

MTAS CAI3G Interface for ST AS

INTERWORK DESCR



© Ericsson AB 2014

Disclaimer Statements

No part of this document may be reproduced in any form without the written permission of the copyright owner.

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 damages of any kind resulting from the use of this document.

Trademark List

All trademarks are the property of their respective owners.

Contents

1	Document History	4
2	Scope and Purpose	4
2.1	Interface Entities	4
2.2	Interface Role.....	5
2.3	Documents	5
2.3.1	Services	5
2.4	Encapsulation and Addressing	6
2.4.1	CAI3G Interface	6
2.4.2	XML Namespaces.....	6
2.4.3	Managed Object Type.....	7
2.4.4	Service data version	7
2.5	Message Protocol	7
2.5.1	ST AS Schema to extend CAI3G.....	7
3	Procedures	8
3.1	Overview	8
3.2	Lower Level Procedures	8
3.3	CAI3G Request and Response.....	8
4	Information Model	8
4.1	General	8
4.2	HTTP.....	9
4.2.1	HTTP Request	9
4.2.2	HTTP Response	9
5	Formal Syntax or Schema	19
5.1	Requests and Responses.....	19
5.2	Information Model	20



5.2.1	General	20
5.2.2	Create SIP Trunking	20
5.2.3	Set SIP Trunking	21
5.2.4	GetResponse SIP Trunking	21
5.2.5	SIP Trunking Control	22
5.2.6	ST Call Admission Control	24
5.2.7	ST Carrier Pre-Select Rn	24
5.2.8	ST Carrier Select Rn	25
5.2.9	ST Common Data	25
5.2.10	ST Communication Diversion	26
5.2.11	ST Incoming Communication Barring	29
5.2.12	ST Incoming Communication Barring Ruleset	31
5.2.13	ST Malicious Communication Identification	33
5.2.14	ST Operator Controlled Outgoing Barring Programs	34
5.2.15	ST Originating Identity Presentation	36
5.2.16	ST Originating Identity Presentation Restriction	36
5.2.17	ST Outgoing Communication Barring	37
5.2.18	ST Outgoing Communication Barring Ruleset	39
5.2.19	ST Terminating Identity Presentation	42
5.2.20	ST Terminating Identity Presentation Restriction	43
5.2.21	Identity Condition	44
5.2.22	Create SIP Trunking Referral	45
5.2.23	Set SIP Trunking Referral	46
5.2.24	Get SIP Trunking Referral	46
5.3	Schemas	46
6	Related Standards	47
7	Terminology	47
7.1	Abbreviations	47
7.2	Definitions	47
8	References	47



1 Document History

Rev	Date	Sign	Comment
A	2014-11-27	ERATLIM	Initial version
B	2015-02-09	ERATLIM	Added error messages if Carrier Pre-Select Rn or Carrier Pre-Select Rn services do not have area-code and country-code set in Common Data service The description for element rule-deactivated is extended in services CDIV, ICB and OCB Elements icb-actiona and ocb-actions are corrected to cb-actions
C	2015-02-11	ERATLIM	Added TIP and TIR services. Added in chapter 5.2.12 four elements that belong to function "play segmented announcement".
D	2016-03-09	XMILMAT	MTASv 1.0 Updated References: CBA link to MOM.
PE1	2016-06-01	ERATLIM	Updated due to TR HU65203, In chapter 4.2.2.2.1 added information.

2 Scope and Purpose

2.1 Interface Entities

This interface is offered by ST AS to the CAI3G manager within the IMS architecture for handling the SIP Trunking services by CAI3G.

This document describes the specific parts for the ST AS CAI3G interface. Refer also to CAI3G IWD for MTAS, ref [2], for the generic CAI3G functions shared with other application servers in MTAS.

A pre-requisite for the offered service is that the CAI3G manager is authorized in ST AS and handles document for PBXs, which

- are IMS users
- must have been provisioned with the SIP Trunking Service or SIP Trunking Referral documents

This document describes how ST AS deploys this interface.



Any routers or proxies that may be installed between the CAI3G manager and ST AS are excluded from the scope of this document.

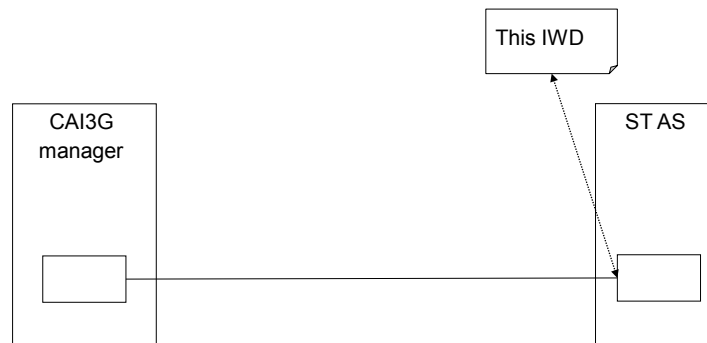


Figure 1 CAI3G manager and ST AS

2.2 Interface Role

This IWD describes the format of provisioning messages for the ST AS services.

2.3 Documents

The following are documents for the SIP Trunking services.

Table 1: SIP Trunking Documents

Document Type	Description
SIP Trunking	This XML document contains settings and subscriptions for PBX services.
SIP Trunking Referral	This XML document contains reference to the main PBX identity for provisioned number ranges in

2.3.1 Services

Table 2: Offered SIP Trunking Services

Offered Service	Description
SIP Trunking Control	The SIP Trunking Control service
ST Call Admission Control	The ST Call Admission Control service
ST Carrier Pre-Select Rn	The ST Carrier Pre-Select Rn service
ST Carrier Select Rn	The ST Carrier Select Rn service
ST Common Data	The ST Common Data available across services
ST Communication Diversion	The ST Communication diversion service



ST Incoming Communication Barring	The ST Incoming Communication Barring service
ST Malicious Communication Identification	The ST Malicious Communication Identification service
ST Operator Controlled Outgoing Barring Programs	The ST Operator-Controlled Outgoing Barring Programs service
ST Originating Identity Presentation	The ST Originating Identity Presentation service
ST Originating Identity Presentation Restriction	The ST Originating Identity Presentation Restriction service
ST Outgoing Communication Barring	The ST Outgoing Communication Barring service
ST Terminating Identity Presentation	The ST Terminating Identity Presentation service
ST Terminating Identity Presentation Restriction	The ST Terminating Identity Presentation Restriction service

Table 3: Used Services

Used Service	Description
--------------	-------------

–

2.4 Encapsulation and Addressing

2.4.1 CAI3G Interface

The interface CAI3G is used to provision the SIP Trunking services per PBX. Provisioning operations consist of create, set, get and delete.

2.4.2 XML Namespaces

Table 4 lists the prefix and namespace in the ST AS.

Table 4: ST AS prefix and namespace

Prefix	Namespace	Purpose
st	http://schemas.ericsson.com/mtas/st/cai3g	SIP Trunking services and Referral elements



2.4.3 Managed Object Type

The managed object (MO) type represents the type that is managed over this interface. This interface supports specific MO Types for ST AS.

Table 5: Specific MO Types for ST AS

Service	MO Type	Namespace
SIP Trunking	ST@http://schemas.ericsson.com/mtas/st/cai3g	http://schemas.ericsson.com/mtas/st/cai3g
SIP Trunking Referral	ST_REFERRAL@http://schemas.ericsson.com/mtas/st/cai3g	http://schemas.ericsson.com/mtas/st/cai3g

2.4.4 Service data version

The CM attribute *mtasShlfDataVersion* [3] controls what format to use when updating the subscriber data on HSS. ST AS uses version 3.1, which is the default setting.

2.5 Message Protocol

2.5.1 ST AS Schema to extend CAI3G

The table below maps the CAI3G messages which have ST AS extensions to the actual XML elements that define the extension.

Table 6: Mapping CAI3G Message to XML Element

Extended CAI3G Message	Matching XML Element
Create Request	st:creates st:createStReferral
Get Response	st:getResponseSt st:getResponseStReferral
Set Request	st:setSt st:setStReferral

Note: Delete Request uses the standard CAI3G element.



3 Procedures

3.1 Overview

The CAI3G request is sent in HTTP/SOAP, ref. [7], method POST. The CAI3G protocol includes login, logout, create, set, get or delete request in the body of the POST message. A CAI3G response may include information in the body of the HTTP/SOAP message.

3.2 Lower Level Procedures

-

3.3 CAI3G Request and Response

The same sequence is used for all login, logout, create, set, get and delete requests and responses.

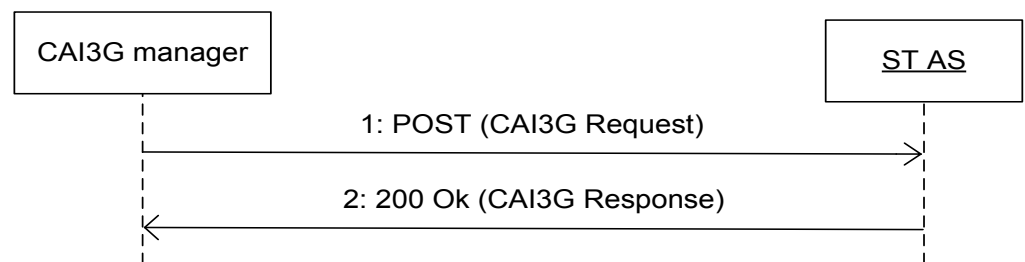


Figure 2 CAI3G Request/Response

1. ST AS receives a POST message with a body including a CAI3G Request with information.

2. ST AS sends 200 OK including a CAI3G Response.

4 Information Model

4.1 General

This section describes the parameters used by ST AS.

