identity in the history-info header field when the user executes a diversion service.

It is possible for the user to activate or deactivate this feature by changing the default settings in the user data and to interrogate the feature status.

2.1.7 Multi-Subscriber Number

The Multi-Subscriber Number (MSN) service is an extension to the FIP subfunction. MSN allows the operator to provision a served user with multiple identities. The served user can then select which of these MSN identities to use at call establishment using an SSC. The selected MSN identity is handled the same way as a FIP identity.

2.1.8 Originating Calling Name Identity Presentation

The Originating Calling Name Identity Presentation subfunction makes it possible for a Terminating User to see the display name of the Originating User as provided by the subscriber data in the HSS. If the OCNIP function is requested, the display-name portion of the P-Asserted-Identity and From headers can be changed.

Like CNIP, the OCNIP function has two modes of operation: ‘‘always’’ and ‘‘interrogate-on-unavailability’’. In ‘‘interrogate-on-unavailability’’ mode the OCNIP function only retrieves the display name if the display-name is missing from identity provided in the SIP request from the Originating User in both the P-Asserted-Identity and From headers. In ‘‘always’’ mode, the display name is always retrieved.

2.2 Traffic View

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

1. Service invocation, an event triggers the execution of Identity Presentation, for example, incoming `INVITE`.
2. Service execution, Identity Presentation evaluates the served user's settings and determines if the identity is to be presented or not.

The traffic view of Identity Presentation is shown in Figure 1.

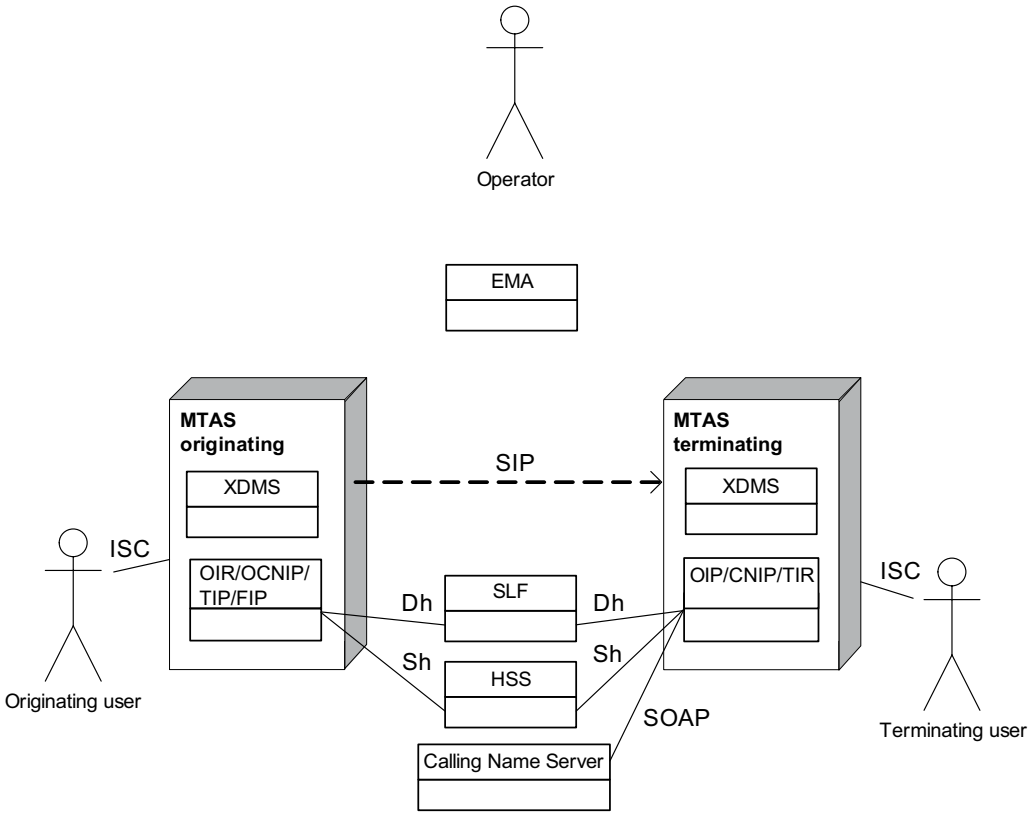

Figure 1 Traffic View of Identity Presentation

The different subfunctions of 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 or not. In case the served user's settings determines that the CNIP function is to be executed the calling name is retrieved from an external database.

