

Wi-Fi Calling Provisioning over CAI3G

Ericsson Dynamic Activation 1

INTERFACE DESCRIPTION

Copyright

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

Disclaimer

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

Trademark List

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



Contents

1	Introduction	1
1.1	Purpose and Scope	1
1.2	Target Groups	1
1.3	Typographic Conventions	1
1.4	Prerequisites	1
1.5	Web Service Interface	1
1.6	MOType	2
1.7	MOld	2
2	Voice over Wi-Fi Subscription	3
2.1	Create VoWifiService	3
2.1.1	Request Data	3
2.1.2	Response Data	4
2.1.3	Example	4
2.2	Set VoWifiService	5
2.2.1	Request Data	5
2.2.2	Example	7
2.3	Delete VoWifiService	8
2.3.1	Request Data	8
2.3.2	Example	9
3	NonSIM HSS User Subscription	11
3.1	Create NonSIMHSSUser	11
3.1.1	Request Data	11
3.1.2	Example	12
3.2	Set NonSIMHSSUser	12
3.2.1	Request Data	12
3.2.2	Example	13
3.3	Delete NonSIMHSSUser	14
3.3.1	Request Data	14
3.3.2	Example	14
4	HSS ISM Subscription	16
4.1	Create IMPI	16
4.1.1	Request Data	16
4.1.2	Example	17
4.2	Delete IMPI	18
4.2.1	Request Data	18
4.2.2	Example	20



4.3	Set IMPI	20
4.3.1	Request Data	20
4.3.2	Example	22
4.4	Get IMPI	22
4.4.1	Request Data	22
4.4.2	Response Data	23
4.4.3	Example	23
5	IPWorks NonSiM AAA User Subscription	25
5.1	Create AAANSUser	25
5.1.1	Request Data	25
5.1.2	Example	26
5.2	Set AAANSUser	27
5.2.1	Request Data	27
5.2.2	Example	29
5.3	Delete AAANSUser	33
5.3.1	Request Data	33
5.3.2	Example	34
5.4	Get AAANSUser	34
5.4.1	Request Data	34
5.4.2	Response Data	34
5.4.3	Example	35
6	Ercisson Certificate Authority Server Subscription	37
6.1	Create ECASCertificate	37
6.1.1	Request Data	37
6.1.2	Response Data	38
6.1.3	Example	38
6.2	Set ECASCertificate	40
6.2.1	Request Data	40
6.2.2	Response Data	40
6.2.3	Example	41
6.3	Delete ECASCertificate	42
6.3.1	Request Data	42
6.3.2	Example	43
6.4	Get ECASCertificate	43
6.4.1	Request Data	44
6.4.2	Response Data	44
6.4.3	Example	45
7	Error Codes	47
	Reference List	50



1 Introduction

This section contains information about the prerequisites, purpose, scope, and target group for the document. This section also contains information about typographic conventions used in this document.

1.1 Purpose and Scope

This document covers descriptions of installation, interface and configuration of Ericsson™ Dynamic Activation (EDA).

In the Secure Entitlement Server (SES) solution, Dynamic Activation is responsible for user and service profile provisioning towards the monolithic nodes, for example IPWorks.

Note: This document is not a tutorial of CAI3G, it must be used together with document *Generic CAI3G Interface 1.2*, Reference [2].

1.2 Target Groups

The target group for this document is as follows:

- System Integrator

For more information about the different target groups, see *Library Overview*, Reference [1].

1.3 Typographic Conventions

Typographic conventions are described in the document *Library Overview*, Reference [1].

1.4 Prerequisites

This document is written with the assumption that the users:

- Have basic knowledge about the Dynamic Activation product.
- Have knowledge about *Generic CAI3G Interface 1.2*, Reference [2].

1.5 Web Service Interface

The Web Services Definition Language (WSDL) and XML Schema Definition Language (XSD) files that describe the provisioning interface can be found in



/home/dveinstaller/ma/. It is also possible to download the files and view or store them in an appropriate area by following below instruction:

1. Save the zip file, [Dynamic_Activation_WSDL_and_XSD_files.zip](#), to a local folder.
2. Unpack the zip file.

1.6 MOType

MOType is a plain text string based on the type `xs:string`. An MOType consists of two parts. One is the namespace of the MO, and the other is the MO name string that is always starting with an alphabetical character in either upper or lower case, followed by zero or more alphabetical characters, digits or underscores.

Those two parts are connected with symbol @. The syntax of the MOType string is `MO_Name@MO_Namespace`. The name string of an MOType must follow the regular expression: `[A-Za-z][A-Za-z0-9]*`

The MO name together with the MO namespace must be globally unique.

1.7 MOId

MOId is an XML fragment containing the MOId parameter-value pairs that are used to identify an MO instance in the interface data model. CAI3G 1.2 standard supports compound MO identifiers or multiple MO identifier. The following is an example of an MOId:

```
<MOId>
  <msisdn>46455395000</msisdn>
  <imsi>46234563545000</imsi>
</MOId>
```

Example 1 Example of MOId

The MOId is defined as a sequence of `xs:any` element in CAI3G schema file. It is the developers responsibility to define the real schema for this parameter.

The MOId is also the key attributes that must be defined in the top-level element, `CreateMODefinition` or `SetMODefinition`, within `MOAttributes` parameter.

Each implementation of CAI3G interface is to define own logic relationship of MOId. It is also the CAI3GAgents responsibility to interpret this parameter correctly by either the hard-coded logic or the dynamic parsing of the schema.



2 Voice over Wi-Fi Subscription

2.1 Create VoWifiService

This section describes how to create VoWifiService.

MOType

VoWifiService@http://schemas.ericsson.com/ma/nonSIM/

2.1.1 Request Data

MOId

Table 1 MOID Parameters of Creating VoWifiService

Parameter	Type	Occurrence	Description
transactionLogId	String Max length = 64	Optional	The transaction ID
vImsi	String Min length = 6 Max length = 16	Mandatory	The virtual IMSI number

MOAttributes

Table 2 MOAttributes of Creating a VoWifiService

Parameter	Type	Occurrence	Description
vImsi	String Min length = 6 Max length = 16	Mandatory	The virtual IMSI number
deviceRealm	String Max length = 128	Mandatory	The Non-SIM device realm
imsi	String Min length = 6 Max length = 16	Mandatory	The SIM device IMSI that is associated with the Non-SIM device
msisdn	String Min length = 5 Max length = 16	Mandatory	The SIM device MSISDN that is associated with the Non-SIM device
impi	String Max length = 256	Mandatory	The private user identity in HSS of the Non-SIM device



Parameter	Type	Occurrence	Description
apn	String	Mandatory	The Access Point Name of the Non-SIM device Format: FQDN
password	String Min length = 15 Max length = 256	Mandatory	The HSS private user password of Non-SIM device Format: Plain text, US-ASCII character set is accepted, except control characters (0-31) and DEL character (127). Linear White Space (LWS) is also accepted.
userStatus	One of the following strings: enable, disable, reset	Optional	The non-SIM device user status. It can be enabled, disabled and reset: <ul style="list-style-type: none">• enable: the user can use the non-SIM service.• disable: the user is blocked for the non-SIM service.• reset: it means to tear down the TLS tunnel.
csr	String	Mandatory	The required certificate sign request for the Non-SIM certificate.

2.1.2

Response Data

MOAttributes

Table 3 MOAttributes of Creating a VoWifiService Response

Parameter	Type	Occurrence	Description
certificate	String	Mandatory	The signed certificate for non-SIM device
certId	String Max length = 64	Mandatory	The signed certificate identity
certExpireTime	dateTime	Mandatory	The signed certificate expiration time

2.1.3

Example

An example for creating VoWifiService is shown as follows.



```

Request:
<cai3:Create>
  <cai3:MOTType>VoWifiService@http://schemas.ericsson.com/ma/nonSIM/
</cai3:MOTType>
  <cai3:MOId>
    <non:vImsi>123456</non:vImsi>
  </cai3:MOId>
  <cai3:MOAttributes>
    <non:CreateVoWifiService xmlns:non="http://schemas.ericsson.com/ma/nonSIM/"
      vImsi="123456">
        <non:vImsi>123456</non:vImsi>
        <non:deviceRealm>ericsson</non:deviceRealm>
        <non:imsi>12345678</non:imsi>
        <non:msisdn>13812345678</non:msisdn>
        <non:impi>impiuser_ewahong</non:impi>
        <non:apn>apn</non:apn>
        <non:password>passwordpassword</non:password>
        <non:userStatus>enable</non:userStatus>
        <non:csr>MIICtTCCAzoCADBxMQswCQYDVQQGEWJjbjEwMBQGA1UEAxMNbWljagVsbGUud2Fu
ZzERMA8GA1UEBxMIC2hhbmdoYWkxETAPBgNVBAoTCGVyaWNzc29uMREwDwYDVQQI
EwhzaGFuZ2hhaTERMA8GA1UECxMIY2JjL3hsZWcwggEiMA0GCSqGSIb3DQEBBQUA
A4IBDwAwggEKAoIBAQC7WXv4WOB6CfGzXwwCDnh7T8JNG34vBNycSKdl3yq2WuCW
5ftyV9/SPRjpsSiUDVIHqEkmhT3yBBsH5JRulfQhkEvw14E8zr7EUFa4JFH03Xtd8
nqh2JFEjayHpa/NWol6NeSS8GrRShZWbiIII+wLw1HRoDjHMFfjDFQwKgnfyNwmZ
avlhkzCoBvIYgYD/lnFZiyaAuAuIBLLVe768qyaP0TUYq0OeJqiKS5B/pVcF1ZIH
GslT8deWTigxLj6ulYAzQoZNbqlgA0xVW+cR7YgbmOoQjFQoS1EZbPs/QAD0d7vX
ZOJoDgtFmKqKRmpYtT2gHeD2qt8v+61mUuQN40NTAgMBAAGgADANBgkqhkiG9w0B
AQQFAAOCAQEAsHczPihsi9PG9IZDYIidUYUadMcKyyAY2AagsupIruVfWARV7cd
rg069vUAh8bZ/goQFW9YTRBckuzxF927pHkyTLQLGc0Z2xGKYd6pAcri8MMNfjQ2
MYvW4sxhBVJv/FTkrW8Iv19X431m0ctND7J/n3dnjRMwYTcf72ZsH9gAYEvMqsvK
3JlMj8JKByx/atsHxxTM59xKYVpnLPprEviZlxzvolAHI+RLu6dQxKK/AOlrvBFY
3Vjxh7D/RAahVMF9eLJ3cMKoEmKmKvkUoGLUgwC+ZhADx2Osm3TOTIFDZKGGgVs7
94jDIFsJP0587t8vLXLtiFe6JcbSOvjLhQ==</non:csr>
    </non:CreateVoWifiService>
  </cai3:MOAttributes>
</cai3:Create>

Response:
<cai3:CreateResponse>
  <cai3:MOId>
    <non:vImsi>?</non:vImsi>
  </cai3:MOId>
  <cai3:MOAttributes>
    <non:CreateResponseVoWifiService>
      <non:certificate>?</non:certificate>
      <non:certId>?</non:certId>
      <non:certExpireTime>?</non:certExpireTime>
    </non:CreateResponseVoWifiService>
  </cai3:MOAttributes>
</cai3:CreateResponse>

```

Example 2 Create VoWifiService

2.2 Set VoWifiService

This section describes how to set VoWifiService.

MOType

VoWifiService@http://schemas.ericsson.com/ma/nonSIM/

2.2.1 Request Data

MOId

**Table 4** *MOID Parameters of Setting VoWifiService*

Parameter	Type	Occurrence	Description
transactionLogId	String Max length = 64	Optional	The transaction ID
vImsi	String Min length = 6 Max length = 16	Mandatory	The virtual IMSI number

MOAttributes**Table 5** *MOAttributes of Setting a VoWifiService*

Parameter	Type	Occurrence	Description
vImsi	String Min length = 6 Max length = 16	Mandatory	The virtual IMSI number
deviceRealm	String Max length = 128	Mandatory	The Non-SIM device realm
imsi	String Min length = 6 Max length = 16	Optional	The SIM device IMSI that is associated with the Non-SIM device
msisdn	String Min length = 5 Max length = 16	Optional	The SIM device MSISDN that is associated with the Non-SIM device
impi	String Max length = 256	Optional	The private user identity in HSS of the Non-SIM device
apn	String	Optional	The Access Point Name of the Non-SIM device Format: FQDN
password	String Min length = 15 Max length = 256	Optional	The HSS private user password of Non-SIM device Format: Plain text, US-ASCII character set is accepted, except control characters (0-31) and DEL character (127). Linear White Space (LWS) is also accepted.