The CAI3G Requests and Responses are sent in HTTP/SOAP messages.



4.2 HTTP

4.2.1 HTTP Request

CAI3G manager uses the HTTP/SOAP POST method for requests.

4.2.2 HTTP Response

These are the ST AS specific provisioning fault messages.

4.2.2.1 404 Not Found

The server has not found anything matching the Request-URI.

This is sent in the following case:

Table 7: HTTP 404

CAI3G Error Code	SOAP Error Code	Description	Retry on Failure
3002	Client	Object Does Not Exist	No

4.2.2.2 500 Internal Server Error

4.2.2.2.1 Additional Error Information

Extra information about the error is provided in the reasonText element of some CAI3G Faults. If there are more errors in the document the order of the reasonText is not predictable, but all errors must be corrected before the document is stored.

The actual text is shown in the following tables.

Error 3013, Invalid Parameter

Table 8: Error 3013 ReasonText Values Common Across Multiple Services

Num	Reason Text	Description
-----	-------------	-------------



Num	Reason Text	Description
1.	Failed to meet an application constraint: The service element, "<service>", is present without being activated by the operator	<p>Each service element may only be present if the corresponding service has been activated by the operator.</p> <p>The absence of the service element signals to the user that the corresponding service is not activated.</p> <p><service> indicates the specific service.</p>
2.	Failed to meet an application constraint: The service element, "<service>", is absent when it is activated by the operator	<p>The service element must be present if the corresponding service has been activated by the operator.</p> <p>The presence of the service element signals to the user that the corresponding service is activated.</p> <p><service> indicates the specific service.</p>
3.	Failed to meet an application constraint: The number "<ORIGINAL_NUMBER-1>" is not suitable, please re-enter. The number "<ORIGINAL_NUMBER-N>" is not suitable, please re-enter.	<p>The request contains one or more numbers that cannot be converted to a normalized form. The response will contain a separate sentence for each faulty number or number is not valid SIP or TEL URI.</p> <p><i>The shown text has sentence for each of the two faulty numbers.</i></p>
4.	Failed to meet an application constraint: The number "<ORIGINAL_NUMBER-1>" is not normalized, please re-enter as "<SUGGESTED_NUMBER-1>". The number "<ORIGINAL_NUMBER-N>" is not normalized, please re-enter as "<SUGGESTED_NUMBER-N>".	<p>The request contains one or more numbers that are not in a normal form. The response shows the number in the expected form. The response will contain a separate sentence for each faulty number.</p> <p><i>The shown text has two sentences for two non-normal numbers and a corresponding normalized number for each.</i></p>
5.	Failed to meet an application constraint: Sub-MO Failure: Service: <service>, <element-name>="<element-value>" modify syntax used within a create context, key="<key-name>", value="<key-value>"	<p>The request includes the syntax to modify an existing sub-MO inside a create message or a create sub-MO request within a message.</p> <p>Within the context of a create message or create sub-MO, all references to child sub-MOs must also use create syntax (key attribute and key element both present and with the same value).</p>



Num	Reason Text	Description
6.	Failed to meet an application constraint: Sub-MO Failure: Service: <service>, <element-name>=<element-value> target of create already exists for key=<key-name>, value=<target-key-value>	A request to create a sub-MO cannot be performed because another sub-MO already exists with the proposed target key value.
7.	Failed to meet an application constraint: Sub-MO Failure: Service: <service>, <element-name>=<element-value> target of rename already exists for key=<key-name>, value=<target-key-value>	A request to rename an existing sub-MO cannot be performed because another sub-MO already exists with the proposed target key value.
8.	Failed to meet an application constraint: Sub-MO Failure: Service: <service>, <element-name>=<element-value> no element found for key=<key-name>, value=<key-value>	A request referring to an existing sub-MO cannot be performed because the sub-MO does not exist within the current document.
9.	Failed to meet an application constraint: Number of rules for "<service>" exceeds service limit.	A request to update the service contains more rules than allowed for the service. <service> indicates which service.
10.	Failed to meet an application constraint: Number of rules in Document exceeds total limit.	A request to update the Document contains more service rules than allowed by the total limit set in service common-data.

Table 9: Error 3013 Reason Text – ST Call Admission Control

1.	Failed to meet an application constraint: ST Call Admission Control Failure: Originating All Limit must be less than or equal to the Total All Limit	The ST Call Admission Control limits are inconsistent – the Originating All Limit must be less than or equal to the Total All Limit.
2.	Failed to meet an application constraint: ST Call Admission Control Failure: Terminating All Limit must be less than or equal to the Total All Limit	The ST Call Admission Control limits are inconsistent – the Terminating All Limit must be less than or equal to the Total All Limit.

Table 10: Error 3013 Reason Text – ST Carrier Pre-Select Rn



1.	Failed to meet an application constraint: ST Carrier Pre-Select Rn Failure: User may not have ST Carrier Pre-Select Rn service without the country code and the area code defined	ST Carrier Pre-Select Rn service requires the area-code and country-code to be set in service ST Common Data.
----	---	---

Table 11: Error 3013 Reason Text – ST Carrier Select Rn

1.	Failed to meet an application constraint: ST Carrier Select Rn Failure: User may not have ST Carrier Select Rn service without the country code and the area code defined	ST Carrier Select Rn service requires the area-code and country-code to be set in service ST Common Data.
----	---	---

Table 12: Error 3013 Reason Text – ST Communication Barring

Num	Reason Text	Description
1.	Failed to meet an application constraint: ST Communication Barring Failure: Rule id="<rule-id>", multiple "<condition>" elements	<p>Each ST Incoming Communication Barring rule must have at most one of each of the following <condition> elements:</p> <ul style="list-style-type: none"> • anonymous • communication-diverted • identity • other-identity • rule-deactivated <p>Each ST Outgoing Communication Barring rule must have at most one of each of the following <condition> elements:</p> <ul style="list-style-type: none"> • identity • other-identity • rule-deactivated • carrier • carrier-select-code
2.	Failed to meet an application constraint: ST Communication Barring Failure: Rule id="<rule-id>", not SIP or TEL URI in "except"	Within an identity condition of a ST Communication Barring rule, the id attribute in the element "except" must start with 'sip:' or 'tel:'.



Num	Reason Text	Description
3.	Failed to meet an application constraint: ST Communication Barring Failure: Rule id="<rule-id>", "except Id" <identity> does not start with sip:	Within an identity condition of a ST Communication Barring rule, the id attribute in the element "except" of a "many" condition with a domain attribute must start with 'sip:'.
4.	Failed to meet an application constraint: ST Communication Barring Failure: Rule id="<rule-id>", "except" domain <except-domain> does not match "many" domain <many-domain>	Within an identity condition of a ST Communication Barring rule, the "except" elements within a "many" element with a domain attribute must have an "id" attribute that is a SIP URI within that domain.
5.	Failed to meet an application constraint: ST Communication Barring Failure: Rule id="<rule-id>", identity is not SIP or TEL URI in "one"	Within an identity condition of an ST Outgoing Communication Barring rule, each "one" element must have an id attribute that starts with 'sip:' or 'tel:'.
6.	Failed to meet an application constraint: ST Communication Barring Failure: Rule id="<rule-id>", missing "actions"	Each ST Communication Barring rule must have one "allow" action.
7.	Failed to meet an application constraint: ST Communication Barring Failure: Rule id="<rule-id>", must not contain both "id" and "domain" in "except"	The element "except" within an identity condition must either have a single identity "id" attribute or a "domain" attribute. It must not have both.
8.	Failed to meet an application constraint: ST Communication Barring Failure: Rule id="<rule-id>", cannot have "play-announcement"/"play-segmented-announcement" and "allow" with value = "true"	The elements "play-announcement"/"play-segmented-announcement" and "allow" with value = "true" are contradictory so it is prohibited to have them in the same rule.
9.	Failed to meet an application constraint: ST Communication Barring Failure: Rule id="<rule-id>", cannot have both "play-announcement" and "play-segmented-announcement" in "actions"	Each ST Incoming Communication Barring rule cannot have both play-announcement and play-segmented-announcement in <actions>.



Table 13: Error 3013 Reason Text – ST Incoming Communication Barring

Num	Reason Text	Description
1.	Failed to meet an application constraint: Message: "Element not found on Operator side". Service: "st-incoming-communication-barring". Condition: "<condition>"	<p>An attempt has been made to use an ST Incoming Communication Barring <condition> which the user has not subscribed to.</p> <p>Possible values for <condition> are:</p> <ul style="list-style-type: none"> • anonymous • communication-diverted • identity • other-identity
2.	Failed to meet an application constraint: Message: "Element deactivated on Operator side". Service: "st-incoming-communication-barring". Condition: "<condition>"	<p>An attempt has been made to use an ST Incoming Communication Barring <condition> which the user has not subscribed to.</p> <p>Possible values for <condition> are:</p> <ul style="list-style-type: none"> • anonymous • communication-diverted • identity • other-identity
3.	Failed to meet an application constraint: Message: "Element not found on Operator side". Service: "st-incoming-communication-barring". Action: "<action>"	<p>An attempt has been made to use an ST Incoming Communication Barring <action> which the user has not subscribed to.</p> <p>Possible values for <action> are:</p> <ul style="list-style-type: none"> • allow • play-announcement • play-segmented-announcement
4.	Failed to meet an application constraint: Message: "Element deactivated on Operator side". Service: "st-incoming-communication-barring". Action: "<action>"	<p>An attempt has been made to use an ST Incoming Communication Barring <action> which the user has not subscribed to.</p> <p>Possible values for <action> are:</p> <ul style="list-style-type: none"> • allow • play-announcement • play-segmented-announcement



Num	Reason Text	Description
5.	Failed to meet an application constraint: ST Incoming Communication Barring Failure: Rule id="<rule-id>", cannot have "identity" and "anonymous" elements	The elements "identity" and "anonymous" are contradictory so it is prohibited to have them in the same rule.