2.3 Configuration View

There are two categories of configuration, as follows:

- Node level configuration
- User configuration

Node level configuration is performed by the operator who can lock and unlock both the Identity Presentation function and the CNIP function. The CNIP function depends on the Identity Presentation function, as follows:

- The Identity Presentation has to be unlocked before the CNIP and OCNIP can be unlocked.

- The CNIP and OCNIP must be locked before Identity Presentation can be locked.
- The CNIP license is to be applied to the node serving the terminating user for CNIP service. The same license is applied serving the originating user for OCNIP service.

The user configuration is managed through the XML Document Management Server (XDMS) that provides the Ut interface (XCAP over HTTP) to the served user and CAI3G interface to the operator. The XDMS uses Sh (Diameter) to update the HSS. The served user accesses the XDMS directly and the operator accesses it through a Business Support System.

The configuration view of Identity Presentation is shown in Figure 2.

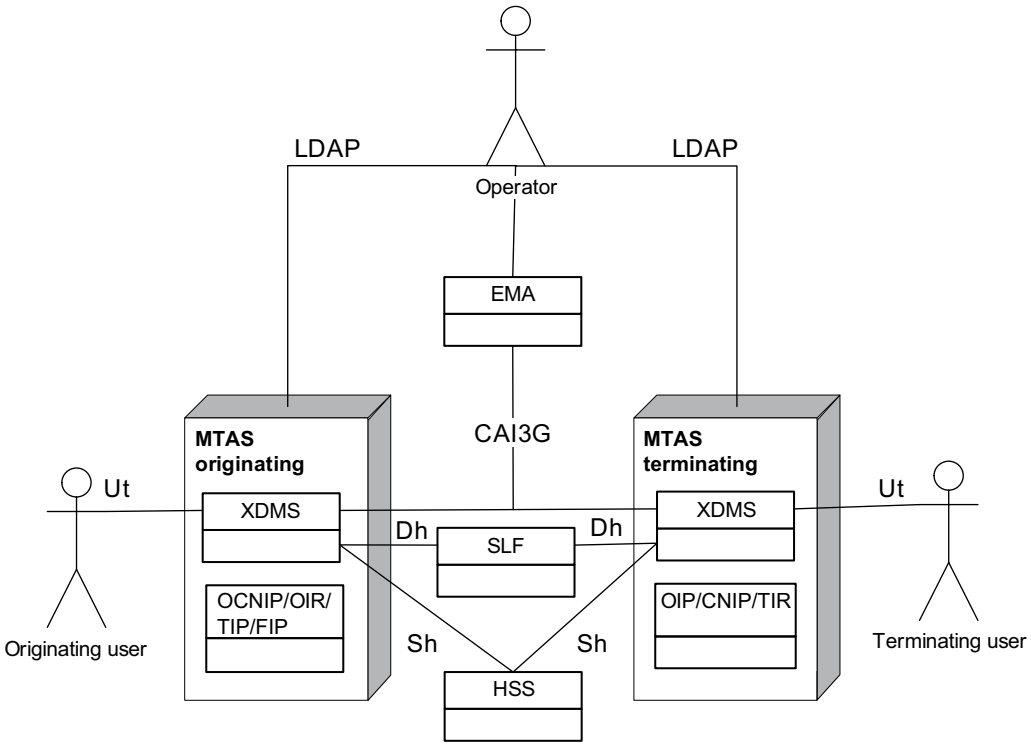

Figure 2 Configuration View of Identity Presentation

If the Identity Presentation function is locked, all identity information is passed unchanged and the OIR/TIR requests are ignored.