Parameter	Type	Occurrence	Description
userStatus	One of the following strings: enable, disable, reset	Optional	The non-SIM device user status. It can be enabled, disabled and reset: <ul style="list-style-type: none"> • enable: the user can use the non-SIM service. • disable: the user is blocked for the non-SIM service. • reset: it means to tear down the TLS tunnel.
csr	String	Optional	The required certificate sign request for the Non-SIM certificate.
certId	String Max length = 64	Optional	The signed certificate identity

2.2.2

Example

An example for setting VoWifiService is shown as follows.

```
Request:
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:cai3="http://schemas.ericsson.com/cai3gl.2/" xmlns:non="http://schemas.ericsson.com/ma/nonSIM/">
  <soapenv:Header>
    <cai3:SessionId>a9dd468448dd4d389f6367ac04993930</cai3:SessionId>
  </soapenv:Header>
  <soapenv:Body>
    <cai3:Set>
      <cai3:MOTType>VoWifiService@http://schemas.ericsson.com/ma/nonSIM/
      </cai3:MOTType>
      <cai3:MOId>
        <!--Optional:-->
        <non:transactionLogId>transactionid9999#SetVoWifiService
        </non:transactionLogId>
        <non:vImsi>112233</non:vImsi>
      </cai3:MOId>
      <cai3:MOAttributes>
        <non:SetVoWifiService vImsi="112233">
          <non:deviceRealm>ericsson</non:deviceRealm>
          <!--Optional:-->
          <non:csr>-----BEGIN CERTIFICATE REQUEST-----
MIICqzCCAZMCADBnMQswCQYDVQQGEWJjbjEVMBMGA1UEAxMMbW1jaGVsbGUuY29t
MREwDwYDVQQHEWhzaGFuZ2hhaTEMMAoGA1UEChMDY2JjMREwDwYDVQQIEWhzaGFu
Z2hhaTENMASGA1UECXMEEGxlZzCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBANMPKqyLgIZ4S2MMrJjCM2u0U+J8AhpCmV5Dc7x0wL3Z5Rn2KR59YeTt8t6
7SZt14g0I5lfEKAsS77ED4NT+eXGA3HoJ5Mvk+QX0KmsB7h5Ah9/bwYNbM21EBCG
5fjtfDn3W+XCEL9cp21l16LloclIoCjIuKNWBwu7+bmGGQuaXJQqPw4s2sbuHhO
hpGDalY/CiWxEbNw3XIIAHoc3xjHmoQjeTkbmiD++hcbkOu9jTNlAq9WMj5Y9JGK
FpL07PxtAlFxmGY7fbOwXDIge6zurldqpZ5G0l/pjOpeZhW07Ien6UP+v9b/qnTC
a5gE7dw3THCbYVLNJqWAP5ssnMsCAwEAAaAAMA0GCSqGSIb3DQEBBAAUAA4IBAQBp
h4qYL8tftlVnyyW2hliP+B0P1lQOjSEn/0r0C9o49IAFzWTs2s70GydCXkKt4IYq
txvTGAhvUWVQKRe71xSRrvUoMIPglD9tTbtCAhuTm1lQKd8qhgeCebYau9PPQb20
VWV5RYglr8zji5010App5v4hQPstEGlMky/vLUZjwze/aCkl3bmfgZoxOpyVh9QM
QV9q8Sexb8ToI6fOep6T+eQsargXcXPISS2RRtpIhanmDwlhWr7TtVynY99q2/FW
iMWjAsUx/y3NjM0JxLcX700J9Rk2V1qAMDWCvLeFx0RrUs1Cvjnzqiik4TESNli3
v8MoYNDU+2R+H8tlgdX5
-----END CERTIFICATE REQUEST-----</non:csr>
          <!--Optional:-->
          <non:certId>2007d7a7804a918</non:certId>
        </non:SetVoWifiService>
      </non:MOAttributes>
    </cai3:Set>
  </soapenv:Body>
</soapenv:Envelope>
```



```

        </cai3:MOAttributes>
      </cai3:Set>
    </soapenv:Body>
  </soapenv:Envelope>

Response

<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:cai3g="http://schemas.ericsson.com/cai3g1.2/">
  <S:Header>
    <cai3g:SessionId>a9dd468448dd4d389f6367ac04993930</cai3g:SessionId>
  </S:Header>
  <S:Body>
    <ns2:SetResponse xmlns:ns2="http://schemas.ericsson.com/cai3g1.2/">
      <ns2:MOAttributes>
        <nonsim:SetResponseVoWifiService xmlns:nonsim="http://
          schemas.ericsson.com/ma/nonSIM/">
          <nonsim:certificate>LS0tLS1CRUdJTiBDRVJUSUZJQ0FUR
S0tLS0tCk1JSURkakNDQWw2Z0F3SUJBZ01JREV4TWVzdHVhMHd3RFFZSktvWk1odm
NOQVFFFRkJRQXd0ekVSTUE4R0ExVUUKQXd3SVFXUnRhVzVEUVRFeEZUQVRVRC05WQkFv
TURFVktRa05CSUZ0aGJYQnNaEVMTUFR0ExVUVCaE1DVTBVdWpIaGNOTVRRd09EQT
JNRFV6TnpVMFdoY05NVF13T0RBMU1EVXp0e1UwV2pBK01SZ3dGZ11EVlFRFRERBOHhN
VEl5Ck16TkFaWEpWWTNOemIyNHhGVFUFQmdOVkJBb01ERVZLUWtOQklGTmhiWEJzWlR
FTE1Ba0dBmVVFQmhNQ1UwVXcKZ2dFaU1BMEdDU3FHU01iM0RRRUJBUVVBQTRJQkR3QX
dnZ0VLQW9JQkFRFRREeXFzaTRDR2VfGpES31Zd2p0CgpnOUZQaWZBQjZRCGxlUTNPOG
RNQzkyZVVAOWlrZWZXSgs3ZkxldTBtYmRlSU5DT1pYeENnTEV1K3hBK0RVL25sCnhnTng
2Q2VUTDVQa0Y5Q3ByQUW0ZVFJZmYyOEdEV3pOdFJBWWh1WDQ3WHc1OTF2bHdoQy9YS2Rw
WmRlaTVhSEoKU0tBb31MalNqVmJdTHUvbTVoaGtMbWx5VUtqOE9MTnJHN2g0VG9hUmcydFJ
Qd29sc1JHemNOMX1DQUI2SE44WQp4NXFFSTNnNUc1b2cvdm9YRzVEcnZZMHPaUUt2VmpJK1
dQU1JpaGFTOU96MTdRSlJjVEJtTzMyenNGd3lJSHVzCjdxNVhhcVdlUmpwZjZzenFYbVl
WanV5SHArbEQvci9XLzZwMHdtVlCTZnJtB4d20yRlN6U2FsZ0QrYkxKekwKQWdNQkFB
R2pmekI5TUIwR0ExVWREZ1FXQkJRNU9oUXBvY2l2ZTJ6V3A1N3JPdDNrK0poTGFqQU1CZ
05WSFJNQgpBZjhFQWpBQU1COEdBMVVKsXdrWU1CYUFGQkEyZHp6WxNETExJczdIVzNIZE
gvc1VqZnk2TUE0R0ExVWREd0VCCi93UUVBd01GNERBZEJnTlZlU1VFRmpBVUJnZ3JCZ0V
GQlFjREFnWU1Ld11CQlFVSEF3UXdEUUV1KS29aSW2Y04KQVFFFRkJRQUrnZ0VCQ1GvN
MSWdXSUdxbzVCOVJUV0hYzKRXYZN1V3VBdHo5QUZHV1YzWW1aazZKRGkyZ0hnZworVW
tncE91RjNnUXg1Nm85NVFmTmc3aGs1ZFlXRmNKAitwbUhzeKhHMDVoaFRxeU1taJj5Q
U1kN01xWWV3M1I1Cko0TmJRazRqSjdsawZTalpsOVlPdnpmV3FQMLZEbEtjc2d3WWI3
axJsa3ZTYWx3M3A0aEkzQ1pNTEFSMG5kM0cKNE5ODFJTFl6TEhoYzVCOTVLTjh0cEd
SdlA4NmE5eXFNZk13MEpqV0ZvZERjRj12Z2VYbTBKS0V6N21iQnorVQpKaVfoYk5yM
S9icG5JajRsZUxMWkIvWU5sOxk5WE5GVjJuRHJxN2Z6dXBdWj1wTj1lCVjFGd3BmN1t
naFpyNkp2ClB1MjFkakVLV1B1RWg3SE5qY2ZGbw5uQk1XcC9FRTJMeTR3PQotLS0t
LUVORCBDRVJUSUZJQ0FURS0tLS0t</nonsim:certificate>
          <nonsim:certId>c4c4c7acb6e6b4c</nonsim:certId>
          <nonsim:certExpireTime>2016-08-05T05:37:54+00:00
          </nonsim:certExpireTime>
        </nonsim:SetResponseVoWifiService>
      </ns2:MOAttributes>
    </ns2:SetResponse>
  </S:Body>
</S:Envelope>

```

Example 3 Set VoWifiService

2.3 Delete VoWifiService

This section describes how to delete VoWifiService.

MOType

VoWifiService@http://schemas.ericsson.com/ma/nonSIM/

2.3.1 Request Data

MOld



Table 6 *MOID Parameters of Setting VoWifiService*

Parameter	Type	Occurrence	Description
transactionLogId	String Max length = 64	Optional	The transaction ID
vImsi	String Min length = 6 Max length = 16	Mandatory	The virtual IMSI number

MOAttributes

Table 7 *MOAttributes of Setting a VoWifiService*

Parameter	Type	Occurrence	Description
vImsi	String Min length = 6 Max length = 16	Mandatory	The virtual IMSI number
deviceRealm	String Max length = 128	Mandatory	The Non-SIM device realm
imsi	String Min length = 6 Max length = 16	Optional	The SIM device IMSI that is associated with the Non-SIM device
msisdn	String Min length = 5 Max length = 16	Optional	The SIM device MSISDN that is associated with the Non-SIM device
impi	String Max length = 256	Optional	The private user identity in HSS of the Non-SIM device
certId	String Max length = 64	Optional	The signed certificate identity

2.3.2

Example

An example for deleting VoWifiService is shown as follows.

Note: The parameter `certId` in the following example is an optional parameter in the delete request. When a valid `certId` is defined in the delete request, PG NGN revokes the specified certification of the user. Otherwise PG NGN revokes all certifications of the user.



