

MTAS 16B Technical Product Description SIP Trunking AS

TECHN PRODUCT DESCR

© Ericsson AB 2015

All rights reserved. The information in this document is the property of Ericsson. Except as specifically authorized in writing by Ericsson, the receiver of this document shall keep the information contained herein confidential and shall protect the same in whole or in part from disclosure and dissemination to third parties. Disclosure and disseminations to the receiver's employees shall only be made on a strict need to know basis.

Contents

1	Introduction	4
1.1	Scope	4
1.2	Change History	4
2	Overview	4
2.1	ST AS in the network	4
2.2	Network scaling and redundancy	7
3	ST AS Features	9
3.1	Overview	9
3.2	SIP Trunking Connection and Control functions	10
3.3	ST Call Admission Control	28
3.4	ST Carrier Select and Pre-Select Rn	31
3.5	ST Communication Barring	34
3.6	ST Communication Diversion	40
3.7	ST Malicious Communication Identification	45
3.8	ST Number Normalization	46
3.9	ST Identity Presentation	47
4	Concepts and Abbreviations	57
4.1	Concepts	57
4.2	Abbreviations	57
5	Reference Documents	60



1 Introduction

1.1 Scope

This document is part of MTAS TPD document series and focuses on ST AS. For MTAS common features and other application server features, please read other TPD documents.

1.2 Change History

Revision	Date	Comments/Changes
A	2015-11-16	First approved version for 16A
B	2016-04-28	Updated title, header and front page

2 Overview

2.1 ST AS in the network

ST AS can be deployed as a stand-alone network element or co-located with other application servers in MTAS.

2.1.1 Session Control and Service Interaction

ST AS is involved in signaling sessions that originates from a PBX user and signaling sessions that terminates to a PBX user.

The figures 1 and 2 below show connecting of a PBX in peering mode that is applicable for the static mode connect. The model is described in and based on ref [3] and [4].

The figures 3 and 4 show the connecting of a PBX in dynamic mode. The P-CSCF supports an IP-PBX to connect either using SIP Connect 1.1 procedures defined in [9] or through procedures as defined in [4] subscription mode.

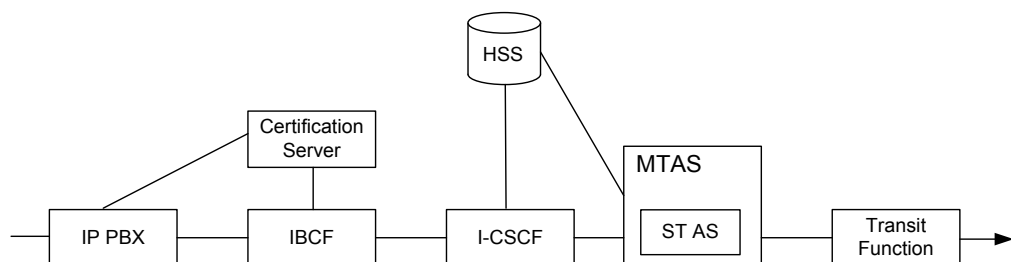


Figure 1: SIP Trunking solution for static mode connect PBX Originating Call over Ma



The IBCF provides a connection point for static mode connected IP-PBX. Its role includes authenticating the IP-PBX, managing and terminating TLS connections and anchoring signaling and Media.

ST AS is invoked by the I-CSCF over the Ma interface.

The Transit function works as a routing function. For PBX originating calls the ST AS inserts a pre-defined route set and forwards the call to the transit function.

The HSS stores the provisioning data for the IP-PBX.

In static mode the IP-PBX is assigned the following identities:

- One main IP-PBX identity, a PSI that represents the IP-PBX. This identity is used to store a service document, in transparent data, the service configuration of the PBX.
- One or more wildcarded PSI. Each wildcarded PSI represents a number series of the IP-PBX. Each wildcarded PSI contains a reference in transparent data to the main PBX identity. The main IP-PBX identity points to the Service document for the PBX. The service document for a PBX contains provisioning data for ST basic functions and supplementary services for the PBX.

In dynamic mode the IP PBX contains the following:

- One Implicit Registration Set (IRS) containing the following identities:
 - One Main IP-PBX identity. A distinct IMPU is used by the ST AS to store a service Document, in transparent data, the service configuration of one or more distinctive IMPUs used for the IP-PBX.
 - One or more distinctive IMPUs used for registration (representing the IP-PBX routes).
 - One or more wildcarded IMPUs. Each wildcarded IMPU represents a number series of the IP-PBX. All wildcarded IMPUs resides in the same IRS as the main IP-PBX identity in order to get registered.

The P-CSCF provides connectivity for dynamic mode connected PBXs. P-CSCF supports an IP-PBX to connect either using SIP Connect 1.1 procedures defined in [9] through procedures as defined in [4] subscription mode.

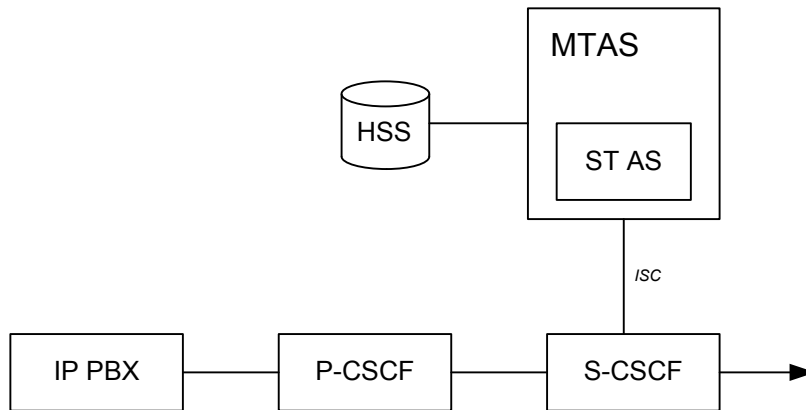


Figure 2: Dynamic Mode PBX Originating call

The IP-PBX sends a request to the P-CSCF that follows the service route stored at registration to the S-CSCF. The S-CSCF executes originating IFCs sending the request to the ST AS over ISC. The ST AS executes services and follows the route inserted by S-CSCF back to S-CSCF that routes the call to the terminating network.

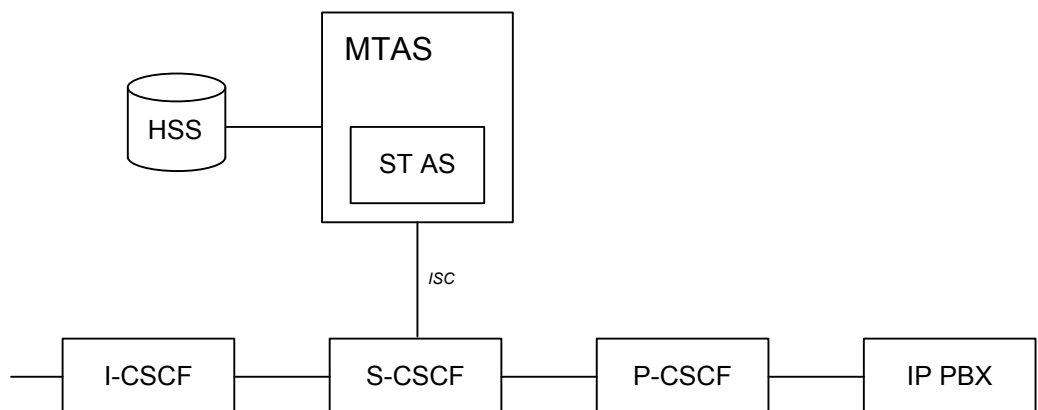


Figure 3: Dynamic Mode Terminating call

The request is received in the terminating I-CSCF that makes a location query to HSS based on the Request-URI, receives the S-CSCF address and forwards the request to S-CSCF. The S-CSCF executes terminating IFCs, sending the request to the ST AS over ISC. The ST AS executes terminating services and follows the route inserted by S-CSCF back to the S-CSCF.



2.2 Network scaling and redundancy

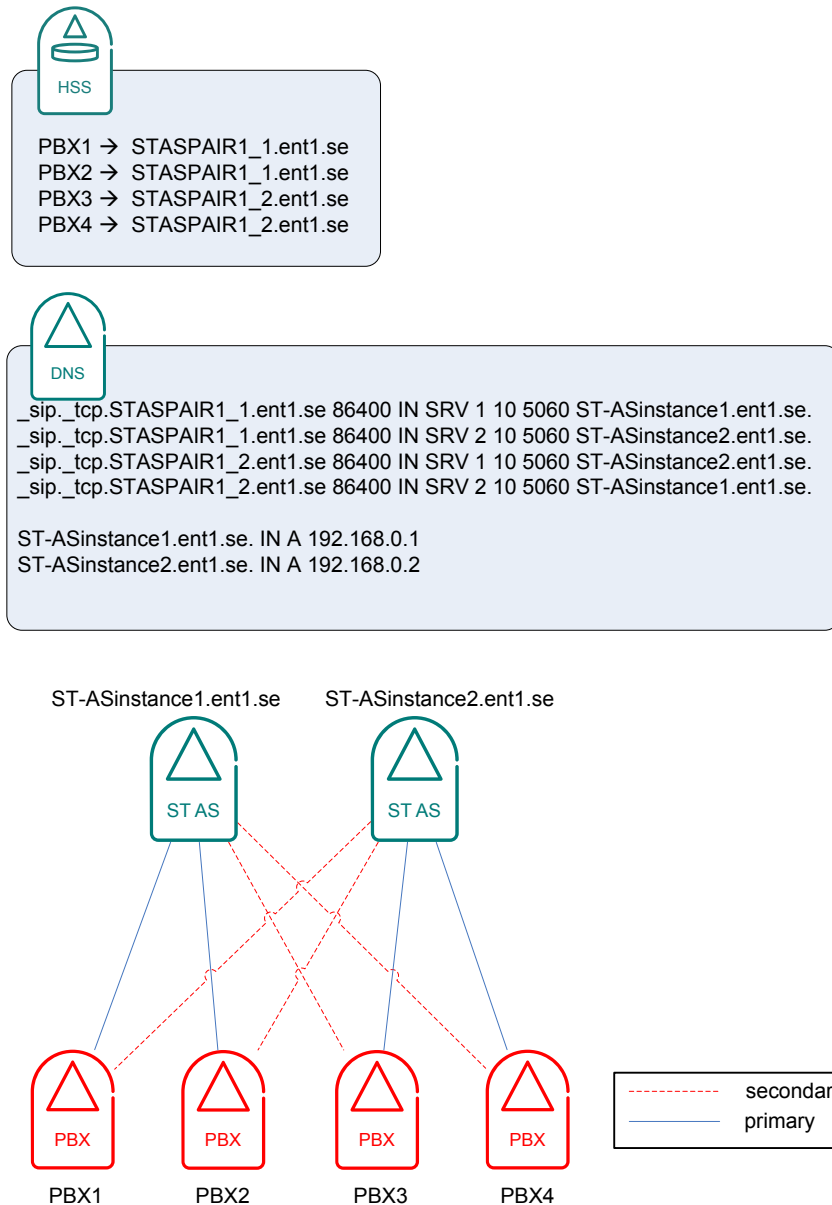
2.2.1 Redundancy

To achieve High Availability, ST ASs are deployed in pairs. For each IP-PBX assigned to a pair, one of the ST AS instances is designated primary and the other as secondary. To optimize resource consumption and ensure efficient failover the solution should be configured so that approximately half of the IP-PBXs that are served by a pair are primary one ST AS instance and the other half on the other instance. An ST AS instance will thus be primary for some IP-PBXs while at the same time secondary for others. To get an even traffic load across both ST AS instances the distribution shall be made on estimated traffic load rather than on an even number of IP-PBXs per ST AS instance as traffic load may differ significantly between individual IP-PBXs (some may be very large and others very small). The even load distribution will help to cater for the situation when one instance is lost and the IP-PBXs being served by that instance failover to the stand-by instance. The stand-by ST AS must be able to handle the increased traffic load. It is thus essential that each of the ST AS instances is dimensioned to handle all of the IP-PBXs assigned to the pair.

In the event that the primary ST AS fails the secondary ST AS will start receiving requests and thus gradually become serving for the IP-PBXs which were served by the failed ST AS. When the failed ST AS becomes available again the IP-PBXs that were assigned to that ST AS as primary will start fail-back. When all IP-PBXs have failed back and none are served by a secondary ST AS anymore the system will have completed restoration and returned to normal operational conditions. Eventually the cached data from the temporarily served IP-PBXs will have been cleared on the secondary ST AS (based on timed out).

Failover and Failback mechanisms:

An FQDN resolving an ST AS pair contains two SRV records, one primary and one secondary. Each ST AS pair has two FQDN resource records in DNS, one which names the first instance as primary and the other as secondary and one resource record which returns them in the opposite order.



Failover and failback is triggered per call from the I-CSCF. The event that triggers the failover is a failed attempt to send a request or response to the ST AS. The I-CSCFs use the same principle where the failed IP-address is put into quarantine for a configured amount of time (the primary SRV is removed and the TTL is reduced), during which the secondary SRV-record is used in instead. After the new TTL has expired the FQDN is resolved again in DNS. If the AS is still not reachable the FQDN is put into quarantine again and the procedure repeats itself.

The ST AS FQDN representing the pair is configured in HSS in the service profile of the IP-PBX.

During a state of failover or failback, some of the calls for a particular IP-PBX are executed on the primary ST AS and some on the secondary.