Similarly, if the CNIP/OCNIP function is locked, no retrieval of the calling information is made.

2.4 Interaction with Other Services

The Identity Presentation interaction with other MTAS services is described in this section.

2.4.1 Application Server Interworking

The AS Interworking provided `From` header is overwritten by the FIP service with the FIP identity. The FIP identity being defined by the operator can be regarded as a network provided or asserted identity so it must comply with the expectation of an AS expected asserted `From` header.

For more information about the AS Interworking service, refer to *MTAS Application Server Interworking Management Guide*.

2.4.2 Calling Party Category

The Calling Party Category (CPC) parameter added to the `P-Asserted-Identity` header by the CPC service is left unchanged when the FIP service replaces the calling user's identify with the FIP identity. If this behavior is not intended, the service interaction is avoided by deactivating the appropriate service.

For more information about the CPC service, refer to *MTAS Calling Party Category Management Guide*.

2.4.3 Charging

The following service-specific Attribute-Value Pair (AVP) is applicable to dynamic ad-hoc identity presentation/restriction:

- Supplementary Service Information – indicating use of OIR

The OIR subfunction at the originating MTAS node updates the ‘‘Calling Party Address Presentation Status’’ and ‘‘From Header Presentation Status’’ stored attributes used to generate charging records.

The TIR subfunction at the terminating MTAS node updates the ‘‘Called Asserted Identity Presentation Status’’ stored attributes used to generate charging records.

The following service-specific Attribute-Value Pair (AVP) is applicable to flexible Identity Presentation:

- Supplementary Service Information – indicating use of FIP

For more information about the Charging service, refer to *MTAS Charging Management Guide*.

2.4.4 Communication Barring

The barring interactions between the OIR and the Anonymous Communication Rejection (ACR) service is described in *MTAS Barring and Dial Plan Services Management Guide*.

2.4.5 Communication Completion

FIP is applied in the originating MTAS during Communication Completion (CC) call. This has no effect on the CC service

FIP is applied in the originating MTAS during CC recall when CC Agent sets up the outgoing call leg of the 3PCC. The CCxx called party receives the FIP identity as the identity of the CCxx caller party.

For more information about the CC service, refer to *MTAS Communication Completion Management Guide*.

2.4.6 Communication Diversion

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

2.4.7 Conference

The Identity Presentation service does not operate at the conference focus. The conference focus transfers `Privacy` headers received in the initial `INVITE` to establish the conference to all outgoing `INVITE` requests to Conference Participants. `Privacy` headers received in responses to the `INVITE` to Conference Participants are included in the NOTIFY requests sent to the Conference Creator.

For more information about the conference service interaction with the Identity Presentation services, refer to *MTAS Ad-hoc Conference Management Guide*.

2.4.8 Customized Alerting Tones

Interactions between the Identity Presentation and the Customized Alerting Tones services are described in *MTAS Customized Alerting Tones Management Guide*.

2.4.9 Dynamic Black List

When an initial `INVITE` is received that matches the Global Identity Presentation Restriction List, and the served user has the OIP service active and the override option not active, the information stored for use by a Dynamic Black List invocation is marked as anonymous. If Dynamic Black List is started on those stored details, the caller's identity is hidden.

For more information about the Charging service, refer to *MTAS Charging Management Guide*.

2.4.10 Explicit Communication Transfer

The identity handling of the Explicit Communication Transfer service is described in *MTAS Explicit Communication Transfer Management Guide*.

2.4.11 FIP and OIR Interaction

The FIP and the OIR services work on the originating side and affect different headers. The result of both being executed is that the originating identity restriction applies to the FIP identity which replaces the original identity.

2.4.12 Flexible Communication Distribution

The Flexible Communication Distribution (FCD) interactions between the Identity Presentation and the FCD services are described in *MTAS Flexible Communication Distribution Management Guide*.

2.4.13 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 not active, the information stored for use by a Malicious Communication IDentification (MCID) invocation is marked as anonymous. If the MCID is started on those stored details, the caller's identity is not displayed to the served user.