Request:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:cai3="http://schemas.ericsson.com/cai3g1.2/" xmlns:non="http://schemas.ericsson.com/ma/nonSIM/">
  <soapenv:Header>
    <cai3:SessionId>a9dd468448dd4d389f6367ac04993930</cai3:SessionId>
  </soapenv:Header>
  <soapenv:Body>
    <cai3:Delete>
      <cai3:MOType>VoWifiService@http://schemas.ericsson.com/ma/nonSIM/
    </cai3:MOType>
    <cai3:MOId>
      <!--Optional:-->
      <non:transactionLogId>transactionid9999#DeleteVoWifiService
    </non:transactionLogId>
      <non:vImsi>112233</non:vImsi>
    </cai3:MOId>
      <!--Optional:-->
    <cai3:MOAttributes>
      <non:DeleteVoWifiService vImsi="112233">
        <non:deviceRealm>ericsson</non:deviceRealm>
        <!--Optional:-->
        <non:imsi>123456</non:imsi>
        <!--Optional:-->
        <non:msisdn>54321</non:msisdn>
        <!--Optional:-->
        <non:impi>impi_ewahong_123@ericsson.com</non:impi>
        <!--Optional:-->
        <non:certId>c4c4c7acb6e6b4c</non:certId>
      </non:DeleteVoWifiService>
    </cai3:MOAttributes>
  </cai3:Delete>
</soapenv:Body>
</soapenv:Envelope>
```

Response:

```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:cai3g="http://schemas.ericsson.com/cai3g1.2/">
  <S:Header>
    <cai3g:SessionId>a9dd468448dd4d389f6367ac04993930</cai3g:SessionId>
  </S:Header>
  <S:Body>
    <ns2:DeleteResponse xmlns:ns2="http://schemas.ericsson.com/cai3g1.2/">
      <ns2:MOId>
        <non:transactionLogId xmlns:non="http://schemas.ericsson.com/ma/nonSIM/">transactionid9999#DeleteVoWifiService</non:transactionLogId>
        <non:vImsi xmlns:non="http://schemas.ericsson.com/ma/nonSIM/">112233</non:vImsi>
      </ns2:MOId>
    </ns2:DeleteResponse>
  </S:Body>
</S:Envelope>
```

Example 4 Delete VoWifiService



3 NonSIM HSS User Subscription

This section is only for the customized HSS user data mode with xB2BUA deployment scenario. PG NGN will update the Non-SIM HSS user password. After that, HSS subscription is not needed in the next phase Non-SIM device on-boarding, as described in Section 2.1 on page 3.

3.1 Create NonSIMHSSUser

This section describes how to create NonSIMHSSUser.

MOType

NonSIMHSSUser@http://schemas.ericsson.com/ma/nonSIM/

3.1.1 Request Data

MOId

Table 8 MOID Parameters of Creating NonSIMHSSUser

Parameter	Type	Occurrence	Description
transactionLogId	String Max length = 64	Optional	The transaction ID
impi	String Max length = 256	Mandatory	The non-SIM device private user identity in HSS

MOAttributes

Table 9 MOAttributes of Creating a NonSIMHSSUser

Parameter	Type	Occurrence	Description
impi	String Max length = 256	Mandatory	The non-SIM device private user identity in HSS
imsi	String Min length = 6 Max length = 16	Mandatory	The SIM device IMSI that is associated with the Non-SIM device



Parameter	Type	Occurrence	Description
msisdn	String Min length = 5 Max length = 16	Mandatory	The SIM device MSISDN that is associated with the Non-SIM device
password	String Min length = 15 Max length = 256	Mandatory	The password of Non-SIM device user and HSS private user

3.1.2 Example

An example for creating NonSIMHSSUser is shown as follows.

```
Request:
<cai3:Create>
  <cai3:MOType>NonSIMHSSUser@http://schemas.ericsson.com/ma/nonSIM/</cai3:MOType>
  <cai3:MOId>
    <non:impi>impi_nonsim_hssuser_123@ericsson.com</non:impi>
  </cai3:MOId>
  <cai3:MOAttributes>
    <non:CreateNonSIMHSSUser impi="impi_nonsim_hssuser_123@ericsson.com">
      <non:impi>impi_nonsim_hssuser_123@ericsson.com</non:impi>
      <non:imsi>123456</non:imsi>
      <non:msisdn>8613512341234123</non:msisdn>
      <non:password>passwordpasswordpass</non:password>
    </non:CreateNonSIMHSSUser>
  </cai3:MOAttributes>
</cai3:Create>
```

```
Response:
<ns2:CreateResponse xmlns:ns2="http://schemas.ericsson.com/cai3g1.2/">
  <ns2:MOId>
    <non:impi xmlns:non="http://schemas.ericsson.com/ma/nonSIM/">impi_nonsim_hssuser_123@
    ericsson.com</non:impi>
  </ns2:MOId>
</ns2:CreateResponse>
```

Example 5 Create NonSIMHSSUser

3.2 Set NonSIMHSSUser

This section describes how to set NonSIMHSSUser.

MOType

NonSIMHSSUser@http://schemas.ericsson.com/ma/nonSIM/

3.2.1 Request Data

MOLD



Table 10 *MOID Parameters of Setting NonSIMHSSUser*

Parameter	Type	Occurrence	Description
transactionLogId	String Max length = 64	Optional	The transaction ID
impi	String Max length = 256	Mandatory	The non-SIM device private user identity in HSS

MOAttributes

Table 11 *MOAttributes of Setting a NonSIMHSSUser*

Parameter	Type	Occurrence	Description
imsi	String Min length = 6 Max length = 16	Mandatory	The SIM device IMSI that is associated with the Non-SIM device
msisdn	String Min length = 5 Max length = 16	Mandatory	The SIM device MSISDN that is associated with the Non-SIM device
password	String Min length = 15 Max length = 256	Mandatory	The password of Non-SIM device user and HSS private user
impi	String Max length = 256	Mandatory	The non-SIM device private user identity in HSS

3.2.2

Example

An example for setting NonSIMHSSUser is shown as follows.

```
Request:
<cai3:Set>
  <cai3:MOType>NonSIMHSSUser@http://schemas.ericsson.com/ma/nonSIM/</cai3:MOType>
  <cai3:MOId>
    <non:impi>123456@ericsson</non:impi>
  </cai3:MOId>
  <cai3:MOAttributes>
    <non:SetNonSIMHSSUser xmlns:non="http://schemas.ericsson.com/ma/nonSIM/"
      impi="123456@ericsson">
      <non:imsi>12345678</non:imsi>
      <non:msisdn>13812345678</non:msisdn>
      <non:password>passwordpasswordpassword</non:password>
    </non:SetNonSIMHSSUser>
  </cai3:MOAttributes>
</cai3:Set>

Response:
<ns2:SetResponse xmlns:ns2="http://schemas.ericsson.com/cai3g1.2/">
```

Example 6 Set NonSIMHSSUser



3.3 Delete NonSIMHSSUser

This section describes how to delete NonSIMHSSUser.

MOType

NonSIMHSSUser@http://schemas.ericsson.com/ma/nonSIM/

3.3.1 Request Data

MOId

Table 12 MOID Parameters of Deleting NonSIMHSSUser

Parameter	Type	Occurrence	Description
transactionLogId	String Max length = 64	Optional	The transaction ID
impi	String Max length = 256	Mandatory	The non-SIM device private user identity in HSS

MOAttributes

Table 13 MOAttributes of Deleting a NonSIMHSSUser

Parameter	Type	Occurrence	Description
imsi	String Min length = 6 Max length = 16	Mandatory	The SIM device IMSI that is associated with the Non-SIM device
msisdn	String Min length = 5 Max length = 16	Mandatory	The SIM device MSISDN that is associated with the Non-SIM device
impi	String Max length = 256	Mandatory	The non-SIM device private user identity in HSS

3.3.2 Example

An example for deleting NonSIMHSSUser is shown as follows.



```
<cai3:Delete>
  <cai3:MOType>NonSIMHSSUser@http://schemas.ericsson.com/ma/nonSIM/</cai3:MOType>
  <cai3:MOId>
    <non:impi>impi_nonsim_hssuser_123@ericsson.com</non:impi>
  </cai3:MOId>
  <cai3:MOAttributes>
    <non:DeleteNonSIMHSSUser impi="impi_nonsim_hssuser_123@ericsson.com">
      <non:imsi>123456</non:imsi>
      <non:msisdn>8613512341234123</non:msisdn>
    </non:DeleteNonSIMHSSUser>
  </cai3:MOAttributes>
</cai3:Delete>
```

Response:

```
<ns2:DeleteResponse xmlns:ns2="http://schemas.ericsson.com/cai3g1.2/">
  <ns2:MOId>
    <non:impi xmlns:non="http://schemas.ericsson.com/ma/nonSIM/">impi_nonsim_hssuser_123@
      ericsson.com</non:impi>
    </ns2:MOId>
  </ns2:DeleteResponse>
```

Example 7 Delete NonSIMHSSUser



4 HSS ISM Subscription

HSS open interface is for IMS private user (IMPI) data provisioning in monolithic HSS. This interface supports the Set and Get operations. Create, Delete, and Set IMPI data are accomplished by using the Set operation.

4.1 Create IMPI

This section describes how to create IMPI.

MOType

ISMSubscription@http://schemas.ericsson.com/ema/UserProvisioning/HSS/ISM/

4.1.1 Request Data

MOId

Table 14 MOID Parameters of Creating IMPI

Parameter	Type	Occurrence	Description
subscriberId	String Max length = 255	Mandatory	The SIM subscriber identity For example: <imsi>@domain or <msisdn>@domain Domain shall derive from IMPI and do pre-configuration in Dynamic Activation

MOAttributes

Table 15 MOAttributes of Creating IMPI

Parameter	Type	Occurrence	Description
subscriberId	String Max length = 255	Mandatory	The SIM subscriber identity For example: <imsi>@domain or <msisdn>@domain Domain shall derive from IMPI and do pre-configuration in Dynamic Activation
privateUser			



Parameter	Type	Occurrence	Description
privateUserId	String Min length = 1 Max length = 256	Mandatory	The HSS private user identity
userPassword	String Min length = 4 Max length = 256	Optional	Contains the private user password to be used in the SIP Digest authentication.
userPrimaryHAlPassword	String Pattern value= "[0-9A-F]{1,64}"	Optional	Contains the A1 hashed value to be used in SIP Digest authentication. If the value of UserPasswordEncryption in JDV configuration is YES, the value of userPassword is encrypted and stored in userPrimaryHAlPassword.
userSecondaryHAlPassword	String Pattern value= "[0-9A-F]{1,64}"	Optional	Contains the A1 hashed value to be used in SIP Digest authentication.
allowedAuthMechanism	One of the following strings: <ul style="list-style-type: none">• Digest• SSO• NBA	Optional	The default user authorization mechanism
userBarringInd	One of the following strings: <ul style="list-style-type: none">• TRUE• FALSE	Optional	Indicates whether the HSS user is barred.
roamingAllowed	One of the following strings: <ul style="list-style-type: none">• TRUE• FALSE	Optional	Indicates whether the HSS user roaming is allowed.

4.1.2 Example

An example for creating IMPI is shown as follows.



Request:

```
<cai3:Set>
  <cai3:MOType>ISMSubscription@http://schemas.ericsson.com/ema
    /UserProvisioning/HSS/ISM/
  </cai3:MOType>
  <cai3:MOId>
    <subscriberId>123456_1002@ericsson.com</subscriberId>
  </cai3:MOId>
  <cai3:MOAttributes>
    <SetISMSubscription subscriberId="123456_1002@ericsson.com"
      xsi:schemaLocation=
        "http://schemas.ericsson.com/ema/UserProvisioning/HSS/ISM/
        ema_UserProvisioning_HSS_ISM.xsd"
      xmlns="http://schemas.ericsson.com/ema/UserProvisioning/HSS/ISM/"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <privateUser privateUserId="user001@ericsson.com">
        <privateUserId>user001@ericsson.com</privateUserId>
        <userPassword>password001</userPassword>
        <allowedAuthMechanism>Digest</allowedAuthMechanism>
        <userBarringInd>TRUE</userBarringInd>
        <roamingAllowed>TRUE</roamingAllowed>
      </privateUser>
    </SetISMSubscription>
  </cai3:MOAttributes>
</cai3:Set>
```

Response:

```
<ns2:SetResponse xmlns:ns2="http://schemas.ericsson.com/cai3g1.2/">
```

Example 8 Create IMPI

4.2 Delete IMPI

This section describes how to delete IMPI.

MOType

ISMSubscription@http://schemas.ericsson.com/ema/UserProvisioning/HSS/ISM/

4.2.1 Request Data

MOId

Table 16 MOID Parameters of Deleting IMPI

Parameter	Type	Occurrence	Description
subscriberId	String Max length = 255	Mandatory	The SIM subscriber identity For example: <imsi>@domain or <msisdn>@domain Domain shall derive from IMPI and do pre-configuration in Dynamic Activation

MOAttributes



Table 17 MOAttributes of Deleting IMPI

Parameter	Type	Occurrence	Description
subscriberId	String Max length = 255	Mandatory	The SIM subscriber identity For example: <imsi>@domain or <msisdn>@domain Domain shall derive from IMPI and do pre-configuration in Dynamic Activation
privateUser			
privateUserId	String Min length = 1 Max length = 256	Mandatory	The HSS private user identity
userPassword	String Min length = 4 Max length = 256	Optional	Contains the private user password to be used in the SIP Digest authentication.
userPrimaryHA1Password	String Pattern value= "[0-9A-F]{1,64}"	Optional	Contains the A1 hashed value to be used in SIP Digest authentication. If the value of UserPasswordEncryption in JDV configuration is YES, the value of userPassword is encrypted and stored in userPrimaryHA1Password.
userSecondaryHA1Password	String Pattern value= "[0-9A-F]{1,64}"	Optional	Contains the A1 hashed value to be used in SIP Digest authentication.
allowedAuthMechanism	One of the following strings: <ul style="list-style-type: none">• Digest• SSO• NBA	Optional	The default user authorization mechanism
userBarringInd	One of the following strings: <ul style="list-style-type: none">• TRUE• FALSE	Optional	Indicates whether the HSS user is barred.
roamingAllowed	One of the following strings: <ul style="list-style-type: none">• TRUE• FALSE	Optional	Indicates whether the HSS user roaming is allowed.



4.2.2 Example

An example for deleting IMPI is shown as follows.

