3GPP TSG-CN #16 **Tdoc NP-020288**

Marco Island, USA. 5th - 7th June 2002

CR-Form-v5

CHANGE REQUEST

⌘	**24.228**	**CR**	**046**	⌘ **rev**	**~~1~~2** ⌘	Current version:	**5.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☒ ME/UE □ Radio Access Network □ Core Network ☒

Title:	⌘	Adding security parameters to the call flows
Source:	⌘	Nokia, Lucent, mmO2, Siemens, Dynamicsoft, Nortel
Work item code:	⌘	IMS-CCR
Date:	⌘	27~~07~~-05-2002
Category:	⌘	**F**
Release:	⌘	REL-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change:	⌘	The call flows do not contain the ~~'Security-Mechanism'~~necessary security procedures described in draft-ietf-sip-sec-agree-01.txt, ~~header field~~ and the parameters needed for the security association setup.
Summary of change:	⌘	The ~~'Security-Mechanism'~~security procedures ~~header~~ and all the parameters needed for the security association setup are added to the call flows.
Consequences if not approved:	⌘	SA setup related parameters will not be shown in the call flows.

Clauses affected:	⌘	6.2, 6.3, 6.9.2, 6.9.3, 16.2, 16.3	
Other specs affected:	⌘	□ Other core specifications □ Test specifications □ O&M Specifications	⌘
Other comments:	⌘		

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/3G_Specs/CRs.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

6.2 Registration signalling: user not registered

Figure 6.2-1 shows the registration signalling flow for the scenario when the user is not registered. For the purpose of this registration signalling flow, the subscriber is considered to be roaming. This flow also shows the authentication of the private user identity. In this signalling flow, the home network does not have network configuration hiding active.

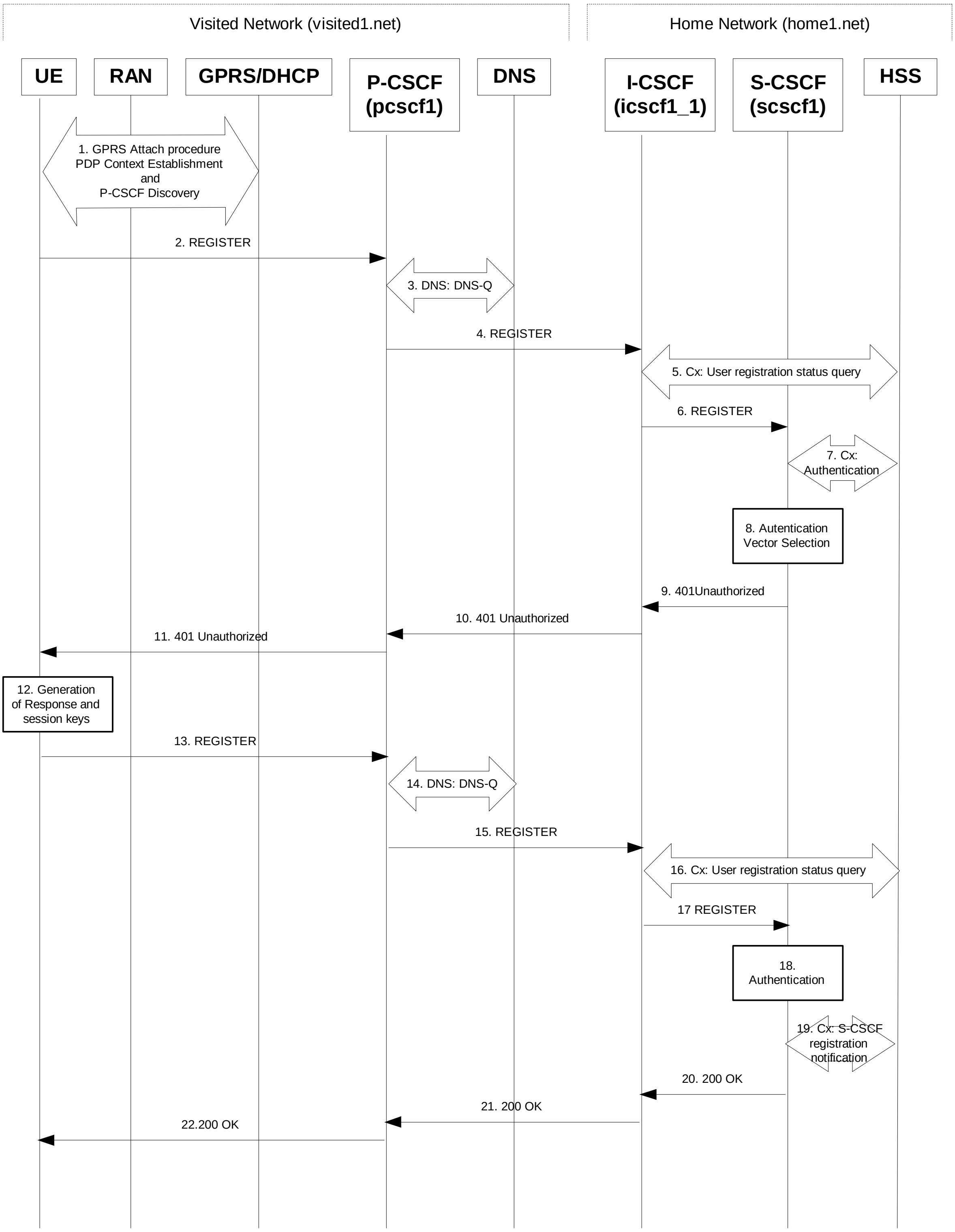

Figure 6.2-1: Registration signalling: user not registered

- 1. **GPRS Attach / PDP Context Establishment and P-CSCF Discovery (UE to GPRS)**
  - This signalling flow is shown to indicate prerequisites for the registration signalling.
  - See subclause 5.2 for details.
- 2. **REGISTER request (UE to P-CSCF) – see example in table 6.2-2**
  - The purpose of this request is to register the user's SIP URI with a S-CSCF in the home network. This request is routed to the P-CSCF because it is the only SIP server known to the UE. In the following SIP request, the Contact field contains the user's host address.
  - The P-CSCF will perform two actions, binding and forwarding. The binding is between the User's SIP address (user1_public1@home1.net) and the host (terminal) address ([5555::aaa:bbb:ccc:ddd]) which was acquired during PDP context activation process.

[Editor's note: The security mode set-up procedure supports the negotiation of different protection mechanisms. This will involve the addition of a "security-setup" field to the SIP REGISTER request and the REGISTER response performing the authentication challenge containing the parameters:

- list of Authentication (integrity} algorithms, and optionally list of encryption (confidentiality) algorithms
- SA-ID that is used to uniquely identify the SA at the receiving side.
- Key length: the length of encryption and authentication (integrity) keys is 128 bits.

The exact format and use for the security mode setup is being worked through IETF and is FFS]

Table 6.2-2: REGISTER request (UE to P-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>
Contact: sip:[5555::aaa:bbb:ccc:ddd]
Call-ID: apb03a0s09dkjdfglkj49111
Authorization: eap eap-p=base64(user1_private1@home1.net)
Security-Client: ipsec-man; alg=HMAC-SHA1; SPI_U_UDP=12345678; SPI_U_TCP=23456789; Port_U_UDP=1357; Port_U_TCP=1358
Require: sec-agree
CSeq: 1 REGISTER
Expires: 7200
Content-Length: 0
```

Request-URI: The Request-URI (the URI that follows the method name, "REGISTER", in the first line) indicates the destination domain of this REGISTER request. The rules for routing a SIP request describe how to use DNS to resolve this domain name ("home1.net") into an address or entry point into the home operator's network (the I-CSCF). This information is stored in the USIM.

Via: IPv6 address of the SIP session allocated during the PDP Context Activation process.

From: This indicates the public user identity originating the REGISTER request. The public user identity may be obtained from the USIM.

To: This indicates the public user identity being registered. This is the identity by which other parties know this subscriber. It may be obtained from the USIM.

Contact: This indicates the point-of-presence for the subscriber - the IP address of the UE. This is the temporary point of contact for the subscriber that is being registered. Subsequent requests destined for this subscriber will be sent to this address. This information is stored in the P-CSCF and S-CSCF.

Authorization: It carries authentication information. The private user identity (user1_private1@home1.net) is carried in the user ID field of the extensible authentication protocol (EAP).

Security-Client:

- lists the supported algorithm(s) by the UE. It encapsulates the detail of each mechanism to be negotiated.
- SPI value is the UE's SA_ID. Two SA_IDs are inserted, one for the SA using transport UDP, the other for TCP. The UE needs to choose the SA_IDs in such a way that those uniquely identify the inbound SAs at the UE.
- Port_U_UDP and Port_U_TCP contain the port number the UE would like receive the SA protected messages.

NOTE: The actual Authorization header value may look like this as it is in base64 form:
Authorization: eap eap-p=QWxhZGRpbjpvcGVuIHNlc2FtZQ==

- Upon receiving this request the P-CSCF will set it's SIP registration timer for this UE to the Expires time in this request.

- 3. **DNS: DNS-Q**
  - Based on the user's URI, the P-CSCF determines that UE is registering from a visiting domain and performs a DNS query to locate the I-CSCF in the home network. The look up in the DNS is based on the address specified in the Request URI.
  - The P-CSCF sends the REGISTER request - after local processing - to the address indicated in the Request-URI. When forwarding the REGISTER request the P-CSCF needs to specify the protocol, port number and IP address of the I-CSCF server in the home network to which to send the REGISTER request. The P-CSCF tries to find this information by querying the DNS. Since the Request-URI does not specify the transport protocol, the P-CSCF selects the UDP.

Table 6.2-3a: DNS: DNS Query (P-CSCF to DNS)

```
OPCODE=SQUERY
QNAME=_sip._udp.registrar.home1.net, QCLASS=IN, QTYPE=SRV
```

- The DNS records are retrieved according to RFC 2782 [4].

Table 6.2-3b: DNS Query Response (DNS to P-CSCF)

```
OPCODE=SQUERY, RESPONSE, AA
QNAME=_sip._udp.registrar.home1.net, QCLASS=IN, QTYPE=SRV

_sip._udp.registrar.home1.net        0 IN SRV 1 10 5060 icscf1_p.home1.net
                                        0 IN SRV 1  0 5060 icscf7_p.home1.net

icscf1_p.home1.net                 0 IN AAAA     5555::aba:dab:aaa:daa
icscf7_p.home1.net                 0 IN AAAA     5555::a1a:b2b:c3c:d4d
```

•

- In the Answer field of the query-response each I-CSCF is identified by its host domain name. The returned SRV Resource Records (RRs) are merged and ordered, and the selection technique (employing the Priority and Weight parameters returned in the RRs) as specified in RFC 2782 [4] is used to select the I-CSCF (i.e. the icscf1_p.home1.net). Since the Additional Data field of the query-response also contains the IP address of the selected I-CSCF (i.e. 5555::aba:dab:aaa:daa), a new query to the DNS is not required.
- Once the IP address of the I-CSCF is obtained, the P-CSCF forwards the REGISTER request to this IP address (i.e. 5555::aba:dab:aaa:daa) using the UDP protocol and port number 5060.

- 4. **REGISTER request (P-CSCF to I-CSCF) - see example in table 6.2-4**
  - The P-CSCF needs to be in the path for all mobile originated and mobile terminated requests for this user. To ensure this, the P-CSCF adds itself to the Path header value for future requests.
  - The P-CSCF binds the public user identity under registration to the Contact header supplied by the user.

- The P-CSCF adds also the Roaming-Info header (if not present). The P-CSCF adds the *vnid* parameter with the contents of the identifier of the P-CSCF network. This may be the visited network domain name or any other identifier that identifies the visited network at the home network.

- This signalling flow shows the REGISTER request being forward from the P-CSCF to the I-CSCF in the home domain.

- P-CSCF removes the Security-Client and Require: sec-agree headers prior to forwarding the message.

Table 6.2-4: REGISTER request (P-CSCF to I-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:pcscf1.visited1.net>
Proxy-require: path
Require: path
Roaming-Info: vnid="Visited Network Number 1"
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

Path: This is the address of the P-CSCF and is included to inform the S-CSCF where to route terminating sessions.

Require:/Proxy-Require: These headers are included to ensure that the recipient correctly handles the Path header. If the recipient does not support the path header, a response will be received with a status code of 420 and an Unsupported header indicating "path". Such a response indicates a misconfiguration of the routing tables and the request has been routed outside the IM CN subsystem.

Roaming-Info: The *vnid* parameter contains the identifier of the P-CSCF network at the home network.

- 5. **Cx: User registration status query procedure**

  - The I-CSCF makes a request for information related to the Subscriber registration status by sending the private user identity, public user identity and visited domain name to the HSS. The HSS returns the S-CSCF required capabilities and the I-CSCF uses this information to select a suitable S-CSCF.

  - For detailed message flows see 3GPP TS 29.228.

  - Table 6.2-5a provides the parameters in the REGISTER request (flow 4) which are sent to the HSS.

Table 6.2-5a Cx: User registration status query procedure (I-CSCF to HSS)

Message source & destination	Cx Information element name	Information Source in REGISTER	Description
I-CSCF to HSS	Private User Identity	Authorization:	The Private User Identity is encoded according to the Authorization protocol.
	Public User Identity	To:	Identity which is used to communicate with other users
	Visited Network Identifier	Roaming Info: vnid	This information indicates the network identifier of the visited network

- 6. **REGISTER request (I-CSCF to S-CSCF) – see example in table 6.2-6**

- I-CSCF does not modify the Path header.

- This signalling flow forwards the REGISTER request from the I-CSCF to the S-CSCF selected.

Table 6.2-6: REGISTER request (I-CSCF to S-CSCF)

```
REGISTER sip:scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=351g45.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:pcscf1.visited1.net>
Proxy-require:
Require:
Roaming-Info:
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

Path: The S-CSCF stores the contents of the Path headers and uses these addresses for routing mobile terminated sessions.

