

ST AS Communication Barring Service Management Guide

MTAS

USER GUIDE

Copyright

© Ericsson AB 2016. 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	Use Cases	4
2.2	Interaction with Other Services	6
2.3	Traffic View	7
2.4	Configuration View	8
3	Service Invocation	11
4	Barring Rules	13
4.1	Relationship Among OCB Types	13
4.2	Relationship Among ICB Types	15
4.3	Global Barring Rules	16
4.4	Global White List	17
4.5	Relationship Among Operator Barring Programs, Operator Permitted Programs, and Operator Diversion Barring Programs	17
4.6	Barring Rules	19
4.7	Evaluation of Rules	23
5	Barring Service Configuration	27
5.1	Overview Tables and Activation	27
5.2	ACR Display Name Evaluation Configuration	29
5.3	Operator Barring Category Configuration	29
5.4	Localness Barring Categories Configuration	33
5.5	Global White List Configuration	34
5.6	Generic Announcement Name Configuration	35
5.7	Communication Barring Administrative State Configuration	36
5.8	Service Data Configuration	36
6	Performance Management	39
7	Fault Management	41
8	Barring Rule Configurations Examples	43



8.1	Bar Incoming Communication from Alice	43
8.2	Bar Incoming Communication from Anonymous	44
8.3	Bar Incoming Communication from example.com except from Alice and Bob	45
8.4	Bar Incoming from Range of Numbers	45
8.5	White List	46
8.6	Playing Generic Announcement – play-announcement	47
8.7	Playing Generic Announcement – play-segmented-announcement	48



1 Introduction

This document describes how to configure the SIP Trunking Application Server (ST AS) Communication Barring (CB) service in the MTAS.

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

Not applicable.

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 ST AS offers a number of barring services, which are controlled by the interaction between the Managed Objects (MOs) and per Private Branch Exchange (PBX) data. The Barring Service makes it possible for a PBX to have barring of certain communication categories.

The ST CB services are co-located and interact with other simulation services in the ST AS, for example, with ST AS Communication Diversion (CDIV).

The barring services are executed both at the originating and terminating ST AS. For an initial `INVITE`, the Outgoing Communication Barring (OCB) service is executed on the originating ST AS, and the Incoming Communication Barring (ICB) service is executed on the terminating ST AS. The OCB can also execute in the terminating side if, for example, the communication is diverted.

For a `REFER`, the OCB service is executed on the `REFER` ST AS of the sender.

The Anonymous Communication Rejection (ACR) service is a special case of the ICB service, which bars anonymous callers. The ACR is realized by the anonymous rule of the rule-based ICB service.

The ST CB service determines to bar or to allow the communication that matches the barring criteria. Communication that is not matched by any of the criteria is not affected by the barring services.

In addition to explicit blacklists, explicit global white lists, and Operator Controlled Outgoing Barring Programs, the served PBX can, for example, do the following using the CB service:

- Bar incoming anonymous communication
- Bar all outgoing communication except for some identities, for example, white list

The rules are built up with different conditions, which can be combined in many ways to express when a type of communication is to be barred. The supported conditions include as follows:

- Identity (the identity can match single user, domains, and so on)
- Anonymous
- Communication-diverted (the communication has previously been diverted)
- Rule-deactivated (makes it possible to disable a rule without deleting it)
- Other-identity (all identities that have not been matched in other rules)



When communication is diverted, the originating services, like OCB, can be executed directly in the terminating ST AS.

2.1 Use Cases

This section describes the use cases of the ST CB service.

2.1.1 Incoming Communication Barring

The ICB service makes it possible for a PBX to have barring of certain categories of incoming communications according to the global ICB blacklist, and the barring rules.

ICB rejects incoming communication when the evaluation of the ICB rules of the served PBX evaluates to `allow=false`. The ICB does not bar communication from calling parties that match with the ICB global white list.

The incoming communication is rejected by a SIP response with the `603 (Decline)` result code.

For more information about how to configure MOs and attributes related to the ST CB services, refer to *Managed Object Model (MOM)*.

2.1.2 Anonymous Communication Rejection

The ACR allows the served PBX to reject incoming communications on which the Public User Identity (PUI) of the originating user is restricted.

For example, the Originating Identity Restriction (OIR) restricts the presentation of the originating PUI, and that triggers the ACR in the terminating ST AS.

The incoming communication is rejected by a SIP response with result code `433 (Anonymity disallowed)`. The originating user is given an appropriate indication that the communication has been rejected because of the ACR.

The ACR is a special case of the ICB service.

2.1.3 Outgoing Communication Barring

The OCB service makes it possible for a PBX to have barring of certain categories of outgoing communications according to the global OCB blacklist, the diversion global blacklist, Operator Barring Program, Operator Permitted Program, Operator Diversion Barring Program, and barring rules of the PBX.

OCB rejects outgoing communications when the evaluation of the Operator Barring Program, Operator Permitted Program, Operator Diversion Barring Program, or OCB rules of the served PBX evaluates to `allow=false`. OCB does not bar Communication to called parties that match with the OCB global



white list except for diverted calls where the diversion global blacklist takes precedence.

The outgoing communication is either rejected by a SIP response with result code 603 (Decline) or answered by 200 OK.

The latter happens if `mtasStOcbPlayEarlyMedia` is set to 0 (disabled) and the CB service is configured with a generic announcement name, or the matched barring rule is requesting to play a generic (segmented) announcement when the generic (segmented) announcement is configured.

2.1.4 Play Announcement

The Play Announcement subfunction plays an announcement for the caller in addition to the result code in the final response by using the Generic Announcement service.

There are two ways of deriving the name of generic announcement to be played, as follows:

- Generic announcement name for the executing barring scenario is derived from the relevant CM attribute
- Generic announcement name is derived from the play-announcement or play-segmented-announcement action element of the matched OCB, ICB, or ACR rule

For more information about how to configure announcements using MTAS Generic Announcement functionality, refer to *MTAS Generic Announcement Management Guide*.

2.1.4.1 Announcement on Early Media or Established Sessions

Attribute `mtasStOcbPlayEarlyMedia` defines if the OCB service is to play announcements on established sessions or early announcement on not established sessions. The default is to play announcement on an early media.

The following attributes determine if an announcement is to be played on an established session or as an early media:

- `mtasStAcrPlayEarlyMedia`
- `mtasStIcbPlayEarlyMedia`
- `mtasStOcbPlayEarlyMedia`

Each of the parameters defines the way of playing announcements for the corresponding service.



2.2 Interaction with Other Services

This section describes the ST CB interaction with other services.

2.2.1 ST Call Admission Control

The ICB service processes the initial `INVITE` before the ST Call Admission Control (CAC) service.

The OCB service processes the initial `INVITE` after the ST CAC service.

For more information about the ST CAC service, refer to *ST AS Call Admission Control Management Guide*.

2.2.2 ST Carrier Select Rn and Carrier Pre-Select Rn

The original domain name in the incoming request is only overwritten with the ST AS domain name of the carrier, after the OCB service processing has been carried out.

For more information about the ST Carrier Select (CS) Rn and ST Carrier Pre-Select (CPS) Rn services, refer to *ST AS Carrier Select Rn and Carrier Pre-Select Rn Management Guide*.

2.2.3 Charging

`INVITE` requests that are processed by the ST CB result in the generation of charging messages. The charging messages include a service-specific Attribute-Value Pair (AVP) identifying the type of barring, for example, ICB. If a communication is allowed or barred because of a matching ICB, OCB, or ACR rule, the identifier of the matched ST CB rule is also included in an extra service-specific AVP.

If the call was rejected by an Operator Barring Program, or an Operator Diversion Barring Program, then the value in the AVP is the one associated with the Operator Barring Category, or special Barring Category that caused the call to be barred.

When OCB applies to a diverted `INVITE`, the service-specific AVP is only included in the charging message generated for the diverted B-to-C leg, for example, it is not included in the charging message generated for the incoming A-to-B leg.

Charging messages are not generated when `REFER` requests are rejected.

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

Note: Only offline charging is applicable to ST CB service.



2.2.4 CLIR Interworking

If the calling party has the OIR active, the ICB rules, which use the identity of the caller, are not evaluated.

2.2.5 ST Communication Diversion

The OCB interacts with the ST CDIV service by inspecting the `INVITE` destined for the diverted-to party before it is sent by the ST AS and is rejecting the communication with `486 (Busy Here)` if it is not allowed.

The ICB also uses the History-Info header inserted by CDIV to check whether an incoming `INVITE` has already been diverted, to evaluate the communication-diverted condition.

For more information about the ST CDIV service, refer to *ST AS Communication Diversion Management Guide*.

When communication is diverted, and Static mode PBX connect is used, OCB service is executed directly in terminating ST AS.

When communication is diverted and AS chaining is enabled (only possible in Dynamic mode PBX connect), the `INVITE` is returned to Serving Call Session Control Function (S-CSCF) after retargeting. Invocation of OCB service is triggered by S-CSCF by sending the `INVITE` to the terminating ST AS (or other AS) for the originating session case.

2.2.6 ST Identity Presentation

The OIR Override service takes precedence over the ACR service. If the served PBX has the OIR Override service, no incoming request is treated as anonymous, even if the `mtasStAcrGlobal` attribute is set to `Enabled`.

For more information about the ST Identity Presentation services, refer to *ST AS Identity Presentation Service Management Guide*.