Both when an IP-PBX fails over to the secondary AS and when an IP-PBX fails back to the primary AS, the ST AS may not have the IP-PBX data cached so it must again cache up the service profiles.

2.2.2 Scalability

The ST AS is based on the MTAS application server platform but unlike the other MTAS based application servers which on node level scales horizontally by adding a single node at a time, the ST AS scales horizontally in pairs.

To ensure an even traffic load across ST AS instances and thus a predictable and robust system, it is recommended to carefully consider the traffic weight of the IP-PBX before it is allocated to a ST AS. This is due to the fact that individual IP-PBXs may vary in traffic weight.

3 ST AS Features

3.1 Overview

ST AS handles managing of access between the operators IMS Network and enterprise PBXs where static and dynamic mode connectivity is supported.

In addition the ST AS serves the operator with Regulatory and Supplementary services.

3.1.1 SIP Trunking Connection and Control functions

These are functions supporting the operator connecting the IP-PBXs to the IMS Network.

- Managing the ST AS administrative state
- License Handling
- Feature tag handling
- Policing of concurrent media streams
- Route registration and de-registration
- PBX originating call
- PBX terminating call including route selection
- ST AS failover procedure



3.1.2 Supplementary and regulatory services:

3.1.2.1 Identity handling

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

3.1.2.2 Communication Diversion

- Communication Diversion – Rule based
 - Communication Forwarding – Unconditional (CFU)
 - Communication Forwarding – Not Reachable (CFNRC)
 - Communication Forwarding – Not Logged In (CFNL)
- Communication Diversion Notification – Caller
- Communication Deflection

3.2 SIP Trunking Connection and Control functions

3.2.1 Description

The SIP Trunking Connection and Control functions in ST AS are described in the following sub-chapters.

3.2.1.1 Manage the ST AS Administrative State

After start of the MTAS node the ST AS administrative state is automatically set to “Locked” and all originating and terminating PBX call attempts is rejected.

By setting the ST AS administrative state to “Unlocked”, new PBX originating and terminating call requests are accepted.

An attempt to “Unlock” the ST AS is rejected if a ST AS capacity license is missing or invalid.



The ST AS administrative state can be set to “shutting down”. This will prohibit any new sessions from being created and when it is detected that the last ongoing session has been terminated, the ST AS administrative state will transition to the state of “Locked”.

The ST AS can be forced to locked state by setting the ST AS administrative state to “Locked”. This will clear down existing session forcefully.

3.2.1.2 ST AS Capacity License

The usage of the ST AS is controlled via a capacity license. The capacity license is based on the total count of simultaneous ongoing PBX originating and terminating calls. An alarm is raised if a valid license is missing when an operator tries to unlock ST AS functionality in MTAS. Another alarm is raised if the license volume limit is exceeded and the alarm can only be cleared by installing a license with higher limit.

3.2.1.3 Feature Tag Handling

Feature tag handling is performed for PBX originating and terminating calls. The processing takes place at session set up when an initial INVITE is received.

ST AS perform feature tag analysis based on pre-configured values and the analysis may result in that the call is rejected or that feature tags are added to the Accept-Contact header (originating call case) or to the Contact header of the 200 OK (INVITE) response (terminating call case).

3.2.1.4 Media Policing of Concurrent Media Streams

The media policing of concurrent media streams use case is triggered whenever a SDP-offer is received from any of the involved users during establishment of a PBX originating and PBX Terminating call or after the call has been established when a session update is performed. If the number of active media lines in the SDP-offer is more than 10 the call or session attempt is rejected.

3.2.1.5 PBX Terminating Call

The PBX user can receive off-net calls when the PBX is configured in the IMS network using the Static mode PBX connect.

Note: PBX terminating calls reach the ST AS via I-CSCF using W-PSI triggering. The PBX Terminating call is triggered when an initial INVITE including a PPK header is received on the ST AS port. All number series served by the PBX must be provisioned in the IMS Core Network as Wild-carded-PSIs. ST AS uses a preloaded route to forward the call request.



3.2.1.6 Route registration and re-registration

For dynamic mode the IP-PBX registers each of its access routes with the IMS network (involving 3rd party registration to ST AS) using IMS registration procedures. The ST AS uses user preferences (Accept-Contact header) to instruct S-CSCF about which access route to use for routing a specific PBX terminating call.

3.2.1.7 Route Selection

A PBX can be connected to IMS with multiple PBX routes simultaneously for increased trunking capacity and robustness. For PBX terminating calls, the ST AS uses random selection among all active routes. If no active route is available, a standby route is used if defined.

3.2.1.8 PBX Originating Call

The PBX user can originate calls when the PBX is configured in the IMS network using the static mode PBX connect. The PBX Originating Call use case is triggered in ST AS when an initial INVITE including a PSU header with session case "orig" is received on the ST AS port.

3.2.1.9 Operator Blocking of a PBX

An operator can block all calls from or to a PBX by setting the PBX to a blocked state. The blocking is done via CAI3G provisioning.

3.2.1.10 Operator blocking of a PBX route

An operator can block usage of a PBX route for routing of terminating calls. The blocking is done via CAI3G provisioning.

3.2.1.11 ST AS Failover

ST AS continues handling traffic after MTAS system restart when PBX routes have been registered via dynamic mode. In case of restart the registration state is lost in ST AS, that means that the route selection is disabled and that terminating calls are rejected by ST AS until successful re-registration of PBX routes.

The ST AS failover procedure is used if the registration state is lost in ST AS when a terminating call is received. The registration state is in that case fetched from S-CSCF. The SIP SUBSCRIBE request is used as specified in 3GPP TS 24.229 (Registration state event package section). The registration state information is returned in SIP NOTIFY from S-CSCF.



3.2.2 Example Call Flows

3.2.2.1 Route Registration and Re-registration

The following diagram shows an example call flow of successful route registration.

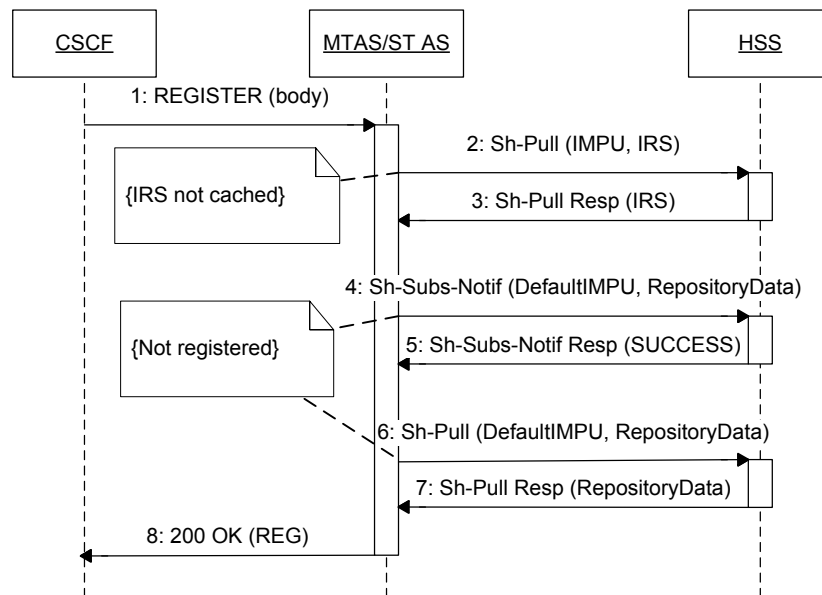


Figure 4: Route registration applicable to dynamic mode

- 1 ST AS receives extended 3rd party sip REGISTER message from S-CSCF. The message body contains contents of the original REGISTER request and response received by the S-CSCF. ST AS parses the body and checks that:
 - It contains a REGISTER and Response message
 - The REGISTER contains one Contact
 - The Response contains at least one Contact
- 2 In case parsing of the body and the analysis of the content is successful the ST AS checks if an IRS for the IMPU contained in the To header of the REGISTER request is already cached locally. If not, ST AS sends request to HSS to fetch the IRS. Otherwise request for IRS is not sent and the next step is skipped.
- 3 ST AS receives the IRS and parses it. The parsed information of the IRS is cached locally.



- 4 ST AS checks if RepositoryData for the Default IMPU of the REGISTER request has an active subscription in HSS. If not, ST AS subscribes to changes in RepositoryData. Otherwise, subscription request is not sent and the next step is skipped.
- 5 ST AS receives confirmation of subscription to changes in RepositoryData for the Default IMPU.
- 6 ST AS checks if RepositoryData for the Default IMPU of the REGISTER request is cached locally. If not, ST AS sends request to fetch RepositoryData and stores it. Otherwise, no request is sent and the next step is skipped.
- 7 ST AS receives the RepositoryData and parses it. The parsed information of the RepositoryData is stored locally. On success, the new PBX route has been registered.
- 8 ST AS checks if the route requested to be registered is provisioned in the PBX service data and sends to S-CSCF a 200 OK response concerning the original REGISTER

3.2.2.2 Successful PBX Originating Call, Static Mode

The following diagram shows an example call flow of successful PBX Originating Call where static mode is applied. Note that IMS network nodes like IBCF and I-CSCF are omitted from the diagram in order to keep the diagram simplified and also to highlight the role of the ST AS.

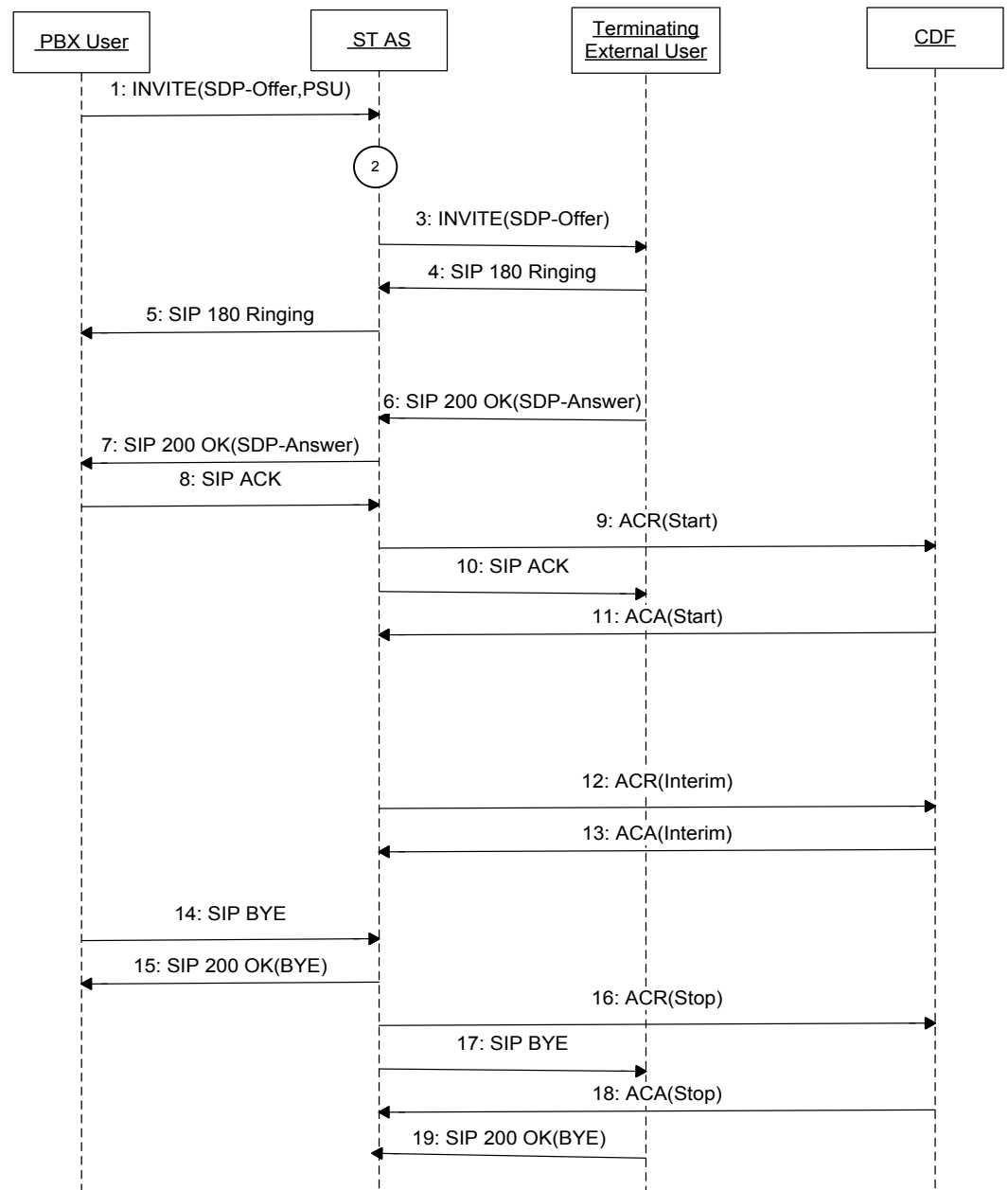


Figure 5 - PBX originating call static mode

- 1 An initial INVITE from a PBX user arrives via the IBCF and I-CSCF (not shown in the sequence diagram). The IBCF adds the P-Served-User header with the identity of the PBX and adds the "orig" parameter. The I-CSCF performs the originating location request using the PSU in LIR and as the served user is not registered a server capability is included in the location request answer. The server capability is resolved in I-CSCF into the ST AS address the I-CSCF re-routes the request to the ST AS serving the PSI.