- Upon receiving this request the S-CSCF may set its SIP registration timer for this UE to the Expires time in this request or the S-CSCF may assign another registration timer for this registration

- 7. **Cx: Authentication procedure**

  - On receiving a REGISTER request from an unauthenticated user, the S-CSCF requires at least one authentication vector to be used in the challenge to the user. If a valid AV is not available, then the S-CSCF requests at least one AV from the HSS.

  - The S-CSCF indicates to the HSS that it has been assigned to serve this user.

  - For detailed message flows see 3GPP TS 29.228.

  - Table 6.2-7a provides the parameters in the REGISTER request (flow 6) which are sent to the HSS.

Table 6.2-7a Cx: S-CSCF authentication information procedure (S-CSCF to HSS)

Message source & destination	Cx Information element name	Information Source in REGISTER	Description
S-CSCF to HSS	Public User Identify	To:	Identity which is used to communicate with other users
	Private User Identity	Authorization:	The Private User Identity is encoded according to the Authorization protocol.
	S-CSCF Name	Request-URI:	This information element contains the name of the S-CSCF. The presence of this IE indicates that the user has not been authenticated yet by the S-CSCF

- 8. **Authentication vector selection**

  - The S-CSCF selects an authentication vector for use in the authentication challenge. For detailed description of the authentication vector, see 3GPP TS 33.203.

NOTE 1: The authentication vector may be of the form as in 3GPP TS 33.203 (if IMS AKA is the selected authentication scheme):

- - AV = $\text{RAND}_n||\text{AUTN}_n||\text{XRES}_n||\text{CK}_n||\text{IK}_n$ where:
  - - RAND: random number used to generate the XRES, CK, IK, and part of the AUTN. It is also used to generate the RES at the UE.
  - - AUTN: Authentication token (including MAC and SQN).
  - - XRES: Expected (correct) result from the UE.
  - - CK: Cipher key (optional).
  - - IK: Integrity key.

- 9. **401 Unauthorized response (S-CSCF to I-CSCF) - see example in table 6.2-9**
  - The authentication challenge is sent in the 401 Unauthorized response towards the UE.

Table 6.2-9: 401 Unauthorized response (S-CSCF to I-CSCF)

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=351g45.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>; tag=5ef4
Call-ID: apb03a0s09dkjdfglkj49111
WWW-Authenticate: eap eap-p=base64(user1_private1@home1.net, RAND, AUTN)
CSeq: 1 REGISTER
Content-Length: 0
```

NOTE 2: The actual WWW-Authenticate header value may look like this as it is in base64 form:
WWW-Authenticate: eap eap-p=QWxh4ZGRpb2jpvcGVuNlctZQ==

Editor's Note: The mechanism to transport the session keys (IK and optionally, CK) from the S-CSCF to the P-CSCF is FFS.

- 10. **401 Unauthorized response (I-CSCF to P-CSCF) - see example in table 6.2-10**
  - The authentication challenge is sent in the 401 Unauthorized response towards the UE.

Table 6.2-10: 401 Unauthorized response (I-CSCF to P-CSCF)

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
WWW-Authenticate:
CSeq:
Content-Length:
```

Editor's Note: The mechanism to transport the session keys (IK and optionally, CK) from the S-CSCF to the P-CSCF is FFS.

- 11. **401 Unauthorized response (P-CSCF to UE) - see example in table 6.2-11**
  - The P-CSCF removes any keys received in the 401 Unauthorized response and forwards the rest of the response to the UE.

Table 6.2-11: 401 Unauthorized response (P-CSCF to UE)

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
WWW-Authenticate: eap eap-p=base64(user1_private1.home1.net, RAND, AUTN)
Security-Server: ipsec-man; q=0.1; alg=HMAC-SHA1; SPI_P_UDP=87654321; SPI_P_TCP=98765432; Port_P_UDP=7531;
Port_P_TCP=8642
CSeq:
Content-Length:
```

Security-Server:

q is the preference value, 0.1 means IPsec is the first preferred choice. The q value represents only relative degradation of all mechanisms listed here. The lower value, the higher prority.

- 12. **Generation of response and session keys at UE**

  - Upon receiving the Unauthorised response, the UE extracts the MAC and the SQN from the AUTN. The UE calculates the XMAC and checks that XMAC matches the received MAC and that the SQN is in the correct range. If both these checks are successful the UE calculates the response, RES, and also computes the session keys IK and CK. The RES is put into the Authorization header and sent back to the registrar in the REGISTER request.

- 13. **REGISTER request (UE to P-CSCF) - see example in table 6.2-13**

Table 6.2-13 REGISTER request (UE to P-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>
Contact: <sip:[5555::aaa:bbb:ccc:ddd]>
Call-ID: apb03a0s09dkjdfglkj49112
Authorization: eap eap-p=base64(user1_private1@home1.net, RES)
Security-Verify: ipsec-man; q=0.1; alg=HMAC-SHA1; SPI_P_UDP=87654321; SPI_P_TCP=98765432; Port_P_UDP=7531;
Port_P_TCP=8642
CSeq: 2 REGISTER
Expires: 7200
Content-Length: 0
```

Authorization: This carries the response to the authentication challenge received in step 11 along with the private user identity both encoded in base64 format.

This message is protected by the IPsec SA negotiated.

- 14. **DNS: DNS-Q**

  - Based on the user's URI, the P-CSCF determines that UE is registering from a visiting domain and performs a DNS query to locate the I-CSCF in the home network. The look up in the DNS is based on the address specified in the Request URI.

  - The P-CSCF sends the REGISTER request - after local processing - to the address indicated in the Request-URI. When forwarding the REGISTER request the P-CSCF needs to specify the protocol, port number and IP address of the I-CSCF server in the home network to which to send the REGISTER request. The P-CSCF tries to find this information by querying the DNS. Since the Request-URI does not specify the transport protocol the, P-CSCF selects the UDP.

Table 6.2-14a DNS: DNS Query (P-CSCF to DNS)

```
OPCODE=SQUERY
QNAME=__sip._udp.registrar.home1.net, QCLASS=IN, QTYPE=SRV
```

-

  - The DNS records are retrieved according to RFC 2782 [4].

Table 6.2-14b DNS Query Response (DNS to P-CSCF)

```
OPCODE=SQUERY, RESPONSE, AA
QNAME=__sip._udp.registrar.home1.net, QCLASS=IN, QTYPE=SRV

_sip._udp.registrar.home1.net        0 IN SRV 1 10 5060 icscf1_p.home1.net
                                        0 IN SRV 1  0 5060 icscf7_p.home1.net

icscf1_p.home1.net                 0 IN AAAA     5555::aba:dab:aaa:daa
icscf7_p.home1.net                 0 IN AAAA     5555::a1a:b2b:c3c:d4d
```

  - In the Answer field of the query-response each I-CSCF is identified by its host domain name. The returned SRV Resource Records (RRs) are merged and ordered, and the selection technique (employing the Priority and Weight parameters returned in the RRs) as specified in RFC2782 [4] is used to select the I-CSCF (i.e. the icscf1_p.home1.net). Since the Additional Data field of the query-response also contains the IP address of the selected I-CSCF (i.e. 5555::aba:dab:aaa:daa), a new query to the DNS is not required.

  - Once the IP address of the I-CSCF is obtained, the P-CSCF forwards the REGISTER request to this IP address (i.e. 5555::aba:dab:aaa:daa) using the UDP protocol and port number 5060.

- 15. **REGISTER request (P-CSCF to I-CSCF) - see example in table 6.2-15**

  - This signalling flow shows the REGISTER request being forwarded from the P-CSCF to the I-CSCF in the home domain.

Table 6.2-15 REGISTER request (P-CSCF to I-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:pcscf1.visited1.net>
Proxy-require: path
Require: path
Roaming-Info: vnid="Visited Network Number 1"
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

Path: This is the address of the P-CSCF and is included to inform the S-CSCF where to route terminating sessions.

- 16. **Cx: User registration status query procedure**

  - The I-CSCF requests information related to the Subscriber registration status by sending the private user identity, public user identity and visited domain name to the HSS. The HSS returns the S-CSCF name which was previously selected in step 5 (Cx: User registration status query procedure).

  - For detailed message flows see 3GPP TS 29.228.

  - Table 6.2-16a provides the parameters in the REGISTER request (flow 15), which are sent to the HSS.

Table 6.2-16a Cx: User registration status query procedure (I-CSCF to HSS)

Message source & destination	Cx Information element name	Information Source in REGISTER	Description

I-CSCF to HSS	Private User Identity	Authorization:	The Private User Identity is encoded according to the Authorization protocol.
	Public User Identity	To:	Identity which is used to communicate with other users
	Visited Network Identifier	Roaming-Info: vnid	This information indicates the network identifier of the visited network

- 17. **REGISTER request (I-CSCF to S-CSCF) - see example in table 6.2-17**
  - This signalling flow forwards the REGISTER request from the I-CSCF to the S-CSCF.

Table 6.2-17: REGISTER request (I-CSCF to S-CSCF)

```
REGISTER sip:scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=351g45.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:pcscf1.visited1.net>
Proxy-require:
Require:
Roaming-Info:
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

Path: The S-CSCF stores the contents of the Path headers and uses these addresses for routing mobile terminated sessions.

- 18. **Authentication**
  - Upon receiving the REGISTER request carrying the authentication response, RES, the S-CSCF checks that the user's active, XRES matches the received RES. If the check is successful then the user has been authenticated and the public user identity is registered in the S-CSCF.
- 19. **Cx: S-CSCF registration notification procedure**
  - On registering a user the S-CSCF informs the HSS that the user has been registered at this instance. Upon being requested by the S-CSCF , the HSS will also include the user profile in the response sent to the S-CSCF.
  - For detailed message flows see 3GPP TS 29.228.
  - Table 6.2-19a provides the parameters in the REGISTER request (flow 17), which are sent to the HSS.

Table 6.2-19a Cx: S-CSCF registration notification procedure (S-CSCF to HSS)

Message source & destination	Cx Information element name	Information Source in REGISTER	Description
S-CSCF to HSS	Public User Identify	To:	Identity which is used to communicate with other users

	Private User Identity	Authorization:	The Private User Identity is encoded according to the Authorization protocol. Unique identity in IMS which is used by network to authenticate this user
	S-CSCF name	Request-URI:	This information indicates the serving CSCF's name of that user

- 20. **200 OK response (S-CSCF to I-CSCF) - see example in table 6.2-20**
  - The S-CSCF sends acknowledgement to the I-CSCF indicating that Registration was successful.

Table 6.2-20: 200 OK response (S-CSCF to I-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=351g45.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:scscf1.home1.net>, <sip:pcscf1.visited1.net>
From:
To:
Call-ID:
Contact: sip:[5555::aaa:bbb:ccc:ddd]
CSeq:
Date: Wed, 11 July 2001 08:49:37 GMT
Expires: 7200
Content-Length:
```

Path: The S-CSCF inserts its own name to the front of the list.

- 21. **200 OK response (I-CSCF to P-CSCF) - see example in table 6.2-21**
  - The I-CSCF forwards acknowledgement from the S-CSCF to the P-CSCF indicating that Registration was successful.

Table 6.2-21: 200 OK response (I-CSCF to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:scscf1.home1.net, <sip:pcscf1.visited1.net>
From:
To:
Call-ID:
Contact:
CSeq:
Date:
Expires:
Content-Length:
```

- 22. **200 OK response (P-CSCF to UE) - see example in table 6.2-22**
  - The P-CSCF removes its address from the Path header, reverses the order of the fields, saves the resulting Path header and associates it with the UE. The P-CSCF then removes the Path header from the 200 OK response. The P-CSCF then forwards acknowledgement from the I-CSCF to the UE indicating that Registration was successful.

Table 6.2-22: 200 OK response (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
Contact:
```

```
CSeq:
Date:
Expires:
Content-Length:
```

6.3 Registration signalling: reregistration - user currently registered

For the purpose of the reregistration signalling flow shown in figure 6.3-1, the subscriber is considered to be roaming. The HSS information indicates that the subscriber is registered and authenticated, and that the S-CSCF has been allocated to this subscriber. In this signalling flow, the home network does not have network configuration hiding active. This flow also shows the authentication of the private user identity.

This signalling flow assumes:

- 1. That the same PDP Context allocated during the initial registration scenario is still used for reregistration. For the case when the UE does not still have an active PDP context then PDP context procedures from subclause 16.2 is completed first.

Editor's Note: If the same PDP-Context is not available, is it guaranteed that the UE will get back the same IP address at this point? If this is not possible, would there be a problem with the binding in the P-CSCF (user_public1@home1.net and [5555::aaa:bbb:ccc:ddd])?

- 2. The DHCP procedure employed for P-CSCF discovery is not needed.

- 3. The S-CSCF selection procedure invoked by the I-CSCF is not needed.