2.3 Traffic View

The ST CB performs the following steps, which apply to all barring services:

1. Service invocation: an event triggers the execution of the ST CB, for example, incoming `INVITE`, see Section 3 on page 11.
2. Rules evaluation: the CB evaluates the served rule set of the PBX, and determines if the communication is barred, see Section 4 on page 13.
3. Send indication: if the communication is barred, an indication is sent to the originating user. The indication is a final SIP response, optionally preceded by playing an announcement.

The traffic view of the ST CB is shown in Figure 1. The use cases of the ST CB are triggered by a SIP event, for example, an outgoing `INVITE` triggers OCB and an incoming `INVITE` triggers ICB and ACR.

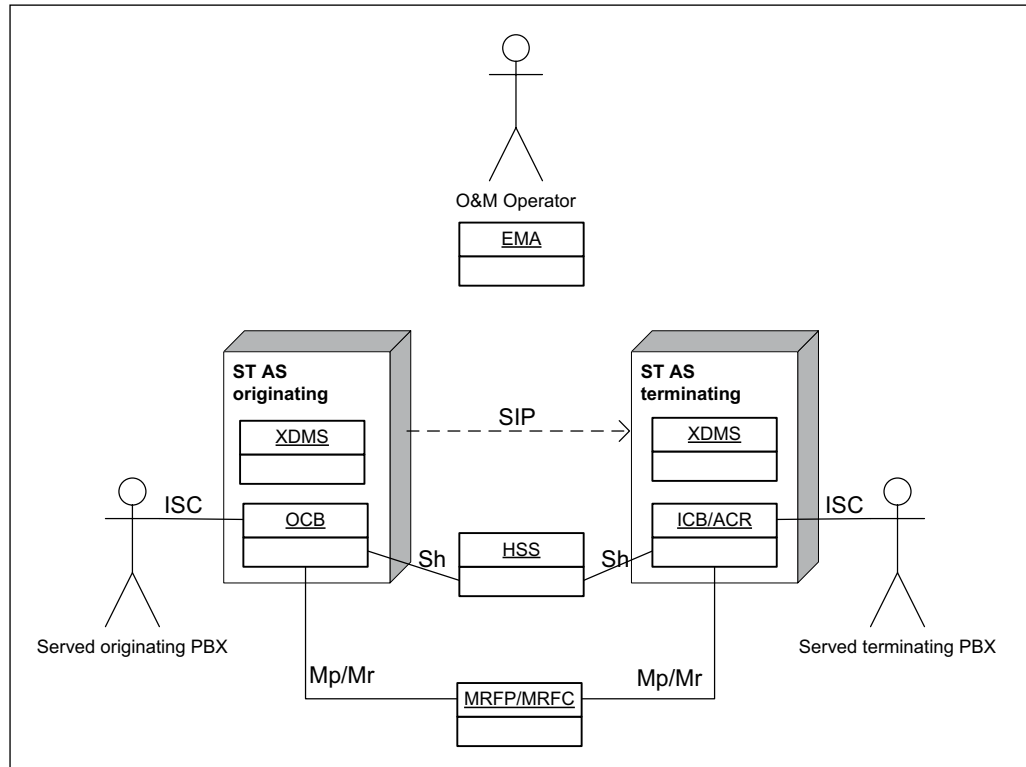


Figure 1 Traffic View of ST CB

2.4 Configuration View

The configuration view of the ST CB is shown in Page 9. The following two main categories of configuration exist:

- ST CB on node level, for example, Lock and Unlock.
- Global barring rules, see Section 4 on page 13.

In node level configuration, the operator customizes the ST CB service by, for example, defining if announcement is used as indication additionally to the SIP response 603 (`Decline`), and the generic announcement name, which defines the generic announcement to be played, defining the white lists, defining the Barring Categories.

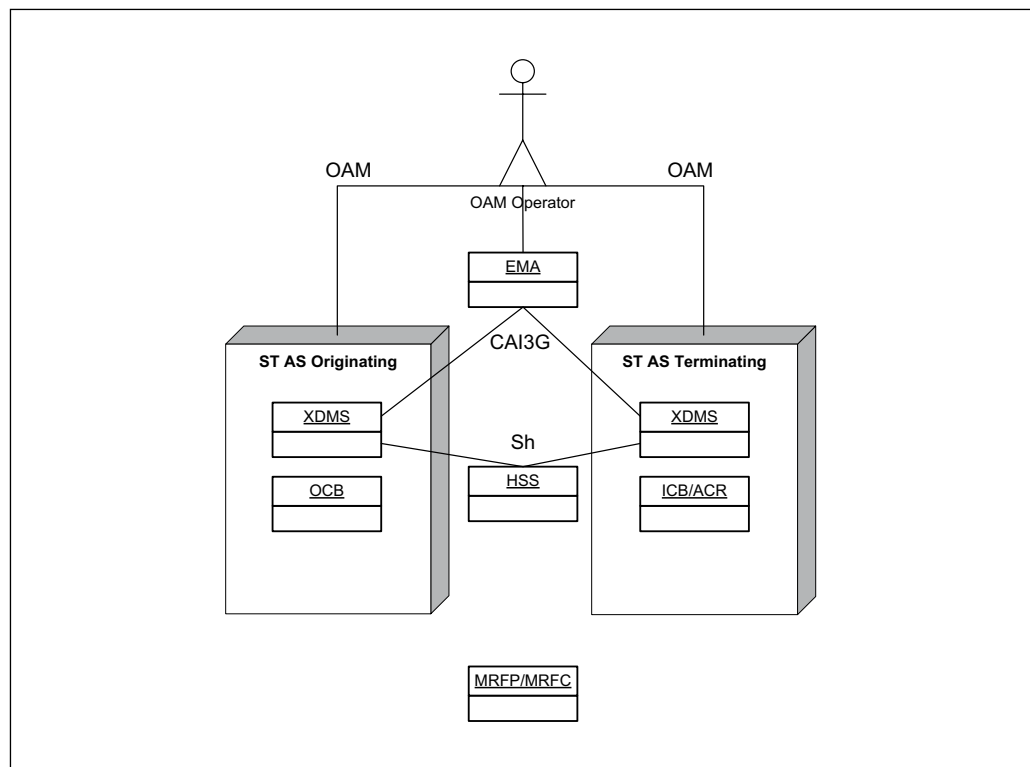


Figure 2 Configuration View of ST CB

The global barring rules are managed by the operator, and consist of an incoming blacklist, an outgoing blacklist, an incoming white list, an outgoing white list (each of which only includes the condition identity), and reject anonymous (*enable* and *disable*).

The Diversion Global Blacklist is managed by the operator and consists of an outgoing blacklist that only applies to diverted calls, and which only includes the condition identity.

The Operator Barring Programs are configured by the operator, managed through the XML Document Management Server (XDMS) that provides the Customer Administration Interface Third Generation (CAI3G) to the operator.

The Operator Diversion Barring Programs are configured by the operator, managed through the XDMS that provides the CAI3G interface to the operator.

The Operator Permitted Programs are managed through the XDMS that provides the CAI3G interface to the operator.

The Barring Programs are configured by the operator, managed through the XDMS that provides the CAI3G interface to the operator.

The barring rules are managed through the XDMS that provides the CAI3G interface to the operator.

XDMS uses *Sh* (*Diameter*) to update the Home Subscriber Server (HSS).



The relationships between different types of the OCB are described in Section 4.1 on page 13, and the different types of the ICB are described in Section 4.2 on page 14.



3 Service Invocation

Service invocation means that the ST AS starts evaluating the services configured for the node and provisioned for the served PBX. The ST CB is started for the served PBX by various SIP events. The use cases are handled in the originating, diverting, or terminating ST AS, as shown in Table 1.

Table 1 Diverting ST AS Acting As Both Terminating and Originating MTAS.

Use Case	ST AS Type
OCB	Originating, Diverting
ICB	Diverting, Terminating
ACR	Diverting, Terminating

If at least one rule evaluates to `allow=false` and no rule evaluates to `allow=true`, then the communication is barred. This means that only starting ST CB does not mean that a communication is barred, but ST CB checks if it is to be barred.

The events that start the ST CB are listed in Table 2.

Table 2 ST CB Service Invocation

ID	Event	ST AS Role	Use Case	Comment
1	INVITE	Originating	OCB	Initial INVITE.
2	INVITE	Terminating	ICB	Initial INVITE ACR is flavor of ICB
3	INVITE	Transit	OCB	Initial INVITE, only applicable for Terminating ST AS and AS chaining disabled.
4	REFER	Originating	OCB	





4 Barring Rules

The ST AS offers a number of Barring services, which are controlled by the interactions of MOs and per PBX data.

MOs and attributes mentioned in the following sections are further described in *Managed Object Model (MOM)*.

4.1 Relationship Among OCB Types

The OCB service controls the destinations that a user is allowed to call. There are several types of OCB. When a call attempt is evaluated by the different types of OCB, the evaluation stops when a result bar or allow is obtained. If no result is obtained, the call is allowed.

The types of OCB are evaluated in the following order:

1. Diversion Global Blacklist

Allows the operator to bar calls being diverted to all addresses containing any of a list of strings.

This list is configured by setting attribute `mtasStCDivBlackList` in the `MtasStCDiv` MO.

The whole of the normalized target Request URI is searched for each entry in `mtasStCdivBlackList`. The normalized form of service numbers is local number, for example, `tel:151;phone-context=telco.com`. The normalized form of other numbers is global number, for example, `tel:+46107196992`. To disallow diversion of calls to a range of service numbers, for example, 110–119, include “tel:11” and “sip:11” in `mtasStCDivBlackList`. To disallow diversion of calls to a range of other numbers, for example, all Swedish numbers, include “+46” in `mtasStCDivBlackList`.