If MCID service is started on an incoming communication from a user with FIP service active the caller's identity (content of `From` and `P-Asserted-Identity` headers) collected by the MCID served user is that provided by the FIP service.

For more information about the MCID service, refer to *MTAS Malicious Communication Identification Management Guide*.

2.4.14 Number Portability

Number portability for incoming communication is triggered on the `P-Asserted-Identity` received. This can be a `P-Asserted-Identity` content provided by the FIP service in the originating domain.

For more information about the Charging service, refer to *MTAS Number Portability Management Guide*.

2.4.15 Short Number Dialing

The Short Number Dialing (SND) service in the originating domain modifies the request URI, and the `From` and `P-Private-Network-Identifier` headers.

FIP service in the originating domain overwrites the `From` header modified by the SND service.

The SND service in the terminating domain recognizes the SND call based on the request URI. If the replacement of the `From` header with the FIP identity is an unwanted behavior from the SND service point of view, the interaction in the originating domain is avoided by deactivating one of the services.

For more information about the SND services, refer to *MTAS Short Number Dialing Management Guide*.

2.4.16 FIP and From Header Screening

When From Header Screening is enabled, only the PAI identity is compared with the identities in the IRS. In case of match, both PAI and FROM identities are replaced with the FIP identity. This is useful when FROM header is in local format (and not present in the IRS). When From Header Screening is disabled, FROM identity can only be replaced with the FIP Identity when matched with an identity in the IRS.

3 Identity Presentation Configuration

The Identity Presentation service is controlled by the *MtasIdPres* Managed Object (MO). An overview of the Identity Presentation MO structure is shown in Figure 3.

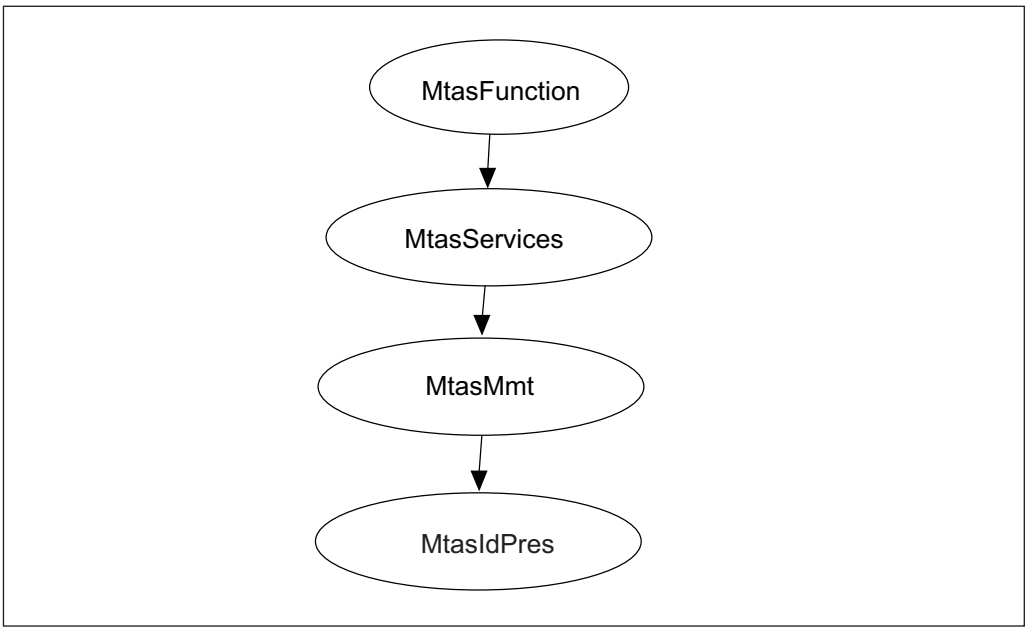

Figure 3 Identity Presentation MO Structure

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

3.1 DNS Configuration

If the MTAS needs to look up a hostname, the DNS Resolver is used. For more information about the DNS configuration, refer to *Managed Object Model (MOM)*.