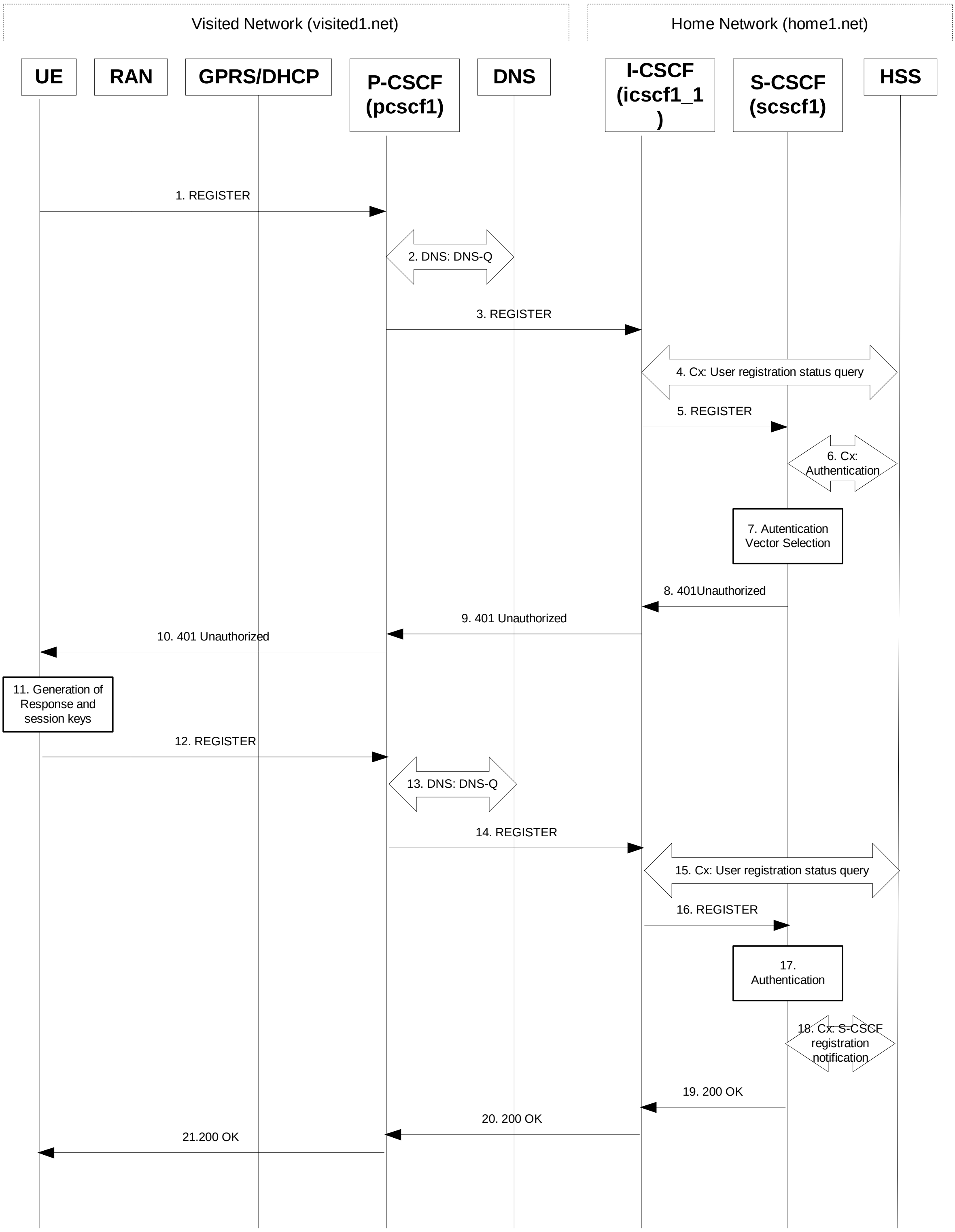

Figure 6.3-1: Reregistration when UE roaming

- 1. **REGISTER request (UE to P-CSCF) - see example in table 6.3-1**
  - The registration expires in the UE. The UE reregisters by sending a new REGISTER request. This request is sent to the same P-CSCF with which the UE initially registered. The P-CSCF maintains the same binding

between the public user address (user1_public1@home1.net) and the host (terminal) address ([5555::aaa:bbb:ccc:ddd]) which it established during the original registration.

Table 6.3-1: REGISTER request (UE to P-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>
Contact: sip:[5555::aaa:bbb:ccc:ddd]
Call-ID: apb03a0s09dkjdfglkj49111
Authorization: eap eap-p=base64(user1_private1@home1.net)
Security-Client: ipsec-man; alg=HMAC-SHA1; SPI_U_UDP=12345678; SPI_U_TCP=23456789; Port_U_UDP=1357; Port_U_TCP=1358
Require: sec-agree
CSeq: 3 REGISTER
Expires: 7200
Content-Length: 0
```

- The header field usage is the same as for the initial registration scenario:

From: This indicates the public user identity originating the REGISTER request. The public user identity may be obtained from the USIM.

To: This indicates public user identity being registered. This is the identity by which other parties know this subscriber.

Contact: This indicates the point-of-presence for the subscriber – the IP address of the UE. This is the temporary identifier for the subscriber that is being registered. Subsequent requests destined for this subscriber will be sent to this address. This information is stored in the P-CSCF and the S-CSCF.

Authorization: It carries authentication information. The private user identity (user1_private1@home1.net) is carried in the user ID field of the extensible authentication protocol (EAP).

NOTE 1: The actual Authorization header value may look like this as it is in base64 form:
Authorization: eap eap-p=QWxhZGRpbjpvcGVuIHNlc2FtZQ==

Request-URI: The Request-URI (the URI that follows the method name, "REGISTER", in the first line) indicates the destination domain of this REGISTER request. The rules for routing a SIP request describe how to use DNS to resolve this domain name ("home1.net") into an address or entry point into the home operator's network (the I-CSCF). This information is stored in the USIM.

- Upon receiving this request the P-CSCF will detect that it already has a registration record for this UE and will reset it's SIP registration timer for this UE to the Expires time in this request.

- 2. **DNS: DNS-Q**

  - Based on the user's URI, the P-CSCF determines that UE is registering from a visiting domain and performs a DNS query to locate the I-CSCF in the home network. The look up in the DNS is based on the address specified in the Request URI. The DNS provides the P-CSCF with an address of the I-CSCF in the home network. The P-CSCF must not use the I-CSCF address cached as a result of the previous registration.

- 3. **REGISTER request (P-CSCF to I-CSCF) - see example in table 6.3-3**

  - This signalling flow shows the REGISTER request being forward from the P-CSCF to the I-CSCF in the home domain.

Table 6.3-3 REGISTER request (P-CSCF to I-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:pcscf1.visited1.net>
Proxy-require: path
Require: path
Roaming-Info: vnid="Visited Network Number 1"
```

```
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

Path: This is the address of the P-CSCF and is included to inform the S-CSCF where to route terminating sessions.

Require:/Proxy-Require: These headers are included to ensure that the recipient correctly handles the Path header. If the recipient does not support the path header, a response will be received with a status code of 420 and an Unsupported header indicating "path". Such a response indicates a misconfiguration of the routing tables and the request has been routed outside the IM CN subsystem.

Roaming-Info: The *vnid* parameter contains the identifier of the P-CSCF network at the home network.

- 4. **Cx: User registration status query procedure**
  - The I-CSCF requests information related to the Subscriber registration status by sending the private user identity, public user identity and visited domain name to the HSS. Because the user has registered, the HSS returns the I-CSCF with the S-CSCF address for the subscriber.
  - For detailed message flows see 3GPP TS 29.228.
  - For the parameters in the REGISTER request (flow 3) which need to be sent to HSS, see table 6.2-5a.
  - Table 6.3-4a provides the parameters in the REGISTER request (flow 5), which are obtained from the information sent back from the HSS.

Table 6.3-4a Cx: User registration status query procedure (HSS to I-CSCF)

Message source & destination	Cx Information element name	Mapping to SIP header in REGISTER	Description
HSS to I-CSCF	S-CSCF name	Request-URI:	This information indicates the serving CSCF’s name of that user

- 5. **REGISTER request (I-CSCF to S-CSCF) - see example in table 6.3-5**
  - This signalling flow forwards the REGISTER request from the I-CSCF to the S-CSCF selected. The Request-URI is changed to the address of the S-CSCF.

Table 6.3-5: REGISTER request (I-CSCF to S-CSCF)

```
REGISTER sip:scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=351g45.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:pcscf1.visited1.net>
Proxy-require:
Require:
Roaming_Info:
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

Path: The S-CSCF stores the contents of the Path headers and uses these addresses for routing mobile terminated sessions.

Roaming-Info: The *vnid* parameter contains the identifier of the P-CSCF network at the home network.

- Upon receiving this request the S-CSCF will detect that it already has a registration record for this UE and will reset it's SIP registration timer for this UE to the Expires time in this request.

- **6. Cx: Authentication procedure**

  - On receiving a REGISTER request from a registered user, the S-CSCF requires at least one authentication vector to be used in the challenge to the user. If a valid AV is not available, then the S-CSCF requests at least one AV from the HSS.

  - For detailed message flows see 3GPP TS 29.228.

  - Table 6.3-6a provides the parameters in the REGISTER request (flow 5) which need to been sent to HSS.

Table 6.3-6a Cx: S-CSCF authentication information procedure (S-CSCF to HSS)

Message source & destination	Cx Information element name	Information Source in REGISTER	Description
S-CSCF to HSS	Public User Identify	To:	Identity which is used to communicate with other users
	Private User Identity	Authorization:	The Private User Identity is encoded according to the Authorization protocol.
	S-CSCF name	Request-URI:	This information indicates the serving CSCF's name of that user

- 7. **Authentication vector selection**

  - The S-CSCF selects an authentication vector for use in the authentication challenge. For detailed description of the authentication vector, see 3GPP TS 33.203.

NOTE 2: The authentication vector may be of the form as in 3GPP TS 33.203 (if IMS AKA is the selected authentication scheme):

- - AV = $RAND_n||AUTN_n||XRES_n||CK_n||IK_n$ where:

  - - RAND: random number used to generate the XRES, CK, IK, and part of the AUTN. It is also used to generate the RES at the UE.

  - - AUTN: Authentication token (including MAC and SQN).

  - - XRES:Expected (correct) result from the UE.

  - - CK: Cipher key (optional).

  - - IK: Integrity key.

- 8. **401 Unauthorized response (S-CSCF to I-CSCF) - see example in table 6.3-8**

  - The authentication challenge is sent in the 401 Unauthorized response towards the UE.

Table 6.3-8: 401 Unauthorized response (S-CSCF to I-CSCF)

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=351g45.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>; tag=5ef4
Contact: <sip:[5555::aaa:bbb:ccc:ddd]>
Call-ID: apb03a0s09dkjdfglkj49111
WWW-Authenticate: eap eap-p=base64(user1_private1@home1.net, RAND, AUTN)
CSeq: 1 REGISTER
Expires: 7200
Content-Length: 0
```

NOTE 3: The actual WWW-Authenticate header value may look like this as it is in base64 form:
WWW-Authenticate: eap eap-p=QWxh4ZGRpb2jpvcGVuNlctZQ==

Editor's Note: The mechanism to transport the session keys (IK and optionally, CK) from the S-CSCF to the P-CSCF is FFS.

- 9. **401 Unauthorized response (I-CSCF to P-CSCF) - see example in table 6.3-9**
  - The authentication challenge is sent in the 401 Unauthorized response towards the UE.

Table 6.3-9: 401 Unauthorized response (I-CSCF to P-CSCF)

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Contact:
Call-ID:
WWW-Authenticate:
CSeq:
Expires:
Content-Length:
```

Editor's Note: The mechanism to transport the session keys (IK and optionally, CK) from the S-CSCF to the P-CSCF is FFS

- 10. **401 Unauthorized response (P-CSCF to UE) - see example in table 6.3-10**
  - The P-CSCF removes any keys received in the 401 Unauthorized response and forwards the rest of the response to the UE.

Table 6.3-10: 401 Unauthorized response (P-CSCF to UE)

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Contact:
Call-ID:
WWW-Authenticate: eap eap-p=base64(user1_private1.home1.net, RAND, AUTN)
Security-Server: ipsec-man; q=0.1; alg=HMAC-SHA1; SPI_P_UDP=87654321; SPI_P_TCP=98765432; Port_P_UDP=7531;
Port_P_TCP=8642
CSeq:
Expires:
Content-Length:
```

- 11. **Generation of response and session keys at UE**
  - Upon receiving the Unauthorised response, the UE extracts the MAC and the SQN from the AUTN. The UE calculates the XMAC and checks that XMAC matches the received MAC and that the SQN is in the correct range. If both these checks are successful the UE calculates the response, RES, and also computes the session

keys IK and CK. The RES is put into the Authorization header and sent back to the registrar in a REGISTER request.

- 12. **REGISTER request (UE to P-CSCF) - see example in table 6.3-12**

Table 6.3-12: REGISTER request (UE to P-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>
Contact: <sip:[5555::aaa:bbb:ccc:ddd]>
Call-ID: apb03a0s09dkjdfglkj49112
Authorization: eap eap-p=base64(user1_private1@home1.net, RES)
Security-Verify: ipsec-man; q=0.1; alg=HMAC-SHA1; SPI_P_UDP=87654321; SPI_P_TCP=98765432; Port_P_UDP=7531;
Port_P_TCP=8642
CSeq: 4 REGISTER
Expires: 7200
Content-Length: 0
```

Authorization: This carries the response to the authentication challenge received in step 10 along with the private user identity both encoded in base64 format.

- 13. **DNS: DNS-Q**
  - Based on the user's URI, the P-CSCF determines that UE is registering from a visiting domain and performs a DNS query to locate the I-CSCF in the home network. The look up in the DNS is based on the address specified in the Request URI.
  - The P-CSCF sends the REGISTER request - after local processing - to the address indicated in the Request-URI. When forwarding the REGISTER request the P-CSCF needs to specify the protocol, port number and IP address of the I-CSCF server in the home network to which to send the REGISTER request. The P-CSCF tries to find this information by querying the DNS. Since the Request-URI does not specify the transport protocol the, P-CSCF selects the UDP.

Table 6.3-13a: DNS: DNS Query (P-CSCF to DNS)

```
OPCODE=SQUERY
QNAME=__sip._udp.registrar.home1.net, QCLASS=IN, QTYPE=SRV
```

- The DNS records are retrieved according to RFC 2782 [4].