2. Global OCB White List

Allows the operator to allow calls to a set of addresses.

The set of addresses is configured by setting attributes `mtasStOcbWhiteListNumIncl`, `mtasStOcbWhiteListNumExcl`, and `mtasStOcbWhiteListDomainIncl` in the `MtasStOcb` MO.

3. Global OCB Blacklist

Allows the operator to bar calls to all addresses containing any of a list of strings.

The whole of the normalized Request URI is searched for each entry in `mtasStOcbBlackList`. The normalized form of service numbers is local number, for example, `tel:151;phone-context=telco.com`. The normalized form of other numbers is global number, for example, `tel:+46107196992`. To disallow calls to a range of service numbers, for example, 110–119, include “tel:11” and “sip:11” in `mtasStOcbBlackList`. To disallow calls to a range of other numbers, for example, all Swedish numbers, include “+46” in `mtasStOcbBlackList`.

4. Operator Barring Program or Operator Permitted Program

The Operator Barring Program is provisioned by the operator in the operator part of the ST document of the PBX. It allows the operator to define classes of telephone numbers and domains, and to bar the calls to combinations of those classes on a per PBX basis.

The Operator Permitted Program is provisioned by the operator in the operator part of the ST document of the PBX. It allows the operator to define the groups of telephone numbers and domains, and to allow the calls to combinations of those classes on a per subscriber basis. No further OCB checks are made if a call is NOT permitted by the Operator Permitted Program.

A PBX cannot have both an Operator Barring Program and an Operator Permitted Program.

This program is configured by setting the attributes in the `MtasStOcbOpBCat`, the `MtasStOcbBCat`, and in the `NumberAnalysis` MO, and its subordinate MOs.

5. Operator Diversion Barring Program

The Operator Diversion Barring Program is provisioned by the operator in the operator part of the ST document of the PBX. It allows the operator to define the classes of telephone numbers and domains, and on a per subscriber basis, bar the calls being diverted to combinations of those classes of telephone numbers.

This program is configured by setting the attributes in the `MtasStOcbOpBCat`, the `MtasStOcbBCat`, and in the `NumberAnalysis` MO, and its subordinate MOs.

6. Outgoing barring rules

The outgoing barring rules allow the operator to bar or allow calls by this PBX based on combinations of the following conditions:

- Called identity
- Carrier



4.2 Relationship Among ICB Types

The ICB service controls who can call a PBX. There are several types of ICB. When a call attempt is evaluated by the different types of ICB, the evaluation stops when a result bar or allow is obtained. If no result is obtained, the call is allowed.

The types of ICB are evaluated in the following order:

1. Global ICB White List

Allows the operator to allow calls from a set of addresses.

The set of addresses is configured by setting attributes `mtasStIcbWhiteListNumIncl`, `mtasStIcbWhiteListNumExcl`, and `mtasStIcbWhiteListDomainIncl` in the `MtasStIcb MO`.

2. Global Anonymous Communication Barring

Allows the operator to bar all incoming calls where the caller is anonymous.

This barring is configured by setting attribute `mtasStAcrGlobal` in the `MtasStACR MO`.

3. Global ICB Blacklist

Allows the operator to bar calls from all addresses that contain any part of a list of strings.

An example of a list of string is as follows:

```
spam
otherbarredword
```

This list is configured by setting attribute `mtasStIcbBlackList` in the `MtasStIcb MO`.

The whole of the URI part of each `P-Asserted-Identity` is searched for each entry in `mtasStIcbBlackList`. The normalized form of service numbers is local number, for example, `tel:151;phone-context=telco.com`. The normalized form of other numbers is global number (for example, `tel:+46107196992`). To disallow calls from a range of service numbers, for example, 110–119, include “tel:11” and “sip:11” in `mtasStIcbBlackList`. To disallow calls from a range of other numbers, for example, all Swedish numbers, include “+46” in `mtasStIcbBlackList`.

4. Incoming barring rules

Incoming barring rules allow the operator to bar (or allow) the calls to this PBX based on combinations of the following conditions:

- Calling identity

- Anonymity of caller
- Call has been diverted to this subscriber

If the calling party has OIR active, then those ICB rules that use the identity of the caller are not evaluated.

For more information about ST Identity Presentation, refer to *ST AS Identity Presentation Service Management Guide*.

4.3 Global Barring Rules

The global barring rules are defined by MO attributes. There is one blacklist for global ICB, one blacklist for global OCB, and one blacklist for diverted global OCB. There is also an MO attribute to enable or disable the ACR on a global level. A list entry can contain a string that is matched with the following:

- P-Asserted-Identity in ICB
- Request URI in OCB
- Refer-To URI in OCB
- Referred-By URI in ICB
- From Header in ICB, if the CM attribute `mtasStIcbUseFromHeader` is set to Enabled.

It is not required that the format of the entry is a SIP or tel URI. The matching of the list entry with a URI is true if the list entry is a substring of the URI.

Example:

The following entries:

```
.se
+468
bob@example.com
spam
```

Matches the following URIs:

```
sven@operator.se
+468112233
bob@example.com
12345@good-spam.com
```

Matching is case-sensitive and US-ASCII is used as the character set.

If it is enabled on the global level, all anonymous communications are rejected by the ST AS.



4.4 Global White List

The global white lists are defined by MO attributes. There is one white list for global OCB and one white list for global ICB. Both the Global OCB White List and Global ICB White List contain three lists of strings; Number Included, Number Excluded, and Domain Included.

- The “Number Included”, `mtasStOcbWhiteListNumIncl`, and `mtasStIcbWhiteListNumIncl`, list specifies the leftmost parts of the normalized numbers that are included in the global white list. This list is only compared with a tel URI or a SIP URI containing a telephone number. Each entry in the list contains a string that represents the leftmost part of a number. A string representing a global number must be prefixed by a “+”. A string representing a local number can include the phone-context parameter.
- The “Number Excluded”, `mtasStOcbWhiteListNumExcl`, and `mtasStIcbWhiteListNumExcl`, list specifies the leftmost parts of the normalized numbers that are excluded from the global white list. This list is only compared with a tel URI or a SIP URI containing a telephone number. Each entry in the list contains a string that represents the leftmost part of a number. A string representing a global number must be prefixed by a “+”. A string containing a local number can include the phone-context parameter. Each string must begin with one of the strings in the “Number included” list, but this is not policed.
- The “Domain Included”, `mtasStOcbWhiteListDomainIncl`, and `mtasStIcbWhiteListDomainIncl`, list specifies the set of domains that are included in the global white List. This list is only compared with a SIP URI that does not contain a telephone number. Each entry in the list contains a string that represents the host part of a URI. If the first character in the string is a “*”, this is to be treated as a wildcard character, and a rightmost match of the domain name from the remote identity is performed with the rest of the characters in the string. If the first character in the string is not a “*”, then the domain name from the remote identity must exactly match the included string.

4.5 Relationship Among Operator Barring Programs, Operator Permitted Programs, and Operator Diversion Barring Programs

Operator Barring Programs, Operator Permitted Programs, and Operator Diversion Barring Programs are based on defining a set of Operator Barring Categories. An Operator Barring Category is defined by a list of numbers and domains to be matched, defined by MOs `mtasStOcbOpBCatNumBarred` and `mtasStOcbOpBCatDomain`, and a list of numbers to be exempted from the barring, defined by MO `mtasStOcbOpBCatNumExempted`. There are ten special Barring Categories named: Local, Non Local, L_National, L_International, L_IntraLata, L_IntraLataToll, L_InterLata,

`L_NanpZone1`, `L_Nanp`, and `Allow Local`, which are defined by setting data in `MO NumberAnalysis`, refer to *Managed Object Model (MOM)*.

An Operator Barring Program of the PBX is defined in the operator part of the XML file of the PBX. The element contains a list of category names; the list can consist of Operator Barring Category Names and special Barring Category names.

An Operator Permitted Program of the PBX is defined in the operator part of the XML file of the PBX instead of an Operator Barring Program. The element contains a list of category names; the list can consist of Operator Barring Category Names and special Barring Category Names except `Allow Local`.

When the PBX user attempts to make an outgoing call, the number is extracted from the Request URI and checked against the set of Operator Barring Categories and special Barring Categories specified for the user. If the Request URI does not contain a telephone number, then the domain is extracted and checked against the set of Operator Barring Categories.

An Operator Diversion Barring Program of the PBX is defined in the operator part of the XML file of the PBX. The element contains a list of category names; the list can consist of, Operator Barring Category Names and special Barring Category Names.

When the PBX user attempts to divert an incoming call, the number is extracted from the Request URI and checked against the set of Operator Barring Categories, and special Barring Categories specified for the PBX in the union of the Operator Barring Program, and the Operator Diversion Barring Program. If the Request URI does not contain a telephone number, then the domain is extracted and checked against the set of Operator Barring Categories.

Note: Which special Barring Categories a call is in, is determined regarding the values in the `NumberAnalysis` MO and its subordinate MOs, refer to *Managed Object Model (MOM)*.

If the set of categories contains any of `L_National`, `L_International`, `L_IntraLata`, `L_IntraLataToll`, `L_InterLata`, `L_NanpZone1`, or `L_Nanp`, the call type is determined by a reference to `MOC NumberAnalysis` and its subordinates. If the call type matches the category, the call is barred, and the generic announcement indicated by the corresponding instance of `mtasStOcbLocalnessBCatAnnouncementName` is played.

