IMS Registration (IMS Registration for an Unauthenticated User)

Visited Network				Internet	Home Network				EventStudio System Designer 4.0
User Equipment	Visited CN		Visited IMS	DNS Server	Home IMS			Home CN	
Subscriber	SGSN	GGSN	P-CSCF	DNS Server	I-CSCF		S-CSCF	HSS	24-Nov-07 18:36 (Page 1)

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.

GPRS Attach

GMM Attach Request

The terminal powers up and attaches to the GPRS network.

GMM Attach Accept

GMM Attach Complete

PDP Context Activation

Activate PDP Context

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

Create PDP Context Request

Create PDP Context Request

Activate PDP Context Accept

P-CSCF IP Address

The terminal receives an IP address for the PDP context. The terminal also receives the IP address of the P-CSCF. The P-CSCF serves as the initial SIP proxy into the IP Multimedia System (IMS).

Unauthenticated IMS Registration Attempt

Store P-CSCF IP Address

The P-CSCF IP address obtained from the PDP Context Accept message is stored.

Extract user public identity from ISIM

The subscriber extracts the user public identify from the ISIM module of the USIM.

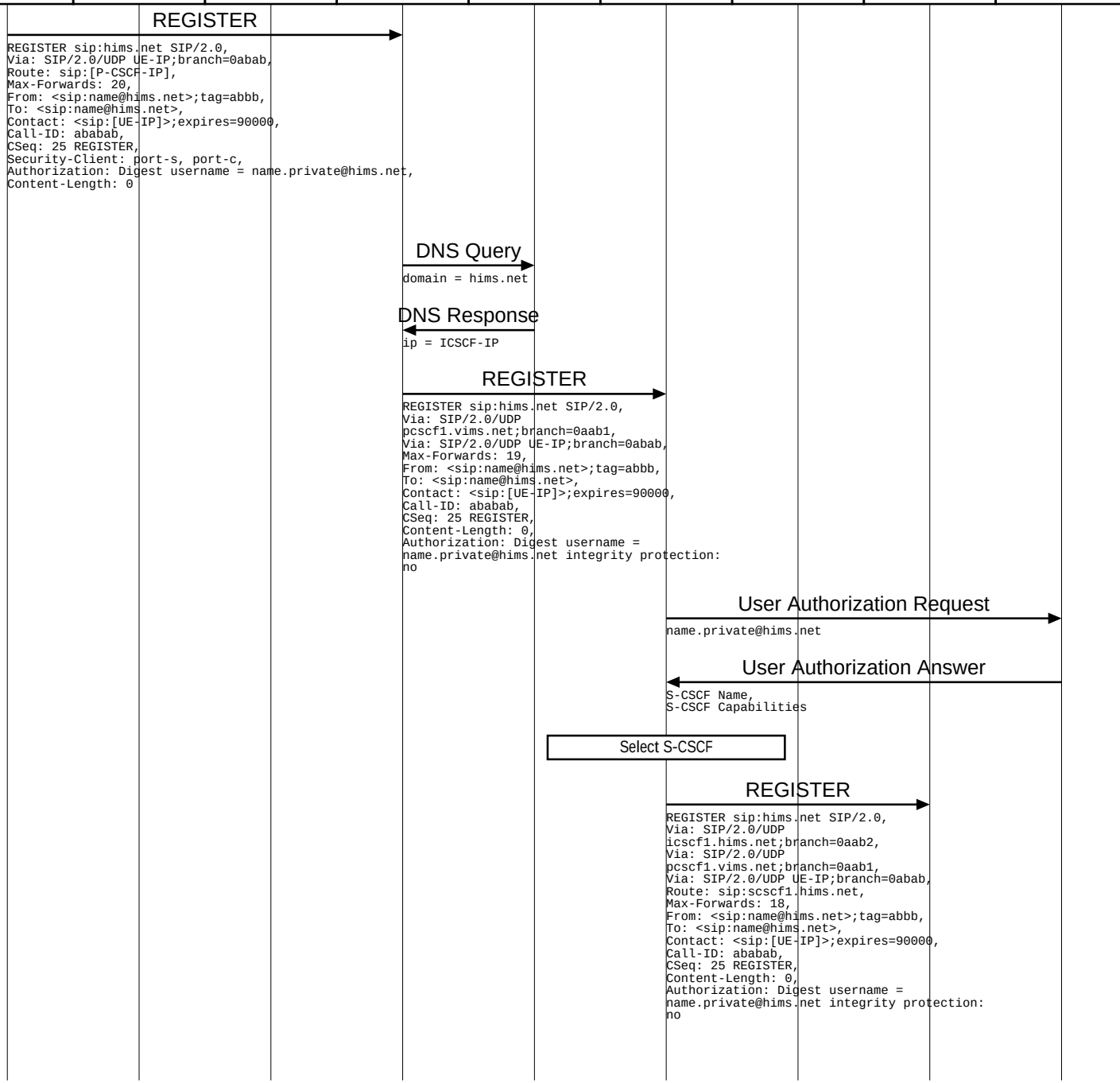
allocate

Subscriber side client and server ports

The SIP terminal allocates the subscriber side client and server ports. These ports will be included in the REGISTER message sent to the P-CSCF.

IMS Registration (IMS Registration for an Unauthenticated User)