Table 6.3-13b: DNS Query Response (DNS to P-CSCF)

```
OPCODE=SQUERY, RESPONSE, AA
QNAME=__sip._udp.registrar.home1.net, QCLASS=IN, QTYPE=SRV

_sip._udp.registrar.home1.net        0 IN SRV 1 10 5060 icscf1_p.home1.net
                                        0 IN SRV 1  0 5060 icscf7_p.home1.net

icscf1_p.home1.net                 0 IN AAAA     5555::aba:dab:aaa:daa
icscf7_p.home1.net                 0 IN AAAA     5555::a1a:b2b:c3c:d4d
```

- In the Answer field of the query-response each I-CSCF is identified by its host domain name. The returned SRV Resource Records (RRs) are merged and ordered, and the selection technique (employing the Priority and Weight parameters returned in the RRs) as specified in RFC 2782 [4] is used to select the I-CSCF (i.e. the icscf1_p.home1.net). Since the Additional Data field of the query-response also contains the IP address of the selected I-CSCF (i.e. 5555::aba:dab:aaa:daa), a new query to the DNS is not required.
- Once the IP address of the I-CSCF is obtained, the P-CSCF forwards the REGISTER request to this IP address (i.e. 5555::aba:dab:aaa:daa) using the UDP protocol and port number 5060.

- 14. **REGISTER request (P-CSCF to I-CSCF) - see example in table 6.2-14**

- This signalling flow shows the REGISTER request being forwarded from the P-CSCF to the I-CSCF in the home domain.

Table 6.3-14: REGISTER request (P-CSCF to I-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:pcscf1.visited1.net>
Proxy-require: path
Require: path
Roaming-Info: vnid="Visited Network Number 1"
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

Path: This is the address of the P-CSCF and is included to inform the S-CSCF where to route terminating sessions.

Roaming-Info: The *vnid* parameter contains the identifier of the P-CSCF network at the home network.

- 15. **Cx: User registration status query procedure**

  - The I-CSCF requests information related to the Subscriber registration status by sending the private user identity, public user identity and visited domain name to the HSS. Because the user has registered, the HSS returns the I-CSCF with the S-CSCF address for the subscriber.
  - For detailed message flows see 3GPP TS 29.228.
  - For the parameters in the REGISTER request (flow 14) which need to be sent to HSS, see table 6.2-16a.
  - Table 6.3-15a provides the parameters in the REGISTER request (flow 16), which are obtained from the information sent back from the HSS

Table 6.3-15a: User registration status query response (*HSS to I-CSCF*)

Message source & destination	Cx Information element name	Mapping to SIP header in REGISTER	Description
HSS to I-CSCF	S-CSCF name	Request-URI:	This information indicates the serving CSCF's name of that user

- 16. **REGISTER request (I-CSCF to S-CSCF) - see example in table 6.3-16**

  - This signalling flow forwards the REGISTER request from the I-CSCF to the S-CSCF selected.

Table 6.3-16: REGISTER request (I-CSCF to S-CSCF)

```
REGISTER sip:scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=351g45.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:pcscf1.visited1.net>
Proxy-require:
Require:
Roaming-Info:
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
```

```
Expires:
Content-Length:
```

Path: The S-CSCF stores the contents of the Path headers and uses these addresses for routing mobile terminated sessions.

- 17. **Authentication**
    - Upon receiving the REGISTER request, carrying the authentication response, RES, the S-CSCF checks that the user's active, XRES matches the received RES. If the check is successful then the user has been authenticated and the public user identity is registered in the S-CSCF.
- 18. **Cx: S-CSCF registration notification procedure**
    - On registering a user the S-CSCF informs the HSS that the user has been re-registered at this instance.
    - For detailed message flows see 3GPP TS 29.228.
- 19. **200 OK response (S-CSCF to I-CSCF) - see example in table 6.3-19**
    - The S-CSCF sends acknowledgement to the I-CSCF indicating that Registration was successful. This response will traverse the path that the REGISTER request took as described in the Via list.

Table 6.3-19 200 OK response (S-CSCF to I-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=351g45.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:scscf1.home1.net>, <sip:pcscf1.visited1.net>
From:
To:
Call-ID:
Contact: sip:[5555::aaa:bbb:ccc:ddd]
CSeq:
Date: Wed, 11 July 2001 08:49:37 GMT
Expires: 7200
Content-Length:
```

Path: The S-CSCF inserts its own name to the front of the list.

- 20. **200 OK response (I-CSCF to P-CSCF) - see example in table 6.3-20**
    - The I-CSCF forwards acknowledgement from the S-CSCF to the P-CSCF indicating that Registration was successful. This response will traverse the path that the REGISTER request took as described in the Via list.

Table 6.3-20: 200 OK response (I-CSCF to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:scscf1.home1.net, <sip:pcscf1.visited1.net>
From:
To:
Call-ID:
Contact:
CSeq:
Date:
Expires:
Content-Length:
```

- 21. **200 OK response (P-CSCF to UE) - see example in table 6.3-21**
    - The P-CSCF removes its address from the Path header, reverses the order of the fields, saves the resulting Path header and associates it with the UE. The P-CSCF then removes the Path header from the 200 OK

response. The P-CSCF then forwards acknowledgement from the I-CSCF to the UE indicating that Registration was successful.

Table 6.3-21: 200 OK response (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
Contact:
CSeq:
Date:
Expires:
Content-Length:
```

6.9.2 User not registered, user not allowed to roam / user unknown

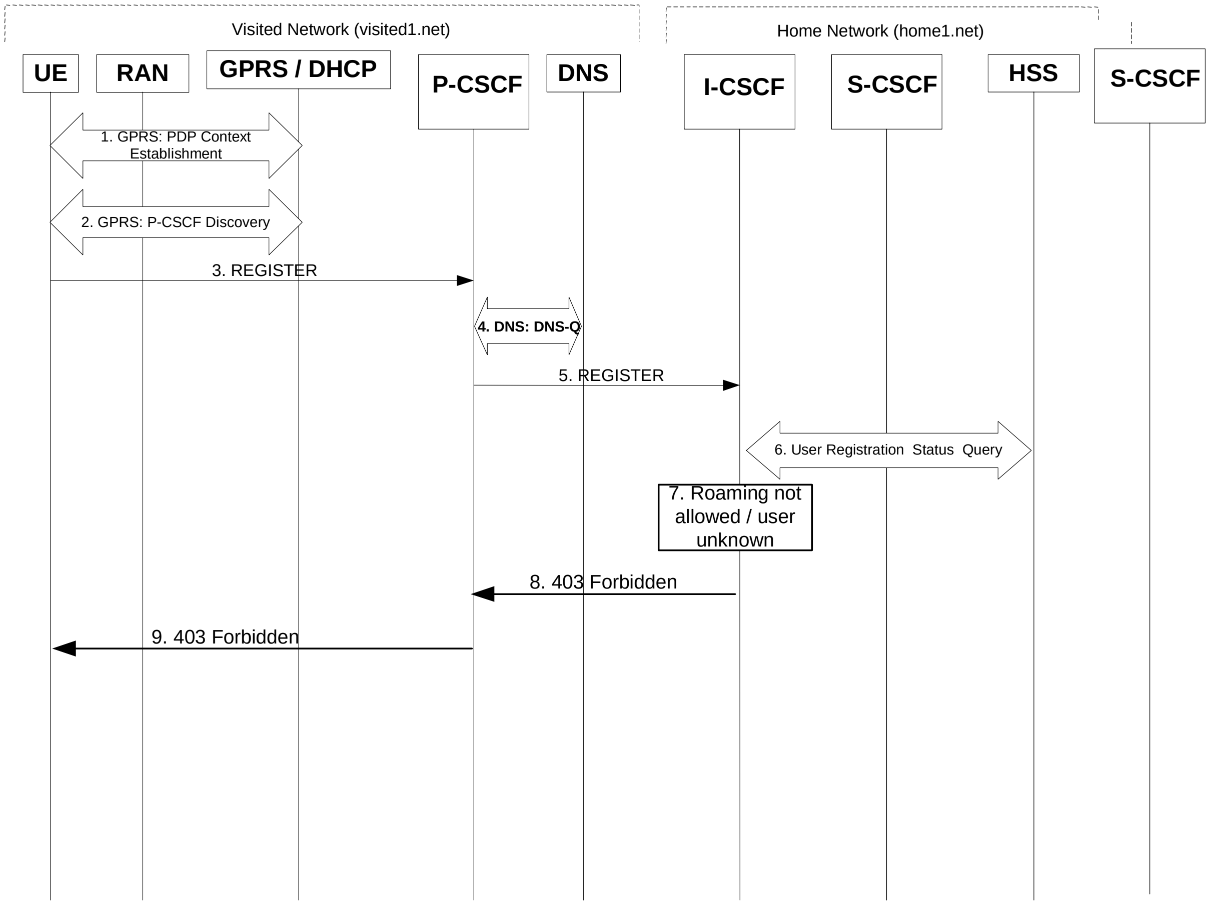
Visited Network (visited1.net)
Home Network (home1.net)
UE
RAN
GPRS / DHCP
P-CSCF
DNS
I-CSCF
S-CSCF
HSS
S-CSCF
1. GPRS: PDP Context Establishment
2. GPRS: P-CSCF Discovery
3. REGISTER
4. DNS: DNS-Q
5. REGISTER
6. User Registration Status Query
7. Roaming not allowed / user unknown
8. 403 Forbidden
9. 403 Forbidden

Figure 6.9.2-1: Registration failure: User not registered, user not allowed to roam

The first six steps are similar with the regular Registration signalling flows described in subclause 16.2.

The "Roaming not allowed" and "User unknown" error conditions would result in the same signalling flow (only the actions taken by I-CSCF will differ), thus the signalling flows are merged and only the I-CSCF action is described depending on the error condition.

- 7. **Roaming not allowed / User unknown**

- The information received as a response to the Cx-Query may indicate that "Roaming is not allowed" for the subscriber from the visited1.net network. In this case I-CSCF needs to send a 403 Forbidden response back to the UE. I-CSCF will insert a warning header in the response, indicating to the UE the reason of refusing the Registration request. Warning header should contain the name of the network inserting the warning header (warn-agent = icscf1.home1.net) and optionally a warn-text. In case the network operator would like to advise the subscriber to attach instead to the CS domain then the warn-code 312 should be inserted in the warning header.

- When the information received as a response to the Cx-Query indicates that the subscriber is unknown to the network or the subscriber does not have a valid subscription, the I-CSCF needs to send a 403 Forbidden response back to the UE. I-CSCF will insert a warning header in the response, indicating to the UE the reason of refusing the Registration request. Warning header should contain the name of the network inserting the warning header (warn-agent = icscf1.home1.net) and optionally a warn-text.

- 8. **403 Forbidden (I-CSCF to P-CSCF) - see example in table 6.9.2-8**

Table 6.9.2-8: 403 Forbidden (I-CSCF to P-CSCF)

```
SIP/2.0 403 Forbidden
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Warning: 312 home1.net "Roaming not allowed from this network"
From:
To:
Call-ID:
Cseq:
Content-Length:
```

- 9. **403 Forbidden (P-CSCF to UE) - see example in table 6.9.2-9**

Table 6.9.2-9: 403 Forbidden (P-CSCF to UE)