To check whether a number or domain is barred by an Operator Barring Program, or permitted by an Operator Permitted Program, the number is checked against each Operator Barring Category, the domain is checked against each Operator Barring Category until a match is found, or all Operator Barring Categories in the set have been checked.

To check whether a number is a match for an Operator Barring Category or Barring Category, the number is front substring compared to each entry in the list of numbers to be barred. If a match is found, the number is front substring compared to each entry in the list of numbers to be exempted. If a match is not

found, the number is barred. If a match is found, the number is exempted, and the checking moves on to the next Operator Barring Category.

To check whether a domain is a match for an Operator Barring Category, the host part of the URI is whole string matched against the list of allowed domains, each of which can contain a single wildcard at the beginning.

4.5.1 Subscriber Data

Use of the operator of the Operator Barring Programs feature is defined in XML, and is part of the transparent data of the PBX held on the HSS. Operator Barring Program has one operator part, as shown in Figure 3.

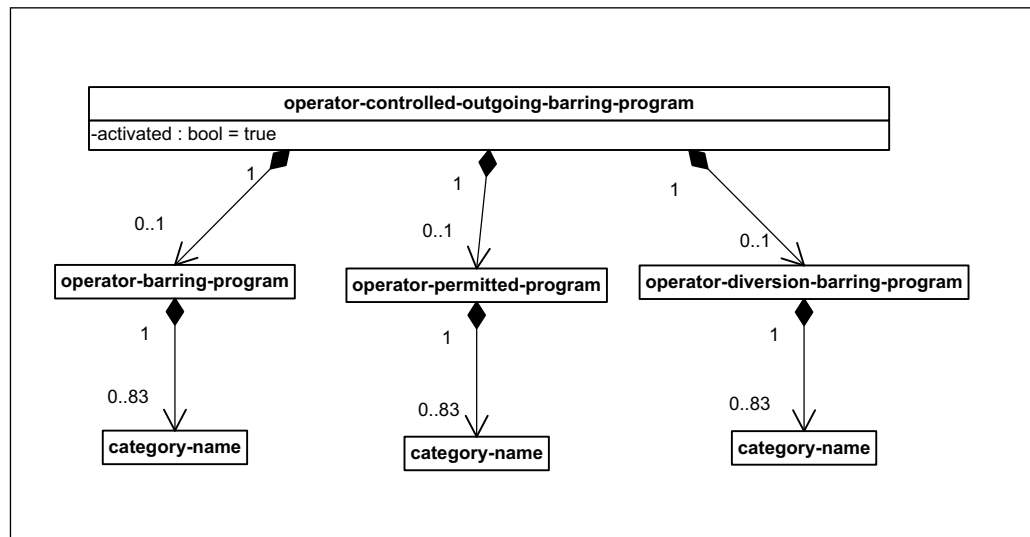


Figure 3 Operator Outgoing Barring Programs Elements

4.6 Barring Rules

The barring rules, defined by XML, are managed per ICB and OCB. ACR is a special case of ICB, and its rules are defined under ICB.

The XML is defined by a schema, and follows the structure illustrated in Figure 4.

The rule set consists of zero or more rules, and each rule consists of zero or more conditions, and one or more actions.

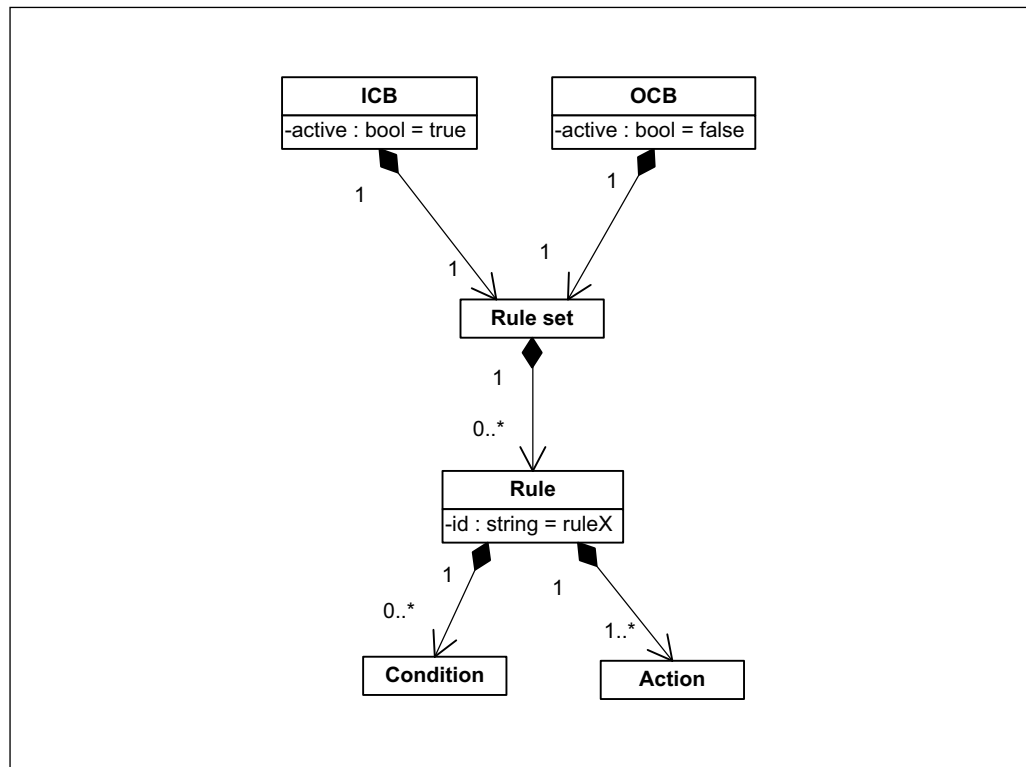


Figure 4 Subscriber Barring Rules Elements

The rule has one mandatory action named `allow` of type Boolean. If it is:

- `True` then allow the communication
- `False` then bar the communication

The other actions that apply to barring are the following:

- `st-serv:play-announcement`

This action is used to indicate CB service to play announcement by using Generic Announcement service if barring is successful. The play-announcement action contains the selected operator named string value to be played to the calling party. The play-announcement action cannot be combined with `allow=true` action within the same rule.

- `st-serv:play-segmented-announcement`

This action is used to indicate CB service to play a segmented announcement by using Generic Announcement service if barring is successful. The play-segmented-announcement action contains the selected operator named string value to be played to the calling party, and the optional list of announcement voice variable name and value pairs. The play-segmented-announcement action cannot be combined with `allow=true` action within the same rule.



The Rule element has one attribute `id` that identifies the rule. It is not used for determining the evaluation order.

The ICB/OCB service elements in the user configuration part of the PBX service configuration document have an attribute `active` of type Boolean. `Active` must be set to `true` for the barring rules to be evaluated if the corresponding service invocation is executed. If the `active` attribute is not present, its default value is `true`.

The conditions that apply to barring are as follows:

- `cp:identity`

For ICB and ACR, this condition evaluates to `true` when the calling user identity matches the value of the identity element. For OCB, this condition evaluates to `true` when the called user identity matches the value of the identity element. In all other cases, the condition evaluates to `false`. The interpretation of the special cases of a `one id` element containing a `hidden: URI` and a `one id` element containing `number-match` element are described in this section. The interpretation of all the other elements of this condition is described in [IETF RFC 4745](#).

If there is more than one URI, the ST CB iterates over all the URIs and evaluates the barring rules. If one evaluates to `allow=false`, then the communication is barred.

The comparison of tel URIs is based on *Section 4* in [IETF RFC 3966](#).

However, for ST CB, the input tel URI is only considered equal to the `one id`, or `except` element in the `cp:identity` condition (the rule URI), if the number parts match and the parameters satisfy the following conditions:

- If there is a `phone context=<pvalue>` parameter in the rule URI, then there must be an identical `phone context=<pvalue>` parameter in the input URI.
- If there is no `phone-context` parameter in the rule URI, then there must be no `phone-context` parameter in the input URI.
- If there is an `ext=<phonedigits>` parameter in the rule URI, then there must be an identical `ext=<phonedigits>` parameter in the input URI.
- If there is no `ext` parameter in the rule URI, then any `ext` parameter in the input URI is ignored.
- If there is an `isub=<subaddress>` parameter in the rule URI, then there must be an identical `isub=<subaddress>` parameter in the input URI.
- If there is no `isub` parameter in the rule URI, then any `isub` parameter in the input URI is ignored.
- Any other parameters are ignored.

For ST CB, the input tel URI is considered to match the `number-match` element in the `cp:identity` condition (the rule URI) if the first few characters of the number part of the input URI match all the characters in the rule URI. Parameters cannot appear in the `number-match` element, so any parameter in the input URI is ignored.

The comparison of SIP URIs is based on *Section 19.1.4* in [IETF RFC 3261](#).

However, only the user and host parts of SIP URIs are considered when comparing for ST CB, that is, the password, port, URI parameters, and headers are ignored for comparing SIP URIs for ST CB. For a SIP URI that was converted from a tel URI, the user part of the SIP URI contains the number and parameters of a tel URI. The comparison must first consider the host part of the SIP URI, and then must treat user part as if it were a tel URI.

The comparison of hidden URIs is performed as if there were a `one id` element in the identity condition for each identity in the corresponding entry in the `operator-dynamic-black-list` element.

If the calling party has OIR active, then those ICB rules, which use the identity of the caller, are not evaluated.

For more information about Identity Presentation, refer to *ST AS Identity Presentation Service Management Guide*.

- `st-serv:anonymous`

For ICB, this condition is evaluated as shown in Figure 6. This condition is not allowed in rules in OCB.