- 2 The ST AS checks that the ST AS Administrative state is unlocked and that there exists a valid ST AS Capacity license. Feature Tag handling is performed. If an SDP-offer is included in the initial INVITE, the ST AS performs media policing of concurrent number of media lines. If all initial checks are successful, the ST AS fetches PBX service data from HSS, unless already cached. The ST AS checks in the PBX service data to see if the PBX is unblocked. If not blocked, it checks and finds that validation of the PBX User Identity shall be performed. Validation is performed where it is verified that the identity of the originating user belongs to the number series defined for the PBX.
- 3 The PBX user identity validation is successful and the ST AS sends a SIP INVITE towards the PBX user.
- 4 A SIP 180 Ringing is received from the called External user. Charging info is captured. The ST AS starts the "ST No Reply Timer"
- 5 ST AS sends a SIP 180 Ringing towards the PBX User
- 6 A SIP 200 OK including a SDP-answer is received from the called User. The "ST No Reply Timer" is stopped. Charging info is captured.
- 7 ST AS sends the SIP 200 OK towards the Calling PBX User.
- 8 A SIP ACK is received from the calling PBX User.
- 9 The Charging Session is started and ST AS sends an ACR(start) to the CDF.
- 10 A SIP ACK is sent towards the Terminating External User
- 11 An ACA(start) is received from the CDF containing an Acct-Interim-Interval AVP with a non-zero value field. An "Interim ACR Timer" is started.
- 12 The call is going on for a long time and the Interim ACR timer expires. ST AS sends an ACA(interim) to the CDF.
- 13 An ACA response is received from the CDF. The Interim ACR Timer is started.
- 14 A BYE is received from the Calling User before the Interim ACR Timer expires.
- 15 ST AS sends a 200 OK(BYE) to the calling PBX user.
- 16 ST AS sends a ACR(Stop) to the CDF.
- 17 ST AS sends a SIP BYE towards the called External User.
- 18 ST AS receives an ACA(Stop) from the CDF.



19 ST AS sends a BYE towards the External User

3.2.2.3 Successful PBX Originating Call, Dynamic Mode

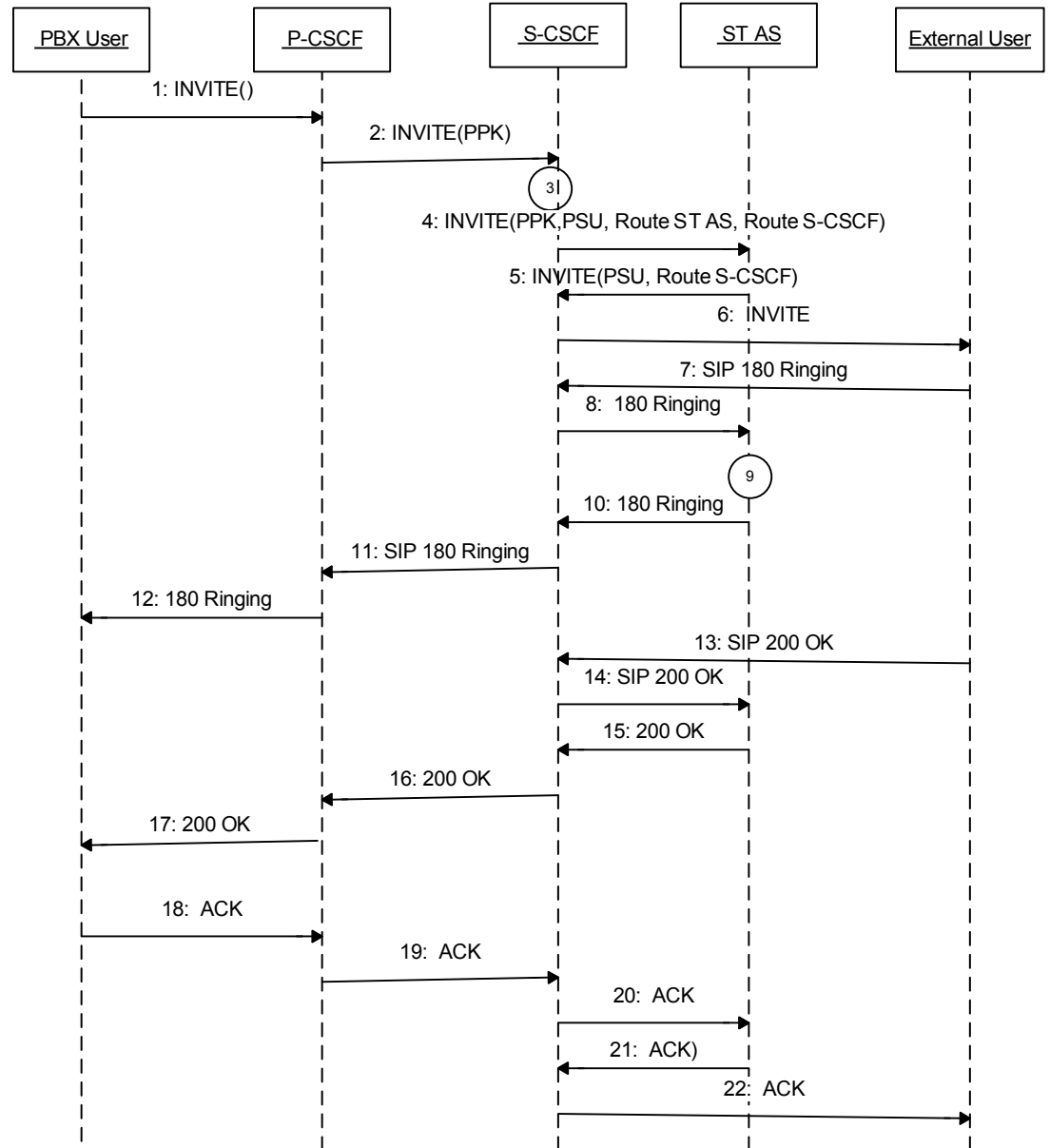


Figure 6: PBX originating call, dynamic mode

- 1 An initial INVITE originating from a PBX user is sent from the IP-PBX to the P-CSCF. The P-CSCF adds a PPK header including the W-IMPU and sends the INVITE to the S-CSCF that performs IFC triggering for terminating call sending the INVITE to ST AS over the ISC interface.



- 2 The P-CSCF adds a PPK header including the W-IMPU and sends the INVITE to the S-CSCF.
- 3 The S-CSCF performs IFC triggering for terminating call, adds the PSU and Route headers and sends the INVITE to ST AS over the ISC interface.
- 4 The ST AS checks that the ST AS Administrative state is unlocked and that there exists a valid ST AS Capacity license. Feature Tag handling is performed. If an SDP-offer is included in the initial INVITE, the ST AS performs media policing of concurrent number of media lines.
- 5 All initial checks are successful and ST AS randomly selects a route among the registered ones. ST AS removes the PPK header and inserts an Accept-Contact header including registration information and routes the INVITE back to S-CSCF.
- 6 The S-CSCF sends the INVITE to the terminating user.
- 7 A SIP 180 Ringing is received from the called External user.
- 8 S-CSCF sends the 180 Ringing to ST AS.
- 9 The ST AS starts the No Reply Timer
- 10 ST AS sends a SIP 180 Ringing back to S-CSCF
- 11 The S-CSCF sends the 180 Ringing to P-CSCF
- 12 P-CSCF sends the 180 Ringing to the PBX user
- 13 A SIP 200 OK including a SDP-answer is received in S-CSCF from the called User.
- 14 S-CSCF sends the 200 OK to ST AS.
- 15 ST AS stops the no reply timer and sends the SIP 200 OK back to S-CSCF
- 16 S-CSCF sends the 200 OK to P-CSCF
- 17 P-CSCF sends the 200 OK towards the PBX user.
- 18 A SIP ACK is received from the calling PBX User.
- 19 P-CSCF sends the ACK to S-CSCF.
- 20 S-CSCF sends the ACK to ST AS
- 21 ST AS sends the ACK back to S-CSCF
- 22 S-CSCF sends the ACK towards the terminating user and normal call handling continues.



3.2.2.4 Successful PBX Terminating Call, Static Mode

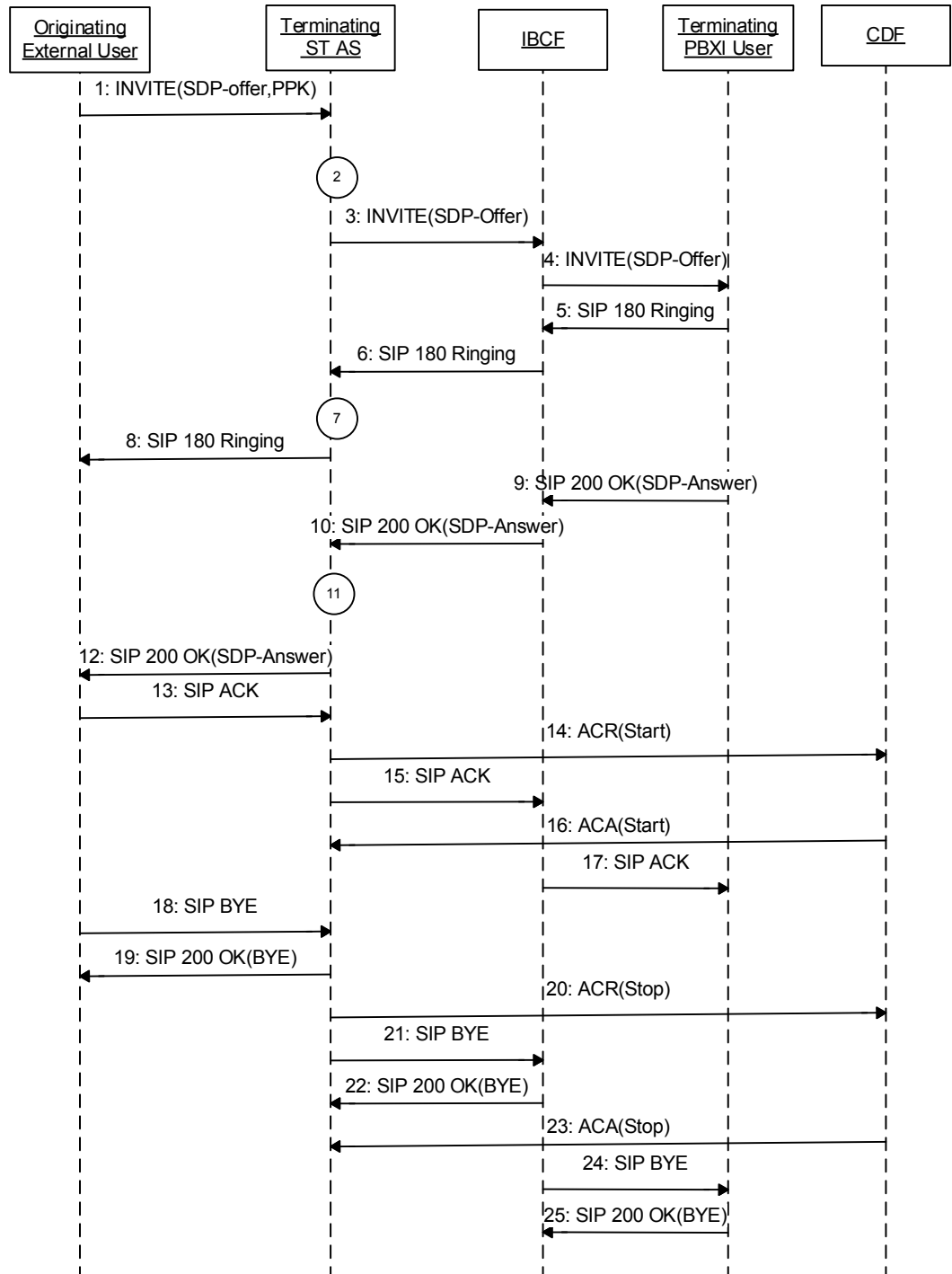




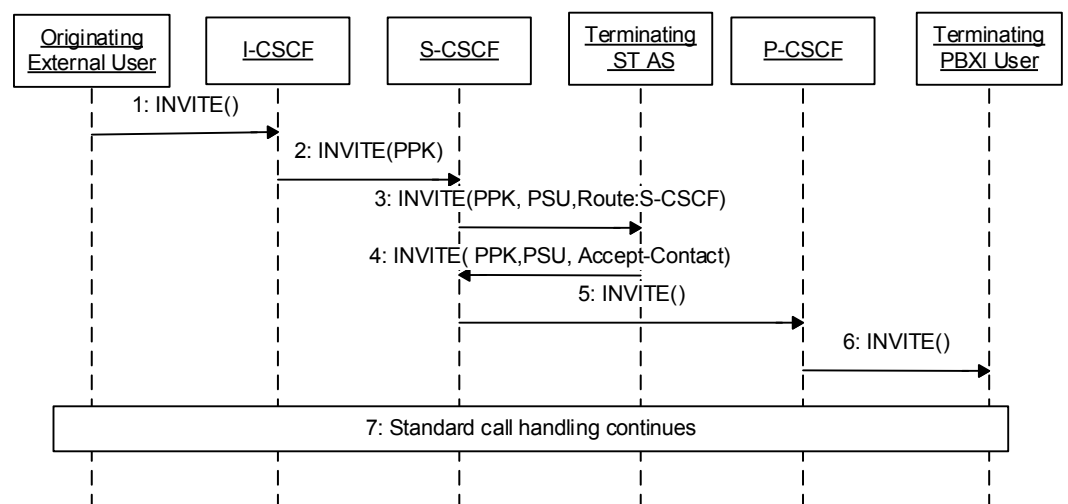
Figure 7 - Session establishment using reliable provisional responses and preconditions

- 1 An INVITE has arrived at I-CSCF for termination in a PBX served by ST AS in this network. I-CSCF performs a location request in HSS (not showed in the sequence diagram) and a W-PSI is returned together with the address of the ST AS. I-CSCF then forwards the request to the ST AS that is assigned to serve the W-PSI. The forwarded request contains the P-Profile-Key header field with the content of the W-PSI.
- 2 ST AS checks that the received INVITE request is a valid request. It determines that this is a terminating scenario because of the missing P-Served-User header field. It checks that the ST AS Capacity License exists and is valid and that the ST AS administrative state is "Unlocked". It performs media policing of concurrent media streams and feature tag handling for terminating calls. If service data for the PBX is not already cached they are fetched from HSS. A check is made in provisioning data to see if the PBX is blocked. If not blocked, Route Selection is performed. If the route selection is successful the terminating route set (IBCF and PBX) is added to the INVITE. It also maps the received request-URI from a TEL URI to a SIP URI and removes the P-Profile-Key header.
- 3 ST AS starts an error guard timer and sends an INVITE to the IBCF. The request reaches the IBCF using standard IMS routing procedures.
- 4 The IBCF sends the INVITE towards the PBX user.
- 5 The PBX User sends a 180 Ringing.
- 6 The IBCF forwards the 180 Ringing to ST AS.
- 7 ST AS stops the "Error Guard" timer and starts the "No Reply" timer.
- 8 The SIP 180 Ringing is sent towards the calling External User.
- 9 A SIP 200 OK including an SDP answer is sent from the PBX User to IBCF.
- 10 The IBCF forwards the 180 Ringing to ST AS.
- 11 ST AS Stops the No Reply Timer.
- 12 The SIP 200 OK is sent to the calling External User.
- 13 A SIP ACK is received in ST AS .
- 14 ST AS sends an ACR(Start) to the CDF.
- 15 ST AS sends a SIP ACK to IBCF.



