Processor Interfaces (IMS Registration for an Unauthenticated User)									
Visi	ited Network		lı	nternet			letwork		EventStudio System Designer 4.0
User Equipment \	Visited CN	Visited I	IMS DN	S Server	Hom	e IMS	Hom	e CN	24-Nov-07 18:36 (Page 1)
GPRS Attach									
GMM Attach F	Request								The terminal powers up and attaches to the GPRS network.
GMM Attach	Accept								of No fictwork.
GMM Attach C	omplete								
PDP Context Activation									
Activate PDP	Context								Once the attach is completed, the terminal initiates a PDP context activation.
Activate PDP Con									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									
R	EGISTER								The subscriber sends a Register message to
REGISTER sip:1 Via: SIP/2.0/1 Route: sip:[P. Max-Forwards: From: <sip:name(25="" <sip="" abab;="" call-id:="" contact:="" cseq:="" regi!="" security-clies<="" td=""><td>hims het SIP/2 UDP UE-IP;branCSCF-IP], 20, me@hims.net>;t. @hims.net>;t. (UE-IP)>;expi: ab, STFR, nt: port-s, po: : Digest usern. hims.het,</td><td>ch=Oabab, ag=abbb, res=90000, rt-c, ame = dot REC Via pc: Via</td><td>DNS Query main = hims.n NS Respor = ICSCF-IP RE GISTER sip:hi a: SIP/2.0/UD scf1.vims.net a: SIP/2.0/UB</td><td>GISTER ms.net SIP/2 p;branch=0aak p UE-IP;bran</td><td>01,</td><td></td><td></td><td></td><td>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</td></sip:name(>	hims het SIP/2 UDP UE-IP;branCSCF-IP], 20, me@hims.net>;t. @hims.net>;t. (UE-IP)>;expi: ab, STFR, nt: port-s, po: : Digest usern. hims.het,	ch=Oabab, ag=abbb, res=90000, rt-c, ame = dot REC Via pc: Via	DNS Query main = hims.n NS Respor = ICSCF-IP RE GISTER sip:hi a: SIP/2.0/UD scf1.vims.net a: SIP/2.0/UB	GISTER ms.net SIP/2 p;branch=0aak p UE-IP;bran	01,				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
		To: Con Cal CSec Con Autl	om: <sip:namee: 25="" <sip:[11-id:="" <sip:nameeh="" ababab="" eq:="" me.private@hime.private@hime.private@hime.<="" ntact:="" ntent-length:="" regist="" td="" thorization:=""><td>ims.net>, UE-IP]>;expi , ER, 0, Digest usern</td><td>ires=90000 name = grity prot</td><td>ection:</td><td></td><td></td><td>been authenticated.</td></sip:namee:>	ims.net>, UE-IP]>;expi , ER, 0, Digest usern	ires=90000 name = grity prot	ection:			been authenticated.
					User A		ation Real	•	Query the HSS to assign the S-CSCF.
					User /	S-CSCF Na			HSS replies with the S-CSCFs.
				Multi	media A		cation F	· ·	ot
				Mult	timedia	Authent		Answe	rHSS passes the Random number (RAND), Authentication token (AUT), signed result (XRES), Cipher key (CK) and Integrity Key (IK).
			401 Ur W-Authenticata: pcscf1, ue			k, ik,			Pass the message to the P-CSCF. CK and IK are carried in the WWW-Authenticate header.
▼ WWW-Authentica	Unauthorize ate: nonce=RAN. er: port-s, po	ed	a. pcscrl, ue	-1Þ					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.

