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)

**Visited Network**
- Internet
- Home Network

**User Equipment**
- Subscriber
- IMS Registration

**Visited IMS**
- DNS Server
- HSS

**DNS Server**
- Home DNS

**Home IMS**
- Home IMS

**Home CN**
- Home CN

**EventStudio System Designer 4.0**
- 24-Nov-07 18:36 (Page 2)

**AUTN, CK and IK are passed in the WWW-Authenticate header.**

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

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

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.

```
Save CK and IK
```

```
allocate P-CSCF side client and server ports
```

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.

```
Authorize 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

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

**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

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.
```

**Authenticated IMS Registration**

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

```
REGISTER 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,
```

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

```
User Authorization Request
```

```
User Authorization Answer
```

```
User Authorization Answer
```

The HSS replies with the S-CSCF.

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

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

The success is relayed back to the P-CSCF.

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

The IMS registration of the user is now complete.