```
SIP/2.0 403 Forbidden
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Warning: 312 home1.net "Roaming not allowed from this network"
From:
To:
Call-ID:
Cseq:
Content-Length:
```

6.9.3 Registration failure – user authentication failure

This clause (see figure 6.9.3-1) shows the signalling flow with user authentication failure at step 19 of subclause 6.2 "Signalling flows for REGISTER" and a final failure of the authentication at step 30.

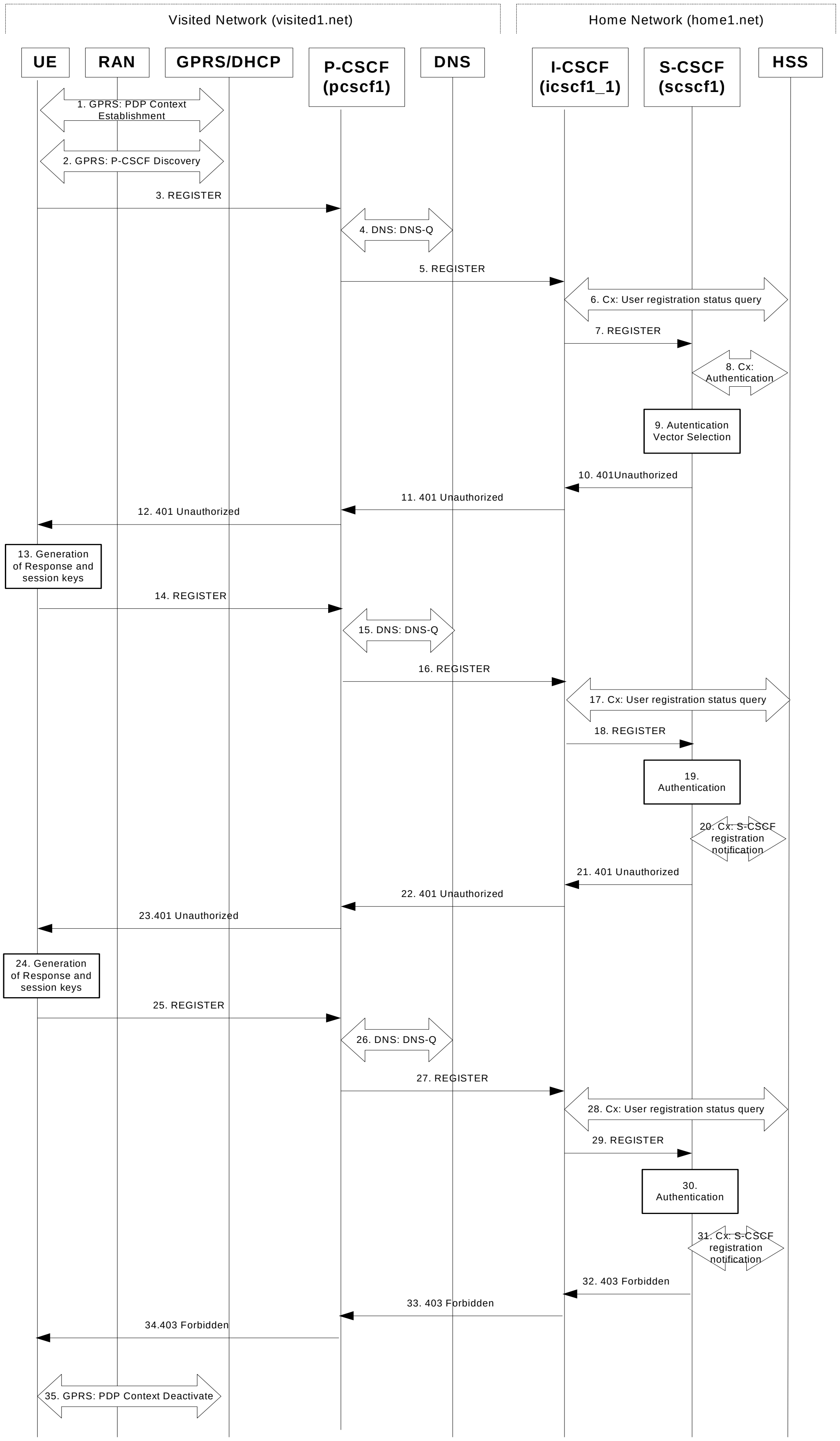
Visited Network (visited1.net)
Home Network (home1.net)
UE
RAN
GPRS/DHCP
P-CSCF (pcscf1)
DNS
I-CSCF (icscf1_1)
S-CSCF (scscf1)
HSS
1. GPRS: PDP Context Establishment
2. GPRS: P-CSCF Discovery
3. REGISTER
4. DNS: DNS-Q
5. REGISTER
6. Cx: User registration status query
7. REGISTER
8. Cx: Authentication
9. Autentication Vector Selection
10. 401Unauthorized
11. 401 Unauthorized
12. 401 Unauthorized
13. Generation of Response and session keys
14. REGISTER
15. DNS: DNS-Q
16. REGISTER
17. Cx: User registration status query
18. REGISTER
19. Authentication
20. Cx: S-CSCF registration notification
21. 401 Unauthorized
22. 401 Unauthorized
23.401 Unauthorized
24. Generation of Response and session keys
25. REGISTER
26. DNS: DNS-Q
27. REGISTER
28. Cx: User registration status query
29. REGISTER
30. Authentication
31. Cx: S-CSCF registration notification
32. 403 Forbidden
33. 403 Forbidden
34.403 Forbidden
35. GPRS: PDP Context Deactivate

Figure 6.9.3-1: User Authentication Failure

Steps 1 through 18 are the same as the signalling flow in subclause 6.2.

- 19. **Authentication: User authentication fails**
  - Upon receiving the REGISTER request carrying the authentication response, RES, the S-CSCF checks that the user's active, XRES matches the received RES. If the check is unsuccessful then this authentication challenge fails and the public user identity is not yet registered in the S-CSCF.
  - At this point the S-CSCF has the option of repeating a number of authentication challenges as given in step 19 through 29. For the purposes of this flow, only one repetition is shown.
- 20. **Cx. SCGF registration notification**
  - The S-CSCF selects new authentication vectors as specified in step 9, either from the list already within the S-CSCF, or by requesting new vectors from the HSS.
- 21. **401 Unauthorized response (S-CSCF to I-CSCF) - see example in table 6.9.3-21**
  - The authentication challenge is sent in the 401 Unauthorized response towards the UE.

Table 6.9.3-21: 401 Unauthorized response (S-CSCF to I-CSCF)

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=351g45.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>; tag=5ef4
Call-ID: apb03a0s09dkjdfglkj49111
WWW-Authenticate: eap eap-p=base64(user1_private1@home1.net, RAND, AUTN)
CSeq: 2 REGISTER
Content-Length: 0
```

NOTE: The actual WWW-Authenticate header value may look like this as it is in base64 form:
WWW-Authenticate: eap eap-p=QWxh4ZGRpb2jpvcGVuNlctZQ==

Editor's Note: The mechanism to transport the session keys (IK and optionally, CK) from the S-CSCF to the P-CSCF is FFS.

- 22. **401 Unauthorized response(I-CSCF to P-CSCF) - see example in table 6.9.3-22**
  - The authentication challenge is sent in the 401 Unauthorized response towards the UE.

Table 6.9.3-22: 401 Unauthorized response (I-CSCF to P-CSCF)

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
WWW-Authenticate:
CSeq:
Content-Length:
```

Editor's Note: The mechanism to transport the session keys (IK and optionally, CK) from the S-CSCF to the P-CSCF is FFS.

- 23. **401 Unauthorized response (P-CSCF to UE) - see example in table 6.9.3-23**
  - The P-CSCF removes any keys received in the 401 Unauthorized response and forwards the rest of the response to the UE.

Table 6.9.3-23: 401 Unauthorized response (P-CSCF to UE)

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
WWW-Authenticate: eap eap-p=base64(user1_private1.home1.net, RAND, AUTN)
Security-Server: ipsec-man; q=0.1; alg=HMAC-SHA1; SPI_P_UDP=87654321; SPI_P_TCP=98765432; Port_P_UDP=7531;
Port_P_TCP=8642
CSeq:
Content-Length:
```

- 24. **Generation of response and session keys at UE**

  - Upon receiving the Unauthorised response, the UE extracts the MAC and the SQN from the AUTN. The UE calculates the XMAC and checks that XMAC matches the received MAC and that the SQN is in the correct range. If both these checks are successful the UE calculates the response, RES, and also computes the session keys IK and CK. The RES is put into the Authorization header and sent back to the registrar in the REGISTER request.

- 25. **REGISTER request (UE to P-CSCF) - see example in table 6.9.3-25**

Table 6.9.3-25: REGISTER request (UE to P-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>
Contact: <sip:[5555::aaa:bbb:ccc:ddd]>
Call-ID: apb03a0s09dkjdfglkj49112
Authorization: eap eap-p=base64(user1_private1@home1.net, RES)
Security-Verify: ipsec-man; q=0.1; alg=HMAC-SHA1; SPI_P_UDP=87654321; SPI_P_TCP=98765432; Port_P_UDP=7531;
Port_P_TCP=8642
CSeq: 3 REGISTER
Expires: 7200
Content-Length: 0
```

Authorization: This carries the response to the authentication challenge received in step 12 along with the private user identity both encoded in base64 format.

- 26. **DNS: DNS-Q**

  - Based on the user's URI, the P-CSCF determines that UE is registering from a visiting domain and performs a DNS query to locate the I-CSCF in the home network. The look up in the DNS is based on the address specified in the Request URI.

  - The P-CSCF sends the REGISTER request - after local processing - to the address indicated in the Request-URI. When forwarding the REGISTER request the P-CSCF needs to specify the protocol, port number and IP address of the I-CSCF server in the home network to which to send the REGISTER request. The P-CSCF tries to find this information by querying the DNS. Since the Request-URI does not specify the transport protocol the, P-CSCF selects the UDP.

Table 6.9.3-26a: DNS: DNS Query (P-CSCF to DNS)

```
OPCODE=SQUERY
QNAME=__sip._udp.registrar.home1.net, QCLASS=IN, QTYPE=SRV
```

  - The DNS records are retrieved according to RFC 2782 [4].

Table 6.9.3-26b: DNS Query Response (DNS to P-CSCF)

```
OPCODE=SQUERY, RESPONSE, AA
```

```
QNAME=__sip._udp.registrar.home1.net, QCLASS=IN, QTYPE=SRV

_sip._udp.registrar.home1.net        0 IN SRV 1 10 5060 icscf1_p.home1.net
                                        0 IN SRV 1  0 5060 icscf7_p.home1.net

icscf1_p.home1.net                 0 IN AAAA     5555::aba:dab:aaa:daa
icscf7_p.home1.net                 0 IN AAAA     5555::a1a:b2b:c3c:d4d
```

- In the Answer field of the query-response each I-CSCF is identified by its host domain name. The returned SRV Resource Records (RRs) are merged and ordered, and the selection technique (employing the Priority and Weight parameters returned in the RRs) as specified in RFC 2782 [4] is used to select the I-CSCF (i.e. the icscf1_p.home1.net). Since the Additional Data field of the query-response also contains the IP address of the selected I-CSCF (i.e. 5555::aba:dab:aaa:daa), a new query to the DNS is not required.

- Once the IP address of the I-CSCF is obtained, the P-CSCF forwards the REGISTER request to this IP address (i.e. 5555::aba:dab:aaa:daa) using the UDP protocol and port number 5060.

- 27. **REGISTER request (P-CSCF to I-CSCF) - see example in table 6.9.3-27**

  - This signalling flow shows the REGISTER request being forwarded from the P-CSCF to the I-CSCF in the home domain.

Table 6.9.3-27: REGISTER request (P-CSCF to I-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:pcscf1.visited1.net>
Proxy-require: path
Require: path
Roaming-Info: vnid="Visited Network Number 1"
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

Path: This is the address of the P-CSCF and is included to inform the S-CSCF where to route terminating sessions.

- 28. **Cx: User registration status query procedure**

  - The I-CSCF requests information related to the Subscriber registration status by sending the private user identity, public user identity and visited domain name to the HSS. The HSS returns the S-CSCF required capabilities and the I-CSCF uses this information to select a suitable S-CSCF.

  - For detailed message flows see 3GPP TS 29.228.

  - Table 6.9.3-28a provides the parameters in the REGISTER request (flow 5) which need to be sent to HSS.

Table 6.9.3-28a Cx: User registration status query procedure (I-CSCF to HSS)

Message source & destination	Cx Information element name	Information Source in REGISTER	Description
I-CSCF to HSS	Private User Identity	Authorization:	The Private User Identity is encoded according to the Authorization protocol.
	Public User Identity	To:	Identity which is used to communicate with other users

	Visited Network Identifier	Roaming-Info: vnid	This information indicates the network identifier of the visited network

- 29. **REGISTER request (I-CSCF to S-CSCF) - see example in table 6.9.3-29**
  - This signalling flow forwards the REGISTER request from the I-CSCF to the S-CSCF selected.

Table 6.9.3-29: REGISTER request (I-CSCF to S-CSCF)

```
REGISTER sip:scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=351g45.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:pcscf1.visited1.net>
Proxy-require:
Require:
Roaming-Info:
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

Path: The S-CSCF stores the contents of the Path headers and uses these addresses for routing mobile terminated sessions.

- 30. **Authentication**
  - Upon receiving the REGISTER request carrying the authentication response, RES, the S-CSCF checks that the user's active, XRES matches the received RES. If the check is unsuccessful, and no more authentication challenges are to be made, then the authentication has failed and the public user identity is not registered in the S-CSCF.

- **31. Cx: S-CSCF registration notification procedure**
  - Upon user authentication failure the S-CSCF informs the HSS that the user has not been registered at this instance. The HSS clears the S-CSCF name for that subscriber.
  - For detailed message flows see 3GPP TS 29.229.
  - Table 6.9.3-31 provides the parameters in the REGISTER request (flow 18) which need to be sent to HSS.

Table 6.9.3-31 Cx: S-CSCF registration notification procedure (S-CSCF to HSS)

Message source & destination	Cx Information element name	Information Source in REGISTER	Description
S-CSCF to HSS	Public User Identify	To:	Identity which is used to communicate with other users
	Private User Identity	Authorization:	The Private User Identity is encoded according to the Authorization protocol. Unique identity in IMS which is used by network to authenticate this user
	S-CSCF name	Request-URI:	This information indicates the serving CSCF's name of that user

- 32. **403 Forbidden response (S-CSCF to I-CSCF) - see example in table 6.9.3-32**
    - The S-CSCF sends an 403 Forbidden response to the I-CSCF indicating that authentication failed. No security parameters are included in this message.

Table 6.9.3-32: 403 Forbidden (S-CSCF to I-CSCF)

```
SIP/2.0 403 Forbidden
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=351g45.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>; tag=5ef4
Call-ID: apb03a0s09dkjdfglkj49111
CSeq: 3 REGISTER
Content-Length: 0
```

- 33. **403 Forbidden response (I-CSCF to P-CSCF) - see example in table 6.9.3-33**
    - The I-CSCF forwards the 403 Forbidden response from the S-CSCF to the P-CSCF indicating that authentication was unsuccessful.

Table 6.9.3-33: 403 Forbidden response (I-CSCF to P-CSCF)

```
SIP/2.0 403 Forbidden
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:
Content-Length:
```

- 34. **403 Forbidden response (P-CSCF to UE) - see example in table 6.9.3-33**
    - The P-CSCF forwards the 403 Forbidden response to the UE.

Table 6.9.3-34: 403 Forbidden response (P-CSCF to UE)

```
SIP/2.0 403 Forbidden
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
CSeq:
Content-Length:
```

- 35. **PDP Context Deactivate**

On receiving the 403 Forbidden response the UE ceases registration and authentication attempts. In this case, if the PDP context on which the SIP signalling was being conducted is not being used for other purposes, the UE deactivates the signalling PDP context.

16.2 Registration signalling: user not registered

Figure 16.2-1 shows the registration signalling flow for the scenario when the user is not registered. For the purpose of this signalling flow, the subscriber is considered to be roaming. This flow also shows the authentication of the private user identity. In this signalling flow, the home network has network configuration hiding active.