Visited Network			Internet	Home Network				EventStudio System Designer 4.0
User Equipment	Visited CN		Visited IMS	DNS Server	Home IMS			Home CN	24-Nov-07 18:36 (Page 2)
Subscriber	SGSN	GGSN	P-CSCF	DNS Server	I-CSCF		S-CSCF	HSS	



The subscriber sends a Register message to inform the network that the specified user public identify (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.

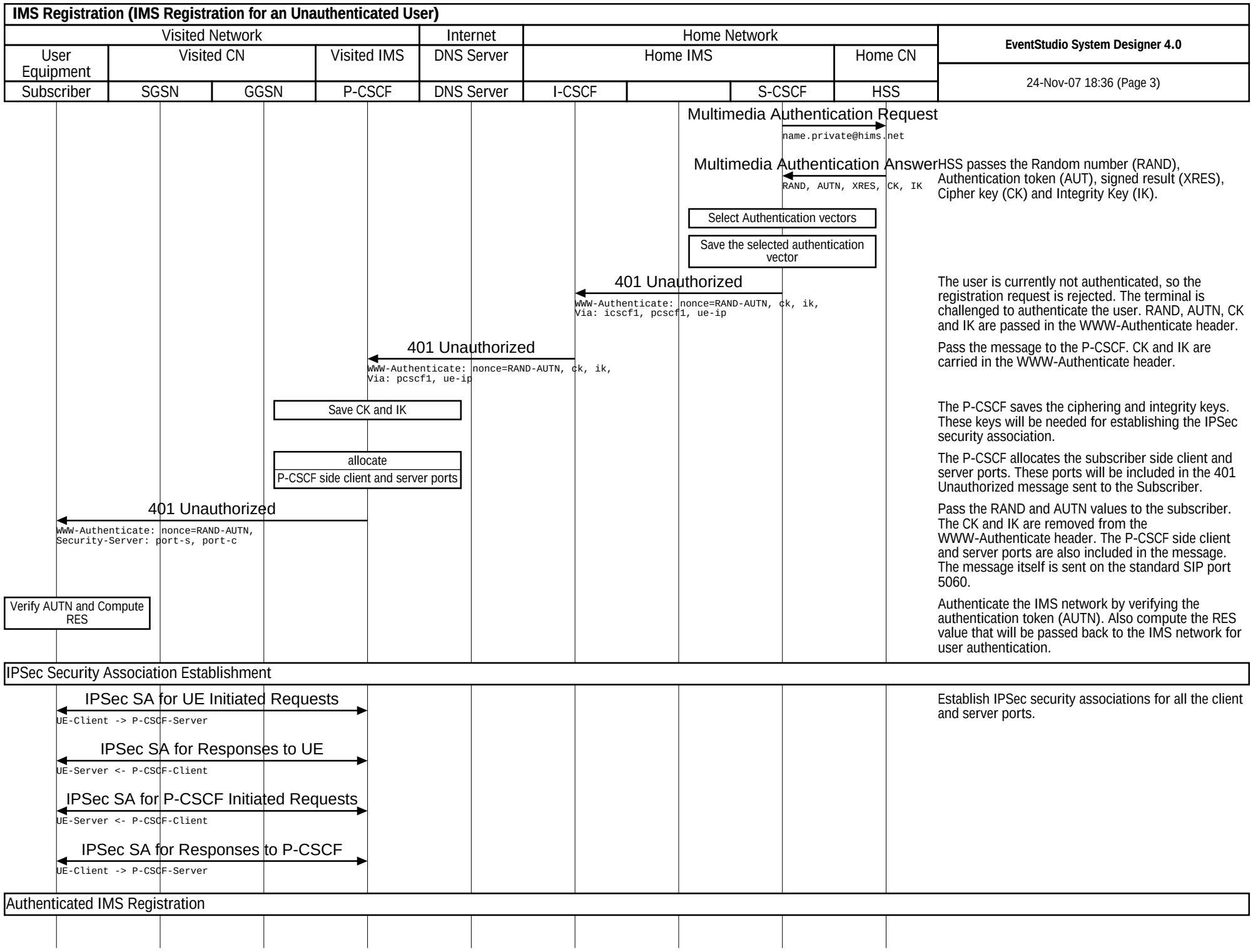
P-CSCF adds a Via header and removes the Route header. The REGISTER message will be routed to the IP address obtained from the DNS response. Note that the integrity protection flag is set to false to signify that the user has not been authenticated.