Table 14: Error 3013 Reason Text – ST Outgoing Communication Barring

Num	Reason Text	Description
1.	Failed to meet an application constraint: Message: "Element not found on Operator side". Service: "st-outgoing-communication-barring". Condition: "<condition>"	<p>An attempt has been made to use an ST Outgoing Communication Barring <condition> which the user has not subscribed to.</p> <p>Possible values for <condition> are:</p> <ul style="list-style-type: none"> • identity • other-identity • carrier • carrier-select-code
2.	Failed to meet an application constraint: Message: "Element deactivated on Operator side". Service: "st-outgoing-communication-barring". Condition: "<condition>"	<p>An attempt has been made to use an ST Outgoing Communication Barring <condition> which the user has not subscribed to.</p> <p>Possible values for <condition> are:</p> <ul style="list-style-type: none"> • identity • other-identity • carrier • carrier-select-code
3.	Failed to meet an application constraint: Message: "Element not found on Operator side". Service: "st-outgoing-communication-barring". Action: "<action>"	<p>An attempt has been made to use an ST Outgoing Communication Barring <action> which the user has not subscribed to.</p> <p>Possible value for <action> is:</p> <ul style="list-style-type: none"> • allow • play-announcement • play-segmented-announcement
4.	Failed to meet an application constraint: Message: "Element deactivated on Operator side". Service: "st-outgoing-communication-barring". Action: "<action>"	<p>An attempt has been made to use an ST Outgoing Communication Barring <action> which the user has not subscribed to.</p> <p>Possible value for <action> is:</p> <ul style="list-style-type: none"> • allow • play-announcement • play-segmented-announcement



Num	Reason Text	Description
5.	Failed to meet an application constraint: ST Outgoing Communication Barring Failure: User may not have the “carrier” condition activated without Carrier Select Rn service activated	Carrier condition can be activated for the user for usage in the ST Outgoing Communication Barring user rule set, only when the user has Carrier Select Rn service activated.
6.	Failed to meet an application constraint: ST Outgoing Communication Barring Failure: User may not have the “carrier-select-code” element activated without Carrier Select Rn service activated	The carrier-select-code element can be activated for the user for usage in the ST Outgoing Communication Barring user rule set, only when the user has Carrier Select Rn service activated.

Table 15: Error 3013 Reason Text – ST Communication Diversion

Num	Reason Text	Description
1.	Failed to meet an application constraint: Message: “Element not found on Operator side”. Service: “st-communication-diversion”. Condition: “<condition>”	An attempt has been made to use a ST Communication Diversion <condition> which the user has not subscribed to. Possible values for <condition> are: <ul style="list-style-type: none"> • not-registered • not-reachable
2.	Failed to meet an application constraint: Message: “Element deactivated on Operator side”. Service: “st-communication-diversion”. Condition: “<condition>”	An attempt has been made to use a ST Communication Diversion <condition> which the user has not subscribed to. Possible values for <condition> are: <ul style="list-style-type: none"> • not-registered • not-reachable
3.	Failed to meet an application constraint: ST Communication Diversion Failure: Rule id=“<rule-id>” multiple “<condition>” elements	Each ST Communication Diversion rule must have at most one of each of the following <condition> elements: <ul style="list-style-type: none"> • not-registered • not-reachable



Num	Reason Text	Description
4.	Failed to meet an application constraint: Message: "Element not found on Operator side". Service: "st-communication-diversion". Action: "<action>"	<p>An attempt has been made to use a ST Communication Diversion <action> which the user has not subscribed to.</p> <p>Possible values for <action> are:</p> <ul style="list-style-type: none"> • notify-caller • reveal-identity-to-caller • reveal-identity-to-target • play-announcement
5.	Failed to meet an application constraint: Message: "Element deactivated on Operator side". Service: "st-communication-diversion". Action: "<action>"	<p>An attempt has been made to use a ST Communication Diversion <action> which the user has not subscribed to.</p> <p>Possible values for <action> are:</p> <ul style="list-style-type: none"> • notify-caller • reveal-identity-to-caller • reveal-identity-to-target • play-announcement
6.	Failed to meet an application constraint: ST Communication Diversion Failure: Rule id="<rule-id>", missing "actions"	Each ST Communication Diversion rule must have one "actions" element.
7.	Failed to meet an application constraint: ST Communication Diversion Failure: Rule id="<rule-id>", identity is not SIP or TEL URI	The element "target" within a forwarding action must be a SIP or TEL URI.
8.	Failed to meet an application constraint: ST Communication Barring conditions identity, "<barred identity>", conflicts with ST Communication Diversion forwarding identity, "<target-identity>"	The target of a ST Communication-Diversion rule, <target-identity> is barred by the end-user's ST Outgoing Communication Barring of an individual <barred identity>.
9.	Failed to meet an application constraint: ST Communication Barring conditions identity with Number Match, "<barred identity>", conflicts with ST Communication Diversion forwarding identity, "<target-identity>"	The target of a ST Communication-Diversion rule, <target-identity> is barred by the end-user's ST Outgoing Communication Barring of an individual <barred identity> using number-match.



Num	Reason Text	Description
10.	Failed to meet an application constraint: ST Communication Diversion entry , "<target-identity>", is barred by universal many condition	The target of a ST Communication-Diversion rule, <target-identity>, is barred by the end-user's ST Outgoing Communication Barring of all identities, and <target-identity> does not appear in an exception.
11.	Failed to meet an application constraint: ST Communication Diversion forwarding identity, "<target-identity>",is barred by many domain, <domain>	The target of a ST Communication Diversion rule, <target-identity>, is barred by the end-PBX's ST Outgoing Communication Barring of all identities within <domain>, and <target-identity> does not appear in an exception.
12.	Failed to meet an application constraint: ST Communication Diversion Failure: Rule id="<rule-id>", multiple "play-announcement" elements	Each ST Communication Diversion rule must have at most one "play-announcement" action.
13.	Failed to meet an application constraint: ST Communication Diversion forwarding identity, "<target>", is barred in Communication Barring by Bar All Outgoing Calls (BAOC)	The target of a st-communication-diversion rule, <target>, is barred in Communication Barring by Bar All Outgoing Calls (BAOC).

Table 16: Error 3013 Reason Text – ST Malicious Communication Identification

Num	Reason Text	Description
1.	Failed to meet an application constraint: ST Malicious Communication Identification Failure: mcid-extension id="<id>", identity is not SIP or TEL URI	Within an identity condition of an Malicious Communication Identification rule, each Malicious Communication Identification element must have an id attribute that starts with 'sip:' or 'tel:'.

5 Formal Syntax or Schema

5.1 Requests and Responses

The syntax for CAI3G Requests and Responses is defined in ref [1].



5.2 Information Model

5.2.1 General

Each of the ST AS-specific XML elements on the interface is described in the following sections. Indentation in the tables is used to indicate nesting in the corresponding XML structure.

5.2.2 Create SIP Trunking

Table 17: Information in a Create SIP Trunking

XML element	Description
<createSt>	Used to create SIP Trunking Aggregated service data.
<publicId>	The default public user identity for the PBX. This identity must already be configured in the HSS.
<sip-trunking-control>	The SIP Trunking Control – see section 5.2.5 for details.
<st-call-admission-control>	The ST Call Admission Control service – see section 5.2.6 for details.
<st-carrier-pre-select-rn>	The ST Carrier Pre-select Rn service – see section 5.2.7 for details.
<st-carrier-select-rn>	The ST Carrier Select Rn service – see section 5.2.8 for details.
<st-common-data>	The ST Common Data – see section 5.2.9 for details.
<st-communication-diversion>	The ST Communication Diversion service – see section 5.2.10 for details.
<st-incoming-communication-barring>	The ST Incoming Communication Barring service – see section 5.2.11 for details.
<st-malicious-communication-identification>	The ST Malicious Communication Identification service – see section 5.2.13 for details.
<st-operator-controlled-outgoing-barring-programs>	The ST Operator-controlled Outgoing Barring Programs service – see section 5.2.14 for details.
<st-originating-identity-presentation>	The ST Originating Identity Presentation service – see section 5.2.15 for details.
<st-originating-identity-presentation-restriction>	The ST Originating Identity Presentation Restriction service – see section 5.2.16 for details.
<st-outgoing-communication-barring>	The ST Outgoing Communication Barring service – see section 5.2.17 for details.
<st-terminating-identity-presentation>	The ST Terminating Identity Presentation service – see section 5.2.19 for details.
<st-terminating-identity-presentation-restriction>	The ST Terminating Identity Presentation Restriction service – see section 5.2.20 for details.