```
Request:
<cai3:Set>
  <cai3:MOType>
    ISMSubscription@http://schemas.ericsson.com/ema/UserProvisioning/HSS/ISM/
  </cai3:MOType>
  <cai3:MOId>
    <subscriberId>123456_1002@ericsson.com</subscriberId>
  </cai3:MOId>
  <cai3:MOAttributes>
    <SetISMSubscription subscriberId="123456_1002@ericsson.com"
      xsi:schemaLocation=
        "http://schemas.ericsson.com/ema/UserProvisioning/HSS/ISM/
        ema_UserProvisioning_HSS_ISM.xsd"
      xmlns="http://schemas.ericsson.com/ema/UserProvisioning/HSS/ISM/"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <privateUser privateUserId="user001@ericsson.com" xsi:nil="true"/>
    </SetISMSubscription>
  </cai3:MOAttributes>
</cai3:Set>

Response:
<ns2:SetResponse xmlns:ns2="http://schemas.ericsson.com/cai3g1.2/">
```

Example 9 Delete IMPI

4.3 Set IMPI

This section describes how to set IMPI.

MOType

ISMSubscription@http://schemas.ericsson.com/ema/UserProvisioning/HSS/ISM/

4.3.1 Request Data

MOId

Table 18 MOID Parameters of Setting IMPI

Parameter	Type	Occurrence	Description
subscriberId	String Max length = 255	Mandatory	The SIM subscriber identity For example: <imsi>@domain or <msisdn>@domain Domain shall derive from IMPI and do pre-configuration in Dynamic Activation

MOAttributes



Table 19 MOAttributes of Setting IMPI

Parameter	Type	Occurrence	Description
subscriberId	String Max length = 255	Mandatory	The SIM subscriber identity For example: <imsi>@domain or <msisdn>@domain Domain shall derive from IMPI and do pre-configuration in Dynamic Activation
privateUser			
privateUserId	String Min length = 1 Max length = 256	Mandatory	The HSS private user identity
userPassword	String Min length = 4 Max length = 256	Optional	Contains the private user password to be used in the SIP Digest authentication.
userPrimaryHA1Password	String Pattern value= "[0-9A-F]{1,64}"	Optional	Contains the A1 hashed value to be used in SIP Digest authentication. If the value of UserPasswordEncryption in JDV configuration is YES, the value of userPassword is encrypted and stored in userPrimaryHA1Password.
userSecondaryHA1Password	String Pattern value= "[0-9A-F]{1,64}"	Optional	Contains the A1 hashed value to be used in SIP Digest authentication.
allowedAuthMechanism	One of the following strings: <ul style="list-style-type: none">• Digest• SSO• NBA	Optional	The default user authorization mechanism
userBarringInd	One of the following strings: <ul style="list-style-type: none">• TRUE• FALSE	Optional	Indicates whether the HSS user is barred.
roamingAllowed	One of the following strings: <ul style="list-style-type: none">• TRUE• FALSE	Optional	Indicates whether the HSS user roaming is allowed.



4.3.2 Example

An example for setting IMPI is shown as follows.

```
Request:
  <cai3:Set>
    <cai3:MOType>
      ISMSubscription@http://schemas.ericsson.com/ema/UserProvisioning/HSS/ISM/
    </cai3:MOType>
    <cai3:MOId>
      <subscriberId>123456_1002@ericsson.com</subscriberId>
    </cai3:MOId>
    <cai3:MOAttributes>
      <SetISMSubscription subscriberId="123456_1002@ericsson.com"
        xsi:schemaLocation=
          "http://schemas.ericsson.com/ema/UserProvisioning/HSS/ISM/
            ema_UserProvisioning_HSS_ISM.xsd"
        xmlns="http://schemas.ericsson.com/ema/UserProvisioning/HSS/ISM/"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <privateUser privateUserId="user002@ericsson.com">
          <userPassword>password</userPassword>
          <allowedAuthMechanism>SSO</allowedAuthMechanism>
          <userBarringInd>FALSE</userBarringInd>
          <roamingAllowed>FALSE</roamingAllowed>
        </privateUser>
      </SetISMSubscription>
    </cai3:MOAttributes>
  </cai3:Set>

Response:
<ns2:SetResponse xmlns:ns2="http://schemas.ericsson.com/cai3g1.2/">
```

Example 10 Set IMPI

4.4 Get IMPI

This section describes how to get IMPI.

MOType

ISMSubscription@http://schemas.ericsson.com/ema/UserProvisioning/HSS/ISM/

4.4.1 Request Data

MOId

Table 20 MOID Parameters of Getting IMPI

Parameter	Type	Occurrence	Description
subscriberId	String Max length = 255	Mandatory	The SIM subscriber identity For example: <imsi>@domain or <msisdn>@domain Domain shall derive from IMPI and do pre-configuration in Dynamic Activation



4.4.2 Response Data

MOAttributes

Table 21 MOAttributes of Getting IMPI Response

Parameter	Type	Occurrence	Description
subscriberId	String Max length = 255	Mandatory	The SIM subscriber identity For example: <imsi>@domain or <msisdn>@domain Domain shall derive from IMPI and do pre-configuration in Dynamic Activation
privateUser			
privateUserId	String Min length = 1 Max length = 256	Mandatory	The HSS private user identity
allowedAuthMechanism	One of the following strings: <ul style="list-style-type: none">• Digest• SSO• NBA	Optional	The default user authorization mechanism
userBarringInd	One of the following strings: <ul style="list-style-type: none">• TRUE• FALSE	Optional	Indicates whether the HSS user is barred.
roamingAllowed	One of the following strings: <ul style="list-style-type: none">• TRUE• FALSE	Optional	Indicates whether the HSS user roaming is allowed.

4.4.3 Example

An example for getting IMPI is shown as follows.



```
Request:
  <cai3:Get>
    <cai3:MOType>
      ISMSubscription@http://schemas.ericsson.com/ema/UserProvisioning/HSS/ISM/
    </cai3:MOType>
    <cai3:MOId>
      <subscriberId>123456_1002@ericsson.com</subscriberId>
    </cai3:MOId>
  </cai3:Get>

Response:
  <ns2:GetResponse xmlns:ns2="http://schemas.ericsson.com/cai3gl.2/">
    <ns2:MOAttributes>
      <ns:getResponseISMSubscription subscriberId="123456_1002@ericsson.com"
        xmlns:ns="http://schemas.ericsson.com/ema/UserProvisioning/HSS/ISM/">
        <ns:subscriberId>123456_1002@ericsson.com</ns:subscriberId>
        <ns:privateUser privateUserId="user001@ericsson.com">
          <ns:privateUserId>user001@ericsson.com</ns:privateUserId>
          <ns:userBarringInd>TRUE</ns:userBarringInd>
          <ns:roamingAllowed>TRUE</ns:roamingAllowed>
          <ns:allowedAuthMechanism>Digest</ns:allowedAuthMechanism>
        </ns:privateUser>
      </ns:getResponseISMSubscription>
    </ns2:MOAttributes>
  </ns2:GetResponse>
```

Example 11 Get IMPI



5 IPWorks NonSiM AAA User Subscription

IPWorks open interface is used for provisioning IPWorks Name Server Daemon (NSD) user directly, including creating, setting, deleting, and getting Domain Name System (DNS) entity. It provides the Create, Delete, Set, and Get operations.

5.1 Create AAANSUser

This section describes how to create AAANSUser.

MOType

AAANSUser@http://schemas.ericsson.com/ma/IPWORKS/

5.1.1 Request Data

MOId

Table 22 MOID Parameters of Creating AAANSUser

Parameter	Type	Occurrence	Description
transactionLogId	String Max Length = 64	Optional	The transaction ID
name	String Pattern value=[^A-Z]{1,256}	Mandatory	The user name of AAANSUser. The common format is *****@domain

MOAttributes

Table 23 MOAttributes of Creating AAANSUser

Parameter	Type	Occurrence	Description
name	String Pattern value=[^A-Z]{1,256}	Mandatory	The user name of AAANSUser. The common format is *****@domain
password	String Min length = 4 Max length = 256	Optional	The password of AAANSUser
imsi	Digit String 6-16 digits Each digit is 0-9	Mandatory	The Non-SIM device IMSI that is associated with the Non-SIM device



Parameter	Type	Occurrence	Description
msisdn	Digit String 5-16 digits Each digit is 0-9	Mandatory	The SIM device MSISDN that is associated with the Non-SIM device
apn	String Multiple values, separated by comma	Optional	The Access Point Name of the Non-SIM device
userStatus	One of the following strings: <ul style="list-style-type: none">• enable• disable	Optional	The status of AAANSUser. Only enable and disable operations are valid when creating the AAANSUser. Enable, disable, and reset operations are valid when setting the AAANSUser.
certificateId	String Max length = 64	Optional	The certificate identity for Non-SIM device. The value of certificateId is a decimal value, which equals to the decimal value converted from the hexadecimal value of certificateSN in the ECAS interface. See Table 33.
certificateIssuer Name	String Max length = 512	Optional	The DN of the certificate issuer. The parameter value equals to the value of certificateIssuerName in the ECAS interface. See Table 34.

5.1.2

Example

An example for creating AAANSUser in IPWorks is shown as follows.



```

Request:
<cai3:Create>
  <cai3:MOType>AAANSUser@http://schemas.ericsson.com/ma/IPWORKS/</cai3:MOType>
  <cai3:MOId>
    <!--Optional:-->
    <ipw:transactionLogId>transactionid9876540000111##999</ipw:transactionLogId>
    <ipw:name>${Properties#AAANSUserNAmeTID001}</ipw:name>
  </cai3:MOId>
  <cai3:MOAttributes>
    <ipw:CreateAAANSUser name="${Properties#AAANSUserNAmeTID001}">
      <ipw:name>${Properties#AAANSUserNAmeTID001}</ipw:name>
      <!--Optional:-->
      <ipw:password>tidpasswd111#0001</ipw:password>
      <ipw:imsi>987654321</ipw:imsi>
      <ipw:msisdn>6543210</ipw:msisdn>
      <!--Optional:-->
      <ipw:apn>aliba.com,aaa.com,ating.cn</ipw:apn>
      <!--Optional:-->
      <ipw:userStatus>enable</ipw:userStatus>
      <!--Optional:-->
      <ipw:certificateId>123456789</ipw:certificateId>
      <!--Optional:-->
      <ipw:certificateIssuerName>ECAS</ipw:certificateIssuerName>
    </ipw:CreateAAANSUser>
  </cai3:MOAttributes>
</cai3:Create>