The `DnsLocalAddress` parameter is to be configured such that DNS communication with the Name Server is displayed on the SIP traffic interface.

3.2 Configuration Activities

Additional configuration activities are listed in the following table:

Table 3 Additional Configuration Activities

Activity	Attribute
Controlling the time-out for the query to the CNS.	mtasIdPresCnipTimeout
Specifying whether the query to the name database (CNS) takes place always or only when both the `From` and `P-Asserted-Identity` display names are absent from the request.	mtasIdPresCnipMode
Specifying if screening of the `From` header is enabled or disabled.	mtasIdPresFromHeaderScreening
Specifying if denormalization of the `From` header is enabled or disabled	mtasIdPresFromHeaderDenorm
Specifying if copying of the Request URI to the `To` header is enabled or disabled.	mtasIdPresCopyUriToToHeader

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

3.3 Identity Presentation Administrative State Configuration

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

`mtasIdPresFromHeaderScreening` cannot be set to 1 (enabled) unless `mtasSndAdministrativeState` is set to 0 (Locked). `mtasIdPresFromHeaderDenorm` cannot be set to 1 (enabled) unless `mtasSndAdministrativeState` is set to 0 (Locked).

3.4 Wholesale for Identity Presentation Configuration

The Identity Presentation service supports Wholesale. Identity Presentation including all subfunctions is configurable on Virtual Telephony Provider level.

Wholesale for Identity Presentation is activated when the following attributes are set to `1` (Unlocked):

- The `vtasIdPresAdministrativeState` attribute in the *VtasIdPres* MO
- The `mtasIdPresAdministrativeState` attribute in the *MtasIdPres* MO

For more information about the Wholesale service, refer to *MTAS Wholesale Support Management Guide*.

3.5 CNIP Administrative State Configuration

The CNIP service is enabled by setting the `mtasIdPresCnipAdminState` attribute in the `MtasIdPres` MO to `1` (Unlocked). If the `mtasIdPresCnipAdminState` is set to `0` (Locked), no CNIP service is provided by the MTAS.

Note: The `mtasIdPresAdministrativeState` attribute in the `MtasIdPres` MO must be set to `1` (Unlocked) before the `mtasIdPresCnipAdminState` attribute is set to `1` (Unlocked).

Likewise, the `mtasIdPresAdministrativeState` attribute must be set to `0` (Locked) before the `mtasIdPresCnipAdminState` attribute is set to `0` (Locked).

3.6 MSN Administrative State Configuration

The MSN service is enabled by setting the `mtasIdPresMsnAdminState` attribute in the `MtasIdPres` MO to `1` (Unlocked) once having defined the command syntax for MSN supplementary service code invocation in `mtasSscIdPresComSynInvMsnSel`.

Note: The `mtasIdPresAdminState` attribute in the `MtasIdPres` MO must be set to `1` (Unlocked) before the `mtasIdPresMsnAdminState` attribute is set to `1` (Unlocked).

Likewise, the `mtasIdPresMsnAdministrativeState` attribute must be set to `0` (Locked) before the `mtasIdPresAdministrativeState` attribute is set to `0` (Locked).

3.7 Reason for Lack of Caller Identity Configuration

Indication of reason for lack of caller identity can be enabled by setting `mtasIdPresReasonIndication` attribute in `MtasIdPres` MO to `1` (Enabled). If `mtasIdPresReasonIndication` is set to `0` (Disabled), then no reason indication is included in the display-name of `P-Asserted-Identity`.

3.8 OCNIP Administrative State Configuration

The OCNIP service is enabled by setting the `mtasIdPresOCnipAdminState` attribute in the MtasIdPres MO to `1` (Unlocked). If the `mtasIdPresOCnipAdminState` is set to `0` (Locked), no Originating Calling Name Identity Presentation service is provided by the MTAS.

Note: The `mtasIdPresAdministrativeState` attribute in the `MtasIdPres` MO must be set to `1` (Unlocked) before the `mtasIdPresOCnipAdminState` attribute is set to `1` (Unlocked).