- 16 An ACA(Start) is received in ST AS.
- 17 IBCF forwards the SIP ACK towards the PBX User.
- 18 The external user sends a BYE.
- 19 ST AS responds with a 200 OK(BYE).
- 20 ST AS sends a ACR(Stop) to CDF.
- 21 ST AS frees the routes that has been used and sends a BYE to the IBCF.
- 22 IBCF sends a 200 OK(BYE) to ST AS.
- 23 An ACA(Stop) is received in ST AS.
- 24 IBCF sends a BYE to the PBX User.
- 25 The PBX User responds with 200 OK(BYE).

3.2.2.5 Successful PBX Terminating Call, Dynamic Mode

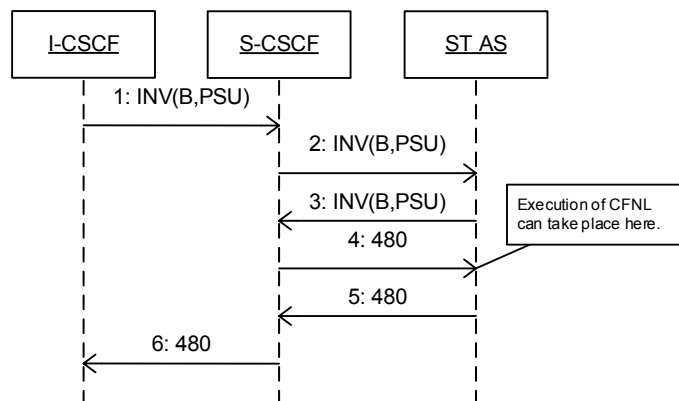


- 1 An INVITE arrives at I-CSCF for termination in a PBX served by ST AS in this network. I-CSCF performs a location request in HSS (not showed in the sequence diagram) and a W-PSI is returned together with the address of the S-CSCF. The I-CSCF adds a PPK header and forwards the request to the S-CSCF.
- 2 The I-CSCF forwards the INVITE request to the S-CSCF.
- 3 The S-CSCF uses the PPK and executes terminating IFCs, adds a PSU header and adds a route back to the S-CSCF and sends the request to the ST AS over the ISC interface.



- 4 ST AS checks that the received INVITE request is a valid request. It performs an analysis of the content of the PPK and PSU headers and finds that it is a dynamic terminating scenario. It checks that the ST AS Capacity License exists and is valid and that the ST AS administrative state is “Unlocked”. It performs media policing of concurrent media streams and feature tag handling for terminating calls. If service data for the PBX is not already cached, they are fetched from the HSS. A check is made in provisioning data to see if the PBX is blocked. If not blocked, a decision is made which PBX route to use for routing. An Accept-Contact header is added with required and explicit user preferences saved from the route registration. It also maps the received request-URI from a TEL URI to a SIP URI and removes the PPK header.
- 5 ST AS follows the route inserted by the S-CSCF and sends the INVITE back to the S-CSCF.
- 6 The S-CSCF terminates the call through the P-CSCF.
- 7 Standard call handling continues.

3.2.2.6 Unregistered PBX Terminating Call, Dynamic Mode

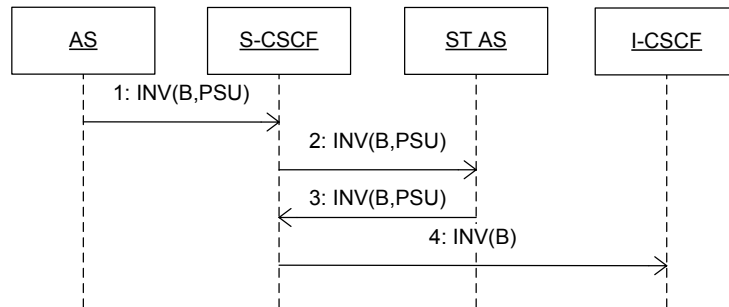


- 1 I-CSCF receives an INVITE request for a terminating call.
- 2 S-CSCF detects an unregistered PBX terminating call and includes the served user, session case and registration state into the P-Served-User header field of the request. The request is forwarded according to the IFC to the ST AS.
- 3 ST AS receives the request, executes any applicable services and returns the request to S-CSCF.
- 4 S-CSCF rejects the request with 480 Temporary Unavailable response code due to the unregistered condition.



- 5 ST AS receives the response, executes any applicable services and forwards the response to S-CSCF.
- 6 S-CSCF forwards the response.

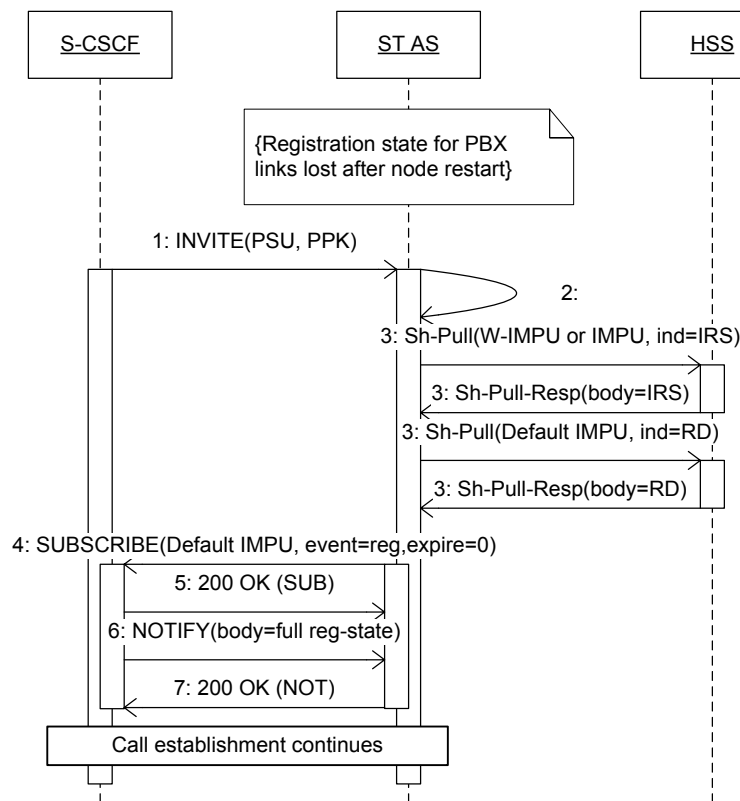
3.2.2.7 Unregistered PBX Originating Call, Dynamic mode



- 1 S-CSCF receives an INVITE request for an originating call.
- 2 S-CSCF detects an unregistered PBX originating call and includes the served user, session case and registration state into the P-Served-User header field of the request. The request is forwarded according to the IFC to the ST AS.
- 3 ST AS receives the request, executes any applicable services and returns the request to S-CSCF.
- 4 S-CSCF forwards the request to I-CSCF for terminating routing.



3.2.2.8 ST AS Failover Procedures



- 1 ST AS receives a new PBX call request (PBX originating or terminating). The P-Served-User header indicates that the call session is originating registered or terminating registered session.
- 2 ST AS uses the P-Profile-Key header, and if not present the served user identity from the P-Served-User header from the original INVITE request in order to determine the served user's identity and session case.
- 3 Because the IRS and PBX service document are not cached in ST AS, the documents are fetched and subscribed to from HSS via the Sh interface.
- 4 Because the session case was determined to be registered, but there are no cached registered contacts associated with the main PBX identity, ST AS sends subscribe to the S-CSCF (derived from the Route header of the INVITE request) for the "reg" event. The subscribed identity in the Request-URI is the main PBX identity, which is the Default IMPU of the previously fetched IRS. The Expire header is set to 0 in order to receive only a single NOTIFY from S-CSCF with the full registration state information for the PBX (and its access routes).



- 5 S-CSCF accepts the SUBSCRIBE request with a 200 OK response.
- 6 S-CSCF sends a NOTIFY request inside the SUBSCRIBE dialog with an XML body containing registration information for all registered contacts (registered access routes) for the PBX. The XML body format is described in RFC 3680. The XML body is parsed and the retrieved contact information is cached in ST AS.
- 7 ST AS parses the full registration state information from the S-CSCF and is now ready to use the registered PBX routes for routing PBX calls. All usage data related to an access route initiated in ST AS during this procedure is reset. The usage data become accurate after all calls originated before the AS failover procedure has terminated.

3.2.2.9 Route Selection for PBX Terminating Call

The flow diagram for route selection in ST AS is described in the figure below.

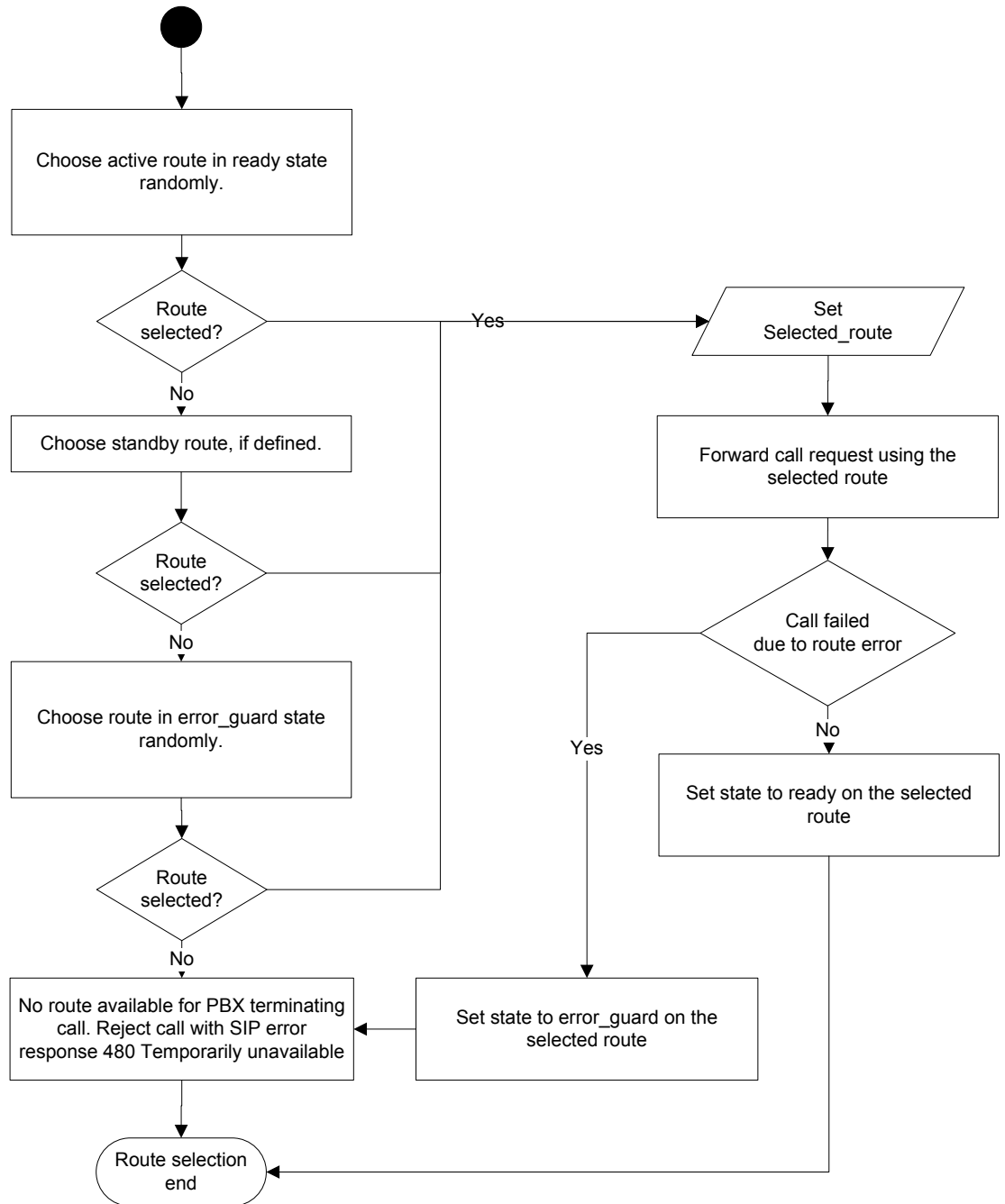


Figure 8: Selection of Route

In the case when ST AS cannot assign any active route due to a pending connection error and there is a stand-by route defined, ST AS will use a stand-by route, if such is provisioned, for routing PBX terminating calls. ST AS will also attempt to use routes in a guard state if there is no other alternative.