- `st-ser:communication-diverted`

This condition evaluates to `true` when the incoming communication has been previously diverted. This condition is not allowed in rules in OCB.

Note: Diverted communication can be recognized by the presence of the `History-Info` header field, refer to *ST AS Communication Diversion Management Guide*.

- `st-serv:rule-deactivated`

This condition always evaluates to `false`. This can be used to deactivate a rule, without losing information. By deleting this condition, the rule can be activated again.

- `ocp:other-identity`

If present in any rule, the `other-identity` element, which is empty, matches all identities that are not referenced in any rule. It allows for specifying a default policy.

- `st-serv:carrier`



This condition consists of the following two optional elements:

- The `carrier-select-code` element contains the dialed Carrier Select Code (CSC). The operator can allow or disallow the use of the `carrier-select-code` element for the user and a complete match is done.
- The `carrier-name` element contains an alias name of the carrier selected for the call on call-by-call basis.

The `st-serv:carrier` condition is not allowed in rules in ICB. For OCB, this condition evaluates to `true` if the carrier selected by the Carrier Select Rn (CS Rn) service is matching to the `carrier-name` or `carrier-selection-code` in the condition.

4.7 Evaluation of Rules

If the rule set is active, then the CB evaluates the rules. The rules are evaluated from top to bottom, for example, rule `n` precedes rule `n+1`.

All the rules in the rule set are evaluated to test if their respective conditions are `true`. A rule is said to be matched if all conditions evaluate to `true`. This means that the evaluation of conditions stops when the first condition is `false` (lazy evaluation).

A rule with no conditions is always matched and can be used to realize an unconditional barring rule.

If exactly one rule matches, then its specified action is executed, for example, if `allow` is as follows:

If exactly one rule matches, then its specified action is executed:

- `allow=true` – the call continues normally
- `allow=false` – the call is barred

If more than one rule matches and one or more evaluates to `allow=true`, then the call continues normally. This means that the evaluation of rules stops when the first matched rule with `allow=true` is encountered. If more than one rule matches and all evaluate to `allow=false`, then the call is barred.

If there are no matching rules, the ST CB execution ends without action and the call is accepted by the ST AS.

4.7.1 Identity Condition

Figure 5 shows the algorithm for extracting the user identity to compare with the identity condition.

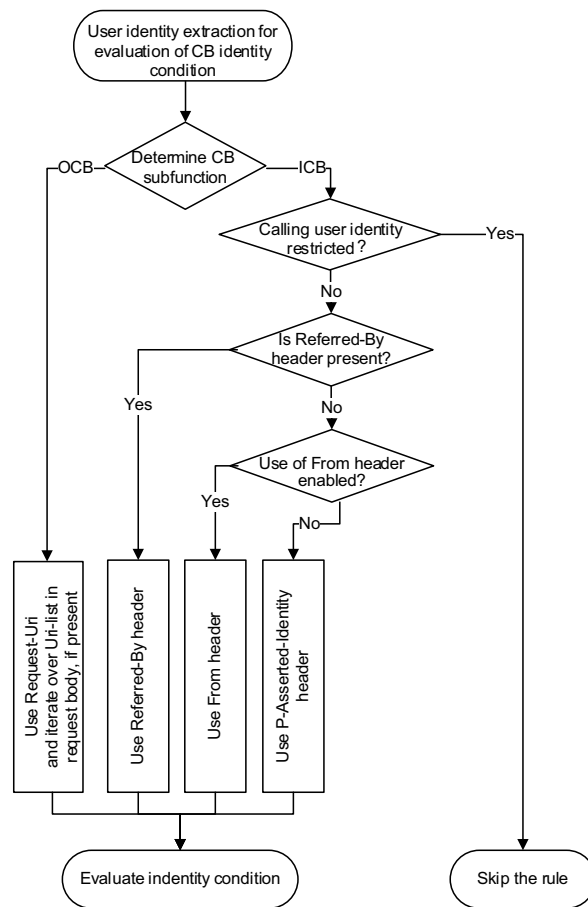


Figure 5 User Identity Extraction for Evaluation of ST CB Identity Condition

It is worth noting that it can be multiple P-Asserted-Identity headers present in the triggering SIP messages and the ST CB service iterates through all them. A SIP `INVITE` request can also include a Uniform Resource Identifier (URI) list in the body that is to be processed by the ST CB. In such cases, the service is started multiple times by one request - once per each identity in the list.

The URIs `sip:+4981770124@example.com;user=phone` and `sip:+4981770124@example.com` are different addresses. These addresses can be related to the same, or a different user. The inclusion of the `user=phone` parameter indicates that the URI is a tel URI that has been converted to a SIP URI in accordance with *Section 19.1.6* in [IETF RFC 3261](#).

4.7.2 Anonymous Condition

Figure 6 shows the algorithm for extracting the user identity to compare with the identity condition.

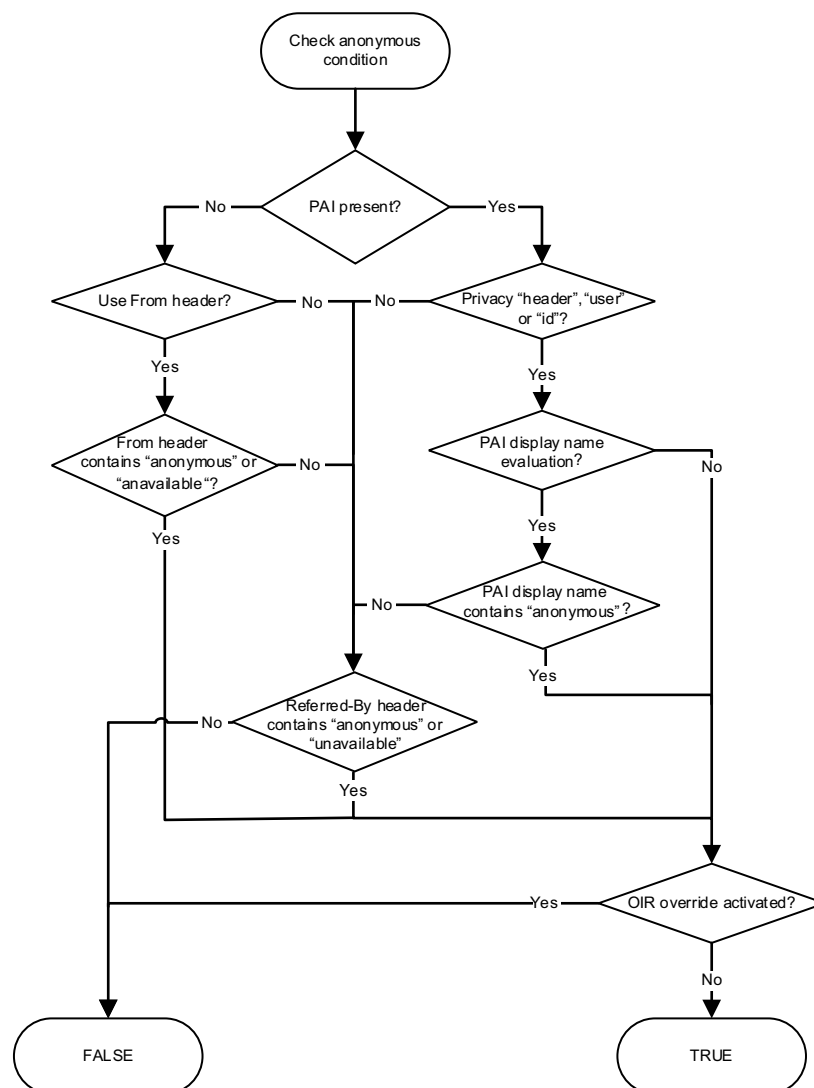


Figure 6 Anonymity Algorithm

Note: A simple case insensitive string search is used to determine if a header field or display name, in respective cases, contains either “anonymous” or “unavailable” strings.





5 Barring Service Configuration

The Barring Service is controlled by the *MtasStCb* MO and its children. An overview of the CB MO structure is shown in Figure 7.

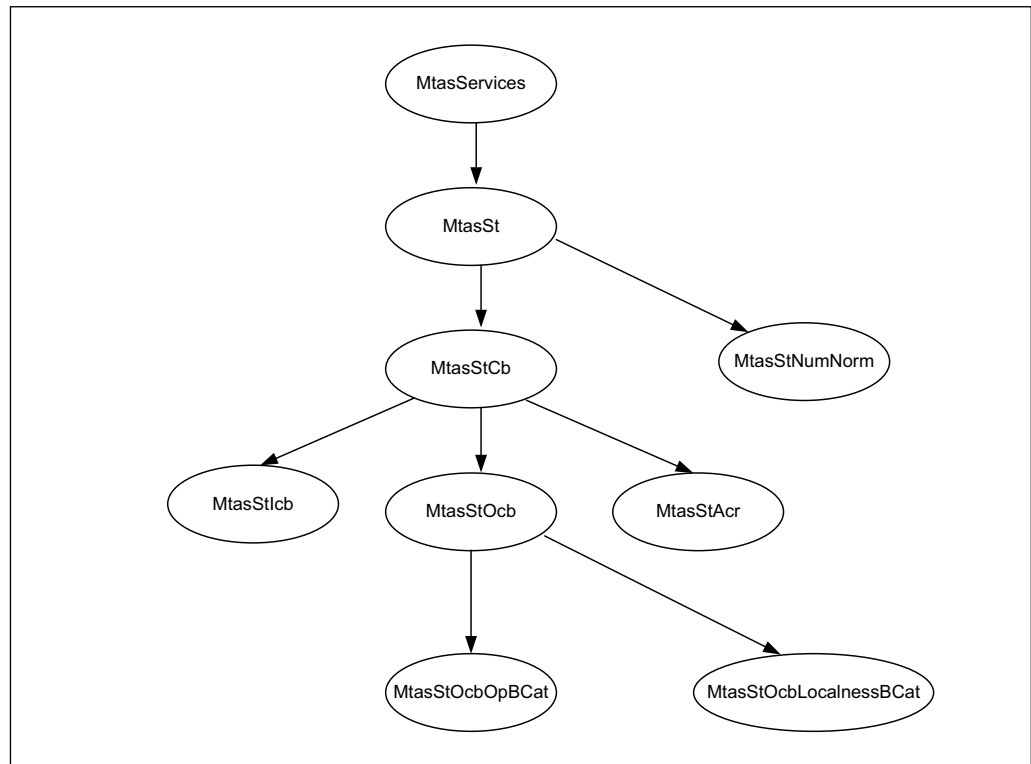


Figure 7 CB MO Structure

For a definition of configurable MOs and attributes related to the ST CB service, refer to *Managed Object Model (MOM)*.