Likewise, the `mtasIdPresAdministrativeState` attribute must be set to 0 (Locked) before the `mtasIdPresOCnipAdminState` attribute is set to 0 (Locked).

3.9 OCNIP Mode Configuration

The OCNIP service mode is controlled by setting the `mtasIdPresOCnipMode` attribute in the `MtasIdPres` MO. If the `mtasIdPresOCnipMode` is set to `0` (interrogate-on-unavailability), query to subscriber data/CNS is always performed only when both the From and P-Asserted-Identity display names are absent from the request. If the `mtasIdPresOCnipMode` is set to `1` (always), query to subscriber data/CNS is to take place always.

3.10 Configure Use of From Header

This `mtasIdPresUseFromHeader` attribute defines whether the From header is to be used (trusted) in the Identity Presentation Service. The default value is 1, that is, From header is trusted.

To modify the ‘‘Use From Header’’ attribute:

1. Navigate to the `MtasIdPres` MO.
2. Set the `mtasIdPresUseFromHeader` attribute to either 0 (Do not use/trust From header) or 1 (Use/trust From header).
3. Click **Submit**.
4. Perform a backup. For more information, refer to *Create Backup*.

3.11 Configure Removal of Privacy Header

This `mtasIdPresOCnipRemovePrivacy` attribute indicates if the privacy header in the incoming SIP signaling is removed before any Identity Presentation service is started in Originating MTAS. The default value is 0, that is. Privacy header is not removed.

To modify the ‘‘Removal of Privacy Header’’ attribute:

1. Navigate to the `MtasIdPres` MO.
2. Set the `mtasIdPresOCnipRemovePrivacy` attribute to either 0 (Keep privacy header) or 1 (Remove privacy header).
3. Click **Submit**.
4. Perform a backup. For more information, refer to *Create Backup*.

3.12 Service Data Configuration

This section describes how to configure the service data.

3.12.1 Operator Subscription Level Service Configuration

Configuration specified in this section is managed by the CAI3G interface by the operator. For more information on all the provisioning constraints for the identity presentation service data refer to *MTAS CAI3G Interface*.

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

3.12.1.1 OIP

The OIP subscription options are listed in Table 4.

The Activated option specifies if the service is activated by the operator.

The OIR override option allows information requested to be restricted to be presented to the Terminating User.

Table 4 OIP Subscription Option

Subscription Option	Value
Activated	true false
OIR override	override no override (default)

3.12.1.2 OIR

The OIR subscription options are listed in Table 5.

The Activated option specifies if the service is activated by the operator.

The Mode option decides if the services can be user configured or not.

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.

Table 5 OIR Subscription Option

Subscription Option	Value
Activated	true false
Mode	permanent mode temporary mode (user specified)
Restriction	restrict asserted identity restrict all private information (default)

3.12.1.3 TIP

The TIP subscription options are listed in Table 6.

The Activated option specifies if the service is activated by the operator.

The TIR override option forces even information requested to be restricted to be presented to the Originating User.

Table 6 TIP Subscription Option

Subscription Option	Value
Activated	true false
TIR override	override no override (default)

3.12.1.4 TIR

The TIR subscription options are listed in Table 7.

The Activated option specifies if the service is activated by the operator.

The Mode option decides if the services can be user configured or not.

Table 7 TIR Subscription Option

Subscription Option	Value
Activated	true false
Mode	permanent mode temporary mode (user specified)

3.12.1.5 CNIP

The CNIP subscription options are listed in Table 8.

The Activated option specifies if the service is activated by the operator.

Table 8 CNIP Subscription Option

Subscription Option	Value
Activated	true false

3.12.1.6 FIP

The FIP subscription options are listed in Table 9.

The Activated option specifies if the service is activated by the operator. FIP-Identity specifies the identity to replace the original calling identity. FIP-Identity is contained by the user part of the schema, but application logic only allows the operator to set it.

Table 9 FIP Subscription Option

Subscription Option	Value
Activated	true false
FIP-Identity	SIP URI
MSN-FIP-Identity	SIP URI

3.12.1.7 OCNIP

The OCNIP subscription options are listed in Table 10.