Query the HSS to assign the S-CSCF.

HSS replies with the S-CSCFs.

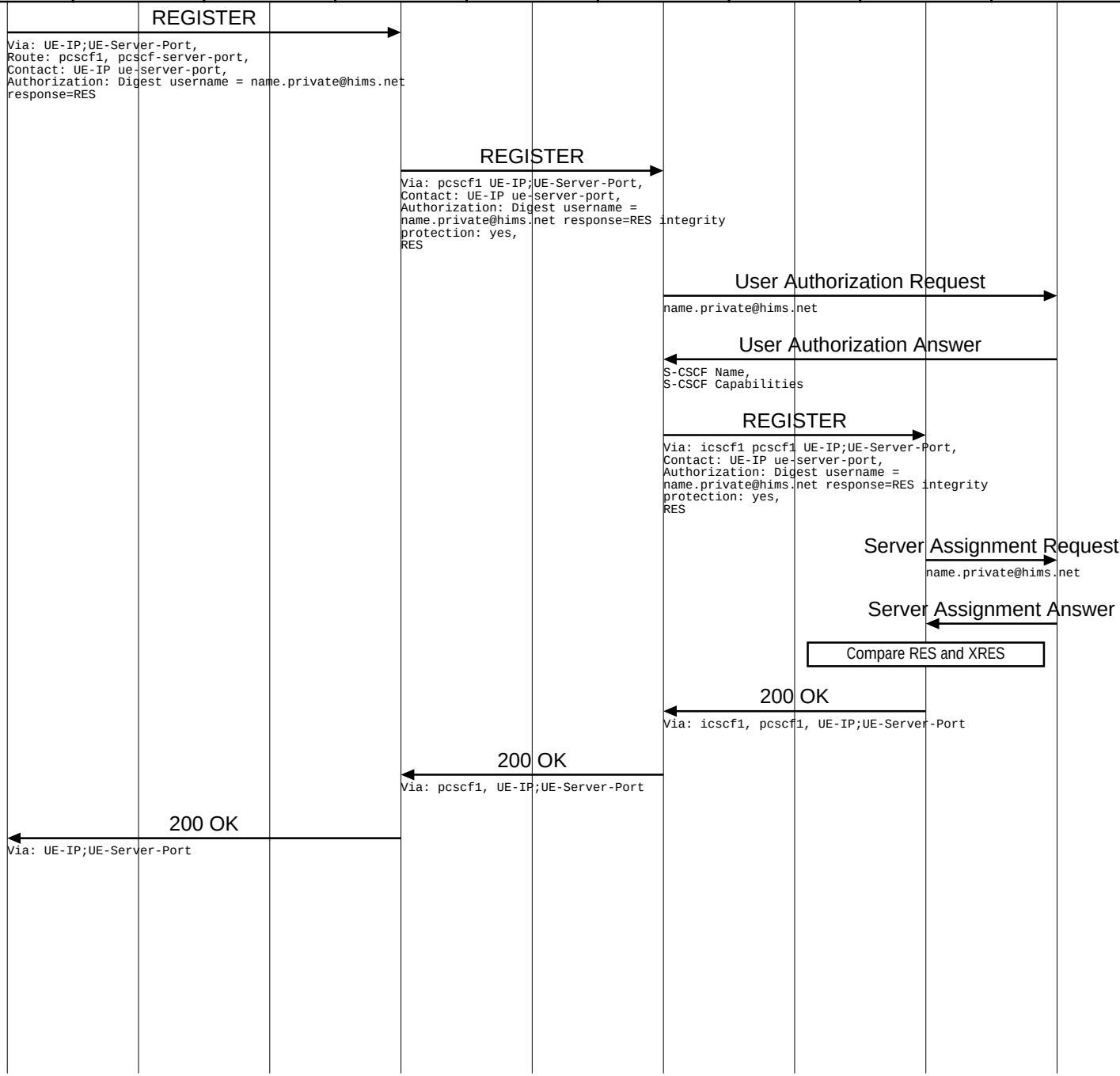
I-CSCF selects the S-CSCF based on the S-CSCF capabilities.

The I-CSCF forwards the REGISTER message to the selected S-CSCF.


IMS Registration (IMS Registration for an Unauthenticated User)
Visited Network
Internet
Home Network
User Equipment
Visited CN
Visited IMS
DNS Server
Home IMS
Home CN
Subscriber
SGSN
GGSN
P-CSCF
DNS Server
I-CSCF
S-CSCF
HSS
Multimedia Authentication Request
name.private@hims.net
Multimedia Authentication Answer
RAND, AUTN, XRES, CK, IK
HSS passes the Random number (RAND), Authentication token (AUT), 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, ck, ik,
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, ck, ik,
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.
allocate
P-CSCF side client and server ports
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.
401 Unauthorized
WWW-Authenticate: nonce=RAND-AUTN,
Security-Server: port-s, port-c
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.
Verify AUTN and Compute RES
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
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
Authenticated IMS Registration

IMS Registration (IMS Registration for an Unauthenticated User)

Visited Network				Internet	Home Network				EventStudio System Designer 4.0
User Equipment	Visited CN		Visited IMS	DNS Server	Home IMS			Home CN	24-Nov-07 18:36 (Page 4)
Subscriber	SGSN	GGSN	P-CSCF	DNS Server	I-CSCF		S-CSCF	HSS	



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.

Query the HSS to assign the S-CSCF.

HSS replies with the S-CSCFs.

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

Request subscriber related information from the HSS.

Received subscriber related information.

Compare the RES reported by the subscriber withe XRES value.

The RES and the XRES matched, so the S-CSCF replies with success.

The success is relayed back to the P-CSCF.

The IMS registration of the user is now complete.