5.2.3 Set SIP Trunking

Table 18: Information in a Set SIP Trunking

XML element	Description
<setSt>	Used to modify SIP Trunking Aggregated service data.
<concurrency-control>	The <concurrency-control> element is an optional element to control concurrent updates. If present, the set request will be accepted only if the service data version is still at the value given in this element, i.e. no other updates have been performed. It is of type integer.
<sip-trunking-control>	The SIP Trunking control – see section 5.2.5 for details.
<st-call-admission-control>	The ST Call Admission Control service – see section 5.2.6 for details.
<st-carrier-pre-select-rn>	The ST Carrier Pre-select Rn service – see section 5.2.7 for details.
<st-carrier-select-rn>	The ST Carrier Select Rn service – see section 5.2.8 for details.
<st-common-data>	The ST Common Data – see section 5.2.9 for details.
<st-communication-diversion>	The ST Communication Diversion service – see section 5.2.10 for details.
<st-incoming-communication-barring>	The ST Incoming Communication Barring service – see section 5.2.11 for details.
<st-malicious-communication-identification>	The ST Malicious Communication Identification service – see section 5.2.13 for details.
<st-operator-controlled-outgoing-barring-programs>	The ST Operator-controlled Outgoing Barring Programs service – see section 5.2.14 for details.
<st-originating-identity-presentation>	The ST Originating Identity Presentation service – see section 5.2.15 for details.
<st-originating-identity-presentation-restriction>	The ST Originating Identity Presentation Restriction service – see section 5.2.16 for details.
<st-outgoing-communication-barring>	The ST Outgoing Communication Barring service – see section 5.2.17 for details.
<st-terminating-identity-presentation>	The ST Terminating Identity Presentation service – see section 5.2.19 for details.
<st-terminating-identity-presentation-restriction>	The ST Terminating Identity Presentation Restriction service – see section 5.2.20 for details.

5.2.4 GetResponse SIP Trunking

Table 19: Information in a Get Response SIP Trunking

XML element	Description
<getResponseSt>	Contains the currently configured SIP Trunking Aggregated service data.



XML element	Description
<publicId>	The default public user identity for the PBX. This identity must already be configured in the HSS.
<concurrency-control>	The <concurrency-control> element is an integer value indicating the current version of the SIP Trunking service data. This value can be used in a subsequent <setSt> request to make sure that no changes have been made to the service data since the version that was read.
<sip-trunking-control>	The SIP Trunking control – see section 5.2.5 for details.
<st-call-admission-control>	The ST Call Admission Control service – see section 5.2.6 for details.
<st-carrier-pre-select-rn>	The ST Carrier Pre-select Rn service – see section 5.2.7 for details.
<st-carrier-select-rn>	The ST Carrier Select Rn service – see section 5.2.8 for details.
<st-common-data>	The ST Common Data – see section 5.2.9 for details.
<st-communication-diversion>	The ST Communication Diversion service – see section 5.2.10 for details.
<st-incoming-communication-barring>	The ST Incoming Communication Barring service – see section 5.2.11 for details.
<st-malicious-communication-identification>	The ST Malicious Communication Identification service – see section 5.2.13 for details.
<st-operator-controlled-outgoing-barring-programs>	The ST Operator-controlled Outgoing Barring Programs service – see section 5.2.14 for details.
<st-originating-identity-presentation>	The ST Originating Identity Presentation service – see section 5.2.15 for details.
<st-originating-identity-presentation-restriction>	The ST Originating Identity Presentation Restriction service – see section 5.2.16 for details.
<st-outgoing-communication-barring>	The ST Outgoing Communication Barring service – see section 5.2.17 for details.
<st-terminating-identity-presentation>	The ST Terminating Identity Presentation service – see section 5.2.19 for details.
<st-terminating-identity-presentation-restriction>	The ST Terminating Identity Presentation Restriction service – see section 5.2.20 for details.

5.2.5

SIP Trunking Control

Table 20: Information in a SIP Trunking Control



XML element					Description
<sip-trunking-control>					The SIP Trunking service. This data is available to the operator. Unlike services, this element should never be withdrawn so it is not nillable. It must be present on the creation of SIP Trunking service.
<operator-configuration>					The configuration parameters for the sip trunking control service that is available to the operator. This must be present on the creation of the sip-trunking-control> service.
<activated>					The <activated> element has values "true" or "false". When set to "true" the PBX is provisioned with the SIP Trunking service. It must be present on the creation of the service.
<disable-identity-validation>					The <disabled-identity-validation> element disables the confirmation of the identity of the PBX. Use xsi:nil="true" to withdraw this element.
<auxiliary-identity>					The auxiliary PBX identity is one of the identities used in static mode PBX connect to validate the calling user identity received in the P-Asserted-Identity headers. If a valid P-Asserted-Identity header is missing, the auxiliary identity is used to populate the P-Asserted-Identity header field. This parameter is a sip URI with or without the user part. Use xsi:nil="true" to withdraw this element. Examples: sip:+4680123456@st.operator.com;user=phone or sip:st.operator.com
<static-route>					The <static-route> element is a sub-MO allowing multiple instances with "id" as the unique key. The static-route and dynamic-route are mutually exclusive. Use xsi:nil="true" to withdraw this element.
<id>					The <id> of the static route. It must be unique within the scope of the complete document. It must be present on the creation of a static-route.
<disabled>					The <disabled> element is set to disable the route. Use xsi:nil="true" to withdraw this element.
<stand-by-route>					The <standby-route> element is set if this is a standby route. Use xsi:nil="true" to withdraw this element.
<routes>					The <routes> element can have 0 or any number of route elements. The content of this element define the preloaded route-set used to target this static route. Use xsi:nil="true" to withdraw this routes.
<route>					The <route> element is a sub-MO allowing multiple instances with "id" as the unique key. Its content define the Route header field inserted into the preloaded route.set. Use xsi:nil="true" to withdraw this element.
<id>					The <id> of the route. It must be unique within the scope of the complete document. It must be present on the creation of the route.



XML element					Description
				<uri>	The route URI. It must take the form of a sip URI. It must be present on the creation of the route. Examples: sip:sbc1.operator.com or sip:[2000:fe::12fe]:5060
				<dynamic-route>	The <dynamic-route> element is a sub-MO allowing multiple instances with "id" as the unique key. The static-route and dynamic-route are mutually exclusive. Use xsi:nil="true" to withdraw this element.
				<id>	The <id> of the dynamic route. It must be a sip URI specifying the Address of Record used for registration of the route. It must be unique within the scope of the complete document. It must be present on the creation of the dynamic-route.
				<disabled>	The <disabled> element is set to disable the route. Use xsi:nil="true" to withdraw this element.
				<stand-by-route>	The <standby-route> element is set if this is a standby route. Use xsi:nil="true" to withdraw this element.

5.2.6 ST Call Admission Control

Table 21: Information in a ST Call Admission Control

XML element					Description
				<st-call-admission-control>	The call admission control service. Use xsi:nil="true" to withdraw the entire service.
				<operator-configuration>	The configuration parameters for the ST Call Admission Control service that are available to the operator rather than the user. It must be present on the creation of the <st-call-admission-control> service.
				<activated>	The activated element has values "true" or "false". When set to "true" the PBX is provisioned with the ST call admission control service. If set to "false" this will withdraw the service from the PBX. It must be present on the creation of the <st-call-admission-control> service.
				<orig-all-limit>	Defines the limit of all originating sessions for this PBX. It must be present on the creation of the <st-call-admission-control-service>.
				<term-all-limit>	Defines the limit of all terminating sessions for this PBX. It must be present on the creation of the <st-call-admission-control> service.
				<total-all-limit>	Defines the limit of all sessions for this PBX. It must be present on the creation of the <st-call-admission-control> service.

5.2.7 ST Carrier Pre-Select Rn

Table 22: Information in a ST Carrier Pre-Select Rn



XML element			Description
<st-carrier-pre-select-rn>			The ST carrier pre-select rn service. Use xsi:nil="true" to withdraw the entire service.
	<operator-configuration>		The configuration parameters for the ST carrier pre select rn service are available to the operator. This part must be present on the creation of the ST carrier pre select rn service.
		<activated>	The <activated> element has values "true" or "false". When set to "true", the PBX is provisioned with the ST carrier pre-select rn service. If set to "false", the service is withdrawn from the PBX. It must be present on the creation of the ST carrier pre select rn service.
		<call-type-carrier-rn>	The <call-type-carrier-rn> element specifies a mapping between a call type and the global carrier code to be pre-selected for calls of that type along with the domain for that carrier. The <call-type-carrier-rn> element is a sub-MO allowing either one or two instances with "call-type" as the unique key.
		<call-type>	The type of call either "LOCAL" or "REMOTE". The value "LOCAL" corresponds to calls to numbers with the same area code as the user. The value "REMOTE" corresponds to all other calls. This must be present on the creation of a <call-type-carrier-rn>.
		<global-carrier-code>	The global carrier code to be used for a call of the given type. This is a string of between 3 and 8 digits. This must be present on the creation of a <call-type-carrier-rn>.

5.2.8 ST Carrier Select Rn

Table 23: Information in a ST Carrier Select Rn

XML element			Description
<st-carrier-select-rn>			The ST carrier select rn service. Use xsi:nil="true" to withdraw the entire service.
	<operator-configuration>		The configuration parameters for the ST carrier select rn service are available to the operator. This part must be present on the creation of the ST carrier select rn service.
		<activated>	The <activated> element has values "true" or "false". When set to "true" the PBX is provisioned with the ST carrier select rn service. If set to "false", the service is withdrawn from the PBX. It must be present on the creation of the ST carrier select rn service.

5.2.9 ST Common Data

Table 24: Information in a ST Common Data



XML element		Description
<st-common-data>		The ST common data available across services. This data is available to the operator. Unlike services this should never be withdrawn so it is not nillable.
	<area-code>	Area code 0-6 digits. Leave empty for numbering plans to which it does not apply. Use xsi:nil="true" to withdraw this element.
	<country-code>	Country code 1-4 digits. Use xsi:nil="true" to withdraw this element.
	<rule-global-limit>	The maximum number of allowed rules in the PBX service document. Not specified or zero limit means no limit.