5.1 Overview Tables and Activation

This section describes the general knowledge needed for handling and activation of tables needed for configuring an operator barring category, see Section 5.3 on page 29.

5.1.1 View Selection and Standby Tables Edit

In the CM browser, the ST AS offers one active and one standby view. The same MO attribute is used to display both the active and the standby table. By default, the active table is presented.

The view can be changed at any time in the CM browser using attribute `mtasStOcbOpBCatView`. This attribute can have values 0 (Active view) or 1 (Standby view).

Editing of the tables in active view is not allowed. In standby view, however, the standby tables can be edited without affecting the traffic in any way. The changes take effect when the standby tables are activated.

Activation can be done either with immediate effect, see Section 5.1.2 on page 28, or by setting a scheduled change time, see Section 5.1.3 on page 28. On activation the active and the standby tables are swapped. The effects of the last activation procedure can be canceled simply by repeating the activation procedure. The new entries become effective in the upcoming new sessions. Before activation, validity checks are executed on the entries.

If a configuration or activation request is rejected because of invalid data, an error with a text pointing out the reason for failure is presented to the user in the CM browser.

5.1.2 Activation State Configuration

Attribute `mtasStOcbOpBCatActivationState` describes the activation state of the standby dial plan table and can have one of the following values:

0=Idle	This is the default state. There is no operation in progress.
1=Activate	Activation with immediate effect is requested. When the operator sets this state, the values in the standby table become active unless they are invalid. If invalid data, the activation request is rejected.
2=Processing	A table copy operation is in progress. During this time editing the entries, changing the activation state, or entering a scheduled change time (see Section 5.1.3 on page 28) is disabled. When the operation has finished, the state is changed automatically to 0=Idle.
3=CopyToStandby	Starts an asynchronous operation which copies the entries from the active table to the standby table. The values previously stored in the standby table are overwritten.

An activation with immediate effect can be triggered by setting `mtasStOcbOpBCatActivationState` to 1=Activate. While loading the data, incoming traffic requests are queued. The requests are answered when the data is fully loaded. In addition, the ST AS offers a functionality which copies the active entries to the standby table (see state 3=CopyToStandby) as a preparation for changing the currently active entries. This operation does not affect the traffic in any way, but it implicitly cancels any scheduled activation.



5.1.3 Activation Schedule Configuration

The attribute `mtasStOcbOpBCatChangeTime` can be used to define a time point in the future when the standby table is activated. By default `mtasStOcbOpBCatChangeTime` is set to empty string, meaning that no change is scheduled.

The format used to specify a valid change time is: `YYYY-MM-DDThh:mm:ss`, see *ISO 8601:2004(E)*. For example, value `2011-07-23T18:15:00` schedules changing the active table at 18:15:00 on 23 of July 2011.

An activation can be scheduled only in state `0=Idle`. The execution time is limited to two weeks. When `mtasStOcbOpBCatChangeTime` is set to a valid time in the future, and the current standby entries are valid a change is scheduled, otherwise the configuration attempt is rejected.

The scheduled activation is handled similar to setting `mtasStOcbOpBCatActivationState` to `1=Activate`, with the only difference that the standby table does not become effective immediately but later.

A scheduled activation can be canceled by setting `mtasStOcbOpBCatChangeTime` to the empty string at any time. Setting `mtasStOcbOpBCatChangeTime` to a valid time in the future reschedules the activation.

While the data is loading, the activation state is changed automatically to `2=Processing`. Canceling or rescheduling activation is not possible when the loading of the data has started. When the data is fully loaded, `mtasStOcbOpBCatChangeTime` is set back to empty string.

5.2 ACR Display Name Evaluation Configuration

ACR evaluates reasons for lack of caller identity when determining whether a call is an anonymous call. If `mtasStAcrDisplayNameEvaluation` in `MO MtasStIdPres` is set to `1 (Enabled)`, then anonymous calls are only rejected when `display-name` portion of `P-Asserted-Identity` contains "Anonymous". When set to `0 (Disable)`, then the `display-name` of `P-Asserted-Identity` is not checked by the service.

5.3 Operator Barring Category Configuration

The following sections describe how to create, modify, and delete an Operator Barring Category.

5.3.1 Configure Operator Barring Category

The ST AS stores one active and one standby table for each MO. Both the active and the standby table is accessible at any time. Changing the entries is



possible only in the standby table. Changes become effective for new sessions after the standby table is activated.

Refer to Section 5.1 on page 27 for details on selecting and editing the tables.

To create an Operator Barring Category:

1. Navigate to the `MtasStOcb` MO, refer to Figure 7 for where it is placed in the MO hierarchy.
2. Right-click `MtasStOcb` and select **New** in the pop-up menu. This results in the **Set Entry Object Classes** window.
3. If there are any classes in the **Selected Classes** field, select them and click **Remove**.
4. Select `MtasStOcbOpBCat` from the alphabetic list in the **Available Classes** field.

Enter the Relative Distinguished Name (RDN), for example, `MtasStOcbOpBCat=0`, and click **Add**. The RDN for `MtasStOcbOpBCat` must be an integer in the range of 0–63.

5. Click **OK**.

A new `MtasStOcbOpBCat` MO is presented in the CM browser.

6. In the **Table Editor** window, set attribute `mtasStOcbOpBCatName` to a meaningful name for this Operator Barring Category. Each Operator Barring Category must have a unique name across all instances of User Barring Category and Operator Barring Category. No Operator Barring Category can have the name “Local”, “Non Local”, “L_National”, “L_International”, “L_IntraLata”, “L_IntraLataToll”, “L_InterLata”, “L_NanpZone1”, “L_Nanp”, or “Allow Local”.
7. Set the `mtasOcbOpBCatView` attribute of the MO to 1 (stand by view).
8. Click **Submit**.
9. In the **Table Editor** window, set attribute `mtasStOcbOpBCatBarred` to a list of strings.

Each entry in the list of strings is shown by a separate row in the **Table Editor** window.

To add an entry to the list, right-click the attribute name, and select **Add Another Value** from the pop-up menu.

This results in another row in the **Table Editor**, labeled `mtasStOcbOpBCatBarred`. Each string is the leftmost part of a set of telephone numbers that are to be included in this Operator Barring Category. For example, `+447` matches mobile numbers in the United Kingdom, and `150` can match operator inquiry numbers.



10. In the **Table Editor** window, set attribute `mtasStOcbOpBCatExempted` to a list of strings.

Each entry in the list of strings is shown by a separate row in the **Table Editor** window.

To add an entry to the list, right-click the attribute name, and select **Add Another Value** from the pop-up menu.

This results in another row in the **Table Editor** window, labeled as `mtasStOcbOpBCatExempted`. Each string is the leftmost part of a set of telephone numbers that are to be exempted from inclusion in this Operator Barring Category. Each exemption string begins with one of the barred strings in this Operator Barring Category. For example, `+4476` matches pager numbers in the United Kingdom, and `150;phone-context=company.com` matches inquiry number of the company.

11. In the **Table Editor** window, set the attribute `mtasStOcbOpBCatDomain` to a list of strings.

Each entry in the list of strings is shown by a separate row in the **Table Editor** window.

To add an entry to the list, right-click the attribute name, and select **Add Another Value** from the pop-up menu.

This results in another row in the **Table Editor** window, labeled `mtasStOcbOpBCatDomain`. Each string represents the host part of a non-numerical Internationalized Resource Identifier (IRI) to be included in this Operator Barring Category. If the first character in the string is a "*", this is treated as a wildcard character, and a rightmost comparison of the host part of the URI is performed with the rest of the characters in the string. If the first character in the string is not an "*", then the host part of the URI must exactly match the string.

For example, `*.co.uk` matches `ericsson.co.uk` and `virgin.co.uk`, `virgin.co.uk` matches only `virgin.co.uk`, and `virgin*.co.uk` matches only `virgin*.co.uk`.

12. In the **Table Editor** window, set attribute `mtasStOcbOpBCatAnnouncementName` to the name of a Generic Announcement, that is, an instance of `MtasGaAnn`. For more information about Generic Announcements, refer to *MTAS Generic Announcement Management Guide*.
13. In the **Table Editor** window, set attribute `mtasStOcbOpBCatSSID` to the value to be reported in the Supplementary Service Identity AVP in the charging message generated when a call is barred by this Barring Category.