For handling of connection errors, ST AS supports configurable profiles. From start, only a *Default* access profile will be supported, see example below. The profile defines the fault codes to be classified as connection errors, the value of *access timeout* and the value of *error guard timer*. The Default profile will be used for all PBX routes.

A connection error implies that ST AS puts the route into *error_guard* state and cancels the outstanding INVITE request if necessary. Re-selection of another route is not attempted.

Any non-2XX response that does not qualify as access error will be forwarded by ST AS to the caller.

3.2.3 Configuration

Examples of node-level configuration parameters related to the basic ST AS communication and control service are:

- The SIP port number for handling ST AS signaling.
- Timers related to SIP protocol, sessions and no reply.
- Primary/Secondary Feature Tag(s).
- Allow or reject session establishment with no feature tag.
- The Service Indication used for provisioning a ST Referral document in HSS.
- The Service indication to use for provisioning a PBX Service Document in HSS.
- The address of the Transit Function.

3.2.4 Performance Management

-

3.2.5 Fault Management

MtasLicenses, ST AS Capacity License Absent

MtasLicenses, ST AS Capacity License Exceeded



3.3 ST Call Admission Control

3.3.1 Description

The ST Call Admission Control (ST CAC) supplementary service enables the operator to restrict:

- the number of all sessions a served Private Branch Exchange (PBX) is involved in
- the number of all originating sessions a served PBX is involved in
- the number of all terminating sessions a served PBX is involved in

In case of rejection of terminating communication when a limit is exceeded, the ST CAC services respond 486 Busy Here, which may be intercepted by other services, such as ST Communication Diversion (ST CDIV).

In case of rejection of originating communication when a limit is exceeded, the ST CAC service optionally play an announcement, then responds 606 Not Acceptable.

3.3.2 Example Call Flow

3.3.2.1 Example Reject Terminating Communication

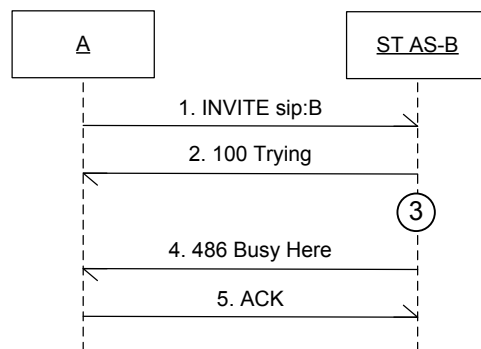


Figure 9 Reject terminating communication

1. Caller (A) sends an INVITE request to PBX user B.
2. ST AS-B sends 100 Trying response.
3. ST AS CAC determines that the new session would cause the served PBX to exceed the maximum number of all terminating sessions.
4. ST AS-B responds with 486 Busy Here.



5. User A acknowledges receipt of the final response.

3.3.2.2 Example Reject Originating Communication

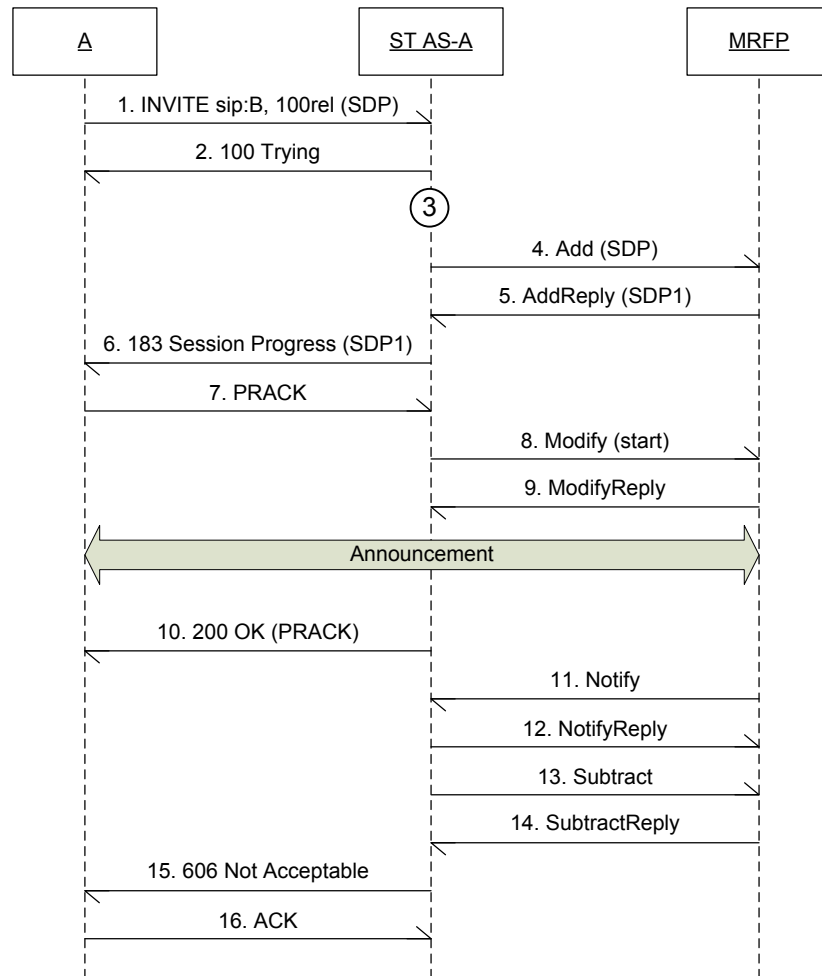


Figure 10 Reject originating communication.

1. PBX user A sends an INVITE request to B.
2. ST AS-A sends 100 Trying response.
3. ST CAC determines that the new session would cause the served PBX to exceed the maximum number of all originating sessions, and determines that an announcement can be played.
4. ST CAC issues an H.248 Add for a new termination.
5. ST CAC receives the early media session SDP answer.



6. ST CAC sends a 183 (Session Progress) that includes:
 - The Require header field with the option tag 100rel.
 - An answer to the SDP in the INVITE request.
 - A P-Early-Media header field set to "sendonly" (backward early media).
7. PBX user A sends PRACK to ST AS-A
8. ST CAC issues an H.248 Modify to start playing the announcement.
9. The MRFC replies.
At this point the announcement is being played to the end user
10. ST AS-A sends 200 OK (PRACK) to PBX user A.
11. MRFP notifies ST CAC that it has finished playing the announcement.
12. ST AS-A replies to MRFP.
13. ST AS-A releases the MRFP resources.
14. MRFP replies to ST AS-A
15. ST AS-A responds to the initial INVITE with 606 Not Acceptable.
16. PBX user A acknowledges receipt of the final response.

3.3.3 Service Interaction

3.3.3.1 ST Communication Diversion

The ST AS can be configured to exert access control over diverted communication by including or excluding diverted calls from CAC counts. When counting diverted sessions, the ST CAC service treats the sessions as originating sessions.

3.3.3.2 ST Incoming Communication Barring

The ST ICB service processes the initial INVITE before the ST CAC service.

3.3.3.2.1 ST Identity Presentation

The ST Identity Presentation services shall process all provisional and final response messages generated by the ST CAC services on a Terminating ST AS.



3.3.3.3 ST Outgoing Communication Barring

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

3.3.4 Configuration

- Activation (active/ disabled)
- Configure announcement name
- Configure whether to count diverted sessions or not

3.3.5 Performance Management

Performance counters related to the ST CAC service are:

- Number of originating session initiations that were rejected by the ST CAC service.
- Number of terminating session initiations that were rejected by the ST CAC service.

3.4 ST Carrier Select and Pre-Select Rn

3.4.1 Description

MTAS offers the following ST Carrier Select Rn services to its served PBXs:

- ST Carrier Pre-Select Rn (CPS Rn)
- ST Carrier Select Rn (CS Rn)

3.4.1.1 ST Carrier Pre-Select Rn

The ST Carrier Pre-Select Rn service allows calls from each served PBX to be handled by a carrier other than the default one, depending whether the call is local or remote.

Congestion control is applied to the ST Carrier Pre-Select Rn communication on receipt of a congestion error message. This is known as Crank back.

The ST Carrier Pre-Select Rn service is an originating service normally executed for the originating session case.

After Communication Diversion on a terminating MTAS when AS chaining is disabled, the MTAS will continue to execute the ST Carrier Pre-Select Rn in the terminating session case.



When AS chaining is enabled the INVITE is routed back to S-CSCF after Communication Diversion is executed, the S-CSCF can then initiate triggering of the Carrier Pre-Select Rn for the originating session case in any AS.

3.4.1.2 ST Carrier Select Rn

The ST Carrier Select Rn service allows an end-user to choose which carrier to select for a particular call. The ST Carrier Select Rn overrides the ST Carrier Pre-Select Rn.

The main function of the ST Carrier Select Rn service is to:

- Check that a user is allowed to use a carrier identified from a dialed Carrier Select Code (CSC) prefixed to the dialed number
- Take the appropriate action which includes the addition of the rn parameter.

ST prevents from using ST Carrier Select Rn service for PBXs who have not been provisioned with it.

The ST Carrier Select Rn service is an originating service normally executed for the originating session case.

After ST Communication Diversion on a terminating MTAS when AS chaining is disabled, the MTAS will continue to execute ST Carrier Select Rn in the terminating session case.

When AS chaining is enabled, the INVITE is routed back to S-CSCF after ST Communication Diversion is executed, the S-CSCF can then initiate triggering of ST Carrier Select Rn for the originating session case in any AS.

3.4.2 Service Interaction

3.4.2.1 ST Carrier Select Rn vs ST Carrier Pre-Select Rn

ST Carrier Select Rn service has precedence over ST Carrier Pre-Select Rn Service. This means that a PBX provisioned with both ST Carrier Select Rn and ST Carrier Pre-Select Rn invokes call-by-call carrier select then the call will be routed using the ST Carrier Select Rn service.

3.4.2.2 ST Communication Diversion

If the target address of a diversion contains a phone number, the INVITE to the target will be subject to the same ST Carrier Select Rn and ST Carrier Pre-Select Rn logic as if the served PBX originated the call to the target.



After ST Communication Diversion either terminating MTAS continues to trigger ST Carrier Select Rn or ST Carrier Pre-Select Rn for the terminating session case or the INVITE is routed back to the serving S-CSCF, in which case terminating MTAS is invoked from S-CSCF and triggers originating services for the originating session case.

3.4.2.3 ST Outgoing Communication Barring

The original domain name in the incoming request is only overwritten with the Carrier's domain name, after Originating Communication Barring service (OCB) interaction has been carried out.

It is possible to create Outgoing Communication Barring rules, that bar or allow calls based on carrier selected by the caller.

3.4.3 Configuration

Examples of node-level configuration parameters related to the ST Carrier Select Rn services are:

- Enable/disable CPS Rn or CS Rn service
- Configure announcement name for invalid Carrier Select Code
- Configure reason codes for congestion control
- Configure Carrier Access Code for CS Rn service
- Configure CSC table with CarrierId and CarrierName for CS Rn service
- Configure carrier domain and destinations disallowed for CarrierId
- Configure local/remote test numbers for CPS Rn service

3.4.4 Performance Management

Performance counters related to the ST Carrier Select Rn services are:

- MtasStCpsOk counts all the communication attempts, where the originating or transit ST AS applied the Carrier Pre-Select Rn service, and the call is to be routed through a pre-selected carrier.
- MtasStCsOk counts all the communication attempts, where the originating or transit ST AS applied the Carrier Select Rn service, and the call is to be routed through a user selected carrier.
- MtasStCsFailed counts all the communication attempts, where the originating or transit ST AS applied the Carrier Select Rn service, but the called party is not allowed to be the subject of carrier selection.



3.5 ST Communication Barring

3.5.1 Description

The Communication Barring (CB) supplementary service enables a PBX to have barring of certain categories of communication. This service is standardized by 3GPP for communication session initiation scenarios, see ref [10].

For an initial INVITE, the sub-function Outgoing Communication Barring (OCB) is executed on the originating ST AS and the sub-function Incoming Communication Barring (ICB) is executed on the terminating ST AS.

The CB is a series of checks which determine if a communication shall be barred or allowed. The following sections cover the different types of checks that make up the CB service.

3.5.1.1 Rule Based Barring

The rules are built up by conditions and actions, which can be combined in many ways to express when a communication shall be barred or allowed.

The different conditions can be based on:

- Whether the identity match a user, domain, range of numbers, etc.
- Whether the calling user's identity is anonymous
- Whether the communication has previously been diverted
- The carrier selected with on-demand (dialed) by the Carrier Select Rn service.

The different actions are:

- Allow or bar communication
- Play generic or segmented announcement

3.5.1.2 Anonymous Communication Rejection (ACR)

ACR is a particular case of Incoming Communication Barring, which bars anonymous callers. The incoming communication is rejected by a SIP response with result code 433 (Anonymity Disallowed).