Response:
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:cai3g="http://schemas.ericsson.com/cai3g1.2/">
  <S:Header>
    <cai3g:SessionId>c5feda708a4a4c07890dcc32dc041a75</cai3g:SessionId>
  </S:Header>
  <S:Body>
    <ns2:CreateResponse xmlns:ns2="http://schemas.ericsson.com/cai3g1.2/">
      <ns2:MOId>
        <ipw:transactionLogId xmlns:ipw="http://schemas.ericsson.com/ma/IPWORKS/">
          transactionid9876540000111##999</ipw:transactionLogId>
        <ipw:name xmlns:ipw="http://schemas.ericsson.com/ma/IPWORKS/">aaansduser002
        </ipw:name>
      </ns2:MOId>
    </ns2:CreateResponse>
  </S:Body>
</S:Envelope>

```

Example 12 Create AAANSUser

5.2 Set AAANSUser

This section describes how to set AAANSUser.

MOType

AAANSUser@http://schemas.ericsson.com/ma/IPWORKS/

5.2.1 Request Data

MOId

**Table 24** *MOID Parameters of Setting AAANSUser*

Parameter	Type	Occurrence	Description
transactionLogId	String Max Length = 64	Optional	The transaction ID
name	String Pattern value=[^A-Z]{1,256}	Mandatory	The user name of AAANSUser. The common format is *****@domain

MOAttributes

Table 25 *MOAttributes of Setting AAANSUser*

Parameter	Type	Occurrence	Description
name	String Pattern value=[^A-Z]{1,256}	Mandatory	The user name of AAANSUser. The common format is *****@domain
password	String Min length = 4 Max length = 256	Optional	The password of AAANSUser
apn	String[nillable] ⁽¹⁾ Multiple values, separated by comma or Single value	Optional	The Access Point Name of the Non-SIM device Use xsi:nil="true" to remove apnlist.
userStatus	One of the following strings: <ul style="list-style-type: none">• enable• disable	Optional	The status of AAANSUser. Only enable and disable operations are valid when creating the AAANSUser. Enable, disable, and reset operations are valid when setting the AAANSUser.
certificateId	String Max length = 64	Optional	The certificate identity for Non-SIM device. The value of certificateId is a decimal value, which equals to the decimal value converted from the hexadecimal value of certificateSN in the ECAS interface. See Table 33.
certificateIssuer Name	String Max length = 512	Optional	The DN of the certificate issuer. The parameter value equals to the value of certificateIssuerName in the ECAS interface. See Table 34.

(1) There are two scenarios for nillable: Remove a single apn value such as <apn value="apnNeedRemove" xsi:nil="true"/>; remove all apn values such as <apn xsi:nil="true"/>.



5.2.2

Example

An example for setting AAANSUser (including password, apn, and user status) in IPWorks is shown as follows.

Request:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:cai3="http://schemas.ericsson.com/cai3gl.2/"
  xmlns:ipw="http://schemas.ericsson.com/ma/IPWORKS/">
  <soapenv:Header>
    <cai3:SessionId>${Properties#sessionId}</cai3:SessionId>
  </soapenv:Header>
  <soapenv:Body>
    <cai3:Set>
      <cai3:MOType>AAANSUser@http://schemas.ericsson.com/ma/IPWORKS/
    </cai3:MOType>
    <cai3:MOId>
      <!--Optional:-->
      <ipw:transactionLogId>${Properties#transactionLogId}</ipw:transactionLogId>
      <ipw:name>${Properties#imsi}@aaansd</ipw:name>
    </cai3:MOId>
    <cai3:MOAttributes>
      <ipw:SetAAANSUser name="${Properties#imsi}@aaansd">
        <!--Optional:-->
        <ipw:password>originPas</ipw:password>
        <!--Zero or more repetitions:-->
        <ipw:apn>mnc007.mcc490.3gppnetworks.org</ipw:apn>
        <!--Optional:-->
        <ipw:userStatus>disable</ipw:userStatus>
        <!--Optional:-->
        <ipw:certificateId>123456789222</ipw:certificateId>
        <!--Optional:-->
        <ipw:certificateIssuerName>ECAS</ipw:certificateIssuerName>
      </ipw:SetAAANSUser>
    </cai3:MOAttributes>
  </cai3:Set>
</soapenv:Body>
</soapenv:Envelope>
```

Response:

```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:cai3g="http://schemas.ericsson.com/cai3gl.2/">
  <S:Header>
    <cai3g:SessionId>1a1fe8d5e8c042429322f0359ee3756f</cai3g:SessionId>
  </S:Header>
  <S:Body>
    <SetResponse xmlns="http://schemas.ericsson.com/cai3gl.2/">
  </S:Body>
</S:Envelope>
```

Example 13 Set AAANSUser

If the user status is set to `disable`, the system updates the user status to `disable` and then disconnects the session between AAA and ePDG.

If the user status is set to `reset`, the system disconnects the session between AAA and ePDG directly.

Examples for apn operations are shown as follows:



```
Request:
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:cai3="http://schemas.ericsson.com/cai3gl.2/"
  xmlns:ipw="http://schemas.ericsson.com/ma/IPWORKS/">
  <soapenv:Header>
    <cai3:SessionId>${Properties#sessionId}</cai3:SessionId>
  </soapenv:Header>
  <soapenv:Body>
    <cai3:Set>
      <cai3:MOType>AAANSUser@http://schemas.ericsson.com/ma/IPWORKS/</cai3:MOType>
      <cai3:MOId>
        <!--Optional:-->
        <!--<ipw:transactionLogId>transactionid9876540000111@333#enable
        </ipw:transactionLogId>-->
        <ipw:name>${Properties#AAANSUserNameTID001}</ipw:name>
      </cai3:MOId>
      <cai3:MOAttributes>
        <ipw:SetAAANSUser name="${Properties#AAANSUserNameTID001}">
          <ipw:apn>apn1, apn1, apn1, apn2, apn3, apn4</ipw:apn>
        </ipw:SetAAANSUser>
      </cai3:MOAttributes>
    </cai3:Set>
  </soapenv:Body>
</soapenv:Envelope>

Response:
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:cai3g="http://schemas.ericsson.com/cai3gl.2/">
  <S:Header>
    <cai3g:SessionId>4e00a89d1ec946b187c33f7aac611391</cai3g:SessionId>
  </S:Header>
  <S:Body>
    <ns2:SetResponse xmlns:ns2="http://schemas.ericsson.com/cai3gl.2/">
  </S:Body>
</S:Envelope>
```

Example 14 Set AAANSUser - Update All apn List



```

Request:
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:cai3="http://schemas.ericsson.com/cai3g1.2/"
  xmlns:ipw="http://schemas.ericsson.com/ma/IPWORKS/">
  <soapenv:Header>
    <cai3:SessionId>${Properties#sessionId}</cai3:SessionId>
  </soapenv:Header>
  <soapenv:Body>
    <cai3:Set>
      <cai3:MOTType>AAANSUser@http://schemas.ericsson.com/ma/IPWORKS/</cai3:MOTType>
      <cai3:MOId>
        <!--Optional:-->
        <!--<ipw:transactionLogId>transactionid9876540000111@333#enable
        </ipw:transactionLogId>-->
        <ipw:name>${Properties#AAANSUserNameTID001}</ipw:name>
      </cai3:MOId>
      <cai3:MOAttributes>
        <ipw:SetAAANSUser name="${Properties#AAANSUserNameTID001}">
          <ipw:apn value="value1">value1</ipw:apn>
          <ipw:apn value="value2">value2</ipw:apn>
        </ipw:SetAAANSUser>
      </cai3:MOAttributes>
    </cai3:Set>
  </soapenv:Body>
</soapenv:Envelope>

Response:
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:cai3g="http://schemas.ericsson.com/cai3g1.2/">
  <S:Header>
    <cai3g:SessionId>4e00a89d1ec946b187c33f7aac611391</cai3g:SessionId>
  </S:Header>
  <S:Body>
    <ns2:SetResponse xmlns:ns2="http://schemas.ericsson.com/cai3g1.2/">
  </S:Body>
</S:Envelope>

```

Example 15 Set AAANSUser - Add New apn Values



Request:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:cai3="http://schemas.ericsson.com/cai3gl.2/"
  xmlns:ipw="http://schemas.ericsson.com/ma/IPWORKS/">
  <soapenv:Header>
    <cai3:SessionId>${Properties#sessionId}</cai3:SessionId>
  </soapenv:Header>
  <soapenv:Body>
    <cai3:Set>
      <cai3:MOType>AAANSUser@http://schemas.ericsson.com/ma/IPWORKS/</cai3:MOType>
      <cai3:MOId>
        <!--Optional:-->
        <!--<ipw:transactionLogId>transactionid9876540000111@333#enable
        </ipw:transactionLogId>-->
        <ipw:name>${Properties#AAANSUserNameTID001}</ipw:name>
      </cai3:MOId>
      <cai3:MOAttributes>
        <ipw:SetAAANSUser name="${Properties#AAANSUserNameTID001}">
          <ipw:apn value="apnNeedRemove" xsi:nil="true"/>
        </ipw:SetAAANSUser>
      </cai3:MOAttributes>
    </cai3:Set>
  </soapenv:Body>
</soapenv:Envelope>
```

Response:

```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:cai3g="http://schemas.ericsson.com/cai3gl.2/">
  <S:Header>
    <cai3g:SessionId>4e00a89d1ec946b187c33f7aac611391</cai3g:SessionId>
  </S:Header>
  <S:Body>
    <ns2:SetResponse xmlns:ns2="http://schemas.ericsson.com/cai3gl.2/">
  </S:Body>
</S:Envelope>
```

Example 16 Set AAANSUser - Remove a Single apn Value



```

Request:
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:cai3="http://schemas.ericsson.com/cai3g1.2/"
  xmlns:ipw="http://schemas.ericsson.com/ma/IPWORKS/">
  <soapenv:Header>
    <cai3:SessionId>${Properties#sessionId}</cai3:SessionId>
  </soapenv:Header>
  <soapenv:Body>
    <cai3:Set>
      <cai3:MOType>AAANSUser@http://schemas.ericsson.com/ma/IPWORKS/</cai3:MOType>
      <cai3:MOId>
        <!--Optional:-->
        <!--ipw:transactionLogId>transactionid9876540000111@333#enable
        </ipw:transactionLogId-->
        <ipw:name>${Properties#AAANSUserNameTID001}</ipw:name>
      </cai3:MOId>
      <cai3:MOAttributes>
        <ipw:SetAAANSUser name="${Properties#AAANSUserNameTID001}">
          <ipw:apn xsi:nil="true"/>
        </ipw:SetAAANSUser>
      </cai3:MOAttributes>
    </cai3:Set>
  </soapenv:Body>
</soapenv:Envelope>

Response:
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:cai3g="http://schemas.ericsson.com/cai3g1.2/">
  <S:Header>
    <cai3g:SessionId>4e00a89d1ec946b187c33f7aac611391</cai3g:SessionId>
  </S:Header>
  <S:Body>
    <ns2:SetResponse xmlns:ns2="http://schemas.ericsson.com/cai3g1.2/">
  </S:Body>
</S:Envelope>

```

Example 17 Set AAANSUser - Remove the apn List

5.3 Delete AAANSUser

This section describes how to delete AAANSUser.

MOType

AAANSUser@http://schemas.ericsson.com/ma/IPWORKS/

5.3.1 Request Data

MOId

Table 26 MOID Parameters of Deleting AAANSUser

Parameter	Type	Occurrence	Description
transactionLogId	String Max Length = 64	Optional	The transaction ID
name	String Pattern value=[^A-Z]{1,256}	Mandatory	The user name of AAANSUser. The common format is *****@domain



5.3.2 Example

An example for deleting AAANSUser from IPWorks is shown as follows.

The system deletes AAANSUser first and then disconnects the session between AAA and ePDG.

```
Request:
  <cai3:Delete>
    <cai3:MOType>AAANSUser@http://schemas.ericsson.com/ma/IPWORKS/</cai3:MOType>
    <cai3:MOId>
      <ipw:name xmlns:ipw="http://schemas.ericsson.com/ma/IPWORKS/">
        123456@ericsson</ipw:name>
      </cai3:MOId>
    </cai3:Delete>

Response:
  <ns2:DeleteResponse xmlns:ns2="http://schemas.ericsson.com/cai3g1.2/">
    <ns2:MOId>
      <ipw:name xmlns:ipw="http://schemas.ericsson.com/ma/IPWORKS/">
        123456@ericsson</ipw:name>
      </ns2:MOId>
    </ns2:DeleteResponse>
```

Example 18 Delete AAANSUser

5.4 Get AAANSUser

This section describes how to get AAANSUser.

MOType

AAANSUser@http://schemas.ericsson.com/ma/IPWORKS/

5.4.1 Request Data

MOId

Table 27 MOID Parameters of Getting AAANSUser

Parameter	Type	Occurrence	Description
transactionLogId	String Max Length = 64	Optional	The transaction ID
name	String Pattern value=[^A-Z]{1,256}	Mandatory	The user name of AAANSUser. The common format is *****@domain

5.4.2 Response Data

MOAttributes



Table 28 *MOAttributes of Getting AAANSUser Response*

Parameter	Type	Occurrence	Description
name	String Pattern value=[^A-Z]{1,256}	Mandatory	The user name of AAANSUser. The common format is *****@domain
imsi	Digit String 6-16 digits Each digit is 0-9	Mandatory	The SIM device IMSI that is associated with the Non-SIM device
msisdn	Digit String 5-16 digits Each digit is 0-9	Mandatory	The SIM device MSISDN that is associated with the Non-SIM device
apn	String	Mandatory	The Access Point Name of the Non-SIM device
userStatus	One of the following strings: <ul style="list-style-type: none"> • enable • disable 	Mandatory	The status of AAANSUser. Only enable and disable operations are valid when creating the AAANSUser. Enable, disable, and reset operations are valid when setting the AAANSUser.
certificateId	String Max length = 64	Optional	The certificate identity for Non-SIM device. The value of certificateId is a decimal value, which equals to the decimal value converted from the hexadecimal value of certificateSN in the ECAS interface. See Table 33.
certificateIssuerName	String Max length = 512	Optional	The DN of the certificate issuer. The parameter value equals to the value of certificateIssuerName in the ECAS interface. See Table 34.

5.4.3 Example

An example for getting the AAANSUser from IPWorks is shown as follows.