5.2.10

ST Communication Diversion

Table 25: Information in a ST Communication Diversion

XML element		Description
<st-communication-diversion>		The ST communication diversion service. Use xsi:nil="true" to withdraw the entire service.
	<operator-configuration>	The configuration parameters for the ST communication diversion service that is available to the operator. It must be present on the creation of the ST communication diversion service. Use xsi:nil="true" to withdraw this element.
	<activated>	The <activated> element has values "true" or "false". When set to "true" the PBX is provisioned with the ST communication diversion service. If set to "false", the service is withdrawn while the st-cdiv-user-configuration element is preserved. It must be present on the creation of the ST communication diversion service.
	<cdiv-op-conditions>	The <cdiv-op-conditions> element is a grouping element for fine-grain provisioning options that control which conditions the PBX is permitted to use in communication diversion rules. Use xsi:nil="true" to withdraw this element.
	<not-registered-condition>	The <not-registered-condition> element has values "activated" or "deactivated". When set to "activated" it allows the PBX to use the <cdiv-call-state> condition with the value of "not-registered" in communication diversion rules. Note <not-registered-condition> is not applicable for a PBX in static mode.
	<not-reachable-condition>	The <not-reachable-condition> element has values "activated" or "deactivated". When set to "activated" it allows the subscriber to use the <cdiv-call-state> condition with the value of "not-reachable" in communication diversion rules.



XML element			Description
		<cdiv-op-actions>	The <cdiv-op-actions> element is a grouping element for fine-grain provisioning options to control which actions the user is permitted to use for communication diversion rules.
		<notify-caller-action>	The <notify-caller-action> element has values “activated” or “deactivated”. When set to “activated” it allows the PBX to use the <notify-caller> action in communication diversion rules to control whether the caller is notified that the call is being forwarded.
		<reveal-identity-to-caller-action>	The <reveal-identity-to-caller-action> has values “activated” or “deactivated”. When set to “activated” it allows the PBX to use the <reveal-identity-to-caller> action in communication diversion rules to control whether the caller being notified that the call is being forwarded receives the target’s identity information.
		<reveal-identity-to-target-action>	The <reveal-identity-to-target-action> has values “activated” or “deactivated”. When set to “activated” it allows the PBX to use the <reveal-identity-to-target> action in communication diversion rules to control whether the diverted-to party receives identity information of the diverting party.
		<play-announcement-action>	The <play-announcement-action> element has values “activated” or “deactivated”. When set to “activated” it allows the PBX to use the play-announcement action in communication diversion rules to control whether the caller is presented by specific announcement handled by generic announcement service.
		<rule-limit>	The maximum number of allowed CDIV rules in the user document. Not specified or zero limit means no limit.
		<user-configuration>	The configuration parameters for the ST communication diversion service can be set on the PBX’s behalf by the operator. This shall only be present if the service is provisioned i.e. <operator-configuration> is present and activated is “true”.
		<active>	The <active> element has values “true” or “false”. It controls whether the ST communication diversion service is active or not for this PBX.
		<cdiv-ruleset>	Grouping element for a set of zero or more user rules.
		<cdiv-rule>	An individual rule controlling communication diversion behavior. The <cdiv-rule> element is a sub-MO allowing multiple instances with “id” as the unique key.
		<id>	A unique identifier for an individual rule. It must be unique within the scope of the complete document. It must be present on the creation of a <cdiv-rule>.



XML element					Description
				<cdiv-conditions>	The <cdiv-conditions> element is a grouping element for conditions for a rule. All conditions must be satisfied for the rule to take effect. If no conditions are present then the rule is always applicable. The conditions that are permitted depend on the fine grain provisioning options in <cdiv-op-conditions>.
				<rule-deactivated>	The <rule-deactivated> element has values "true" or "false". If present with the value "true", this has the effect of deactivating the individual rule and the rule is not checked. This condition is removed when set to "false".
				<cdiv-call-state>	The <cdiv-call-state> condition controls which state the PBX must be in for the rule to apply. The value " not-registered " applies when none of the configured links have been registered by the PBX (valid only in dynamic mode), The value " not-reachable " applies when the PBX is not reachable because either a specific response has been received or the Access Profile Timeout timer expires. The value " unconditional " is used to clear the other call state values so that the condition is satisfied regardless of the PBX's call state.
				<cdiv-actions>	The <cdiv-actions> element is a grouping element for the actions for a rule. It must be present on the creation of a <cdiv-rule>.
				<forward-to>	The <forward-to> element is a grouping element with details of the target to which the communication should be diverted and optional control of notifications and which identities are revealed to whom. This must be present on the creation of a <cdiv-rule>.
				<target>	The <target> element specifies the identity to which the communication should be diverted. It can take the form of a sip or tel URI. A tel URI and sip URI that was converted from a tel URI according to section 19.1.6 of RFC 3261 [6], is normalized before it is stored. It must be present on the creation of a <cdiv-rule>.
				<notify-caller>	The <notify-caller> element has values "true" or "false". It controls whether the caller is notified that the call is being forwarded. If it is not included then the default behavior is to notify the caller (true).
				<reveal-identity-to-caller>	The <reveal-identity-to-caller> element has values "true" or "false". It controls whether the caller being notified that the call is being forwarded receives the target's identity information. If it is not included, the default behavior is to reveal the target's identity to the caller (true).



XML element						Description
					<reveal-identity-to-target>	The <reveal-identity-to-target> element has values “true” and “false”. It controls whether the diverted-to party receives identity information of the diverting party. If it is not included then the default behavior is to reveal the diverting party’s identity to the target (true).
					<play-announcement>	When the play-announcement action is set with the string value containing characters with the length between 1 to 32, the caller will be presented with the specific announcement handled by generic announcement service. When the play-announcement action is set with zero-length string, the play-announcement action element in the rule is deleted from the rule.

5.2.11

ST Incoming Communication Barring

Table 26: Information in a ST Incoming Communication Barring

XML element						Description
					<st-incoming-communication-barring>	The ST incoming communication barring service. Use xsi:nil=”true” to withdraw the entire service.
					<operator-configuration>	The configuration parameters for the ST incoming communication barring service available to the operator. It must be present on the creation of the <st-incoming-communication-barring> service.
					<activated>	The activated element has values “true” or “false”. When set to “true” the user is provisioned with the ST incoming communication barring service. If set to “false” the user service is withdrawn, but the user-configuration element is preserved. It must be present on the creation of the st-incoming-communication-barring service.
					<icb-op-conditions>	The <icb-op-conditions> element is a grouping element for fine-grain provisioning options that control which condition elements the user is permitted to use in ST incoming communication barring rules.
					<anonymous-condition>	The <anonymous-condition> element has values “activated” or “deactivated”. When set to “activated” it allows the subscriber to use the <anonymous> condition in ST incoming communication barring rules.
					<communication-diverted-condition>	The <communication-diverted-condition> element has values “activated” or “deactivated”. When set to “activated” it allows the subscriber to use the <communication-diverted> condition in ST incoming communication barring rules.



XML element			Description
		<identity-condition>	The <identity-condition> element has values “activated” or “deactivated”. When set to “activated” it allows the subscriber to use the <identity> condition in ST incoming communication barring rules.
		<other-identity-condition>	The <other-identity-condition> element has values “activated” or “deactivated”. When set to “activated” it allows the subscriber to use the <other-identity> condition in ST incoming communication barring rules.
		<icb-op-actions>	The <icb-op-actions> element is a grouping element for fine-grain provisioning options to control which action elements the user is permitted to use in ST incoming communication barring rules.
		<allow-true-action>	The <allow-true-action> element has values “activated” or “deactivated”. When set to “activated” it allows the subscriber to use the <allow> action with the value of “true” in ST incoming communication barring rules to explicitly allow ST incoming communications that match the associated conditions. With this absent or set to “deactivated” the subscriber is only permitted to use the <allow> action with the value of “false” to bar incoming communications.
		<play-announcement-action>	The <play-announcement-action> element has values “activated” or “deactivated”. When set to “activated” it allows the subscriber to use the play-announcement action in ST incoming communication barring rules to control whether the caller is presented by specific announcement handled by generic announcement service.
		<play-segmented-announcement-action>	The <play-announcement-action> element has values “activated” or “deactivated”. When set to “activated” it allows the subscriber to use the play-segmented-announcement action in ST incoming communication barring rules to control whether the caller is presented by specific segmented announcement handled by generic announcement service.
		<rule-limit>	The maximum number of allowed incoming communication barring rules in the user document. Not specified or zero limit means no limit.
		<user-configuration>	The configuration parameters for the ST incoming communication barring service available to be set on behalf of the PBX. It shall only be present if the service is provisioned i.e. <operator-configuration> is present and activated is “true”.



XML element			Description
		<active>	The <active> element has values “true” or “false”. It controls whether the ST incoming communication barring service is active or not for this subscriber. Note that this controls the user rules but has no effect on the operator rules.
		<icb-ruleset>	Grouping element for a set of zero or more user rules. See section 5.2.12 for details of the contents of the <icb-ruleset> element.