3.5.1.3 Rule definition

Examples of barring rules that can be defined in MTAS are:



- Bar all outgoing communication except to sip:+3611234567@ericsson.com;user=phone
- Bar every type of communication to tel:+3611234567 between 08.00-11.00 2009-10-14
- Bar all calls to numbers in Coventry, UK
(In this example the conditions are based only on Destination)

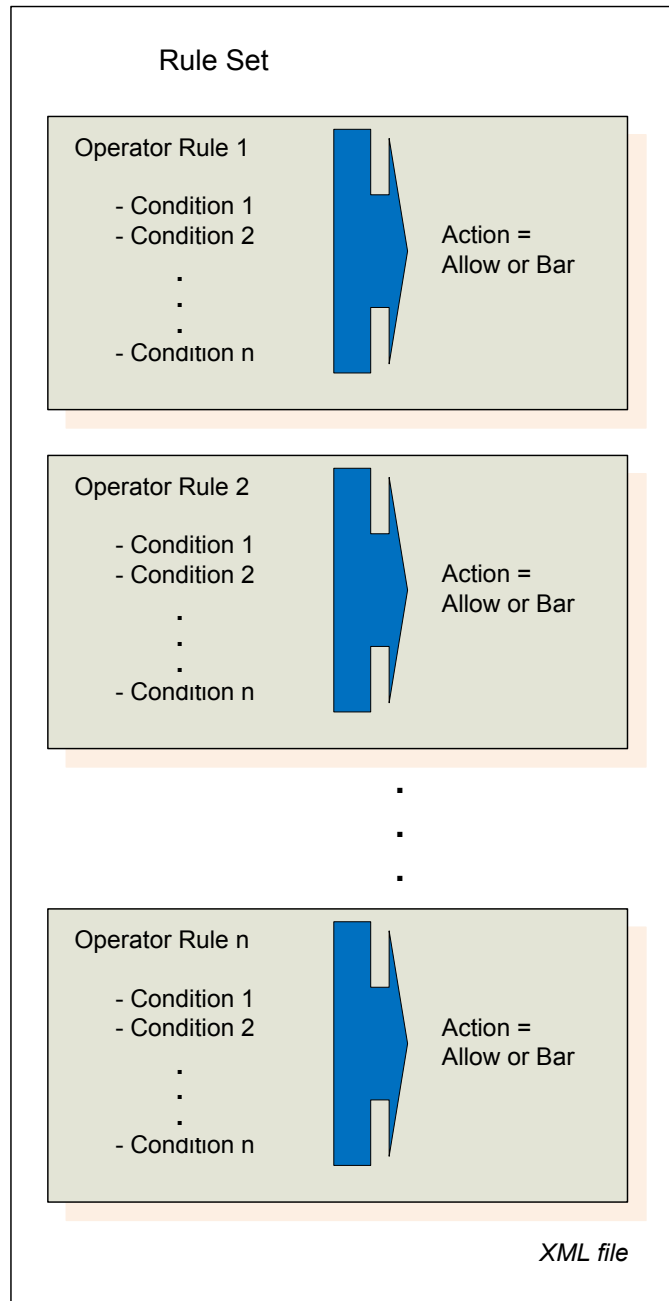


Figure 11 - Barring rule set



The rules are arranged in an OCB rule set and an ICB rule set. The evaluation method is characterized as follows:

- All the rules in the rule set are evaluated sequentially to test if their respective condition(s) are true.
- A rule is said to be matched if all conditions are evaluated as true.
- If exactly one rule matches within the rule set:
This rule's specified action is executed, i.e. if "Allow" then the call is allowed, if "Bar" then the call is barred.
- If more than one rule matches within the rule set:
The communication is barred only when all rule's action is Bar (i.e. "Allow" takes precedence over a "Bar").

3.5.1.4 Operator Black Lists

The operator can create a global ICB Black List to filter out the communication coming into the terminating ST AS and a global OCB Black List to filter out the communication originated from the originating ST AS and a global CDIV Black List to filter out communication diverted by ST AS.

Entries in the OCB Black List are matched with the "Request-URI" value of the INVITE message whereas in some use cases they are matched with the "Refer-To URI" values.

Entries in the ICB Black List are matched with the "P-Asserted-Identity" value of the INVITE message whereas in some use cases they are matched with the "Referred-By URI" value).

Entries in the CDIV Black List are matched with the "Request-URI" value of the diverted INVITE message.

The entry in the list can be part of a URI, it is not required to add a complete SIP URI or TEL URI to the list (i.e. the comparison is a sub-string match).

For example:

The following entries:

.se
+468
bob@example.com
spam

-will match 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.



3.5.1.5 Operator Anonymous Communication Rejection

The operator can enable/disable the anonymous communication on node-level.

If the Operator ACR is enabled on the global level then all anonymous communications are rejected by the ST AS.

3.5.1.6 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 number ranges to be included, a list of number ranges to be excluded, and a list of domains to be included.

A PBX's Operator Barring Program is defined in the operator part of the PBX data, as an alternative to the Operator Permitted Program. It contains a list of category names; the list can consist of Operator Barring Category Names, and ten special categories: Local, Non Local, Allow Local, L_National, L_International, L_IntraLata, L_IntraLataToll, L_InterLata, L_NanpZone1, and L_Nanp.

When a PBX user attempts to make an outgoing call, the Request URI is checked against the set of categories specified for the PBX, and the call is barred if the address is included in one of the categories.

A PBX's Operator Permitted Program is defined in the operator part of the PBX data as an alternative to the Operator Barring Program. It contains a list of category names; the list can consist of Operator Barring Category Names, and nine special categories: Local, Non Local, L_National, L_International, L_IntraLata, L_IntraLataToll, L_InterLata, L_NanpZone1, and L_Nanp.

When a PBX user attempts to make an outgoing call, the Request URI is checked against the set of categories specified for the PBX, and the call is barred if the address is not included in one of the categories.

A PBX's Operator Diversion Barring Program is defined in the operator part of the PBX data. It contains a list of category names; the list can consist of Operator Barring Category Names, and ten special categories Local, Non Local, Allow Local, L_National, L_International, L_IntraLata, L_IntraLataToll, L_InterLata, L_NanpZone1, and L_Nanp.

When the PBX user attempts to divert an incoming call, the number is checked against the set of categories specified for the PBX, and the call is barred if the address is included in one of the categories.

When a communication is barred by an Operator Barring Program or Operator Diversion Barring Program, a final SIP response 603 (Decline) is sent to the caller as an indication. In addition to the response an audio or video announcement can be played. Playing the announcements is configurable by the operator.



When a communication is barred by an Operator Permitted Program, a final SIP response 603 (Decline) is sent to the caller as an indication. In addition to the response an audio or video announcement can be played. Playing the announcements is configurable by the operator.

The audio or video announcement is sent in-band using the early media session, if and only if the caller's SDP offer supports it.

3.5.1.7 Operator White Lists

It is possible for the operator to define one global ICB White List and one global OCB White List.

Both the ICB White List and the OCB White List are defined by 3 lists of strings. (Numbers Included, Numbers Excluded, Domains Included).

- The 'Numbers Included' list specifies the leftmost parts of the normalized numbers that are not to be barred by the global white list. This list is front-substring matched with Tel URIs and SIP URIs containing a telephone number.
- The 'Numbers Excluded' list specifies the leftmost parts of the normalized numbers that are to be barred by the global white list. This list is front-substring matched with Tel URIs and SIP URIs containing a telephone number.
- The 'Domains Included' list specifies the set of domains that are not to be barred by the global white List. This list is only compared with SIP URIs that does not contain a telephone number. Each entry in the list is a string which represents the host part of a URI. If the first character in the string is a '*' this is treated as a wildcarded character and a rightmost match of the domain name from the URI will be 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 URI must exactly match the included string.

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

3.5.1.8 Play Announcement

When a communication is barred a final SIP response 603 (Decline) is sent to the caller as an indication. In addition to the response an audio or video announcement can be played. Playing the announcements is configurable by the operator. The audio or video announcement is sent in-band using the early media session or established session, if and only if the caller's SDP offer supports it. The way of playing announcements is configurable by the operator.



3.5.1.9 Precedence order of barring rules

For session initiation and ICB, the following series of checks are performed (in precedence order):

- 1 ICB White List
- 2 Global Anonymous Communication Barring
- 3 ICB Black List
- 4 Incoming barring

For session initiation and OCB, the following series of checks are performed (in precedence order):

- 1 CDIV Black List
- 2 OCB White List
- 3 OCB Black List
- 4 Operator Barring Program OR Operator Permitted Program
- 5 Operator Diversion Barring Program
- 6 Outgoing barring rules
- 7 Barring Program

3.5.2 Service Interaction

CB interacts with following services:

3.5.2.1 ST Identity Presentation

Originating Identification Presentation (OIP) has an effect on ACR. When OIP is disabled and ACR is set for a particular PBX all of its incoming communication will be rejected as the identity information will be removed from the SIP messages.

If the PBX has the OIP service active including OIR Override then this takes precedence over the ACR service. If the served PBX has the OIR Override service, no incoming request shall be treated as anonymous.

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



3.5.2.2 ST Communication Diversion

The OCB interacts with the Communication Diversion (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.

3.5.3 Configuration

Examples of node-level configuration parameters related to the Communication Barring service are:

- Enable/disable all Communication Barring.
- Configure Operator White Lists and Operator Black Lists
- Configure announcement names separately for ICB, ACR, OCB, each Operator Barring Category, and each special Barring Category.
- Configure Barring Categories

3.5.4 Performance Management

Examples of performance counters related to the Communication Barring services are:

- Number of barred outgoing communications
- Number of barred incoming communications
- Number of barred anonymous incoming communication
- Number of barred incoming diverted communications

3.6 ST Communication Diversion

3.6.1 Description

The ST Communication Diversion (ST CDIV) supplementary service enables a PBX to have the network redirect incoming communication to another user either automatically – communication diversion - based on the served user's CDIV rule set.

Communication Deflection (CD) is a flavor which does not require any rules but diverts, depending on node level configuration data, when triggered by a “deflection” redirect response from the served user's UA.



The ST CDIV feature exists both in the originating and terminating ST AS. ST Communication diversion is executed by the terminating ST AS.

The CDIV rules are built up with different conditions and actions and can be combined in many ways to express if a communication shall be diverted or not and if notifications shall be sent.

The different condition can be based on:

- The served PBX being not registered.
- The served PBX being not reachable.

There is also a possibility to deactivate a rule without deleting the rule configuration.

In the action part of the rule the target of the diversion is defined. Other action settings are:

- Caller can be notified.
- Diverted-to user's identity can be revealed to caller.
- Served user's identity can be revealed to diverted-to party.
- Play generic announcement

The rule sets include one or more rules, each rule having one or more conditions as illustrated in the figure below. Each rule in the full set of rules is evaluated, from top to bottom.

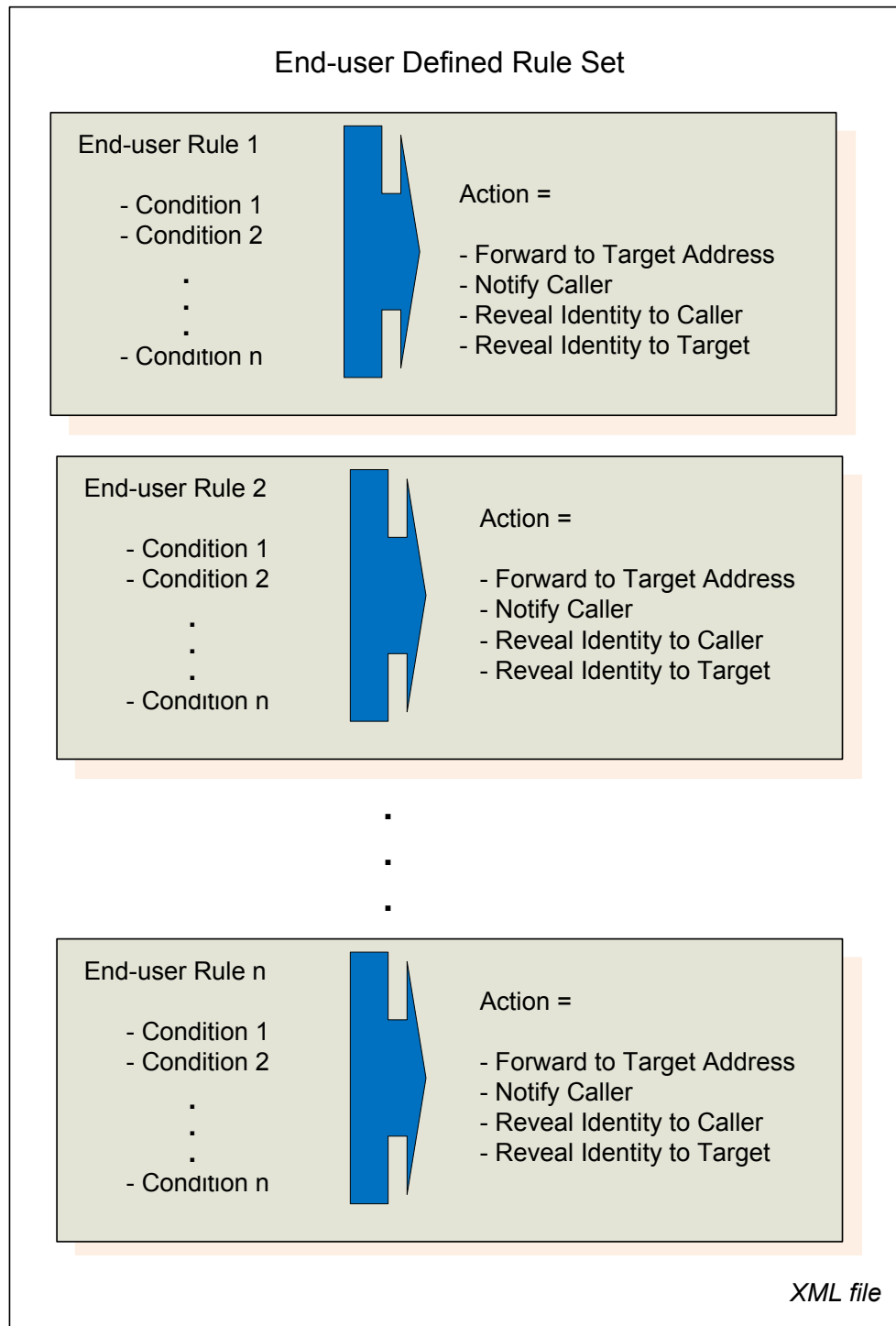


Figure 12 - CDIV Rule Set

It is possible to configure the maximum number of diversions permitted for each communication in ST AS. If enabled, the communication is rejected when the maximum is exceeded. The number of diversions is calculated based on the number of entries in the History-Info header including a 'cause' URI parameter related to the communication diversion service.



