Processor Interfaces (IMS Registration for an Unauthenticated User)

<table>
<thead>
<tr>
<th>Visited Network</th>
<th>Internet</th>
<th>Home Network</th>
<th>EventStudio System Designer 4.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Equipment</td>
<td>Visited CN</td>
<td>Visited IMS</td>
<td>DNS Server</td>
</tr>
</tbody>
</table>

GPRS Attach

1. **GMM Attach Request**
2. **GMM Attach Accept**
3. **GMM Attach Complete**

The terminal powers up and attaches to the GPRS network.

PDP Context Activation

1. **Activate PDP Context**
2. **Activate PDP Context Accept**

Once the attach is completed, the terminal initiates a PDP context activation.

Unauthenticated IMS Registration Attempt

REGISTER

```plaintext
REGISTER sip:hims.net SIP/2.0,
Via: SIP/2.0/UDP UE-IP;branch=0abab,
Max-Forwards: 20,
From: <sip:name@hims.net>;tag=abbb,
To: <sip:name@hims.net>,
Contact: <sip:[UE-IP]>;expires=90000,
Call-ID: ababab,
CSeq: 25 REGISTER,
Security-Client: port-s, port-c,
Authorization: Digest username = name.private@hims.net, integrity protection: no
Content-Length: 0
```  

DNS Query

```
domain = hims.net
```  

DNS Response

```
Ip = ICSCF-IP
```  

REGISTER

```plaintext
REGISTER sip:hims.net SIP/2.0,
Via: SIP/2.0/UDP pcscf1.vims.net;branch=0aabb,
Max-Forwards: 19,
From: <sip:name@hims.net>;tag=abbb,
To: <sip:name@hims.net>,
Contact: <sip:[UE-IP]>;expires=90000,
Call-ID: ababab,
CSeq: 25 REGISTER,
Content-Length: 0,
Authorization: Digest username = name.private@hims.net, integrity protection: no
```  

User Authorization Request

Query the HSS to assign the S-CSCF.

User Authorization Answer

HSS replies with the S-CSCFs.

Multimedia Authentication Request

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

Multimedia Authentication Answer

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

401 Unauthorized

```
WWW-Authenticate: nonce=RAND-AUTN, ck, ik,
```  

P-CSF 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.

401 Unauthorized

```
WWW-Authenticate: nonce=RAND-AUTH, cl, ik,
```  

Pass the RAND and AUTN values to the subscriber. The CK and IK are removed from the WWW-Authenticate header. The P-CSF sideclient and server ports are also included in the message. The message itself is sent on the standard SIP port 5060.
### 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

### Authenticated IMS Registration

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

2. **REGISTER**
   - Via: pcscfl UE-IP,
   - Contact: UE-IP ue-server-port,
   - Authorization: Digest username = name.private@hims.net response=RES integrity protection: yes,
   - RES

3. **User Authorization Request**
   - Query the HSS to assign the S-CSCF.
   - HSS replies with the S-CSCF.

4. **User Authorization Answer**
   - HSS replies with the S-CSCF Capabilities.

5. **Server Assignment Request**
   - Request subscriber related information from the HSS.

6. **Server Assignment Answer**
   - Received subscriber related information.

7. **200 OK**
   - Via: pcscfl, UE-IP;UE-Server-Port

8. **200 OK**
   - Via: UE-IP;UE-Server-Port

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.

User Authorization Request
- Query the HSS to assign the S-CSCF.
- HSS replies with the S-CSCF.

User Authorization Answer
- HSS replies with the S-CSCF Capabilities.

Server Assignment Request
- Request subscriber related information from the HSS.

Server Assignment Answer
- Received subscriber related information.

The success is relayed back to the P-CSCF.

The IMS registration of the user is now complete.