The Activated option specifies if the service is activated by the operator. Display-name specifies the display name to set.

Table 10 OCNIP Subscription Option

Subscription Option	Value
Activated	true false
display-name	This is subscriber's name of length between 0-64. This is set to FROM and PAI header(s) by OCNIP service when the service is active. Provisioned in the common part.

3.12.2 Subscriber Subscription Level Service Configuration

The user subscriber data is configured through the Ut interface using the XDMS. The Ut interface and The XML schema for the Ut interface are described in the following documents:

- *MTAS Ut Interface*
- *MTAS Ut Structure*

3.12.2.1 OIP and OIR

The following XML example shows an element instance for user level configuration of OIP and OIR:

```
<?xml version="1.0" encoding="UTF 8"?>
<simservs xmlns="http://uri.etsi.org/ngn/params/xml/simservs/xcap">
   <originating identity presentation active="true"/>
   <originating identity presentation restriction active="true">
       <default behavior>presentation restricted</default-behavior>
   </originating identity presentation restriction>
</simservs>
```

OIP has one attribute, active, to activate or deactivate OIP. OIR has two attributes, active and ‘‘default behavior’’. Active is used to activate OIR and the ‘‘default behavior’’ is used to specify the default behavior for temporary mode, presentation restricted, or presentation not restricted.

3.12.2.2 TIP and TIR

The following XML example shows an element instance for user level configuration of TIP and TIR:

```
<?xml version="1.0" encoding="UTF 8"?>
<simservs xmlns="http://uri.etsi.org/ngn/params/xml/simservs/xcap">
   <terminating identity presentation active="true"/>
   <terminating identity presentation restriction active="true">
       <default behavior>presentation restricted</default-behavior>
   </terminating identity presentation restriction>
</simservs>
```

TIP has one attribute, active, to activate or deactivate TIP. TIR has two attributes, active and ‘‘default behavior’’. Active is used to activate TIR and the ‘‘default behavior’’ is used to specify the default behavior for temporary mode, presentation restricted, or presentation not restricted.

3.12.2.3 CNIP

The following XML example shows an element instance for user level configuration of CNIP:

```
<?xml version="1.0" encoding="UTF 8"?>
<simservs xmlns="http://uri.etsi.org/ngn/params/xml/simservs/xcap">
   <calling-name identity presentation active="true"/>
</simservs>
```

CNIP has one attribute, active, to activate or deactivate CNIP.

3.12.2.4 FIP

The following XML example shows an element instance for user level configuration of FIP:

```
<?xml version="1.0" encoding="UTF 8"?>
<simservs xmlns="http://uri.etsi.org/ngn/params/xml/simservs/xcap">
   <flexible-identity-presentation active="true"/>
    <fip-identity>MailScanner has detected a possible fraud attempt from ⇒
"sip:+4681234567@operator.com sip:+4681234567@operator.com<fip-identity/>
    <msn-fip-identity id="1">MailScanner has detected a possible fraud attempt from ⇒
"sip:+4687654321@operator.com sip:+4687654321@operator.com<fip-identity/>
    <msn-fip-identity id="2">MailScanner has detected a possible fraud attempt from ⇒
"sip:+4688765432@operator.com sip:+4688765432@operator.com<fip-identity/>
   </flexible identity presentation>
</simservs>
```

FIP has two attributes, active, to activate or deactivate FIP and fip-identity to specify the new identity. Application logic does not allow fip-identity to be changed by the subscriber.

3.12.2.5 Checks of Subscriber Data Performed at XDMS

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

The XDMS rejects service provisioning of FIP service if the user already has Ad-hoc Conference service activated and the node level collocation is disabled.

The XDMS rejects fip-identity update attempts over the Ut interface.

4 Performance Management

Measurements related to the Identity Presentation service are detailed in the *Managed Object Model (MOM)*.

5 Fault Management

Alarms related to the Identity Presentation service are listed in *MTAS Alarm List*.