```
Request:
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:cai3="http://schemas.ericsson.com/cai3g1.2/"
  xmlns:ipw="http://schemas.ericsson.com/ma/IPWORKS/">
  <soapenv:Header>
    <cai3:SessionId>${Properties#sessionId}</cai3:SessionId>
  </soapenv:Header>
  <soapenv:Body>
    <cai3:Get>
      <cai3:MOType>AAANSUser@http://schemas.ericsson.com/ma/IPWORKS/
    </cai3:MOType>
    <cai3:MOId>
      <!--Optional:-->
      <ipw:name>${Properties#AAANSUserNameTID001}</ipw:name>
    </cai3:MOId>
    </cai3:Get>
  </soapenv:Body>
</soapenv:Envelope>

Response:
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:cai3g="http://schemas.ericsson.com/cai3g1.2/">
  <S:Header>
    <cai3g:SessionId>4e00a89d1ec946b187c33f7aac611391</cai3g:SessionId>
  </S:Header>
  <S:Body>
    <ns2:GetResponse xmlns:ns2="http://schemas.ericsson.com/cai3g1.2/">
      <ns2:MOAttributes>
        <ip:GetResponseAAANSUser xmlns:ip="http://schemas.ericsson.com/ma/IPWORKS/">
          <ip:name>aaansduser002</ip:name>
          <ip:imsi>987654321</ip:imsi>
          <ip:msisdn>6543210</ip:msisdn>
          <ip:apn>aliba.com,aaa.com,ating.cn</ip:apn>
          <ip:userStatus>enable</ip:userStatus>
          <ip:certificateId>123456789111</ip:certificateId>
          <ip:certificateIssuerName>ECAS_NEW</ip:certificateIssuerName>
        </ip:GetResponseAAANSUser>
      </ns2:MOAttributes>
    </ns2:GetResponse>
  </S:Body>
</S:Envelope>
```

Example 19 Get AAANSUser



6 Ericsson Certificate Authority Server Subscription

ECAS CAI3G interface is provided by PG NGN for the provisioning of CA directly including certification enrollment, renewal, revocation, and retrieval.

The ECAS operation includes the Create, Delete, Set, and Get operations.

6.1 Create ECASCertificate

This section describes how to create ECASCertificate.

MOType

ECASCertificate@http://schemas.ericsson.com/ma/ECAS/

6.1.1 Request Data

MOId

Table 29 MOID Parameters of Creating ECASCertificate

Parameter	Type	Occurrence	Description
username	String Max length = 256	Mandatory	Entity user name, used to create an end entity in CA server

MOAttributes

Table 30 MOAttributes of Creating ECASCertificate

Parameter	Type	Occurrence	Description
username	String Max length = 256	Mandatory	Entity user name, used to create an end entity in CA server
password	String Min length = 8 Max length = 256	Optional	Entity user password
caName	String Max length = 512	Optional	The CA name that is used to sign the CSR. The CA name should be as same as the definition in CA server.



Parameter	Type	Occurrence	Description
csr	String	Mandatory	Certificate Sign Request. PKCS10 request in base64 encode.
certificateSN	String Max length = 512	Optional	The certificate's serial number

6.1.2

Response Data

MOAttributes

Table 31 MOAttributes of Creating ECASCertificate Response

Parameter	Type	Occurrence	Description
certificate	String	Mandatory	The signed certificate
certificateSN	String Max length = 64	Mandatory	The certificate's serial number
certificateExpireTime	dateTime	Mandatory	The certificate expiration time
certificateIssuerName	String Max length = 512	Mandatory	The DN of the certificate issuer.

6.1.3

Example

The Create operation of the ECASCertificate provider interface generates a certification according to given csr and returns a signed certificate.

An example for creating ECASCertificate is shown as follows.

```
Request:
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:cai3="http://schemas.ericsson.com/cai3g1.2/"
  xmlns:ecas="http://schemas.ericsson.com/ma/ECAS/">
  <soapenv:Header>
    <cai3:SessionId>${Properties#sessionId}</cai3:SessionId>
  </soapenv:Header>
  <soapenv:Body>
    <cai3:Create>
      <cai3:MOTYPE>ECASCertificate@http://schemas.ericsson.com/ma/ECAS/</cai3:MOTYPE>
      <cai3:MOId>
        <ecas:username>${username_1}</ecas:username>
      </cai3:MOId>
      <cai3:MOAttributes>
        <ecas:CreateECASCertificate username="${username_1}">
          <ecas:username>${username_1}</ecas:username>
          <!--Optional:-->
          <ecas:password>onetimePassword</ecas:password>
          <!--Optional:-->
          <ecas:caName>ManagementCA</ecas:caName>
          <ecas:csr>
MIICpjCCAY4CADBiMQswCQYDVQQGEWJDTjEVMBMGAlUEAxMMY29tbW9uTmFtZVZQX
MREwDwYDVQQHEWhzaGFuZ2hhaTENMAsGA1UEChMEYnVzcwELMAkGA1UECBMCU0gx
DTALBgNVBAsTBHhsZXQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDD
g+zZICj1fmJGMzI7q1NTC+EcoCXIK40aXIVzPQ9RJ5iCW7cNB8LIVfYKCMNWrVNM
Bv9PLlZ8Tq6HtxAQtz/SyYJj15Sp1kpPU98pSNXoy1zJF9mknMMea0g5D1FPvGM7
pgjLaYtMyaKSY9z8h93CAQQBHKjVA+eRtm+LDF6PsvHYTuvTOWUqkRpntyQMupvi
```



```

n9jAZxNjg+dvAMhjSgg8gruKhuD85NGOwsZKlzMVVVKzFRoaY7r2bksvdHgep0VR
Ka0DkVw+ON0UzDn/FkWA7oXjhUlnqYFwRL0B6gbXbF3eD66K8MzU2X6RN+uFNJg+
2M/F2X4Uz+0J7ckdFLJdAgMBAAGgADANBgkqhkiG9w0BAQQFAAOCAQEAuIC+aBQi
GK1IIbCRccJYyySaZPZ1Sen7OMRh87/0a5PwSHyOvQEGdybUCoJOWvySHtNqpsw
hLM05k3s2DdZSy2wUnLihuIm46ttNq7tslycxv+p506vP8GSN5CeaZLeDWeXZTLm
3+Ry50Cn7ygvZ/oaikKZub1/lj07vHYJNGswiflp9b1W8MuxyWRIPmxwCDATMiWj
lO83mmDrKw29cW/LewMWZccD9F4fGHtLRc7JoKhb80C0hgdwDttRMCZ4IcwklzJw
UPutqKcKgJp75L/anQBsW7G3LxeeWLBllxTcDuXGLzhBoF3t3fnRDIzJDU7/9rjz
/bDz6Jjp7uHu0w==</ecas:csr>
    <!--Optional:-->
    <!--<ecas:subjectDN>CN=ezhimen@Ericsson</ecas:subjectDN>-->
  </ecas:CreateECASCertificate>
</cai3:MOAttributes>
</cai3:Create>
</soapenv:Body>
</soapenv:Envelope>