5.2.12

ST Incoming Communication Barring Ruleset

Table 27: Information in a ST Incoming Communication Barring Ruleset

XML element			Description
		<icb-rule>	An individual rule controlling ST incoming communication barring behavior. The <icb-rule> element is a sub-MO allowing multiple instances with “id” as the unique key.
		<id>	A unique identifier for an individual rule. It must be unique within the scope of the complete document. It must be present on the creation of an <icb-rule> element.
		<icb-conditions>	The <icb-conditions> element is a grouping element for conditions for a rule. All conditions must be satisfied for the rule to take effect. If no conditions are present, the rule is always applicable.
		<rule-deactivated>	The <rule-deactivated> element has values “true” or “false”. If present with the value “true”, it has the effect of deactivating the individual rule and the rule is not checked. This condition is removed when set to “false”.
		<icb-caller-identity>	The <icb-caller-identity> element is a grouping element for conditions which are based on the caller’s identity (or lack of an identity in the case of anonymous).
		<anonymous>	The <anonymous> element is an empty element specifying a condition which is satisfied if the caller is anonymous. This can be removed by deleting the enclosing <icb-caller-identity> element or by replacing it with an <identity> or <other-identity> element. The elements <anonymous>, <identity> and <other-identity> are mutually exclusive.



			<code><other-identity></code>	The <code><other-identity></code> element is an empty element which matches any identity that has not been specified by any of the other rules in the ruleset. It allows for setting a default policy. This can be removed by deleting the enclosing <code><icb-caller-identity></code> element or by replacing it with an <code><anonymous></code> or <code><identity></code> element. The elements <code><anonymous></code> , <code><identity></code> and <code><other-identity></code> are mutually exclusive.
			<code><identity></code>	The <code><identity></code> element is a grouping element for conditions which are based on the caller's identity. The condition is satisfied if any of the included <code><one></code> or <code><many></code> elements within it is matched. This can be removed by deleting the enclosing <code><icb-caller-identity></code> element or by replacing it with an <code><anonymous></code> or <code><other-identity></code> element. The elements <code><anonymous></code> , <code><identity></code> and <code><other-identity></code> are mutually exclusive. See section 5.2.21 for details of the contents of the <code><identity></code> element.
			<code><communication-diverted></code>	The <code><communication-diverted></code> element has values "true" or "false". If present with the value "true", the condition is satisfied when the communication has been diverted. This condition is removed when set to "false".
			<code><cb-actions></code>	The <code><cb-actions></code> element is a grouping element for the actions for a rule. For communication barring an <code><allow></code> action must be present in each rule. This must be present on the creation of an <code><icb-rule></code> element. There is a choice: either a <code><play-announcement></code> or a <code><play-segmented-announcement></code> can be defined in the list of actions.
			<code><allow></code>	The <code><allow></code> element has values "true" or "false". If set to "false", any ST incoming communications barring satisfying the corresponding conditions will be barred unless overridden by another rule with <code><allow></code> set to "true". If set to "true", any ST incoming communications barring satisfying the corresponding conditions will be allowed i.e. not barred. It must be present on the creation of an <code><icb-rule></code> element.
			<code><play-announcement></code>	When the play-announcement action is set with the string value containing characters with the length between 1 to 32 and if there is any communications satisfying the corresponding conditions and being barred (allow=false), the caller will be presented with the announcement associated with the announcement name pointed out by the string value. When the play-announcement action is set with zero-length string, the play-announcement action element in the rule will be deleted from the rule.



				<play-segmented-announcement>	<p>If there is any communications satisfying the corresponding conditions, the caller will be presented with the segmented announcement associated with the announcement code pointed out by the “announcement-name” attribute of the element.</p> <p>The keyed “play-segmented-announcement” action with the “announcement-name” attribute can be deleted from the list of actions by setting the “xsi:nil” attribute to “true”.</p> <p>The “play-segmented-announcement” element is a sub-MO allowing instance with “announcement-name” as the unique key.</p>
				<announcement-name>	<p>The name of the announcement to be played. This must be present on the creation of a play-segmented-announcement element.</p>
				<announcement-variable>	<p>The announcement variable to be embedded into the announcement. It's use is optional, i.e. a segmented announcement may or may not contain any variable segment. Maximum 32 announcement variables can be embedded into a segmented announcement. A keyed “announcement-variable” element with the “variable-name” attribute can be deleted from the list of announcement variables by setting the “xsi:nil” attribute to true.</p> <p>The “announcement-variable” element is a sub-MO allowing multiple instances with “variable-name” as the unique key.</p>
				<variable-name>	<p>The name of the announcement variable to be embedded. This must be present on the creation of an announcement-variable element inside a play-segmented-announcement element.</p>
				<variable-value>	<p>The variable value is defined in the variable-value child element of the announcement-variable element. According to H.248.9, the allowed characters in place of a variable value are ASCII 0x09, 0x20-0x7E</p>

5.2.13

ST Malicious Communication Identification

Table 28: Information in a ST Malicious Communication Identification

XML element	Description
<st-malicious-communication-identification>	<p>The ST malicious communication identification service.</p> <p>Use xsi:nil=”true” to withdraw the entire service.</p>



XML element			Description
	<operator-configuration>		The configuration parameters for the malicious communication identification service that is available to the operator. It must be present on the creation of the <st-malicious-communication-identification> service.
		<activated>	The activated element has values "true" or "false". When set to "true" the PBX is provisioned with the malicious communication identification service. If set to "false", the service is withdrawn from the PBX. It must be present on the creation of the st-malicious-communication-identification service.
		<mcid- extension>	The <mcid extension> element specifies an extension number in the PBX that has MCID activated. The element is a sub-MO allowing multiple instances with "id" as the unique key and is limited to 50 instances. If empty, all extension of the PBX has MCID activated.
		<id>	A unique identifier for an individual MCID extension. It must be unique within the scope of the complete document. It must be present on the creation of a <mcid-extension> element.
		<uri>	The uri is the identity of the mcid extension number. It can take the form of a sip or tel URI . A tel URI, or a sip URI that was converted from a tel URI according to section 19.1.6 of RFC 3261 [6], is normalized before it is stored. It must be present on the creation of a <mcid-extension> element.

5.2.14

ST Operator Controlled Outgoing Barring Programs

Table 29: Information in a ST Operator Controlled Outgoing Barring Programs

XML element			Description
	<st-operator-controlled-outgoing-barring-programs>		The ST operator controlled outgoing barring programs service. Use xsi:nil="true" to withdraw the entire service.
		<operator-configuration>	The configuration parameters for the ST operator controlled outgoing barring programs service are available to the operator. It must be present on the creation of the <st-operator-controlled-outgoing-barring-programs> service.



XML element			Description
		<activated>	The activated element has values "true" or "false". When set to "true" the user is provisioned with the st operator controlled outgoing barring programs service. If set to "false", the service is withdrawn from the PBX. It must be present on the creation of the operator-controlled-outgoing-barring-programs service.
		<operator-barring-program>	The <operator-barring-program> element is a container for each of the categories of outgoing communications that is to be barred by the service. The operator-barring-program and operator-permitted-program are mutually exclusive.
		<category-name>	The <category-name> element contains the name of a category of calls to be barred. This is a multi-value parameter and can appear between 0 and 83 times to cover each category of outgoing communications to be barred. The value of each <category-name> element is a string of up to 32 characters that should match one of the category names defined by the mtasStOcbOpBCatName attributes [3] or one of the special values "Local", "Non Local" or "Allow Local".
		<operator-permitted-program>	The <operator-permitted-program> element is a container for each of the categories of outgoing communications that is to be allowed by the service – any identity not matched by one of these categories or the global white list is barred. The operator-barring-program and operator-permitted-program are mutually exclusive.
		<category-name>	The <category-name> element contains the name of a category of calls to be permitted. This is a multi-value parameter and can appear between 0 and 83 times to cover each category of outgoing communications to be permitted. The value of each category-name element is a string of up to 32 characters that should match one of the category names defined by the mtasStOcbOpBCatName attributes [3] or one of the special values "Local" or "Non Local".
		<operator-diversion-barring-program>	The <operator-diversion-barring-program> element is a container for each of the categories of outgoing communications that should be barred as diversion targets.
		<category-name>	The <category-name> element contains the name of a category of calls to be barred for diverted communications. This is a multi-value parameter and can appear between 0 and 83 times to cover each category of outgoing communications to be barred. The value of each <category-name> element is a string of up to 32 characters that should match one of the category names defined by the mtasStOcbOpBCatName attributes [3] one of the special values "Local", "Non Local" or "Allow Local".



5.2.15

ST Originating Identity Presentation

Table 30: Information in a ST Originating Identity Presentation

XML element		Description
<st-originating-identity-presentation>		The ST originating identity presentation service. Use xsi:nil="true" to withdraw the entire service.
	<operator-configuration>	The configuration parameters for the ST originating identity presentation service available to the operator. It must be present on the creation of the ST originating identity presentation service.
	<activated>	The <activated> element has values "true" or "false". When set to "true" the PBX is provisioned with the ST originating identity presentation service. If set to "false", the service is withdrawn, but the user-configuration element is preserved. It must be present on the creation of the ST originating identity presentation service.
	<restriction-override>	The <restriction-override> element has values "override-active" or "override-not-active". The value "override-active" means that the originating identity will be presented even if the calling party has requested for their presentation to be restricted.
	<user-configuration>	The configuration parameters for the ST originating identity presentation service can be set on the PBX's behalf by the operator. This shall only be present if the service is provisioned i.e. <operator-configuration> is present and activated is "true".
	<active>	The <active> element has values "true" or "false". It controls whether the ST originating identity presentation service is active or not for this PBX.

5.2.16

ST Originating Identity Presentation Restriction

Table 31: Information in a ST Originating Identity Presentation Restriction

XML element		Description
<st-originating-identity-presentation-restriction>		The ST originating identity presentation restriction service. Use xsi:nil="true" to withdraw the entire service.
	<operator-configuration>	The configuration parameters for the ST originating identity presentation restriction service that is available to the operator. It must be present on the creation of the ST originating identity presentation restriction service.