CDIV is broken down into the following features:

3.6.1.1 Communication Forwarding – Unconditional (CFU)

This feature enables the end-user to forward all incoming communication to another destination.

In case of CFU, the rule does not contain any condition therefore each incoming communication will be forwarded.

The CFU only operates on the initial INVITE method.

3.6.1.2 Communication Forwarding – Not Logged-in (CFNL)

The PBX can forward incoming communication when PBX is unregistered. This service is only applicable for ST AS in dynamic mode.

3.6.1.3 Communication Forwarding – Not Reachable (CFNRc)

The PBX can forward incoming communication when PBX is out of reach, e.g. in some kind of access network temporary failure or out of reach for radio.

In case of CFNRc the communication will be forwarded if the PBX is not reachable, i.e. when ST AS receives a final response codes that indicate permanent error on a PBX route (default 408, 500, or 504) from the served PBX.

3.6.1.4 Communication Deflection (CD)

The PBX user can deflect the incoming communication by sending a 302 Moved Temporarily response including a contact address to where the call shall be forwarded.

3.6.2 Charging

Terminating charging is performed on the incoming leg (A->B) and Originating charging is performed on the outgoing leg (B->C).

3.6.3 Service Interaction

3.6.3.1 ST Identity Presentation

3.6.3.1.1 OIP

The P-Asserted-Identity remains unchanged by ST CDIV.



3.6.3.1.2 OIR

The Privacy header “history” is escaped within the hi-targeted-to-uri field (in the History-Info header) containing the diverting PBX’s identity in the INVITE message, if the served PBX has OIR.

Note: No conversion from Tel URI is required since the last History-Info entry containing the diverting user’s identity will always contain a SIP URI.

The To-header is changed to the target’s URI if the served PBX has OIR.

3.6.3.1.3 TIP

A P-Asserted-Identity and History-Info header field received in the SIP response by the diverting AS is passed unmodified to the originating entity. The originating S-CSCF is responsible for the interpretation of the Privacy header field.

3.6.3.1.4 TIR

A P-Asserted-Identity header field received in a SIP response the diverting AS is passed unmodified to the originating entity.

If the served PBX has TIR, the Privacy header field is included in the 181 (Call is Being Forwarded)/183 Progress responses. If the served PBX has TIR, the Privacy header “history” is escaped within the hi-targeted-to-uri field containing the diverting PBX’s identity in the History-Info header passed to the originating entity in all responses. This applies whether the History-Info header was included by the ST AS or was already in the response. The originating CSCF is responsible for the interpretation of the Privacy header field.

Note: Conversion from Tel URI to SIP URI may be required because the History-Info might contain a Tel URI in the last History-Info entry and Tel URI do not support the Privacy header.

3.6.3.2 Call Completion

CCBS/CCNR/CCNL possible indications are removed if received by the forwarded-to network.

In case a 486/600/603 busy response including a Call-Info header including a CCBS possible indication is received from the forwarded-to network as response to the INVITE, the ST AS removes the CCBS possible indication from the 486/600/603 response before sending it to the caller A.

In case a 180 Ringing including a Call-Info header including a CCNR possible indication is received from the forwarded-to network as response to the INVITE, the ST AS removes the CCNR possible indication from the 180 Ringing before sending it to the caller A.



In case a 480 error response including a Call-Info header including a CCNL possible indication is received from the forwarded-to network as response to the INVITE, the ST AS removes the CCNL possible indication from the 480 response before sending it to the caller A.

3.6.4 Configuration

Examples of node-level configuration parameters related to the Communication Diversion service are:

- Configure the maximum number of times the same communication is allowed to be forwarded
- Configure announcement name for notify the caller

3.6.5 Performance Management

Performance counters related to the Communication Diversion services are:

- Number of unsuccessful communication diversions for any reason
- Number of successfully establishes communication sessions following diversion of an incoming communication
- Number of communication diversion session attempts

3.6.6 Fault Management

Not applicable

3.7 ST Malicious Communication Identification

3.7.1 Description

The ST MCID service is based on the 3GPP standards. The terminating ST AS uses information received in the initial INVITE request for identification purposes. It does not support the generation of SIP INFO requests to obtain identification information that is not present in the INVITE request.

The captured ST MCID information is configured either to be reported to the Communication Details Server via the ComDetails interface or to be stored locally on the file system.

The local storage function is based on the ACR Storage functionality. The ST MCID information is stored as ACR files that follow the ACR file format described in. The stored ACR files can be transferred to a remote host by the use of the File Transfer Utility.



3.7.2 Configuration

Examples of node-level configuration parameters related to the ST MCID service are:

- Enable/disable ST MCID service
- Configure ST MCID reporting type (via CDS interface or local storage)
- Configure local storage maximal file size
- Configure local storage maximal time duration of an MCID ACR file
- Configure local storage maximal number of ACR messages

3.7.3 Performance Management

Performance counters related to the ST MCID services are:

- MtasStMcidNumberOfAttempt shall be introduced to count all the ST MCID usage attempts.
- MtasComDetailsLocalStorageOk shall be introduced to count the successfully stored ST and MMTel MCID information requests per File Server.
- MtasComDetailsLocalStorageNOk shall be introduced to count the unsuccessfully stored ST and MMTel MCID information requests per File Server.

3.8 ST Number Normalization

3.8.1 Description

SIP URI and tel URI [7] can be presented to the ST AS via a number of interfaces, these being:

- Ma, ISC interface from the CSCF
- CAI3G interface

The MTAS Number Normalization feature is capable of normalizing SIP and tel URI by using contexts from:

- Request URI context, or
- P-Asserted-Identity context, or
- <userIdentity> element on CAI3G



ST AS is capable of inserting a user=phone parameter if parameter is missing in the SIP URI.

ST AS is also capable of detecting a “name” in SIP URI and not acting upon it, returning it unchanged.

After number normalization ST AS updates the input-URI with the normalized number or Null if normalization is not possible.

The number normalization output may be a:

- Global E.164 format number in SIP or TEL format
- Nationally Significant Number (NSN) with a Country Code (CC) context or domain name context
- Operator Service Number (OSN) with a Country Code (CC) or domain name context of the OSN operator

3.8.2 Configuration

MTAS provides the operator a number of node-level configuration parameters which affects the behavior of the Number Normalization:

- Profile name in string for which the Number Normalization data will be defined.
By default the profile should be a country name.
- Warning text string that defines the nature of number Normalization failure
- String of the rules context consisting of digits or domain name.

3.8.3 Performance Management

The following performance counters are provided by ST AS to evaluate the usage and quality of service:

- Number of input string which is not recognized as a valid tel or SIP URI or is deemed to be a malformed tel or SIP URI
- Number of failed attempts to normalize a NSN, OSN, or normal tel or SIP URI number because no rules contexts could be found to match against the contexts provided

3.9 ST Identity Presentation

3.9.1 Description

MTAS offers the following identity presentation services to its served PBXs:



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

Both the OIP and TIP services enables presentation of the identities of participants in a communication to the other participants. Both the OIR and TIR services enables a participant to withhold his identity information from the other participants. The restriction by both OIR and TIR services may be overridden by the OIP/TIP service for participants with the override option.

3.9.1.1 Originating Identity Presentation (OIP)

OIP enables presentation of the originating user's identity to the terminating PBXs. ST AS responsibility is to remove identity information and privacy headers when the terminating PBX does not have the OIP service and when restriction is requested. If override is active, the identity is not removed even if requested. This use case can optionally present the From header in a locally format that can be dialed, and optionally copy the content of the Request-URI to the To header.

If the reason indication for anonymity is enabled (*mtasStldPresReasonIndication*) and the Privacy header value is id, the reason indication in the PAI's display-name portion is copied to the From header display-name portion.

OIP Global Identity Presentation Restriction list

Global Identity Presentation Restriction is a sub-function of the OIP service, which allows the operator to specify ranges of numbers which are never presented to end-users.

This sub-function is executed on SIP INVITE for PBXs with the OIP service active and override not active.

The number ranges subject to Global Identity Presentation Restriction are defined by *mtasStldPresOipGlobalRestrictionList*, which specifies number ranges to be restricted, and *mtasStldPresOipGlobalExemptList*, which specifies sub-ranges within restricted number ranges that are not to be restricted.

The *mtasStldPresOipRestrictHeader* attribute specifies if the From header, the P-Asserted-Identity header or both From and P-Asserted-Identity headers are used to match with the Global Identity Presentation Restriction List (GIPRL).

If From header is to be checked and it matches the GIPRL with no exemption, it will be anonymized.



If P-Asserted-Identity header is to be checked and it matches the GIPRL with no exemption, it will be removed. If more than one P-Asserted-Identity is present, only the matching one will be removed.

If either From or P-Asserted-Identity header matched the GIPRL with no exemption, Privacy user and header setting will be removed. If last P-Asserted-Identity header is removed, id setting will also be removed.

If either From or P-Asserted-Identity header matched the GIPRL with no exemption, and Privacy is set to user, user level headers described in Table 1 below will be removed.

SIP header	Action
Call-ID	<i>Due to the ST AS B2BUA behavior, no information about the originator of the request is revealed in this header.</i>
Subject	<i>Removed</i>
Call-Info	<i>Removed</i>
Organization	<i>Removed</i>
User-Agent	<i>Removed</i>
Reply-To	<i>Removed</i>
In-Reply-To	<i>Removed</i>
From	<i>Anonymized, except in cases described in 2.4.1.1.</i>
Server	<i>Removed</i>
Warning	<i>Removed</i>

Table 1 Affected headers when privacy header value is “user”

3.9.1.2 Originating Identity Restriction (OIR)

OIR is a use case that restricts the originating PBX's identity from being presented to the terminating users. The ST AS responsibility is to indicate in the signaling that the originating PBX wants to restrict the presentation of the identity. The OIR use case can optionally also perform basic screening of the From header. This means that the P-Asserted-Identity is copied to the From header.

If reason indication for anonymity is enabled, ST AS updates the display-name portion of the P-Asserted-Identity(s) to “Anonymous” at identity restriction.

This use case is described as 3 use cases:

- OIR permanent mode
- OIR temporary mode, with default behavior restricted
- OIR temporary mode, with default behavior not restricted



The OIR service can optionally also perform basic screening of the From header. This means that the P-Asserted-Identity is copied to the From header.

If the reason indication for anonymity is enabled (*mtasStIdPresReasonIndication*) and the Privacy header value is id, the reason indication in the P-Asserted-Identity display-name portion is copied to the From header display-name portion.

3.9.1.3 Terminating Identity Presentation (TIP)

TIP enables presentation of the terminating user's identity to the originating PBXs. ST AS responsibility is to remove identity information and privacy headers when the originating PBX does not have the TIP service and when restriction is requested. If override is active, the identity is not removed even if requested..

The main case for TIP is that the originating user has TIP and then no actions are performed in ST AS.

In the alternative case where the originating user does not have TIP the AS will remove identity information from the messages.

If the served PBX does not have TIP enabled then:

- The P-Asserted-Identity and P-Preferred-Identity headers and Privacy header values "none", "user", "header" and "id" are removed.

In case restriction is requested with the Privacy header ST AS will always remove identity information from the messages as listed in Table 2. The only exception is if the served PBX has TIR Override.

Privacy header value	Affected Headers
none	No privacy is required.
id	'Network asserted user identity' privacy requested.(i.e. P-Asserted-Identity, P-Preferred-Identity headers)
user	'Headers added by the user' privacy (i.e. From, Subject, Call-Info, Organization, User-Agent, Reply-To, In-Reply-To, Server, Warning, Referred-By headers).
header	'Headers added by the network' privacy.(i.e. Via, Contact, Record-Route headers)

Table 2 Privacy header value

TIR Override

TIR Override makes it possible for the originating PBX to see the identity information of the terminating user even though the terminating user has requested the identity to not be shown. This part of the TIP function is usually only enabled for specific users.



If the served PBX has TIR Override, Privacy header values “none”, “user”, “header” and “id” are removed and no other headers are modified.

3.9.1.4 Terminating Identity Restriction (TIR)

TIR is a use case that restricts the terminating PBX’s identity from being presented to the originating users. The ST AS responsibility is to indicate in the signaling that the terminating PBX wants to restrict the presentation of the identity..