Response:
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:cai3g="http://schemas.ericsson.com/cai3g1.2/">
  <S:Header>
    <cai3g:SessionId>3c31a1fa9409472ba1c148a823702e48</cai3g:SessionId>
  </S:Header>
  <S:Body>
    <ns2:CreateResponse xmlns:ns2="http://schemas.ericsson.com/cai3g1.2/">
      <ns2:MOId>
        <ecas:username xmlns:ecas="http://schemas.ericsson.com/ma/ECAS/">
          ezhimen@ericsson.com</ecas:username>
        </ns2:MOId>
        <ns2:MOAttributes>
          <ecas:CreateResponseECASCertificate
            xmlns:ecas="http://schemas.ericsson.com/ma/ECAS/">
            <ecas:certificate>LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tL
S0tCk1JSURXekNDQWtPZ0F3SUJBZ0lJRFPjWJXlOMWI5enN3RFFZSktvWklodmNOQV
FRkJRQXdPekVWUjNR0ExVUUKQXN3TVRXXRnVZV2RsYldwWRRFTkxJNU1V3RXZFRFZRU
UteQXhGU2tKRFFFTQlRZVzF3YkdVeEN6QUUpCZ05WQkFZVApBbE5GTUI0WERURTFNRFV
5TnpBek1EWXpOVm9YRFRFRM01EVXlOafF6TURZek5Wb3dIekVkJTUJzR0ExVUVD3dVC
lpYcG9hVzFsYmtCbGNTbGpjM052Ymk1amIyMHdnZ0VpTUeWRONTcUdTSWIzRFFQkF
RVUFBNElCRHdBd2dnRUsKQW9JQkFRFRERnK3paSUNqMWZtSkdNekk3cTFOVEMrRWNvQ
1hJSzQwYVhJVnpQUt1SSjVpQ1c3Y05COExJVmZSZWpDbU5XclZOTUJ2OVBMFTFo4VHE
2SHR4QVF0ei9TeVlKajE1U3Axa3BQVTk4cFNOWG95MXpKRjltA25NTVhVhMGc1CkRrR
1B2R003cGdGtGFZde15YUuTWt16OGg5M0NBUBVFCSEtqVkerZVJ0bStMREY2UHN2SFl
UdxZUT1dVcWtScG4KdHlRTXVwdmluOWpBWnhOamcrZHBTWhqU3FnoHFYdUtodUQ4N
U5HT3dzWktsek1NVlZLekZSb2FZN3IyYmtzdGpkSGdlcDBWUkthMERrVncrT04wVXp
Ebi9Ga1dB2N29YamhVbE5xWUZ3UkwwQjZnYlhiRjNlRDY2SzhNelUyWDZSCk4rdUZOS
mcrMk0vrRjYJNFV6KzBKN2NrZEZMSmRBZ0lCQUFHamZ6QjlnQjBHQTfVZERNuVdCQ1I
5aj13VTVMQ24KQldrTX13WctRUdRNKzMrSFVUQU1CZ05WSFJNqkFmOEVBakFBFTUI4R
0ExVWRJd1FZTUJhQUZOTFEExSxhiT0ZSbAorMmh0Znovb1lHTUdiS1lXTUE0R0ExVWR
Ed0VCL3dRRUF3SUY0REFkQmdOVkhTVUUGakFVQmdncnkjRnRUZCUWNECKFmWU1Ld1lCQ
1FVSEF3UXdeUUV1KS29aSWH2Y05BUUVGQ1FBRGdnRUJBR0tkrjhEUUFF4OENJNGNTVW1
zRU1XQlkKZFh6YzJnRkxncE1UUmV1Y0lQVt1XQ3BIWGrpTETKY1pNdVpSc1EwQk9jS
GJnemhQOF1vekpQdUp3Y0pCa0dINApSczNYsXkxU0xYK3ZYTFJYds9EM3ppVU95Yz1
6WfVav3kxZkc4SV1CZEtTRXNsYVZYd3VURHp4MXFPpRHZ6RFNVCKzQk2hTekcra3Q5T
0JQK2kzdUJnQzJKbEdid3ZUCt2VnFxaEZwdG1BK1ZISzJhdy93elZQaFARQzRqZTR
0R04KeFZyT3BsdDNMT0RZeFlURHQ3M1V0ZVfhQnFJde9oTnZvRk1QYnBoMzNmKfMQzd
EpwZHVjaElNMS9neW9JOHU1eQp0VDI5TVFOcXQ1MGfJL3gWw1VFYtUzRkxWSFZjdmV
qcmRIVFZQZC9MNdOemtVY21JVEhXm3VsTjdmUT1DcTQ9Ci0tLS0tRU5EIEFmFmRJR
kldQVRFLS0tLS0=</ecas:certificate>
          <ecas:certificateSN>d9218c8dd5bf73b</ecas:certificateSN>
          <ecas:certificateExpireTime>2017-05-26T03:06:35+00:00
          </ecas:certificateExpireTime>
          <ecas:certificateIssuerName>C=SE, O=EJBCA Sample, CN=ManagementCA
          </ecas:certificateIssuerName>
        </ecas:CreateResponseECASCertificate>
      </ns2:MOAttributes>
    </ns2:CreateResponse>
  </S:Body>
</S:Envelope>

```

Example 20 Create ECASCertificate



6.2 Set ECASCertificate

This section describes how to set ECASCertificate.

MOType

ECASCertificate@http://schemas.ericsson.com/ma/ECAS/

6.2.1 Request Data

MOId

Table 32 MOID Parameters of Setting ECASCertificate

Parameter	Type	Occurrence	Description
username	String Max length = 256	Mandatory	Entity user name, used to create an end entity in CA server

MOAttributes

Table 33 MOAttributes of Setting ECASCertificate

Parameter	Type	Occurrence	Description
username	String Max length = 256	Mandatory	Entity user name, used to create an end entity in CA server
password	String Min length = 8 Max length = 256	Optional	Entity user password
certificateSN	String Max length = 64	Mandatory	The certificate's serial number
caName	String Max length = 512	Optional	The CA name that is used to sign the CSR. The CA name should be as same as the definition in CA server.
csr	String	Mandatory	Certificate Sign Request. PKCS10 request in base64 encode.
subjectDN	String Max length = 512	Optional	Certificate user DN. CA server considers it as the Subject DN when generating a certificate.
issuerDN	String Max length = 512	Optional	CA's DN, for example, CN=AdminCA1,O=EJB CA Sample,C=SE

6.2.2 Response Data

MOAttributes



Table 34 MOAttributes of Setting ECASCertificate Response

Parameter	Type	Occurrence	Description
certificate	String	Mandatory	The signed certificate
certificateSN	String Max length = 64	Mandatory	The certificate's serial number
certificateExpire Time	dateTime	Mandatory	The certificate expiration time
certificateIssuer Name	String Max length = 512	Mandatory	The DN of the certificate issuer.

6.2.3

Example

The Set operation of the ECASCertificate renews a certificate of the given user. It contains two steps during the provisioning: revoking the old certificate; signing and issuing a certificate.

An example for setting ECASCertificate is shown as follows.

Request:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:cai3="http://schemas.ericsson.com/cai3g1.2/"
  xmlns:ecas="http://schemas.ericsson.com/ma/ECAS/">
  <soapenv:Header>
    <cai3:SessionId>${Properties#sessionId}</cai3:SessionId>
  </soapenv:Header>
  <soapenv:Body>
    <cai3:Set>
      <cai3:MOTYPE>ECASCertificate@http://schemas.ericsson.com/ma/ECAS/</cai3:MOTYPE>
      <cai3:MOId>
        <ecas:username>${username_1}</ecas:username>
      </cai3:MOId>
      <cai3:MOAttributes>
        <ecas:SetECASCertificate username="${username_1}">
          <!--Optional:-->
          <ecas:password>setPassword</ecas:password>
          <!--This set operation will revoke certification which declare in request
and issue one new certification-->
          <ecas:certificateSN>${certificateSN1}</ecas:certificateSN>
          <!--Optional:-->
          <ecas:caName>ManagementCA</ecas:caName>
          <ecas:csr>
MIICpJCCAY4CADBiMQswCQYDVQQGEwJDTjEVMBMGA1UEAxMMY29tbW9uTmFtZVZQx
MREwDwYDVQQHEWhzaGFuZ2hhaTENMA5GA1UEChMEYnVzcwELMAkGA1UECBMUC0gx
DTALBgNVBAsTBHhsZXQwggEiMA0GCSqGSIb3DQEBQUAA4IBDwAwggEKAoIBAQQDD
g+zzZICj1fmJGMzI7q1NTC+EcoCXIK40aXIVzPQ9RJ5iCW7cNB8LIVfYKcMNRvNM
Bv9PLLZ8Tg6HtxAQtz/SyYUj15SplkpPU98pSNXoy1zJF9mknMMea0g5DlFPvGM7
pgjLaYtMyaKSY9z8h93CAQQBHKjVA+eRtm+LDF6PsvHYTuvTOWUgkRpntYQMupvi
n9jAZxNjg+dvAMhjSgg8gruKhuD85NGOwsZKlzMVVKzFRoaY7r2bksvdHgep0VR
Ka0DkVw+ON0UzDn/FkWA7oXjhU1NgYFwRL0B6gbXbF3eD66K8MzU2X6RN+uFNJg+
2M/F2X4Uz+0J7ckdFLJdAgMBAAGgADANBgkqhkiG9w0BAQQFAAOCAQEAuIC+aBQi
GKlIIibCRccJYyySaZPZ1Sen7OMRh87/0a5PwSHyOvQEGdybUCoJOWvvySHTnqpsw
hLM05k3s2DdZSY2wUnLIhuIm46ttNq7tslycxv+p506vP8GSN5CeaZLeDWeXZTLm
3+Ry5OCn7ygvZ/oaikKZub1/1jO7vHYJNGswiflp9b1W8MuxyWRIPMxwCDATMiWj
1083mmDrKw29cW/LEwMWZccD9F4fGHtLRc7JoKhb80C0hgdwDttRMCZ4IcwklzJw
UPutqKcKgJp75L/anQBsW7G3LxeeWLB1LxTcDuXGLzhBOf3t3fnRDIZJDU7/9rjZ
/bDz6Jjp7uHu0w==</ecas:csr>
          <!--Optional:-->
          <!--<ecas:subjectDN>CN=ezhimen@Ericsson</ecas:subjectDN>-->
          <!--Optional:-->
          <!--<ecas:issuerDN>CN=AdminCA1,O=EJBCA Sample,C=SE</ecas:issuerDN>-->
          <ecas:issuerDN>CN=ManagementCA,O=EJBCA Sample,C=SE</ecas:issuerDN>
        </ecas:SetECASCertificate>
      </cai3:MOAttributes>
    </cai3:Set>
  </soapenv:Body>
</soapenv:Envelope>
```

```
</ca:ca:Set>
</soapenv:Body>
</soapenv:Envelope>

Response:
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:ca:3g="http://schemas.ericsson.com/cai3g1.2/">
  <S:Header>
    <ca:3g:SessionId>8e8a11f9acf34e3fbf807aa68a9d7dd1</ca:3g:SessionId>
  </S:Header>
  <S:Body>
    <ns2:SetResponse xmlns:ns2="http://schemas.ericsson.com/cai3g1.2/">
      <ns2:MOAttributes>
        <ecas:SetResponseECASCertificate
          xmlns:ecas="http://schemas.ericsson.com/ma/ECAS/">
            <ecas:certificate>LS0tLS1CRUdJTiBDRVJUSUZJQ0FUR5S0tLS0tCk1JS
URXekNDQWtPZ0F3SUJBZ01JLTlE3dDY1VWpKOUV3RFFZSktvWklodmNOQVFFRkRJRQXdPekVWUTUJ
NR0ExVUUKQXkd3TVXRhRnRnVZV2RSYldwWRRFTkJNULV3RXdZRFZRUUUEQXhGU2tKRFFFTQlRZVzF3Y
kdVeEN6QUpCZ05WQkFZVApBbE5GTUI0WERURTFNFRFV5TmPBMU1gRXp0Rm9YRFRFM01EVXl0VEE
xTWpFek5Gb3dIdkVtUJzR0ExVUVBd3dVClpYcG9hVzFsYmtCbGNTbGpjM052Ymk1amIyMHdnZ
0VpTUeWR0NtCUdTSWIRnRFFQKFRVUBFNE1CRHdBd2dnrUSk9JFRFRERnK3paSUNgMVWZStSkd
Nekk3cTFOVEMrRWNvQ1hJzSjQwYVhVJnpQUTlSSjVpQ1c3Y05COExJmVZZSwpDbU5XclZOTUJZ2O
VBMTFo4VHE2SHR4QVFOei9TeVlKajE1U3Axa3BQVTK4cFNOWG95MXpKRjltA25NTWVhMgc1Ckr
SRlB2R003cGdGtGFZde15YUtTWTl6OGg5MONBUVFCSEtQvKerZVJ0bstMREY2UHN2SF1UdxZUT
dVcWtScG4KdHlRTXVwdmUuOWpBWnhOamcrZHZBTWhgU3FnOHFYdUtoDQ4NU5HT3dzWktsek1
NVlZLekZSb2FZN3IyYmtzdgpkSGdlcDBWUkthMERrVncrT04wVXpEbi9GaldBN29YamhVbE5xw
UZ3UkwwQjZnYlhiRjNlRDY2SzhNelUyWDZSck4rdUZOsmcrMk0vRjJYJNFV6KzBKN2NrzEZMSr
BZ01CQUFHAmZ6Qj1NQjBHQTFVZERnUvUdCQlI5ajI3VTVMQ24KQldrTXl3WctRUdRnKzMrSFVUQ
U1CZ05WSFJNQkFmOEVBakFBTUI4R0ExVWRJRjd1FZTUJhQUZOTFEEXShiTOZSbAorMmh0Znovb1l
HTUdis1lXTUE0R0ExVWREd0VCL3dRRUF3SUY0REFKQmd0vKhTVUUGakFVQmdnckJnRUZCUWNEC
kFnWU1Ldl1CQlFVSEF3UXdEUUV1KS29aSWhtY05BUUVGQlFBRGdnRUJBRElyOTJUQ1lEZFFVYmN
pcWUyMHRjcWMKOS90NXJka0t1RVL1DUSSzaXVoay96NkR3QTFhU2FmMGl6MmoxalBVA040Uk5me
lh5MWY5RHpWnmR3cU96Y0Y3WgpEd3l1M1o1OUdpVDVMbVndOUdKNE9RUys5T3dmQ1hlcGxoeSt
TbEdDSS92djZEVnVKSVMNWU4xZnpITENiQk5BCnJ4ZWxNUUVvU3h0eG1XVEg5emQxcjczd010a
ZdMS283ZGhOS2hr2EybgGFpZnYzMGhKSZziN05mNXixNUdgVUkKQWZKNhRDTA0bFpHnnpqaWg
wTMRGylg0bm1DM1ZyeUs1NWyZcm5GWULqS2dXUwtTejd3eDc3YXNjSEYlZStEQgo5VG11RnQ5V
1lkUnRGN3BOTXZmTS9YUmJldFWUUF1LMTNkU1lHWndOWkw4Z3JkVWVJZT1NoUHYrVHC0cEt6cOU
9Ci0tLS0tRU5EIEFNFULRJRklDQVRFLS0tLS0t=</ecas:certificate>
        <ecas:certificateSN>350eedeb952327d1</ecas:certificateSN>
        <ecas:certificateExpireTime>2017-05-25T05:21:34+00:00
        </ecas:certificateExpireTime>
        <ecas:certificateIssuerName>C=SE, O=EJBCA Sample, CN=ManagementCA
        </ecas:certificateIssuerName>
      </ecas:SetResponseECASCertificate>
    </ns2:MOAttributes>
  </ns2:SetResponse>
</S:Body>
</S:Envelope>
```

Example 21 Set ECASCertificate

6.3 Delete ECASCertificate

This section describes how to delete ECASCertificate.

MOType

ECASCertificate@http://schemas.ericsson.com/ma/ECAS/

6.3.1 Request Data

Mold



Table 35 *MOID Parameters of Deleting ECASCertificate*

Parameter	Type	Occurrence	Description
username	String Max length = 256	Mandatory	Entity user name, used to create an end entity in CA server

MOAttributes

Table 36 *MOAttributes of Deleting ECASCertificate*

Parameter	Type	Occurrence	Description
username	String Max length = 256	Mandatory	Entity user name, used to create an end entity in CA server
password	String Min length = 8 Max length = 256	Optional	Entity user password
issuerDN	String Max length = 512	Optional	CA's DN, for example, CN=AdminCA1, O=EJBCA Sample, C=SE
certificateSN	String Max length = 64	Optional	The certificate's serial number

6.3.2

Example

The Delete operation of the ECASCertificate provides the capacity to revoke a certificate or end entity. When the certificate SN is provided, PG NGN tries to revoke the given certificate. If only username is provided, PG NGN tries to revoke all the certificates of the end entity.

An example for deleting ECASCertificate is shown as follows.

```
Request1: revoke the certificate according to certificateSN.
<ecas:DeleteECASCertificate username="username">
  <ecas:issuerDN>CN=AdminCA1,O=EJBCA Sample,C=SE</ecas:issuerDN>
  <ecas:certificateSN>44b9b175bb6b2244</ecas:certificateSN>
</ecas:DeleteECASCertificate>

Response 1
<ns2:revokeCertResponse xmlns:ns2="http://ws.protocol.core.ejbca.org/">

Request 2: revoke all certificates that belong to the given user
<ecas:DeleteECASCertificate username="username">
</ecas:DeleteECASCertificate>

Response 2
<ns2:revokeCertResponse xmlns:ns2="http://ws.protocol.core.ejbca.org/">
```

Example 22 Delete ECASCertificate

6.4

Get ECASCertificate

This section describes how to get ECASCertificate.