XML element		Description
	<activated>	The <activated> element has values “true” or “false”. When set to “true” the PBX is provisioned with the ST originating identity presentation restriction service. If set to “false”, the service is withdrawn, but the user-configuration element is preserved. It must be present on the creation of the ST originating identity presentation restriction service.
	<mode>	The <mode> element has values “permanent” or “temporary”. The value “permanent” is used to give the PBX a permanent restriction service. In this case there must be no <user-configuration> element. The value “temporary” gives an identity presentation restriction service where the PBX can choose default behavior and also whether to override this on a per-call basis. It must be present on the creation of the ST originating identity presentation restriction service.
	<restriction>	The <restriction> element has values “only-identity” or “all-private-information” and selects whether just the identity of the PBX is restricted or all private information. It must be present on the creation of the ST originating identity presentation restriction service.
	<from-header-screening>	The element controls execution of From header screening in requests sent by the originating PBX. It can be set to “enabled” or “disabled”. If not present, the From header screening feature is instead controlled by the <i>mtasStFromHeaderScreening</i> node parameter. Use <i>xsi:nil="true"</i> to withdraw this element.
	<user-configuration>	The configuration parameters for the ST originating identity presentation restriction service can be set on the PBX's behalf by the operator. It shall only be present if the service is provisioned i.e. <operator-configuration> is present and activated is “true”.
	<active>	The <active> element has values “true” or “false”. It controls whether the ST originating identity presentation restriction service is active or not for this PBX.
	<default-behaviour>	The <default-behaviour> element has values “presentation-restricted” or “presentation-not-restricted”. It selects the default behaviour in temporary mode when the PBX does not select explicitly within the call whether to restrict their identity or not.

5.2.17

ST Outgoing Communication Barring

Table 32: Information in a ST Outgoing Communication Barring



XML element			Description
<st-outgoing-communication-barring>			The ST outgoing communication barring service. Use xsi:nil="true" to withdraw the entire service.
	<operator-configuration>		The configuration parameters for the ST outgoing communication barring service available to the operator. It must be present on the creation of the <st-outgoing-communication-barring> service.
	<activated>		The activated element has values "true" or "false". When set to "true" the user is provisioned with the ST outgoing communication barring service. If set to "false", the service is withdrawn, but the user-configuration element is preserved. It must be present on the creation of the outgoing-communication-barring service.
	<ocb-op-conditions>		The <ocb-op-conditions> element is a grouping element for fine-grain provisioning options that control which condition elements the user is permitted to use in ST outgoing communication barring rules.
		<identity-condition>	The <identity-condition> element has values "activated" or "deactivated". When set to "activated" it allows the subscriber to use the <identity> condition in ST outgoing communication barring rules.
		<other-identity-condition>	The <other-identity-condition> element has values "activated" or "deactivated". When set to "activated" it allows the subscriber to use the <other-identity> condition in ST outgoing communication barring rules.
		<carrier-condition>	The <carrier-condition> element has values "activated" or "deactivated". When set to "activated" it allows the subscriber to use the <carrier> condition in ST outgoing communication barring rules.
		<carrier-select-code>	The <carrier-select-code> element has values "activated" or "deactivated". When set to "activated" it allows the subscriber to use the <carrier-select-code> element of the <carrier> condition in ST outgoing communication barring rules.
	<ocb-op-actions>		The <ocb-op-actions> element is a grouping element for fine-grain provisioning options to control which action elements the user is permitted to use in ST outgoing communication barring rules.
		<allow-true-action>	The <allow-true-action> element has values "activated" or "deactivated". When set to "activated" it allows the subscriber to use the <allow> action with the value of "true" in ST outgoing communication barring rules to explicitly allow outgoing communications that match the associated conditions. With this absent or set to "deactivated" the subscriber is only permitted to use the <allow> action with the value of "false" to bar outgoing communications.



XML element			Description
		<play-announcement-action>	The <play-announcement-action> element has values “activated” or “deactivated”. When set to “activated” it allows the subscriber to use the play-announcement action in ST outgoing communication barring rules to control whether the caller is presented by specific announcement handled by generic announcement service.
		<play-segmented-announcement-action>	The <play-announcement-action> element has values “activated” or “deactivated”. When set to “activated” it allows the subscriber to use the <play-segmented-announcement> action in ST outgoing communication barring rules to control whether the caller is presented by specific segmented announcement handled by generic announcement service.
		<rule-limit>	The maximum number of allowed ST outgoing communication barring rules in the user document. Not specified or zero limit means no limit.
		<user-configuration>	The configuration parameters for the ST outgoing communication barring service available to be set on behalf of the PBX.. It shall only be present if the service is provisioned i.e. <operator-configuration> is present and activated is “true”.
		<active>	The <active> element has values “true” or “false”. It controls whether the ST outgoing communication barring service is active or not for this PBX. Note that this controls the user rules but has no effect on the operator rules.
		<ocb-ruleset>	Grouping element for a set of zero or more user rules. See section 5.2.18 for details of the content of the <ocb-ruleset>.

5.2.18

ST Outgoing Communication Barring Ruleset

Table 33: Information in a ST Outgoing Communication BarringRuleset

XML element			Description
		<ocb-ruleset>	Grouping element for a set of zero or more ST outgoing communication barring rules.
		<ocb-rule>	An individual rule controlling ST outgoing communication barring behavior. The <ocb-rule> element is a sub-MO allowing multiple instances with “id” as the unique key.
		<id>	A unique identifier for an individual rule. It must be unique within the scope of the complete document. It must be present on the creation of an <ocb-rule> element.
		<ocb-conditions>	The <ocb-conditions> element is a grouping element for conditions for a rule. All conditions must be satisfied for the rule to take effect. If no conditions are present, the rule is always applicable.



XML element				Description
			<rule-deactivated>	The <rule-deactivated> element has values "true" or "false". If present with the value "true", it has the effect of deactivating the individual rule and the rule is not checked. This condition is removed when set to "false".
			<ocb-caller-identity>	The <ocb-caller-identity> element is a grouping element for conditions which are based on the called party's identity.
			<other-identity>	The <other-identity> element is an empty element which matches any identity that has not been specified by any of the other rules in the ruleset. It allows for setting a default policy. This can be removed by deleting the enclosing <ocb-caller-identity> element or by replacing it with an <identity> element. The elements <identity> and <other-identity> are mutually exclusive.
			<identity>	The <identity> element is a grouping element for conditions which are based on the called party's identity. The condition is satisfied if any of the included <one> or <many> elements within it is matched. This can be removed by deleting the enclosing <ocb-caller-identity> element or by replacing it with an <other-identity> element. The elements <identity> and <other-identity> are mutually exclusive. . See section 5.2.21 for details of the contents of the <identity> element.
			<carrier>	The <carrier> element is a grouping element for conditions which are based on the carrier selected for the call on call-by-call basis. If no sub-element is specified, all carriers are matched. The carriers that match to the pre-subscribed carriers for the current call-type are subject to this condition.
			<carrier-select-code>	The <carrier-select-code> element contains the dialed Carrier Select Code. This is a multi-value parameter so it can appear more than once with several Carrier Select Codes. If any of them is matches, the carrier condition is fulfilled.
			<carrier-name>	The <carrier-name> element contains an alias name of the carrier selected for the call on call-by-call basis. This is a multi-value parameter so it can appear more than once with several carrier names. If any of them is matches, the carrier condition is fulfilled.



XML element				Description
			<cb-actions>	<p>The <cb-actions> element is a grouping element for the actions for a rule. For communication barring an <allow> action must be present in each rule.</p> <p>It must be present on the creation of an <ocb-rule> element.</p> <p>There is a choice: either a <play-announcement> or a <play-segmented-announcement> can be defined in the list of actions.</p>
			<allow>	<p>The <allow> element has values “true” or “false”. If set to “false” then any outgoing communications satisfying the corresponding conditions will be barred unless overridden by another rule with <allow> set to “true”. If set to “true” then any outgoing communications satisfying the corresponding conditions will be allowed by this service i.e. not barred.</p> <p>It must be present on the creation of an <ocb-rule> element.</p>
			<play-announcement>	<p>When the play-announcement action is set with the string value containing characters with the length between 1 to 32, if there is any communications satisfying the corresponding conditions and being barred (allow=false), the caller will be presented with the announcement associated with the announcement code pointed by the string value. When the play-announcement action is set with the string value containing character with a zero-length string, any play-announcement action element in the rule will be deleted from the rule.</p>
			<play-segmented-announcement>	<p>If there is any communications satisfying the corresponding conditions, the caller will be presented with the segmented announcement associated with the announcement code pointed by the “announcement-name” attribute of the element.</p> <p>The keyed “play-segmented-announcement” action with the “announcement-name” attribute can be deleted from the list of actions by setting the “xsi:nil” attribute to “true”.</p> <p>The “play-segmented-announcement” element is a sub-MO allowing instance with “announcement-name” as the unique key.</p>
			<announcement-name>	<p>The name of the announcement to be played. This must be present on the creation of a play-segmented-announcement element.</p>



XML element					Description
				<announcement-variable>	The announcement variable to be embedded into the announcement. It's use is optional, i.e. a segmented announcement may or may not contain any variable segment. Maximum 32 announcement variables can be embedded into a segmented announcement. A keyed "announcement-variable" element with the "variable-name" attribute can be deleted from the list of announcement variables by setting the "xsi:nil" attribute to true. The "announcement-variable" element is a sub-MO allowing multiple instances with "variable-name" as the unique key.
				<variable-name>	The name of the announcement variable to be embedded. This must be present on the creation of an announcement-variable element inside a play-segmented-announcement element.
				<variable-value>	The variable value is defined in the variable-value child element of the announcement-variable element. According to H.248.9, the allowed characters in place of a variable value are ASCII 0x09, 0x20-0x7E

5.2.19

ST Terminating Identity Presentation

Table 34: Information in a ST Terminating Identity Presentation

XML element					Description
				<st-terminating-identity-presentation>	The ST terminating identity presentation service. Use xsi:nil="true" to withdraw the entire service.
				<operator-configuration>	The configuration parameters for the ST terminating identity presentation service available to the operator. It must be present on the creation of the ST terminating identity presentation service.
				<activated>	The <activated> element has values "true" or "false". When set to "true" the PBX is provisioned with the ST terminating identity presentation service. If set to "false", the service is withdrawn, but the user-configuration element is preserved. It must be present on the creation of the ST terminating identity presentation service.
				<restriction-override>	The <restriction-override> element has values "override-active" or "override-not-active". The value "override-active" means that the terminating identity will be presented even if the calling party has requested for their presentation to be restricted.



