This sequence diagram describes the IMS Registration of a terminal. The IMS registration goes through the following sequence:

1. **GPRS Attach**: The terminal registers to the GPRS Network.
2. **PDP Context Activation**: An IP address is assigned to the terminal.
3. **Unauthenticated IMS Registration Attempt**: The terminal attempts an IMS registration but is challenged by the IMS network to authenticate itself.
4. **IPSec Security Association Establishment**: The terminal establishes a protected session with the IMS network.
5. **Authenticated IMS Registration**: Registration is reattempted. This time the terminal is successfully authenticated and accepted.

This sequence diagram was generated with EventStudio System Designer 4.0 (http://www.EventHelix.com/EventStudio). Copyright © 2007 EventHelix.com Inc. All Rights Reserved.
IMS Registration (IMS Registration for an Unauthenticated User)

The subscriber sends a Register message to inform the network that the specified user public identity (myname@mynetwork.com) is available at the IP address indicated in the Contact Header. The User Equipment (UE) also adds a via header to record that the message had traversed the UE. The REGISTER message also includes the server and client ports. Note that the message itself is sent on the standard SIP port 5060.

The SIP REGISTER message also includes the private identity of the user. This identity will be used by the S-CSCF and HSS to identify the user.

The P-CSCF receives the REGISTER message and uses the DNS to translate from the domain hims.net to the IP address of the home network.

P-CSCF adds a Via header and removes the Route header. The REGISTER message will be routed to the IP address obtained from the DNS response. Note that the integrity protection flag is set to false to signify that the user has not been authenticated.

P-CSCF selects the S-CSCF based on the S-CSCF capabilities.

The I-CSCF forwards the REGISTER message to the selected S-CSCF.
## IMS Registration (IMS Registration for an Unauthenticated User)

<table>
<thead>
<tr>
<th>Visited Network</th>
<th>Internet</th>
<th>Home Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Equipment</td>
<td>Visited CN</td>
<td>Visited IMS</td>
</tr>
<tr>
<td>Subscriber</td>
<td>SGSN</td>
<td>GGSN</td>
</tr>
</tbody>
</table>

### Multimedia Authentication Request

```
name.private@hims.net
```

### Multimedia Authentication Answer

- RAND, AUTN, XRES, CK, IK

HSS passes the Random number (RAND), Authentication token (AUTN), signed result (XRES), Cipher key (CK) and Integrity Key (IK).

### Select Authentication vectors

- Save the selected authentication vector

### 401 Unauthorized

```
WWW-Authenticate: nonce=RAND-AUTN, ik, ck, via: icscf1, pcscf1, ue-ip
```

The user is currently not authenticated, so the registration request is rejected. The terminal is challenged to authenticate the user. RAND, AUTN, CK and IK are passed in the WWW-Authenticate header.

### 401 Unauthorized

```
WWW-Authenticate: nonce=RAND-AUTN, ik, ck, via: pcscf1, ue-ip
```

Pass the message to the P-CSCF. CK and IK are carried in the WWW-Authenticate header.

### Save CK and IK

- The P-CSCF saves the ciphering and integrity keys. These keys will be needed for establishing the IPSec security association.
- The P-CSCF allocates the subscriber side client and server ports. These ports will be included in the 401 Unauthorized message sent to the Subscriber.
- Pass the RAND and AUTN values to the subscriber. The CK and IK are removed from the WWW-Authenticate header. The P-CSCF side client and server ports are also included in the message.
- The message itself is sent on the standard SIP port 5060.
- Authenticate the IMS network by verifying the authentication token (AUTN). Also compute the RES value that will be passed back to the IMS network for user authentication.

### IPSec Security Association Establishment

- **IPSec SA for UE Initiated Requests**
  - UE-Client -> P-CSCF-Server
- **IPSec SA for Responses to UE**
  - UE-Server <- P-CSCF-Client
- **IPSec SA for P-CSCF Initiated Requests**
  - UE-Server <- P-CSCF-Client
- **IPSec SA for Responses to P-CSCF**
  - UE-Client -> P-CSCF-Server

Establish IPSec security associations for all the client and server ports.

### Authenticated IMS Registration

...
The Subscriber has now established the IPSec security associations with the P-CSCF. At this point, the SIP REGISTER message is sent again. This time the message is protected by IPSec and the message is addressed to the P-CSCF server port passed in the 401 Unauthorized message. The message contains the RES in the Authorization header.

```
The Subscriber has now established the IPSec security associations with the P-CSCF. At this point, the SIP REGISTER message is sent again. This time the message is protected by IPSec and the message is addressed to the P-CSCF server port passed in the 401 Unauthorized message. The message contains the RES in the Authorization header.
```

Pass the REGISTER message to the I-CSCF. This time the Authorization header indicates that integrity protection is enabled.

```
Pass the REGISTER message to the I-CSCF. This time the Authorization header indicates that integrity protection is enabled.
```

Query the HSS to assign the S-CSCF.

```
Query the HSS to assign the S-CSCF.
```

HSS replies with the S-CSCFs.

```
HSS replies with the S-CSCFs.
```

The SIP REGISTER message is finally delivered to the S-CSCF.

```
The SIP REGISTER message is finally delivered to the S-CSCF.
```

```
User Authorization Request
name.private@hims.net
```

```
User Authorization Answer
P-CSCF Name,
P-CSCF Capabilities
```

```
Server Assignment Request
Request subscriber related information from the HSS.
name.private@hims.net
```

```
Server Assignment Answer
Received subscriber related information.
```

```
Compare RES and XRES
```

```
200 OK
```

```
200 OK
```

```
200 OK
```

```
200 OK
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: pcscf1, pcscf1, UE-IP;UE-Server-Port
```

```
Via: pcscf1, pcscf1, UE-IP;UE-Server-Port
```

```
Via: pcscf1, UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: pcscf1, UE-IP;UE-Server-Port,
Contact: UE-IP ue-server-port,
Authorization: Digest username = name.private@hims.net response=RES integrity protection: yes,
RES
```

```
Via: pcscf1 UE-IP;UE-Server-Port,
Contact: UE-IP ue-server-port,
Authorization: Digest username = name.private@hims.net response=RES
```

```
Via: pcscf1 UE-IP;UE-Server-Port,
Contact: UE-IP ue-server-port,
Authorization: Digest username = name.private@hims.net response=RES integrity protection: yes,
RES
```

```
Via: icscf1 pcscf1 UE-IP;UE-Server-Port,
Contact: UE-IP ue-server-port,
Authorization: Digest username = name.private@hims.net response=RES integrity protection: yes,
RES
```

```
Via: icscf1, pcscf1, UE-IP;UE-Server-Port
```

```
Via: pcscf1, UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```

```
Via: UE-IP;UE-Server-Port
```