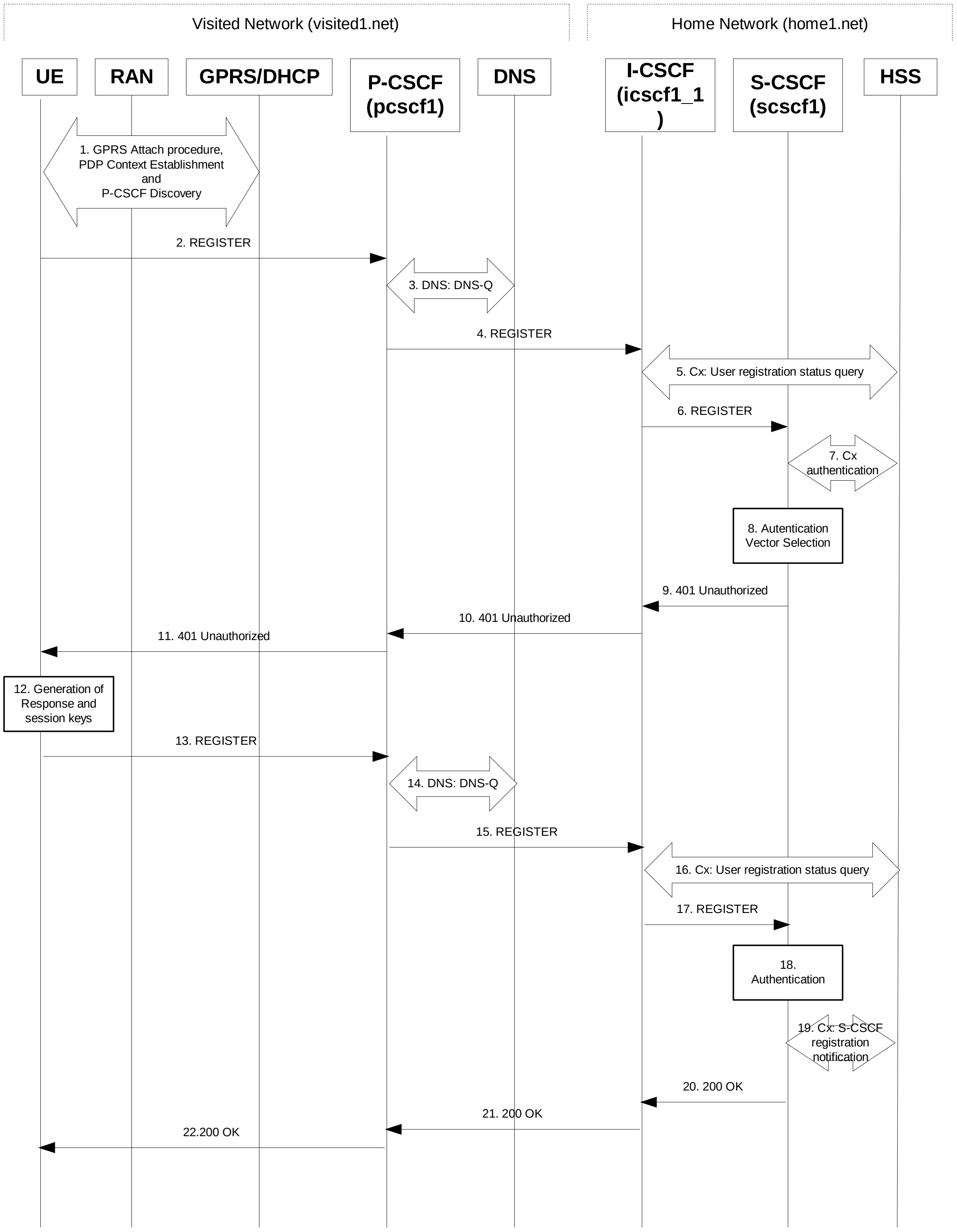

Figure 16.2-1: Registration when UE roaming

- 1. **GPRS Attach / PDP Context Establishment and P-CSCF Discovery (UE to GPRS)**
  - This signalling flow is shown to indicate prerequisites for the registration signalling.
  - See subclause 5.2 for details.

- 2. **REGISTER request (UE to P-CSCF) – see example in table 16.2-2**

  - The purpose of this request is to register the user's SIP URI with a S-CSCF in the home network. This request is routed to the P-CSCF because it is the only SIP server known to the UE. In the following SIP request, the Contact field contains the user's host address.

  - The P-CSCF will perform two actions, binding and forwarding. The binding is between the User's SIP address (user1_public1@home1.net) and the host (terminal) address ([5555::aaa:bbb:ccc:ddd]) which was acquired during PDP context activation process.

Editor's note: The security mode set-up procedure supports the negotiation of different protection mechanisms. This will involve the addition of a "security-setup" field to the SIP REGISTER request and the REGISTER response performing the authentication challenge containing the parameters:

list of Authentication (integrity} algorithms, and optionally list of encryption (confidentiality) algorithms

SA-ID that is used to uniquely identify the SA at the receiving side.

Key length: the length of encryption and authentication (integrity) keys is 128 bits.

The exact format and use for the security mode setup is being worked through IETF and is FFS

Table 16.2-2 REGISTER request (UE to P-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>
Contact: <sip:[5555::aaa:bbb:ccc:ddd]>
Call-ID: apb03a0s09dkjdfglkj49111
Authorization: eap eap-p=base64(user1_private1@home1.net)
Security-Client: ipsec-man; alg=HMAC-SHA1; SPI_U_UDP=12345678; SPI_U_TCP=23456789; Port_U_UDP=1357; Port_U_TCP=1358
Require: sec-agree
CSeq: 1 REGISTER
Expires: 7200
Content-Length: 0
```

Request-URI: The Request-URI (the URI that follows the method name, "REGISTER", in the first line) indicates the destination domain of this REGISTER request. The rules for routing a SIP request describe how to use DNS to resolve this domain name ("home1.net") into an address or entry point into the home operator's network (the I-CSCF). This information is stored in the USIM.

Via: IPv6 PDP address of the SIP session allocated during the PDP Context Activation process.

From: This indicates the public user identity originating the REGISTER request. The public user identity may be obtained from the USIM.

To: This indicates the public user identity being registered. This is the identity by which other parties know this subscriber. It may be obtained from the USIM.

Contact: This indicates the point-of-presence for the subscriber – the IP address of the UE. This is the temporary point of contact for the subscriber that is being registered. Subsequent requests destined for this subscriber will be sent to this address. This information is stored in the P-CSCF and S-CSCF.

Editor's note: It is for further study whether this information is stored in the HSS and the S-CSCF for the subscriber in order to support multiple registrations.

Authorization: It carries authentication information. The private user identity (user1_private1@home1.net) is carried in the user ID field of the extensible authentication protocol (EAP).

- Upon receiving this request the P-CSCF will set it's SIP registration timer for this UE to the Expires time in this request.

- 3. **DNS: DNS-Q**

  - Based on the user's URI, the P-CSCF determines that UE is registering from a visiting domain and performs a DNS query to locate the I-CSCF in the home network. The look up in the DNS is based on the address specified in the Request URI.

  - The P-CSCF sends the REGISTER request - after local processing - to the address indicated in the Request-URI. When forwarding the REGISTER request the P-CSCF needs to specify the protocol, port number and IP address of the I-CSCF server in the home network to which to send the REGISTER request. The P-CSCF tries to find this information by querying the DNS. Since the Request-URI does not specify the transport protocol the, P-CSCF selects the UDP.

Table 16.2-3a DNS: DNS Query (P-CSCF to DNS)

```
OPCODE=SQUERY
QNAME=_sip._udp.registrar.home1.net, QCLASS=IN, QTYPE=SRV
```

•

- The DNS records are retrieved according to RFC 2782 [4].

Table 16.2-3b DNS: DNS Query Response (DNS to P-CSCF)

```
OPCODE=SQUERY, RESPONSE, AA
QNAME=_sip._udp.registrar.home1.net, QCLASS=IN, QTYPE=SRV

_sip._udp.registrar.home1.net           0 IN SRV 1 10 5060 icscf1_p.home1.com
                                        0 IN SRV 1  0 5060 icscf7_p.home1.com

icscf1_p.home1.net                      0 IN AAAA     5555::aba:dab:aaa:daa
icscf7_p.home1.net                      0 IN AAAA     5555::a1a:b2b:c3c:d4d
```

•

- In the Answer field of the query-response each I-CSCF is identified by its host domain name. The returned SRV Resource Records (RRs) are merged and ordered, and the selection technique (employing the Priority and Weight parameters returned in the RRs) as specified in RFC 2782 [4] is used to select the I-CSCF (i.e. the icscf1_p.home1.net). Since the Additional Data field of the query-response also contains the IP address of the selected I-CSCF (i.e. 5555::aba:dab:aaa:daa), a new query to the DNS is not required.

- Once the IP address of the I-CSCF is obtained, the P-CSCF forwards the REGISTER request to this IP address (i.e. 5555::aba:dab:aaa:daa) using the UDP protocol and port number 5060.

- 4. **REGISTER request (P-CSCF to I-CSCF) – see example in table 16.2-4**

  - The P-CSCF needs to be in the path for all mobile originated and mobile terminated requests for this user. To ensure this, the P-CSCF adds itself to the path for future requests.

  - The P-CSCF binds the public user identity under registration to the Contact header supplied by the user.

  - The P-CSCF adds also the Roaming-Info header (if not present). The P-CSCF adds the *vnid* parameter with the contents of the identifier of the P-CSCF network. This may be the visited network domain name or any other identifier that identifies the visited network at the home network.

  - This signalling flow shows the REGISTER request being forward from the P-CSCF to the I-CSCF in the home domain.

Table 16.2-4 REGISTER request (P-CSCF to I-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:pcscf1.visited1.net>
Proxy-require: path
Require: path
Roaming-Info: vnid="Visited Network Number 1"
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

Path: This is the address of the P-CSCF and is included to inform the S-CSCF where to route terminating sessions.

Require:/Proxy-Require: These headers are included to ensure that the recipient correctly handles the Path header. If the recipient does not support the path header, a response will be received with a status code of 420 and an Unsupported header indicating "path". Such a response indicates a misconfiguration of the routing tables and the request has been routed outside the IM CN subsystem.

Roaming-Info: The *vnid* parameter contains the identifier of the P-CSCF network at the home network.

- 5. **Cx: User registration status query procedure**
  - The I-CSCF makes a request for information related to the Subscriber registration status by sending the private user identity, public user identity and visited domain name to the HSS. The HSS returns the S-CSCF required capabilities and the I-CSCF uses this information to select a suitable S-CSCF.
  - For detailed message flows see 3GPP TS 29.228.
  - Table 6.2-5a provides the parameters in the REGISTER request (flow 4) which need to been sent to HSS.
- 6. **REGISTER request (I-CSCF to S-CSCF) – see example in table 16.2-6**
  - I-CSCF adds a proper I-CSCF name to the Path header.
  - This signalling flow forwards the REGISTER request from the I-CSCF to the S-CSCF selected. The Request-URI is changed to the address of the S-CSCF.

Table 16.2-6 REGISTER request (I-CSCF to S-CSCF)

```
REGISTER sip:scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=351g45.1, SIP/2.0/UDP
        pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:icscf1_p.home1.net>, <sip:pcscf1.visited1.net>
Proxy-require:
Require:
Roaming-Info:
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

Path: The S-CSCF stores the contents of the Path headers and uses these addresses for routing mobile terminated sessions.

  - Upon receiving this request the S-CSCF will set it's SIP registration timer for this UE to the Expires time in this request.

- 7. **Cx: S-CSCF authentication procedure**

  - On receiving a REGISTER request from an unauthenticated user, the S-CSCF requires at least one authentication vector to be used in the challenge to the user. If a valid AV is not available, then the S-CSCF requests at least one AV from the HSS.

  - For detailed message flows see 3GPP TS 29.228.

  - Table 6.2-7a provides the parameters in the REGISTER request (flow 6) which need to been sent to HSS.

- 8. **Authentication vector selection**

  - The S-CSCF selects an authentication vector for use in the authentication challenge. For detailed description of the authentication vector, see 3GPP TS 33.203.

NOTE 1: The authentication vector may be of the form 3GPP TS 33.203 (if IMS AKA is the selected authentication scheme):

- $AV = RAND_n||AUTN_n||XRES_n||CK_n||IK_n$ where:

  - - RAND: random number used to generate the XRES, CK, IK, and part of the AUTN. It is also used to generate the RES at the UE.

  - - AUTN: Authentication token (including MAC and SQN).

  - - XRES: Expected (correct) result from the UE.

  - - CK: Cipher key (optional).

  - - IK: Integrity key.

- 9. **401 Unauthorized response (S-CSCF to I-CSCF) – see example in table 16.2-9**

  - The authentication challenge is sent in the 401 Unauthorized response towards the UE.

Table 16.2-9: 401 Unauthorized response (S-CSCF to I-CSCF)

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=351g45.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To: <sip:user1_public1@home1.net>; tag=5ef4
Call-ID:
WWW-Authenticate: eap eap-p=base64(user1_private1@home1.net, RAND, AUTN)
CSeq:
Content-Length:
```

NOTE 2: The actual WWW-Authenticate header value may look like this as it is in base64 form:

- - WWW-Authenticate: eap eap-p=QWxh4ZGRpb2jpvcGVuNlctZQ==

Editor's Note: The mechanism to transport the session keys (IK and optionally, CK) from the S-CSCF to the P-CSCF is FFS.

- 10. **401 Unauthorized response (I-CSCF to P-CSCF) – see example in table 16.2-10**

  - The authentication challenge is sent in the 401 Unauthorized response towards the UE.

Table 16.2-10: 401 Unauthorized response (I-CSCF to P-CSCF)

```
SIP/2.0 401 Unauthorized
```

```
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
WWW-Authenticate:
CSeq:
Content-Length:
```

•

Editor's Note: The mechanism to transport the session keys (IK and optionally, CK) from the S-CSCF to the P-CSCF is FFS.

- 11. **401 Unauthorized response (P-CSCF to UE) – see example in table 16.2-11**

  - The P-CSCF removes any keys received in the 401 Unauthorized response and forwards the rest of the response to the UE.

Table 16.2-11: 401 Unauthorized response (P-CSCF to UE)

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
WWW-Authenticate:
Security-Server: ipsec-man; q=0.1; alg=HMAC-SHA1; SPI_P_UDP=87654321; SPI_P_TCP=98765432; Port_P_UDP=7531; Port_P_TCP=8642
CSeq:
Content-Length:
```

- 12. **Generation of response and session keys at UE**

  - Upon receiving the Unauthorized response, the UE extracts the MAC and the SQN from the AUTN. The UE calculates the XMAC and checks that XMAC matches the received MAC and that the SQN is in the correct range. If both these checks are successful the UE calculates the response, RES, and also computes the session keys IK and CK. The RES is put into the Authorization header and sent back to the registrar in the REGISTER request.