The meanings of the allowed values are as follows:

101	OCB
------------	------------



140 National Toll Restriction

141 International Toll Restriction

14. Click **Submit**.

5.3.2 Modify Operator Barring Category

The MTAS stores one active and one standby table for each MO. Both the active and the standby table is accessible at any time. Changing the entries is possible only in the standby table. Changes become effective for new sessions after the standby table is activated.

Refer to Section 5.1 on page 27 for details on selecting and editing the tables.

To modify an Operator Barring Category:

1. Navigate to the `MtasStOcbOpBCat` MO.
2. Select the instance of `MtasStOcbOpBCat` to be modified.
3. In the **Table Editor** window, modify the attributes as required.

To add an entry to `mtasStOcbOpBCatBarred`, `mtasStOcbOpBCatExempted`, or `mtasStOcbOpBCatDomain`, right-click the attribute name and select **Add Another Value** from the pop-up menu.

This results in another row in the **Table Editor** window, labeled appropriately.

Delete an entry from `mtasStOcbOpBCatBarred`, `mtasStOcbOpBCatExempted`, or `mtasStOcbOpBCatDomain` by right-clicking the attribute name and select **Delete** from the pop-up menu.

This results in the selected row being removed from the **Table Editor** window.

Modify an attribute by selecting the contents of the field to be changed and type the new value into the field.

4. Click **Submit**.

5.3.3 Delete Operator Barring Category

The ST AS stores one active and one standby table for each MO. Both the active and the standby table is accessible at any time. Changing the entries is possible only in the standby table. Changes become effective for new sessions after the standby table is activated.

Refer to Section 5.1 on page 27 for details on selecting and editing the tables.

To delete an Operator Barring Category:



1. Navigate to the `MtasStOcbOpBCat` MO.
2. Right-click the instance of `MtasStOcbOpBCat` to be deleted, and select **Delete** in the pop-up menu.

5.4 Localness Barring Categories Configuration

The nine instances of the `MtasStOcbLocalnessBCat` MO are created by the system. None of these can be deleted, and no more can be created. The following section describes how to modify the attributes of a Localness Barring Category.

The nine instances of `MtasStOcbLocalnessBCat` have the following names: “Local”, “Non Local”, “L_National”, “L_International”, “L_IntraLata”, “L_IntraLataToll”, “L_InterLata”, “L_NanpZone1”, and “L_Nanp”

The system creates each instance of `MtasStOcbLocalnessBCat` with the following attribute values:

<empty> `mtasStOcbLocalnessBCatAnnouncementName`

101 `mtasStOcbLocalnessBCatSSId`

5.4.1 Modify Localness Barring Category

To modify a Localness Barring Category:

1. Navigate to the `MtasStOcbLocalnessBCat` MO.
2. Select the instance of `MtasStOcbLocalnessBCat` to be modified.
3. In the **Table Editor** window, modify the attributes as required.

Set attribute `mtasStOcbLocalnessBCatAnnouncementName` to the name of a Generic Announcement, that is, an instance of `MtasGaAnn`. For more information about Generic Announcements, refer to *MTAS Generic Announcement Management Guide*.

Set attribute `mtasStOcbLocalnessBCatSSId` to the value to be reported in the Supplementary Service Identity AVP in the charging message generated when a call is barred by this Barring Category.

The meanings of the allowed values are as follows:

101	OCB
140	National Toll Restriction
141	International Toll Restriction

4. Click **Submit**.



5.5 Global White List Configuration

This section describes how to configure the ICB Global White List. The OCB Global White List configuration is similar.

The ICB Global White List is defined by the following three attributes:

- `mtasStIcbWhiteListNumIncl`
- `mtasStIcbWhiteListNumExcl`
- `mtasStIcbWhiteListDomainIncl`

The `mtasStIcbWhiteListNumIncl` and `mtasStIcbWhiteListNumExcl` attributes define the numerical addresses in the White List.

`mtasStIcbWhiteListNumIncl` lists the leftmost part of numbers to be included in the ICB Global White List. `mtasStIcbWhiteListNumExcl` lists the leftmost part of numbers to be excluded from the ICB Global White List.

The `mtasStIcbWhiteListDomainIncl` attribute defines the non-numerical addresses in the ICB Global White List, by listing the domains to be included in the ICB Global White List.

5.5.1 Modify List of Numbers Included in ICB Global White List

To modify the list of numbers included in the ICB Global White List:

1. Navigate to the `MtasStIcb` MO.
2. In the **Table Editor** window, modify the `mtasStIcbWhiteListNumIncl` attribute as required. To add an entry to `mtasStIcbWhiteListNumIncl`, right-click the attribute name and select **Add Another Value** from the pop-up menu.

This results in another row in the **Table Editor** window, labeled appropriately.

To delete an entry from `mtasStIcbWhiteListNumIncl`, right-click the attribute name, and select **Delete** from the pop-up menu.

This results in the selected row being removed from the **Table Editor** window.

To modify an entry in `mtasStIcbWhiteListNumIncl`, select the contents of the field to be changed, and type the new value into the field.

3. Click **Submit**.

5.5.2 Modify List of Numbers Excluded from ICB Global White List

To modify the list of numbers excluded from the ICB Global White List:



1. Navigate to the `MtasStIcb` MO.
2. In the **Table Editor** window, modify the `mtasStIcbWhiteListNumExcl` attributes as required. To add an entry to `mtasStIcbWhiteListNumExcl`, right-click the attribute name and select **Add Another Value** from the pop-up menu.

This results in another row in the **Table Editor**, labeled appropriately.

To delete an entry from `mtasStIcbWhiteListNumExcl`, right-click the attribute name and select **Delete** from the pop-up menu.

This results in the selected row being removed from the **Table Editor** window.

To modify an entry in `mtasStIcbWhiteListNumExcl`, select the contents of the field to be changed and type the new value into the field.

3. Click **Submit**.

5.5.3

Modify List of Domains Included in ICB Global White List

To modify the list of numbers excluded from the ICB Global White List:

1. Navigate to the `MtasStIcb` MO.
2. In the **Table Editor** window, modify the `mtasStIcbWhiteListDomainIncl` attributes as required. To add an entry to `mtasStIcbWhiteListDomainIncl`, right-click the attribute name and select **Add Another Value** from the pop-up menu.

This results in another row in the **Table Editor**, labeled appropriately.

To delete an entry from `mtasStIcbWhiteListDomainIncl`, right-click the attribute name and select **Delete** from the pop-up menu.

This results in the selected row being removed from the **Table Editor** window.

To modify an entry in `mtasStIcbWhiteListDomainIncl`, select the contents of the field to be changed and type the new value into the field.

3. Click **Submit**.

5.6

Generic Announcement Name Configuration

The ST CB service plays an announcement by using the Generic Announcement service to indicate to the caller that barring is applied.

The ST CB generic announcement name attributes are summarized in Table 3.

Table 3 ST CB Generic Announcement Name Attributes

Use Case	Generic Announcement Name Attribute
ICB	mtasStIcbAnnouncementName
ACR	mtasStAcrAnnouncementName
OCB	mtasStOcbAnnouncementName
Operator Controlled Outgoing Barring Programs (OCOBP)	mtasStOcbLocalnessBCatAnnouncementName mtasStOcbOpBCatAnnouncementName

For details about configuring announcements using MTAS Generic Announcement functionality, refer to *MTAS Generic Announcement Management Guide*.

5.7 Communication Barring Administrative State Configuration

The whole set of barring services is enabled by setting the `mtasStCbAdministrativeState` attribute in the `MtasStCb` MO to **1** (Unlocked). If `mtasStCbAdministrativeState` is set to **0** (Locked), none of the barring services are provided.

5.8 Service Data Configuration

This section describes how to configure the service data.

5.8.1 Subscription Level Service Configuration

The operator can activate or deactivate the ST CB services subscription for the PBX by setting the user data using the CAI3G protocol through the XDMS.

For more information about the CAI3G protocol in the ST AS, refer to *MTAS CAI3G Interface for ST AS*.

For the Subscription Level Service configuration following applies:

- Barring rules

In addition to checking that a modified rule set complies with the appropriate schema, the XDMS rejects an update if any of the following checks fail:

- At most one instance of the ICB service data is displayed in the `simservs` document.



- At most one instance of the OCB service data is displayed in the `simserve` document.
- Only the conditions specified in Section 4 on page 13 appear in each CB rule.
- Each CB rule contains exactly one allow action.
- At most one of the conditions `identity`, `anonymous`, and `other-identity` is displayed in any rule.
- If an `identity` condition contains a `many domain=<host>` part, and if there are `except` parts within that `many domain=<host>` part, then all those `except` parts are `except id=<user>@<host>`. That is, there are no `except domain` parts within a `many domain=<host>` part, and all `except id=<user>` parts in a `many domain=<host>` part are users in the domain.
- The content of each one `id` part of each `identity` condition in an OCB rule is either a SIP URI or a tel URI.
- The content of each one `id` part of each `identity` condition in an ICB rule is either a SIP URI or a tel URI or a `hidden: URI`.
- The content of each `except id` part of each `identity` condition is either a SIP URI or a tel URI.
- If an `identity` condition contains some one `id=<user>` parts and a `many domain=<host>` part, which contains some `except id=<user>@<host>` parts, no `<user>` is displayed in both a one `id` part and an `except id` part.
- Each CB rule contains at most one of each of the following conditions: `anonymous`, `identity`, `other-identity`, `communication-diverted`, or `rule-deactivated`.
- Each tel URI in the rules, and each SIP URI in the rules that was converted from a tel URI according to *Section 19.1.6 in IETF RFC 3261* contains a normalized number.
- In an `identity` condition, each one element has a distinct `id=<user>` part.
- In an `identity` condition, each `many` element that has a `domain=<host>` part has a distinct `<host>` value.
- In an `identity` condition, there is at most one `many` element with no domain.
- In an `identity` condition, each `except` element that has an `id=<user>` part has a distinct `id` value.
- In an `identity` condition, each `except` element that has a `domain=<host>` part has a distinct `<host>` value.