MOType

ECASCertificate@http://schemas.ericsson.com/ma/ECAS/

6.4.1

Request Data

MOId

Table 37 *MOID Parameters of Getting ECASCertificate*

Parameter	Type	Occurrence	Description
username	String Max length = 256	Mandatory	Entity user name, used to create an end entity in CA server

MOAttributes

Table 38 *MOAttributes of Getting ECASCertificate*

Parameter	Type	Occurrence	Description
certificateSN	String Max length = 64	Mandatory	The certificate's serial number
issuerDN	String Max length = 512	Optional	CA's DN, for example, CN=AdminCA1,O=EJBCA Sample,C=SE

6.4.2

Response Data

MOAttributes

Table 39 *MOAttributes of Getting ECASCertificate Response*

Parameter	Type	Occurrence	Description
certificate	String	Mandatory	The signed certificate
certificateSN	String Max length = 64	Mandatory	The certificate's serial number
certificateExpireTime	dateTime	Mandatory	The certificate expiration time
issuerDN	String Max length = 512	Mandatory	CA's DN, for example, CN=AdminCA1,O=EJBCA Sample,C=SE
isRevoked	One of the following strings: <ul style="list-style-type: none">• Yes• No	Mandatory	Indicates whether the certificate is revoked.
revocationDate	dateTime	Optional	The date when the certificate is revoked



6.4.3 Example

The `Get` operation of the `ECASCertificate` retrieves the certificate from CA server according to the given certification's SN and issuer's DN.

An example for getting `ECASCertificate` is shown as follows.



```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:cai3="http://schemas.ericsson.com/cai3g1.2/"
  xmlns:ecas="http://schemas.ericsson.com/ma/ECAS/">
  <soapenv:Header>
    <cai3:SessionId>${Properties#sessionId}</cai3:SessionId>
  </soapenv:Header>
  <soapenv:Body>
    <cai3:Get>
      <cai3:MOTYPE>ECASCertificate@http://schemas.ericsson.com/ma/ECAS/
    </cai3:MOTYPE>
    <cai3:MOId>
      <ecas:username>${username_1}</ecas:username>
    </cai3:MOId>
    <!--Optional:-->
    <cai3:MOAttributes>
      <ecas:GetECASCertificate>
        <ecas:certificateSN>${certificateSN1}</ecas:certificateSN>
        <!--Optional:-->
        <ecas:issuerDN>CN=ManagementCA,O=EJBCA Sample,C=SE</ecas:issuerDN>
      </ecas:GetECASCertificate>
    </cai3:MOAttributes>
    </cai3:Get>
  </soapenv:Body>
</soapenv:Envelope>
```

Response:

```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:cai3g="http://schemas.ericsson.com/cai3g1.2/">
  <S:Header>
    <cai3g:SessionId>8e8a11f9acf34e3fbf807aa68a9d7dd1</cai3g:SessionId>
  </S:Header>
  <S:Body>
    <ns2:GetResponse xmlns:ns2="http://schemas.ericsson.com/cai3g1.2/">
      <ns2:MOAttributes>
        <ecas:GetResponseECASCertificate
          xmlns:ecas="http://schemas.ericsson.com/ma/ECAS/">
          <ecas:certificate>LS0tLS1CRUdJTiBDRVJUSUZJQ0FURSB0tLS0tCk1JSUR
          XekNDQWtPZ0F3SUJBZ01JRm9KSneyMWU5U1l3RFFZSk1vWk1odmNOQVFFRkJRQXdpPekVWtUJNR0E
          xVUUKQXQ3TVRKRnVZV2R2SylldWdWRFTk1JNU1V3RXdzRFRZRUUteEQXhGU2tKRFFFTQ1RZVzF3YkdVeEN
          6QUpCZ05WQkFZVApBbE5GTUI0WERURTFNRFV5Tm1pBMU1qRXPnMW9YRFRFM01EVXl0VEEeXWpPek0
          xb3dIekVktUJzR0ExVUVBd3dVClpYcG9hVzFsYmtCbGNTbGp1M052Ymk1amIyMHdnZ0VpTUEwR0N
          TCUdTSWlZrRFFQkFRVUFBNELCRHdBd2dnRUSKQW9JQkFRFRERnK3paSUNqMWZtSkdNekk3cTF0VEM
          rRWNVQ1hJSzQwYVhJVnpQUt1SSjVpQ1c3Y05COExJVmZzSWpDbU5XclZ0TUJ2OVBMtFo4VHE2SHR
          4QVF0ei9TeVlKajE1U3Axa3BQVTk4cFNOWG95MXpKRjlt25NTWVhMGc1CkRsR1B2R003cGdgTGF
          ZdE15YUUtTWT16OGg5M0NBVFCSEtqVKErZVJ0bStMREY2UHN2SF1UdXZUT1dVcWtScG4KdH1RTXV
          wdm1uOWpBWNhOamcrZHZBTWhqU3FnOHFydUtodUQ4NU5HT3dzWktsek1NVlZLekZSb2FZN3IyYmt
          zdqpkSGdlcDBWUktHMERrVncrT04wVXpEbi9Ga1dBN29YamhVbE5xWUz3UkwwQjZnY1hiRjNlRDY
          2SzhNe1UyWDZSCk4rdUZOsmcrMk0vRjJYNFV6KzBKN2NrZEZMSmRBZ01CQUFHamZ6Qj1NQjBHQTf
          VZERnUvdcQ1I5ajI3VTVMQ24KQldrTXl3WctRUDRNKzMrSFVUQU1CZ05WSFJNQkFmOEVBakFBTUI
          4R0ExVVRJd1FZTUJhQUZOTFEeSXhiT0ZSbAorMmh0Znovb1lHTUdiS1lXTUE0R0ExVWREd0VCL3d
          RRUF3SUy0REFkQmdOVkhTVUVGakFVQmdnckJnRUZCUWNEckFnWU1Ld1lCQ1FVSEF3UXdEUv1KS29
          aSWh2Y05BUUvGQ1FBRGdnRUJBmNYNERFnmFmTHVQNXNram5jVjNHZUsKclp5TzlpYUptQVplTGg
          5TDNPUU9leH1YW9aYVgVnKNDQmdkUXNyWThpRG9SVUFhdVZ4TU4vMmtkNEFNUIExegpDY2NRUlh
          wU3ZORmxnZHRqVU13YkRiYjN6cDNlbXVmdRmdGY1lOT1M5bTBxOT1oc3FkTy93cHZuY1pkadlwSFZ
          uCkx6bXlRTUQ2emVyNlVXSHercXhNbWRnMDNiSWQ4YThzUHZlM2g2NnRGWNNZUNYck5pbStDRGN
          kcnY2MXy3Z0gKVTVMMEE2U210SGJaam1aTFVvbVJyY3luaWE2V1NGRDBKcW1hQXQ0eEpUVEduWmJ
          EYkVld0c2V1hwZ2xKMWFVQp4MnpYaWpsbFh5ZVN0YVF5UFp3aS82QUprXFGQ0oya3N5VmlVUDV
          QWTVpZUhxNnRrc0I1TlNwaUNuSDJvdnc9Ci0tLS0tRU5EIEFNULRJRklDQVRFLS0tLS0=
        </ecas:certificate>
        <ecas:certificateSN>168249ab6d5ef516</ecas:certificateSN>
        <ecas:certificateExpireTime>2017-05-25T05:21:33+00:00
        </ecas:certificateExpireTime>
        <ecas:issuerDN>CN=ManagementCA,O=EJBCA Sample,C=SE</ecas:issuerDN>
        <ecas:isRevoked>No</ecas:isRevoked>
      </ecas:GetResponseECASCertificate>
    </ns2:MOAttributes>
    </ns2:GetResponse>
  </S:Body>
</S:Envelope>
```

Example 23 Get ECASCertificate



7

Error Codes

Table 40 VoWifiService

Error Code	Error Message	MO	Operation
30000	AAA operation failure	VoWifiService	C
30001	CSR renew failure	VoWifiService	S
30002	CSR revocation failure	VoWifiService	S/D
30003	IMPI operation failure, AAA is been cleared	VoWifiService	C
	IMPI operation failure	VoWifiService	C
30004	IMPI operation failure, AAA is not been cleared	VoWifiService	C
30005	CSR enrollment failure, AAA data is been cleared and IMPI is been cleared	VoWifiService	C
	CSR enrollment failure, AAA data is been cleared	VoWifiService	C
30006	CSR enrollment failure, AAA data is not been cleared and IMPI is been cleared	VoWifiService	C
	CSR enrollment failure, AAA data is not been cleared	VoWifiService	C
30007	CSR enrollment failure, AAA data is been cleared and IMPI is not been cleared	VoWifiService	C
30008	CSR enrollment failure, AAA data is not been cleared and IMPI is not been cleared	VoWifiService	C
30009	AAA user removal failure	VoWifiService	D
30010	IMPI data removal failure	VoWifiService	D
30011	IMPI data modification failure	VoWifiService	S
30012	AAA data modification failure	VoWifiService	S
30013	CSR enroll failure	VoWifiService	C/S
30020	CSR enrollment failure, HSS data is cleared	VoWifiService	C
30021	CSR enrollment failure, HSS data is not cleared	VoWifiService	C
30022	AAA operation failure, certificate is cleared and HSS data is cleared	VoWifiService	C
	AAA operation failure, certificate is cleared	VoWifiService	C
30023	AAA operation failure, certificate is not cleared and HSS data is not cleared	VoWifiService	C



Error Code	Error Message	MO	Operation
30024	AAA operation failure, certificate is not cleared and HSS data is cleared	VoWifiService	C
	AAA operation failure, certificate is not cleared	VoWifiService	C
30025	AAA operation failure, certificate is cleared and HSS data is not cleared	VoWifiService	C
30026	AAA certificate update failure, certificate is cleared	VoWifiService	S
30027	AAA certificate update failure, certificate is not cleared	VoWifiService	S

Table 41 NonSIMHSSUser

Error Code	Error Message	MO	Operation
35103	Operations error	NonSIMHSSUser	C/S/D
35104	HSS Cannot contact LDAP server	NonSIMHSSUser	C/S/D
35105	HSS Already exists	NonSIMHSSUser	C
35106	HSS No such object	NonSIMHSSUser	S
35199	Other HSS dependent faults	NonSIMHSSUser	C/S/D

Table 42 HSS Open Interface

Error Code	Error Message	MO	Operation
35101	Missing or invalid parameter	ISMSubscription	C
35102	Invalid DN, missing parameter	ISMSubscription	C
35103	Operations error	ISMSubscription	C/S/G/D
35104	Cannot contact LDAP server	ISMSubscription	C/S/G/D
35105	Already exists	ISMSubscription	C
35106	No such object	ISMSubscription	S/G/D
35108	Type or value exists	ISMSubscription	C
35199	Other HSS dependent faults	ISMSubscription	C/S/G/D

Table 43 IPWorks Open Interface

Error Code	Error Message	MO	Operation
35250	Other IPWorks error	AAANSUser	C/S/G/D
35255	No AAANSUser found	AAANSUser	S/G/D
35256	An AAANSUser with the given name already existed	AAANSUser	C
35257	AAA is in maintenance mode, please try later.	AAANSUser	C/S/G/D



Error Code	Error Message	MO	Operation
35258	OPERATION FAILED, ROLLBACK HAS BEEN PERFORMED SUCCESSFULLY	AAANSUser	C ⁽¹⁾
35259	OPERATION FAILED, ROLLBACK WAS UNSUCCESSFUL	AAANSUser	C ⁽¹⁾

(1) For layered AAANS only.

Table 44 ECAS Open Interface

Error Code	Error Message	MO	Operation
36000	Certificate Enrollment failure	ECASCertificate	C
36001	Certificate Renew failure	ECASCertificate	S
36002	Certificate Revocation failure	ECASCertificate	D
36003	Certificate Retrieve failure	ECASCertificate	G
36004	Certificate Already Revoked	ECASCertificate	D



Reference List

Ericsson Documents

- [1] *Library Overview*, 18/1553-CSH 109 628 Uen
- [2] *Generic CAI3G Interface 1.2*, 2/15519-FAY3020003 Uen