- 13. **REGISTER request (UE to P-CSCF) – see example in table 16.2-13**

Table 16.2-13 REGISTER request (UE to P-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>; tag=5ef4
Contact: <sip:[5555::aaa:bbb:ccc:ddd]>
Call-ID: apb03a0s09dkjdfglkj49112
Authorization: eap eap-p=base64(user1_private1@home1.net, RES)
Security-Verify: ipsec-man; q=0.1; alg=HMAC-SHA1; SPI_P_UDP=87654321; SPI_P_TCP=98765432; Port_P_UDP=7531; Port_P_TCP=8642
CSeq: 2 REGISTER
Expires: 7200
Content-Length: 0
```

Authorization: This carries the response to the authentication challenge received in step 11 along with the private user identity both encoded in base64 format.

- 14. **DNS: DNS-Q**

  - Based on the user's URI, the P-CSCF determines that UE is registering from a visiting domain and performs a DNS query to locate the I-CSCF in the home network. The look up in the DNS is based on the address specified in the Request URI.

  - The P-CSCF sends the REGISTER request - after local processing - to the address indicated in the Request-URI. When forwarding the REGISTER request the P-CSCF needs to specify the protocol, port number and IP address of the I-CSCF server in the home network to which to send the REGISTER request. The P-CSCF tries to find this information by querying the DNS. Since the Request-URI does not specify the transport protocol the, P-CSCF selects the UDP.

Table 16.2-14a DNS: DNS Query (P-CSCF to DNS)

```
OPCODE=SQUERY
QNAME=__sip._udp.registrar.home1.net, QCLASS=IN, QTYPE=SRV
```

- The DNS records are retrieved according to RFC 2782 [4].

Table 16.2-14b DNS Query Response (DNS to P-CSCF)

```
OPCODE=SQUERY, RESPONSE, AA
QNAME=__sip._udp.registrar.home1.net, QCLASS=IN, QTYPE=SRV

_sip._udp.registrar.home1.net           0 IN SRV 1 10 5060 icscf1_p.home1.net
                                        0 IN SRV 1  0 5060 icscf7_p.home1.net

icscf1_p.home1.net                 0 IN AAAA     5555::aba:dab:aaa:daa
icscf7_p.home1.net                 0 IN AAAA     5555::a1a:b2b:c3c:d4d
```

- In the Answer field of the query-response each I-CSCF is identified by its host domain name. The returned SRV Resource Records (RRs) are merged and ordered, and the selection technique (employing the Priority and Weight parameters returned in the RRs) as specified in RFC 2782 [4] is used to select the I-CSCF (i.e. the icscf1_p.home1.net). Since the Additional Data field of the query-response also contains the IP address of the selected I-CSCF (i.e. 5555::aba:dab:aaa:daa), a new query to the DNS is not required.

- Once the IP address of the I-CSCF is obtained, the P-CSCF forwards the REGISTER request to this IP address (i.e. 5555::aba:dab:aaa:daa) using the UDP protocol and port number 5060.

- 15. **REGISTER request (P-CSCF to I-CSCF) – see example in table 16.2-15**

  - This signalling flow shows the REGISTER request being forwarded from the P-CSCF to the I-CSCF in the home domain.

Table 16.2-15 REGISTER request (P-CSCF to I-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:pcscf1.visited1.net>
Proxy-require: path
Require: path
Roaming-Info: vnid="Visited Network Number 1"
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

Path: This is the address of the P-CSCF and is included to inform the S-CSCF where to route terminating sessions.

- 16. **Cx: User registration status query procedure**

  - The I-CSCF requests information related to the Subscriber registration status by sending the private user identity, public user identity and visited domain name to the HSS. The HSS returns the S-CSCF required capabilities and the I-CSCF uses this information to select a suitable S-CSCF.

  - For detailed message flows see 3GPP TS 29.228.

  - Table 6.2-16a provides the parameters in the REGISTER request (flow 15) which need to been sent to HSS.

- 17. **REGISTER request (I-CSCF to S-CSCF) – see example in table 16.2-17**

  - This signalling flow forwards the REGISTER request from the I-CSCF to the S-CSCF selected.

Table 16.2-17 REGISTER request (I-CSCF to S-CSCF)

```
REGISTER sip:scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=351g45.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:icscf1_p.home1.net>, <sip:pcscf1.visited1.net>
Proxy-require:
Require:
Roaming-Info:
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

Path: The S-CSCF stores the contents of the Path headers and uses these addresses for routing mobile terminated sessions.

- 18. **Authentication**

  - Upon receiving the REGISTER request, carrying the authentication response, RES, the S-CSCF checks that the user's active XRES matches the received RES. If the check is successful then the user has been authenticated and the public user identity is registered in the S-CSCF.

- 19. **Cx: S-CSCF registration notification procedure**

  - On registering a user the S-CSCF informs the HSS that the user has been registered at this instance. The HSS stores the S-CSCF name for that subscriber. For a positive response, the HSS will include the user profile in the response sent to the S-CSCF.

  - For detailed message flows see 3GPP TS 29.228.

  - Table 6.2-19a provides the parameters in the SIP REGISTER request (flow 17) which need to been sent to HSS.

- 20. **200 OK response (S-CSCF to I-CSCF) – see example in table 16.2-20**

  - The S-CSCF sends acknowledgement to the I-CSCF indicating that Registration was successful. This response will traverse the path that the REGISTER request took as described in the Via list.

Table 16.2-20 200 OK response (S-CSCF to I-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=351g45.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:scscf1.home1.net>, <sip:icscf1_p.home1.net>, <sip:pcscf1.visited1.net>
From:
To:
Call-ID:
Contact: sip:[5555::aaa:bbb:ccc:ddd]
CSeq:
Date: Wed, 11 July 2001 08:49:37 GMT
Expires: 7200
Content-Length:
```

Path: The S-CSCF inserts its own name to the front of the list.

- 21. **200 OK response (I-CSCF to P-CSCF) – see example in table 16.2-21**
    - The I-CSCF translates the S-CSCF name in the Path header. The I-CSCF forwards acknowledgement from the S-CSCF to the P-CSCF indicating that Registration was successful. This response will traverse the path that the REGISTER request took as described in the Via list.

Table 16.2-21 200 OK response (I-CSCF to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:token(scscf1.home1.net)>, <sip:icscf1_p.home1.net>, <sip:pcscf1.visited1.net>
From:
To:
Call-ID:
Contact:
CSeq:
Date:
Expires:
Content-Length:
```

- 22. **200 OK response (P-CSCF to UE) – see example in table 16.2-22**
    - The P-CSCF removes its address from the Path header, reverses the order of the fields, saves the resulting Path header and associates it with the UE. The P-CSCF then removes the Path header from the 200 OK response. The P-CSCF then forwards acknowledgement from the I-CSCF to the UE indicating that Registration was successful.

Table 16.2-22 200 OK response (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
Contact:
CSeq:
Date:
Expires:
Content-Length:
```

16.3 Registration signalling: reregistration – user currently registered

For the purpose of the reregistration signalling flow shown in figure 16.3-1, the subscriber is considered to be roaming. This flow also shows the authentication of the private user identity. In this signalling flow, the home network has network configuration hiding active.

This signalling flow assumes:

- 1. That the same PDP Context allocated during the initial registration scenario is still used for reregistration. For the case when the UE does not still have an active PDP context then PDP context procedures from subclause 16.2 is completed first.

Editor's Note: If the same PDP-Context is not available, is it guaranteed that the UE will get back the same IP address at this point? If this is not possible, would there be a problem with the binding in the P-CSCF (user_public1@home1.net and [5555::aaa:bbb:ccc:ddd])?2. The DHCP procedure employed for P-CSCF discovery is not needed.

- 2. The S-CSCF selection procedure invoked by the I-CSCF is not needed.

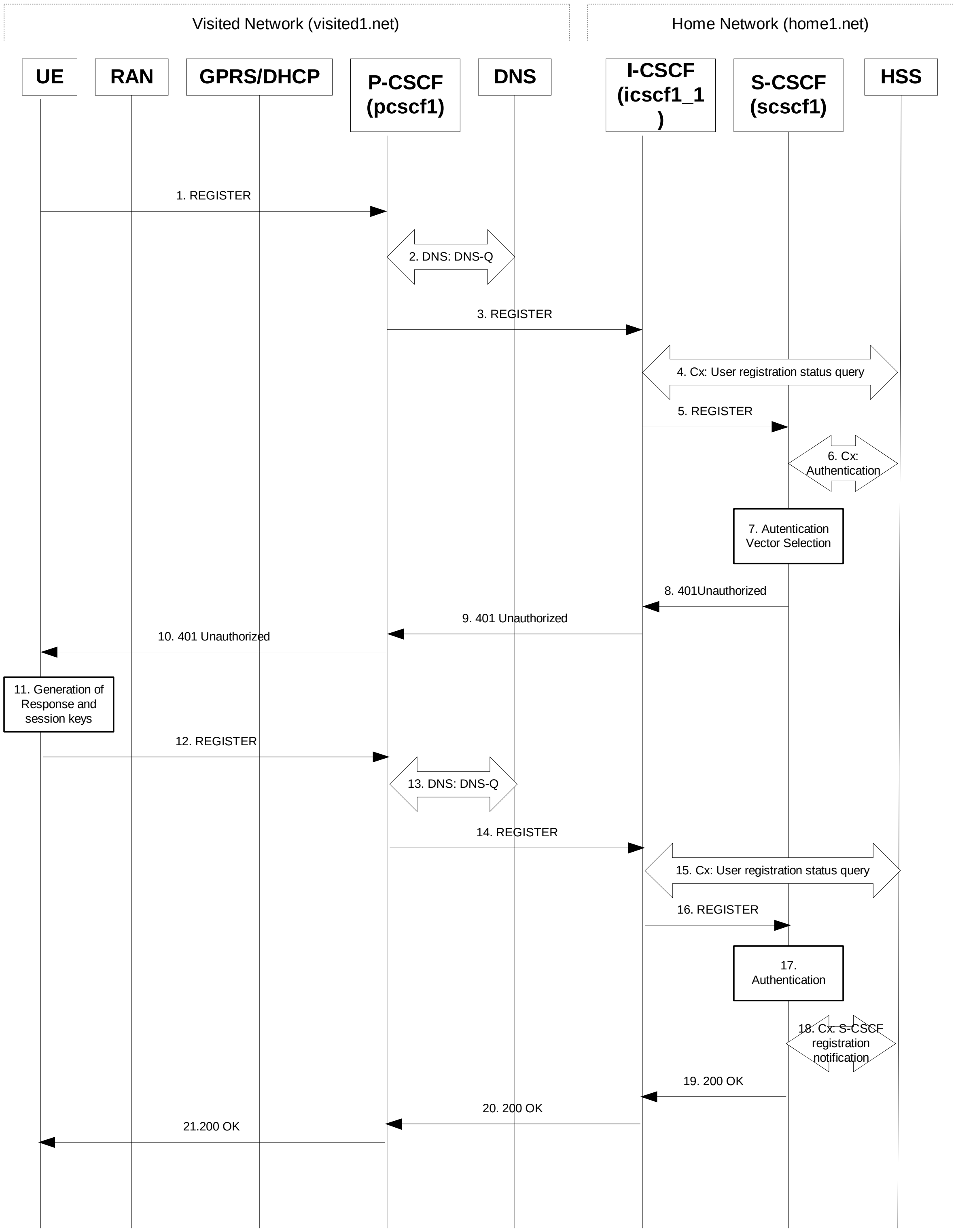

Figure 16.3-1: Reregistration when UE roaming

- 1. **REGISTER request (UE to P-CSCF) – see example in table 16.3-1**
  - The registration expires in the UE. The UE reregisters by sending a new REGISTER request. This request is sent to the same P-CSCF with which the UE initially registered. The P-CSCF maintains the same binding

between the User's SIP public address (user1_public1@home1.net) and the host (terminal) address ([5555::aaa:bbb:ccc:ddd]) which it established during the original registration.

Table 16.3-1 REGISTER request (UE to P-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>; tag=5ef4
Contact: <sip:[5555::aaa:bbb:ccc:ddd]>
Call-ID: apb03a0s09dkjdfglkj49111
Authorization: eap eap-p=base64(user1_private1@home1.net)
Security-Client: ipsec-man; alg=HMAC-SHA1; SPI_U_UDP=12345678; SPI_U_TCP=23456789; Port_U_UDP=1357; Port_U_TCP=1358
Required: sec-agree
CSeq: 3 REGISTER
Expires: 7200
Content-Length: 0
```

The header field usage is the same as for the initial registration scenario:

From: This indicates the public user identity originating the REGISTER request. The public user identity may be obtained from the USIM.

To: This indicates public user identity being registered. This is the identity by which other parties know this subscriber.

Contact: This indicates the point-of-presence for the subscriber – the IP address of the UE. This is the temporary identifier for the subscriber that is being registered. Subsequent requests destined for this subscriber will be sent to this address. This information is stored in the P-CSCF.

Editor's note: It is for further study whether this information is stored in the HSS and the S-CSCF for the subscriber in order to support multiple registrations.

Authorization: It carries authentication information. The private user identity (user1_private1@home1.net) is carried in the user ID field of the extensible authentication protocol (EAP).

Security-Client: The SPIs and port numbers both must be renewed for new SA usage.