XML element		Description
	<user-configuration>	The configuration parameters for the ST terminating identity presentation service can be set on the PBX's behalf by the operator. This shall only be present if the service is provisioned i.e. <operator-configuration> is present and activated is "true".
	<active>	The <active> element has values "true" or "false". It controls whether the ST terminating identity presentation service is active or not for this PBX.

5.2.20

ST Terminating Identity Presentation Restriction

Table 35: Information in a ST Terminating Identity Presentation Restriction

XML element		Description
	<st-terminating-identity-presentation-restriction>	The ST terminating identity presentation restriction service. Use xsi:nil="true" to withdraw the entire service.
	<operator-configuration>	The configuration parameters for the ST terminating identity presentation restriction service that is available to the operator. It must be present on the creation of the ST terminating identity presentation restriction service.
	<activated>	The <activated> element has values "true" or "false". When set to "true" the PBX is provisioned with the ST terminating identity presentation restriction service. If set to "false", the service is withdrawn, but the user-configuration element is preserved. It must be present on the creation of the ST terminating identity presentation restriction service.
	<mode>	The <mode> element has values "permanent" or "temporary". The value "permanent" is used to give the PBX a permanent restriction service. In this case there must be no <user-configuration> element. The value "temporary" gives an identity presentation restriction service where the PBX can choose default behavior and also whether to override this on a per-call basis. It must be present on the creation of the ST terminating identity presentation restriction service.



XML element		Description
	<connected-identity-support>	The <connected-identity-support> element has values “enabled” or “disabled”. When connected identity is not supported, the From-change feature is removed from the Supported header of the initial request sent to the PBX. If the element is not present, the default setting is “disabled”.
	<user-configuration>	The configuration parameters for the ST terminating identity presentation restriction service can be set on the PBX's behalf by the operator. It shall only be present if the service is provisioned i.e. <operator-configuration> is present and activated is “true”.
	<active>	The <active> element has values “true” or “false”. It controls whether the ST terminating identity presentation restriction service is active or not for this PBX.
	<default-behaviour>	The <default-behaviour> element has values “presentation-restricted” or “presentation-not-restricted”. It selects the default behaviour in temporary mode when the PBX does not select explicitly within the call whether to restrict their identity or not.

5.2.21 Identity Condition

Table 36: Information in an Identity Condition

XML element		Description
	<identity>	The <identity> element is a grouping element for conditions which are based on a user's identity. The condition is satisfied if any of the <one> or <many> elements within it is matched. The <identity> condition must contain at least one sub-element to be valid. If an update would result in no contained sub-elements then the <identity> condition should be deleted instead by deleting the element which contains it.
	<one>	The <one> element specifies an individual identity to be matched. The <one> element is a sub-MO allowing multiple instances with “id” as the unique key.
	<id>	The individual identity to be matched. For all uses except incoming communication barring user rules, this takes the form of a si: or tel URI. For use within incoming communication barring user rules, this takes the form of a sip or tel or hidden URI. Each tel URI and sip URI that was converted from a tel URI according to section 19.1.6 of RFC 3261 [6] contains a normalized number. This must be present on the creation of a <one> element.



XML element			Description
	<many>		The <many> element specifies a match for a set of identities. The <many> element is a sub-MO allowing multiple instances with “domain” as the unique key.
		<domain>	The individual domain to be matched. A <many> element with an explicit domain value matches all identities within that domain. A <many> element with the special wildcard value “*” matches all identities. It must be present on the creation of a <many> element.
	<except-id>		An individual identity to be excluded from the identities matching the enclosing <many>. The <except-id> element is a sub-MO allowing multiple instances with “id” as the unique key.
		<id>	The individual identity to be excluded from the match. If this is within a <many> element with a specific domain then the excluded identity must be a sip: URI within that domain. If this is within a <many> element with the special wildcard value of “*”, then it can be a sip or tel URI. Each tel URI and sip URI that was converted from a tel URI according to section 19.1.6 of RFC 3261 [6] contains a normalized number. It must be present on the creation of an <except-id> element.
	<except-domain>		An individual domain to be excluded from a <many> with special value “*” that would otherwise match all identities. The <except-domain> element is a sub-MO allowing multiple instances with “domain” as the unique key.
		<domain>	The individual domain to be excluded from the match. It must be present on the creation of an <except-domain> element.
	<number-match>		The number-match element specifies a match for a set of numerical identities. The number-match element is a sub-MO allowing multiple instances with “starts-with” as the unique key.
		<starts-with>	The first few characters of the normalized form of the number to be matched. It must be present on the creation of a number-match element.

5.2.22 Create SIP Trunking Referral

Table 37: Information in a Create SIP Trunking Referral

XML element		Description
<createStReferral>		Used to create SIP Trunking referral service data.
	<publicId>	The public service identity for service document. This identity must already be configured on the HSS.
	<refer-to-identity>	The <refer-to-identity> element contains public identity of the associated service document. It must be present and may never be withdrawn so it is not nillable.



5.2.23 Set SIP Trunking Referral

Table 38: Information in a Set SIP Trunking Referral

XML element	Description
<setStReferral>	Used to modify SIP Trunking referral service data.
<concurrency-control>	The <concurrency-control> element is an optional element to control concurrent updates. If present then the set request will be accepted only if the service data version is still at the value given in this element i.e. no other updates have been performed. It is of type integer.
<refer-to-identity>	The <refer-to-identity> element contains public identity of the associated service document. It must be present and may never be withdrawn so it is not nillable.

5.2.24 Get SIP Trunking Referral

Table 39: Information in a Get SIP Trunking Referral

XML element	Description
<getResponseStReferral>	Contains the currently configured SIP Trunking referral service data.
<publicId>	The public service identity for service document. This identity must already be configured on the HSS.
<concurrency-control>	The <concurrency-control> element is an integer value indicating the current version of the SIP Trunking Referral service data. This value can be used in a subsequent <setStReferral> request to make sure that no changes have been made to the service data since the version that was read
<refer-to-identity>	The <refer-to-identity> element contains public identity of the associated service document. It must be present and may never be withdrawn so it is not nillable.

5.3 Schemas

The CAI3G interface needs schema files that are defined in ref [5], which are accessed through a relative pathname, therefore in order for the zipped schemas in ref [4] to work out-of-the-box, the directory structure as shown must be used.

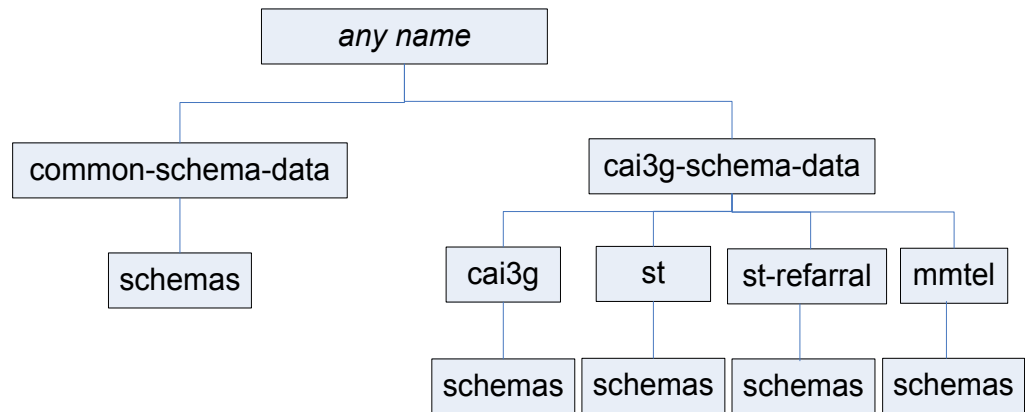


Figure 3

Directory Structure for the ST AS CAI3G Schema Files

6 Related Standards

-

7 Terminology

-

7.1 Abbreviations

ST AS SIP Trunking Application Server

7.2 Definitions

-

8 References

- [1] 2/155 19-FAY3020003 Uen G, Generic CAI3G Interface 1.2
- [2] 22/155 19-AVA 901 18 Uen, CAI3G Interworking Description
- [3] TSP: 1/190 84-AVA 901 09/n ** MTAS, Parameter Description
CBA: 155 54-LZN 765 0163/n ** Managed Object Model MTAS
- [4] 1/190 09-AVA 901 18 Uen, MTAS CAI3G Schemas



- [5] 4/190 09-AVA 901 18 Uen, MTAS Common Types Schemas
- [6] RFC 3261, SIP: Session Initiation Protocol
- [7] *HTTP 1.1*, <http://www.w3.org/Protocols/rfc2616/rfc2616.html>

** See the Customer or Support library for the Application System in question