This use case is described as 3 use cases:

- TIR permanent mode
- TIR temporary mode, with default behavior restricted
- TIR temporary mode, with default behavior not restricted

The TIR service is executed on behalf of the terminating PBX and in the terminating ST AS. The main case for TIR is that the terminating PBX has TIR active. The terminating ST AS will in that case add the Privacy header field ‘user; id’. In permanent mode MTAS updates the Privacy header in each call.

3.9.2 Example Call Flows

3.9.2.1 OIP service enabled with no override

Pre-Conditions:

- The following AdministrativeStates are required to be unlocked: *mtasStControlAdminState* and *mtasStIdPresAdministrativeState*
- The PBX has the OIP service enabled with no override.

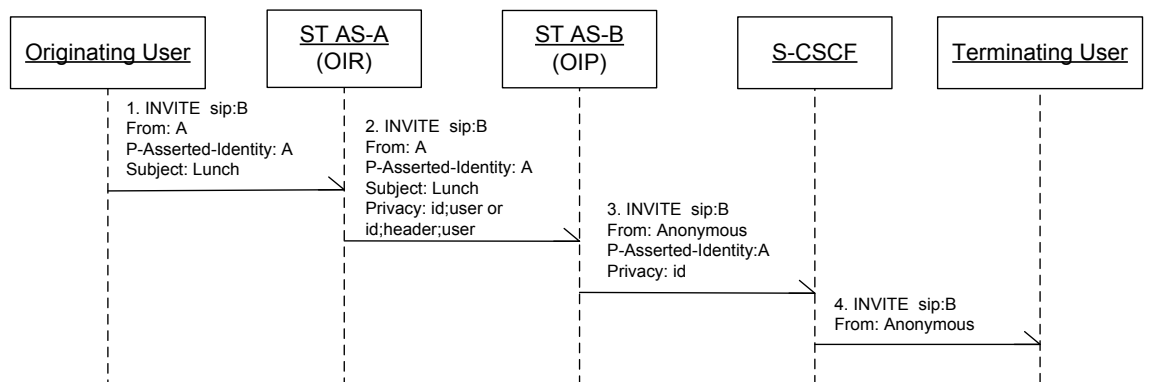


Figure 13: OIP service enabled with no override



1. A sends an INVITE request to B.
2. The OIR service is invoked in ST AS-A where a Privacy header is added.
3. The OIP service is invoked in the terminating ST AS. If a Privacy header is present then ST AS-B ensures that restriction is applied to all relevant headers, and removes the corresponding values from the Privacy header. For impacted headers see Table 1, Table 2 and Table 3. The S-CSCF will handle the "id" level Privacy.
4. The INVITE is sent to the Terminating User with the identity restricted.

SIP header	Action
Via	<i>Due to the ST AS B2BUA behavior, no information about the originator of the request is revealed in this header.</i>
Contact	<i>Due to the ST AS B2BUA behavior, the contact header is set to the ST AS serving the served user.</i>
Record-Route	<i>Due to the ST AS B2BUA behavior, no information about the originator of the request is revealed in this header.</i>

Table 3: Affected headers when privacy header value is "header"

SIP header	Action
P-Asserted-Identity	Removed in the case where the PBX does not subscribe to the OIP service.
From	If reason indication of anonymity is enabled, P-Asserted-Identity's display-name portion is mapped to the From header's display-name portion by the OIP service.

Table 4: Affected headers when privacy header value is "id"

3.9.2.2 OIP service with OIR Override option enabled

The OIR override option makes it possible for the terminating PBX to see the identity information of the originating user even though the originating user has requested the identity to not be shown. This part of the OIP service is usually only activated for specific PBXs.



In the case that the served PBX has the OIR Override option activated as part of the OIP settings, the ST AS is responsible for removing all Privacy header fields to ensure that the identity information is not removed by the network. All other headers containing identity are passed transparently.

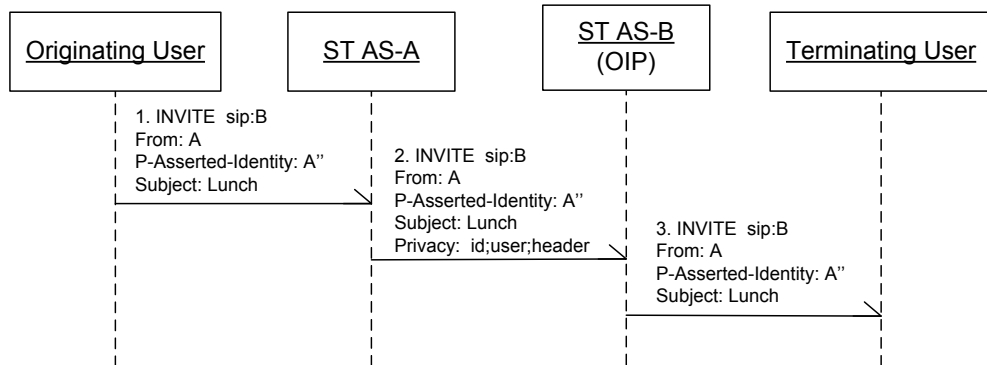


Figure 14 - OIP service with OIR enabled

1. A sends an INVITE request to B
2. The OIR service is invoked in ST AS-A where a Privacy header is added.
3. The OIP service is invoked in ST AS-B. The originating user is requesting privacy, but the terminating PBX has the OIR override option enabled. Then ST AS-B removes all Privacy header fields and leaves all other headers containing identity information unchanged

3.9.3 Charging

3.9.3.1 Originating Identity Restriction

When the OIR service at an originating ST AS node determines that the originating PBX's identity should be restricted, both the Calling-Party-Address-Presentation-Status AVP and the From-Header-Presentation-Status AVP are set to "Presentation Restricted" in the ACR(start) or ACR(event) message.

When the OIR service determines that the originating PBX's identity may be presented both the Calling-Party-Address-Presentation-Status AVP and From-Header-Presentation-Status AVP are set to "Presentation Allowed".

At an originating ST AS node where the OIR service is not applicable, the setting of the Calling-Party-Address-Presentation-Status AVP and the From-Header-Presentation-Status AVP are based on the Privacy header in the INVITE message received by ST AS.



At a terminating ST AS node, the setting of the Calling-Party-Address-Presentation-Status AVP and the From-Header-Presentation-Status AVP are based on the Privacy header in the INVITE message received by ST AS.

The inclusion of the Supplementary-Service-Information, Supplementary-Service-Identity and Supplementary-Service-Action AVPs are dependent on the setting of the *mtasChargingProfileOmitAcr* (where the primary key is set to the vendor ID for Ericsson) configuration parameter.

ACRs generated by the ST AS node may also include a Supplementary-Service-Information AVP, within the ALU-Specific-Extension AVP, containing the following AVPs:

Supplementary-Service-Information (group)	The vendor ID of this AVP is set to the ID for ALU.
Service-Type	Set to 32 (callingLineIDRestriction).
Service-ID	Set to 'Originating Identity Restriction'
Associated-Number	Set to served users number (P-Asserted-Identity or request URI).

The inclusion of the Supplementary-Service-Information, Service-ID and Associated-Number AVPs are dependent on the setting of the *mtasChargingProfileOmitAcr* (where the primary key is set to the vendor ID for ALU) configuration parameter.

3.9.3.2 Terminating Identity Restriction

The TIR service at the terminating ST AS node updates the "Called-Asserted - Identity-Presentation-Status" AVP. The value 'Presentation Restricted' is used when the response contains a P-Asserted-Identity header and contains a Privacy header with content of "id". The value 'Presentation Allowed' is used in all other cases that the response contains a P-Asserted-Identity header.

3.9.4 Service Interaction

3.9.4.1 ST Communication Barring

Interactions between the ST Identity Presentation and ST CB services are described in 3.5.2.1.

3.9.4.2 ST Communication Diversion

Interactions between the ST Identity Presentation and ST CDIV services are described in 3.6.3.1.



3.9.4.3 ST Malicious Communication Identification

When an initial INVITE is received that matches the Global Identity Presentation Restriction List, and the served PBX has the OIP service active and override not active, the information stored for use by an ST AS MCID invocation is marked as anonymous. If ST AS MCID is invoked on those stored details, the caller's identity will be marked as not displayed to served PBX.

Privacy settings do not affect the stored call details

3.9.5 Provisioning

ST AS enables the operator to configure the OIP, OIR, TIP and TIR services on PBX-level through the CAI3G interface. Possible settings are:

- OIP, OIR Override, OIR
- OIR (permanent mode)
- OIR Restriction Level (restrict asserted identity / restrict all private information)
- TIP, TIR Override, TIR
- TIR (permanent mode)
- TIR Restriction Level (restrict asserted identity / restrict all private information)

3.9.6 Configuration

Examples of node-level configuration parameters related to the Identity Presentation services are:

- Enable disable screening of the From header
- Enable disable de-normalization of the From header
- Enable disable copying of the request uri to the To header
- Definition of string to set to the From header when the PBX does not have the OIP provisioned
- Weather to disable or enable the reason indication in the P-asserted-identity headers display name when the anonymity is requested by the caller or permanent OIR is provisioned and the mapping of reason for lack of caller identity from P-Asserted Id header



3.9.7 Performance Management

Examples of performance counters related to the Identity Presentation services are:

- Number of successful invocations of OIP with the option OIR override disabled, when the identity is not restricted
- Number of successful invocations with OIR Override
- Number of sessions where the user, with OIR in temporary mode, decides on a per call basis to allow presentation
- The number of successful invocations with OIR in permanent mode.
- Number of successful invocations of TIP with the option TIR override disabled, when the identity is not restricted
- Number of successful invocations with TIR Override
- Number of sessions where the user, with TIR in temporary mode, decides on a per call basis to allow presentation
- The number of successful invocations with TIR in permanent mode.

3.9.8 Fault Management

Not applicable.



4 Concepts and Abbreviations

4.1 Concepts

Concept	Explanation
Implicit Registration Set	Each PBX connected via the Dynamic mode will have an IRS defined and stored in HSS. The main public identity of the PBX is stored as the default IMPU in the IRS in SIP URI format. The IRS also contains a number of aliases that represent Route IMPUs. The PBX can register multiple access points to the IMS system through the use of Route IMPUs. The IRS also contains a non-empty set of W-IMPUs that define the user number ranges provisioned in the PBX.
PBX Routes	Paths of signaling points that are deterministically mapped onto a SIP Trunk at the IMS Operator border.
PBX Originating Call	A call coming from the PBX and routed to the IMS system for delivery to a user outside the PBX.
PBX Terminating Call	A call originating in the IMS system, and routed to a PBX for delivery to a PBX user.
PBX User	A user defined in, and served by a PBX.
Peering	Peering is an interconnection of administratively separate networks for the purpose of exchanging traffic between the users of each network. The pure definition of peering is settlement-free, meaning that neither party pays the other in association with the exchange of traffic.
ST AS Session	A ST AS SIP session where supplementary services may be executed in addition to what is described in this document.
SIP Trunk	A SIP connection between IP-PBX and IMS Operator border.
Sip Trunking	A complete Trunking service solution managing bundling of access (and SIP trunks) plus the offering of additional services to business customers.

4.2 Abbreviations

AS	Application Server
----	--------------------



CAI3G	Customer Administration Interface 3rd Generation
CD	Communication Deflection
CDF	Charging Data Function
CDTF	Communication Details Transfer Function
CgPN	Calling Party Number
CM	Configuration Management
ENUM	E.164 NUmber Mapping
ETSI	European Telecommunication Standards Institute
FQDN	Fully Qualified Domain Name
HSS	Home Subscriber Server
IBCF	Interconnect Border Control Function
I-CSCF	Interrogating CSCF
ICID	IMS Charging Identifier
iFC	initial Filter Criteria
IMS	IP Multimedia Subsystem
LDAP	Lightweight Directory Access Protocol
MRFC	Media Resource Function Controller
MRFP	Media Resource Function Processor
MTAS	Multimedia Telephony Application Server
OIP	Originating Identity Presentation
OIR	Originating Identity Restriction
PAI	P-Asserted-Identity
RFC	Request for Comment
SDP	Session Description Protocol
SIP	Session Initiation Protocol
ST	SIP Trunking
SSF	Service Switching Function



SSP	Service Switching Point
TCP	Transport Control Protocol
XDMS	XML Data Management Server
XML	eXtensible Markup Language



5 Reference Documents

- [1] MTAS 15B Feature Description 221 04-FGC 101 2242
- [2] MTAS 15B Technical Product Description Common Features 1/221 02-FGC 101 2242
- [3] 3GPP TR 23.897 V1.1.0 (2013-02) Feasibility study on IMS Business Trunking for IP-PBX in static mode of Operation
- [4] ETSI TS 182 025 V3.3.1 (2011-03) Business Trunking Architecture and functional description
- [5] 3GPP TS 32.240 - Charging Management; Charging architecture and principles
- [6] IETF RFC 3892 - The Session Initiation Protocol (SIP) Referred-By Mechanism
- [7] IETF RFC 3966 - The tel URI for telephone Numbers
- [8] ITU-T E.164 - The international public telecommunication numbering plan
- [9] RFC 6140 Registration for Multiple Phone numbers in the Session Initiation Protocol

TS 24.611 V9.3.0 3GPP; Technical Specification Group Core Network and Terminals; Anonymous Communication Rejection (ACR) and Communication Barring (CB); using IP Multimedia (IM) Core Network (CN) subsystem