NOTE 1: The actual Authorization header value may look like this as it is in base64 form:

• - Authorization: eap eap-p=QWxhZGRpbjpvcGVuIHNlc2FtZQ==

Request-URI: The Request-URI (the URI that follows the method name, "REGISTER", in the first line) indicates the destination domain of this REGISTER request. The rules for routing a SIP request describe how to use DNS to resolve this domain name ("home1.net") into an address or entry point into the home operator's network (the I-CSCF). This information is stored in the USIM.

- Upon receiving this request the P-CSCF will detect that it already has a registration record for this UE and will reset it's SIP registration timer for this UE to the Expires time in this request.

- 2. **DNS: DNS-Q**
  - Based on the user's URI, the P-CSCF determines that UE is registering from a visiting domain and performs a DNS query to locate the I-CSCF in the home network. The look up in the DNS is based on the address specified in the Request URI. The DNS provides the P-CSCF with an address of the I-CSCF in the home network. The P-CSCF must not use the I-CSCF address cached as a result of the previous registration.

- 3. **REGISTER request (P-CSCF to I-CSCF) – see example in table 16.3-3**
  - This signalling flow shows the REGISTER request being forward from the P-CSCF to the I-CSCF in the home domain.

Table 16.3-3 REGISTER request (P-CSCF to I-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:pcscf1.visited1.net>
Proxy-require: path
Require: path
Roaming-Info: vnid="Visited Network Number 1"
From:
To:
Contact:Call-ID:
Authorization: eap eap-p=base64(user1_private1@home1.net)
CSeq:
Expires:
Content-Length:
```

Path: This is the address of the P-CSCF and is included to inform the S-CSCF where to route terminating sessions.

Require:/Proxy-Require: These headers are included to ensure that the recipient correctly handles the Path header. If the recipient does not support the path header, a response will be received with a status code of 420 and an Unsupported header indicating "path". Such a response indicates a misconfiguration of the routing tables and the request has been routed outside the IM CN subsystem.

Roaming-Info: The *vnid* parameter contains the identifier of the P-CSCF network at the home network.

- 4. **Cx: User registration status query procedure**
  - The I-CSCF requests information related to the Subscriber registration status by sending the private user identity, public user identity and visited domain name to the HSS. Because the user has registered, the HSS returns the I-CSCF with the S-CSCF address for the subscriber
  - For detailed message flows see 3GPP TS 29.228.
  - For the parameters in the REGISTER request (flow 3), which are sent to the HSS, see table 6.2-5a.
  - Table 6.3-4a provides the parameters in the SIP REGISTER request (flow 5), which are obtained from the information sent back from the HSS.

- 5. **REGISTER request (I-CSCF to S-CSCF) – see example in table 16.3-5**
  - This signalling flow forwards the REGISTER request from the I-CSCF to the S-CSCF selected. The Request-URI is changed to the address of the S-CSCF.
  - I-CSCF adds a proper I-CSCF name to the Path header.

Table 16.3-5 REGISTER request (I-CSCF to S-CSCF)

```
REGISTER sip:scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=351g45.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:icscf1_p.home1.net>, <sip:pcscf1.visited1.net>
Proxy-require:
Require:
Roaming-Info:
From:
To:
Contact:
Authorization: eap eap-p=base64(user1_private1@home1.net)
Call-ID:
CSeq:
Expires:
Content-Length:
```

Path: The S-CSCF stores the contents of the Path headers and uses these addresses for routing mobile terminated sessions.

Roaming-Info: The *vnid* parameter contains the identifier of the P-CSCF network at the home network.

- Upon receiving this request the S-CSCF will detect that it already has a registration record for this UE and will reset it's SIP registration timer for this UE to the Expires time in this request.

- 6. **Cx: Authentication procedure**
    - On receiving a REGISTER request from a registered user, the S-CSCF requires at least one authentication vector to be used in the challenge to the user. If a valid AV is not available, then the S-CSCF requests at least one AV from the HSS.
    - For detailed message flows see 3GPP TS 29.228.
    - Table 6.3-6a provides the parameters in the REGISTER request (flow 5), which are sent to the HSS.
- 7. **Authentication vector selection**
    - The S-CSCF selects an authentication vector for use in the authentication challenge. For detailed description of the authentication vector, see 3GPP TS 33.203.

NOTE 2: The authentication vector may be of the form 3GPP TS 33.203 (if IMS AKA is the selected authentication scheme):

- AV = RANDn||AUTNn||XRESn||CKn||IKn where:
    - - RAND: random number used to generate the XRES, CK, IK, and part of the AUTN. It is also used to generate the RES at the UE.
    - - AUTN: Authentication token (including MAC and SQN).
    - - XRES: Expected (correct) result from the UE.
    - - CK: Cipher key (optional).
    - - IK: Integrity key.

- 8. **401 Unauthorized response (S-CSCF to I-CSCF) – see example in table 16.3-8**
    - The authentication challenge is sent in the 401 Unauthorized response towards the UE.

Table 16.3-8: 401 Unauthorized response (S-CSCF to I-CSCF)

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=351g45.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
WWW-Authenticate: eap eap-p=base64(user1_private1@home1.net, RAND, AUTN)
CSeq:
Content-Length:
```

NOTE 3: The actual WWW-Authenticate header value may look like this as it is in base64 form:

- - WWW-Authenticate: eap eap-p=QWxh4ZGRpb2jpvcGVuNlctZQ==

Editor's Note: The mechanism to transport the session keys (IK and optionally, CK) from the S-CSCF to the P-CSCF is FFS.

- 9. **401 Unauthorized response (I-CSCF to P-CSCF) – see example in table 16.3-9**

- The authentication challenge is sent in the 401 Unauthorized response towards the UE.

Table 16.3-9: 401 Unauthorized response (I-CSCF to P-CSCF)

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
WWW-Authenticate: eap eap-p=base64(user1_private1@home1.net, RAND, AUTN)
CSeq:
Content-Length:
```

•

Editor’s Note: The mechanism to transport the session keys (IK and optionally, CK) from the S-CSCF to the P-CSCF is FFS.

- 10. **401 Unauthorized response (P-CSCF to UE) – see example in table 16.3-10**
  - The P-CSCF removes any keys received in the 401 Unauthorized response and forwards the rest of the response to the UE.

Table 16.3-10: 401 Unauthorized response (P-CSCF to UE)

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
WWW-Authenticate:
Security-Server: ipsec-man; q=0.1; alg=HMAC-SHA1; SPI_P_UDP=87654321; SPI_P_TCP=98765432; Port_P_UDP=7531; Port_P_TCP=8642
CSeq:
Content-Length:
```

Security-Server: P-CSCF will renew SPIs and/or port numbers for new SA usage.

- 11. **Generation of response and session keys at UE**
  - Upon receiving the Unauthorised response, the UE extracts the MAC and the SQN from the AUTN. The UE calculates the XMAC and checks that XMAC matches the received MAC and that the SQN is in the correct range. If both these checks are successful the UE calculates the response, RES, and also computes the session keys IK and CK. The RES is put into the Authorization header and sent back to the registrar in the REGISTER request.
- 12. **REGISTER request (UE to P-CSCF) – see example in table 16.3-12**

Table 16.3-12 REGISTER request (UE to P-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>; tag=5ef4
Contact: <sip:[5555::aaa:bbb:ccc:ddd]>
Call-ID: apb03a0s09dkjdfglkj49112
Authorization: eap eap-p=base64(user1_private1@home1.net, RES)
Security-Verify: ipsec-man; q=0.1; alg=HMAC-SHA1; SPI_P_UDP=87654321; SPI_P_TCP=98765432; Port_P_UDP=7531; Port_P_TCP=8642
CSeq: 4 REGISTER
Expires: 7200
Content-Length: 0
```

•

Authorization: This carries the response to the authentication challenge received in step 10 along with the private user identity both encoded in base64 format.

- 13. **DNS: DNS-Q**

- Based on the user's URI, the P-CSCF determines that UE is registering from a visiting domain and performs a DNS query to locate the I-CSCF in the home network. The look up in the DNS is based on the address specified in the Request URI.

- The P-CSCF sends the REGISTER request - after local processing - to the address indicated in the Request-URI. When forwarding the REGISTER request the P-CSCF needs to specify the protocol, port number and IP address of the I-CSCF server in the home network to which to send the REGISTER request. The P-CSCF tries to find this information by querying the DNS. Since the Request-URI does not specify the transport protocol the, P-CSCF selects the UDP.

Table 16.3-13a DNS: DNS Query (P-CSCF to DNS)

```
OPCODE=SQUERY
QNAME=__sip._udp.registrar.home1.net, QCLASS=IN, QTYPE=SRV
```

•

- The DNS records are retrieved according to RFC2782 [4].

Table 16.3-13b DNS Query Response (DNS to P-CSCF)

```
OPCODE=SQUERY, RESPONSE, AA
QNAME=__sip._udp.registrar.home1.net, QCLASS=IN, QTYPE=SRV

_sip._udp.registrar.home1.net           0 IN SRV 1 10 5060 icscf1_p.home1.net
                                        0 IN SRV 1  0 5060 icscf7_p.home1.net

icscf1_p.home1.net                 0 IN AAAA     5555::aba:dab:aaa:daa
icscf7_p.home1.net                 0 IN AAAA     5555::a1a:b2b:c3c:d4d
```

•

- In the Answer field of the query-response each I-CSCF is identified by its host domain name. The returned SRV Resource Records (RRs) are merged and ordered, and the selection technique (employing the Priority and Weight parameters returned in the RRs) as specified in RFC 2782 [4] is used to select the I-CSCF (i.e. the icscf1_p.home1.net). Since the Additional Data field of the query-response also contains the IP address of the selected I-CSCF (i.e. 5555::aba:dab:aaa:daa), a new query to the DNS is not required.

- Once the IP address of the I-CSCF is obtained, the P-CSCF forwards the REGISTER request to this IP address (i.e. 5555::aba:dab:aaa:daa) using the UDP protocol and port number 5060.

- 14. **REGISTER request (P-CSCF to I-CSCF) – see example in table 16.3-14**

    - This signalling flow shows the REGISTER request being forwarded from the P-CSCF to the I-CSCF in the home domain.

Table 16.3-14 REGISTER request (P-CSCF to I-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:pcscf1.visited1.net>
Proxy-require: path
Require: path
Roaming-Info: vnid="Visited Network Number 1"
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

Path: This is the address of the P-CSCF and is included to inform the S-CSCF where to route terminating sessions.

- 15. **Cx: User registration status query procedure**

  - The I-CSCF requests information related to the Subscriber registration status by sending the private user identity, public user identity and visited domain name to the HSS. Because the user has registered, the HSS returns the I-CSCF with the S-CSCF address for the subscriber.
  - For detailed message flows see 3GPP TS 29.228.
  - For the parameters in the REGISTER request (flow 14), which are sent to the HSS, see table 6.2-16a.
  - Table 6.3-15a provides the parameters in the REGISTER request (flow 16), which are obtained from the information sent back from the HSS.

- 16. **REGISTER request (I-CSCF to S-CSCF) – see example in table 16.3-16**
  - This signalling flow forwards the REGISTER request from the I-CSCF to the S-CSCF selected.

Table 16.3-16 REGISTER request (I-CSCF to S-CSCF)

```
REGISTER sip:scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=351g45.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:pcscf1.visited1.net>
Proxy-require:
Require:
Roaming-Info:
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Expires:
Content-Length:
```

Path: The S-CSCF stores the contents of the Path headers and uses these addresses for routing mobile terminated sessions.

- 17. **Authentication**
  - Upon receiving the REGISTER request, carrying the authentication response, RES, the S-CSCF checks that the user's active XRES matches the received RES. If the check is successful then the user has been authenticated and the public user identity is registered in the S-CSCF.

- 18. **Cx: S-CSCF registration notification procedure**
  - On registering a user the S-CSCF informs the HSS that the user has been registered at this instance. The HSS stores the S-CSCF name for that subscriber. For a positive response, the HSS will include the user profile in the response sent to the S-CSCF.
  - For detailed message flows see 3GPP TS 29.228.
  - For the parameters in the REGISTER request (flow 16), which are sent to HSS, see table 6.2-19a.

- 19. **200 OK response (S-CSCF to I-CSCF) – see example in table 16.3-19**
  - The S-CSCF sends acknowledgement to the I-CSCF indicating that Registration was successful. This response will traverse the path that the REGISTER request took as described in the Via list.

Table 16.3-19 200 OK response (S-CSCF to I-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=351g45.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:scscf1.home1.net>, <sip:icscf1_p.home1.net>, <sip:pcscf1.visited1.net>
From:
To:
Call-ID:
```

```
Contact: sip:[5555::aaa:bbb:ccc:ddd]
CSeq:
Date: Wed, 11 July 2001 08:49:37 GMT
Expires: 7200
Content-Length:
```

Path: The S-CSCF inserts its own name to the front of the list.

- 20. **200 OK response (I-CSCF to P-CSCF) – see example in table 16.3-20**
  - The I-CSCF translates the S-CSCF name in the Path header. The I-CSCF forwards acknowledgement from the S-CSCF to the P-CSCF indicating that Registration was successful. This response will traverse the path that the REGISTER request took as described in the Via list.

Table 16.3-20 200 OK response (I-CSCF to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
Path: <sip:token(scscf1.home1.net)>, <sip:icscf1_p.home1.net>, <sip:pcscf1.visited1.net>
From:
To:
Call-ID:
Contact:
CSeq:
Date:
Expires:
Content-Length:
```

- 21. **200 OK response (P-CSCF to UE) – see example in table 16.3-21**
  - The P-CSCF removes its address from the Path header, reverses the order of the fields, saves the resulting Path header and associates it with the UE. The P-CSCF then removes the Path header from the 200 OK response. The P-CSCF then forwards acknowledgement from the I-CSCF to the UE indicating that Registration was successful.

Table 16.3-21 200 OK response (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
From:
To:
Call-ID:
Contact:
CSeq:
Date:
Expires:
Content-Length:
```