- In an identity condition, each except element contains either an `id=<user>` part or a domain = `<host>` part.
- In an identity condition, each number-match element has a distinct starts-with part.
- If an identity condition contains some number-match starts-with=`<partial number>` part and a many part, which contains some except `id=<user>` part, no `<user>` matches both a number-match starts-with part and an except id part.
- Each ICB rule contains at most one of each of the following actions, play-announcement, and play-segmented-announcement.
- Each OCB rule contains at most one of each of the following actions, play-announcement, and play-segmented-announcement.
- If the action element contains `allow=true`.
- If the action element contains `allow=true` and play-announcement.
- If the action element contains `allow=true` and play-segmented-announcement.
- If the action element contains play-announcement and play-segmented-announcement.
- The number of ST CB rules is less than, or equal to, the maximum number of rules.
- The carrier condition is activated for the user in the operator part of the OCB service, only when the user has the CS Rn service activated.

The check that none of the forward-to targets in the CDIV rule set are barred by the OCB service is supplied by the CDIV, and therefore, is not supplied by the ST CB.

- Operator Barring Programs

The Operator Controlled Barring Programs data in the operator part of the XML file of the subscriber must comply with the operator controlled outgoing barring programs schema, refer to *MTAS CAI3G Interface for ST AS*.



6 Performance Management

For details about measurements related to the ST CB service, refer to *Managed Object Model (MOM)*.





7 Fault Management

The ST CB service has no alarms.





8 Barring Rule Configurations Examples

This section shows examples of rule configurations that can be applied for the ST CB service.

To guarantee its uniqueness, a namespace can often be a long string. The XML allows a namespace to be mapped to a short string (a prefix), which makes the XML documents more readable. The mapping between each namespace and its assigned prefix as used in this section is shown in Table 4.

Table 4 Namespace Prefix Mapping

Prefix	Namespace	Purpose
cp	urn:ietf:params:xml:ns:common-policy	Common Policies for privacy preferences as defined by the IETF.
ocp	urn:oma:xml:xm:common-policy	Common Policies for mobile as defined by the Open Mobile Alliance (OMA).
ss	http://uri.etsi.org/ngn/params/xml/simservs/xcap	User part of the MMTel document as defined by ETSI and TISPAN. User part is also used in ST AS, but in this document referred to as the PBX part.
st-op	http://schemas.ericsson.com/st/operator-service-data	ST operator services.
st-serv	http://schemas.ericsson.com/st/services	Ericsson defined services for inclusion in the ST PBX-data part.

For more information about how the identity can be expressed, refer to [IETF RFC 4745](#).

8.1 Bar Incoming Communication from Alice

In the rule configuration shown in Example 1, the following applies for the served user:

- All incoming communication from `alice@example.com` is blocked.

```
<st-serv:st-incoming-communication-barring active="true">
  <cp:ruleset>
    <cp:rule id="rule1">
      <cp:conditions>
        <cp:identity>
          <cp:one id="sip:alice@example.com"/>
        </cp:identity>
      </cp:conditions>
      <cp:actions>
        <st-serv:allow>false</st-serv:allow>
      </cp:actions>
    </cp:rule>
  </cp:ruleset>
</st-serv:st-incoming-communication-barring>
```

Example 1 Bar Incoming Communication from Alice

8.2 Bar Incoming Communication from Anonymous

In the rule configuration shown in Example 2 the following applies for the served user:

- All incoming communication from an anonymous caller is blocked.

The ACR use case is expressed as the following rule:

- Condition: anonymous
- Action: allow=false

```
<st-serv:st-incoming-communication-barring active="true">
  <cp:ruleset>
    <cp:rule id="rule2">
      <cp:conditions>
        <st-serv:anonymous>
      </cp:conditions>
      <cp:actions>
        <st-serv:allow>false</st-serv:allow>
      </cp:actions>
    </cp:rule>
  </cp:ruleset>
</st-serv:st-incoming-communication-barring>
```

Example 2 Bar Incoming Communication from Anonymous



8.3 Bar Incoming Communication from example.com except from Alice and Bob

In the rule configuration shown in Example 3 the following applies for the served user:

- All incoming communication from `example.com` except from Alice and Bob is blocked.

```
<st-serv:st-incoming-communication-barring active="true">
  <cp:ruleset>
    <cp:rule id="rule3">
      <cp:conditions>
        <cp:identity>
          <cp:many domain="example.com">
            <cp:except id="sip:alice@example.com"/>
            <cp:except id="sip:bob@example.com"/>
          </cp:many>
        </cp:identity>
      </cp:conditions>
      <cp:actions>
        <ss:allow>false</ss:allow>
      </cp:actions>
    </cp:rule>
  </cp:ruleset>
</st-serv:st-incoming-communication-barring>
```

Example 3 Bar Incoming Communication from example.com except from Alice and Bob

8.4 Bar Incoming from Range of Numbers

The element `number-match` is introduced by Ericsson. In the rule configuration shown in Example 4, incoming communication from numbers starting with +4424 are barred.

```
<st-serv:st-incoming-communication-barring active="true">
  <cp:ruleset>
    <cp:rule id="Coventry">
      <cp:conditions>
        <cp:identity>
          <st-serv:number-match starts-with="+4424"/>
        </cp:identity>
      </cp:conditions>
      <cp:actions>
        <st-serv:allow>false</st-serv:allow>
      </cp:actions>
    </cp:rule>
  </cp:ruleset>
</st-serv:st-incoming-communication-barring>
```

Example 4 Bar Incoming from Range of Numbers

8.5 White List

In the rule configurations shown in this section, the same white list is expressed in two variants. In Example 5, the rule is expressed with the element `many` together with `except`. Meanwhile, in Example 6, the rule is expressed with the `ocp:other-identity` element.

The following applies for the served user:

- Only `bob@good.example.net` and `+12125551234` are allowed to establish an incoming communication.

```
<st-serv:st-incoming-communication-barring active="true">
  <cp:ruleset>
    <cp:rule id="rule4">
      <cp:conditions>
        <cp:identity>
          <cp:many>
            <cp:except id="sip:bob@good.example.net"/>
            <cp:except id="tel:+12125551234"/>
          </cp:many>
        </cp:identity>
      </cp:conditions>
      <cp:actions>
        <st-serv:allow>false</st-serv:allow>
      </cp:actions>
    </cp:rule>
  </cp:ruleset>
</st-serv:st-incoming-communication-barring>
```

Example 5 White List Variant One



```
<st-serv:st-incoming-communication-barring active="true">
  <cp:ruleset>
    <cp:rule id="rule6">
      <cp:conditions>
        <cp:identity>
          <cp:one id="sip:bob@good.example.net"/>
          <cp:one id="tel:+12125551234"/>
        </cp:identity>
      </cp:conditions>
      <cp:actions>
        <st-serv:allow>true</st-serv:allow>
      </cp:actions>
    </cp:rule>
    <cp:rule id="rule7">
      <cp:conditions>
        <ocp:other-identity>
      </cp:conditions>
      <cp:actions>
        <st-serv:allow>false</st-serv:allow>
      </cp:actions>
    </cp:rule>
  </cp:ruleset>
</st-serv:st-incoming-communication-barring>
```

Example 6 White List Variant Two

8.6 Playing Generic Announcement – play-announcement

Barring incoming communication from `alice@example.com` and playing operator-named announcement “Call Me Later” to the calling party is shown in Example 7.

```
<st-serv:st-incoming-communication-barring active="true">
  <cp:ruleset>
    <cp:rule id="generic-announcement">
      <cp:conditions>
        <cp:identity>
          <cp:one id="sip:alice@example.com"/>
        </cp:identity>
      </cp:conditions>
      <cp:actions>
        <st-serv:allow>false</st-serv:allow>
        <st-serv:play-announcement>Call Me Later</st-serv:play-announcement>
      </cp:actions>
    </cp:rule>
  </cp:ruleset>
</st-serv:st-incoming-communication-barring>
```

Example 7 Bar Incoming Communication from Alice and Play Generic Announcement

8.7 Playing Generic Announcement – play-segmented-announcement

Barring incoming communication unconditionally and playing operator-named segmented announcement including a number of announcement voice variables to the calling party is shown in Example 8.

```
<st-serv:st-incoming-communication-barring active="true">
  <cp:ruleset>
    <cp:rule id="relocation">
      <cp:conditions/>
      <cp:actions>
        <st-serv:allow>false</st-serv:allow>
        <st-serv:play-segmented-announcement announcement-name="reloc_ann">
          <st-serv:announcement-variable variable-name="NewNumberAreaCode">
            <st-serv:variable-value>0211</st-serv:variable-value>0211>
          </st-serv:announcement-variable>
          <st-serv:announcement-variable variable-name="NewLocalNumber">
            <st-serv:variable-value>3811973</st-serv:variable-value>3811973>
          </st-serv:announcement-variable>
        </st-serv:play-segmented-announcement>
      </cp:actions>
    </cp:rule>
  </cp:ruleset>
</st-serv:st-incoming-communication-barring>
```

Example 8 *Bar Incoming Communication Unconditionally and Play Generic Segmented Announcement*