3GPP TSG SA WG3 Meeting #19 **Tdoc S3-010381**
Newbury, UK, 3rd – 6th July 2001

Title: Liaison Statement on "Progressing the work in SA3 and CN1 on the IP Multimedia core network subsystem"

Source: TSG_SA WG3

To: TSG_CN WG1

cc: TSG_SA WG2, TSG_CN WG4, TSG_CN WG5

Contact Person:
Name: Dr Mike Walker
E-mail Address: mike.walker@vodafone.co.uk
Tel. Number: +44 1635 673886

Attachments: S3-010339

SA3 thanks John O'Hare from Motorola for kindly attending part of this SA3 meeting to present an overview of the security issues arising from CN1.

SA3 discussed the issues highlighted in the presentation (S3-010339) and several observations and assumptions have been made. SA3 understands that this was not a joint meeting with CN1 and so asks CN1 to study the points below and notify SA3 if any of our comments are incorrect:

1. It should be noted that, as yet, no work has been done in SA3 on the ISC interface and SA3 realises the need to begin to work on this, in conjunction with CN1, CN4 and CN5.

2. SA3 would like to make it clear that legal intercept can only be done in the visited (serving) network.

3. It is clear to us now that the OSA API interface will be an interface between 3GPP network operators and 3rd party networks/content providers.

4. SA3 understands that multiple public identities can exist for a single private identity, and that the private identity will be used as the basis for authentication. Can a call be terminated towards a public identity that is not currently registered, if an associated public identity for that subscriber *IS* registered?

5. SA3 have the working assumption that there is always an association in the HSS between the private identity and any public identities.

6. There is a contribution to this meeting in S3-010355 dealing with authentication during registration. Discussions highlighted that it may be necessary to carry the KSI (CKSN in CN1 specifications) in the REGISTER message to help the network identify which vectors are to be used for the next authentication. Work on the security mode setup procedure is also in progress. A contribution to this meeting on the subject is in S3-010326.

7. SA3 noted that in the security functions listed in S3-010339, integrity protection should be added.

8. SA3 is assuming that currently only the registration and re-registration is authenticated, based on the private identity.

9. There is a WI identified in SA3 for end-to-end encryption, but there are not currently enough supporting companies to have it approved and it will be removed from the SA3 work plan.

10. The current working assumption in SA3 is that re-registrations are always routed towards the S-CSCF that is currently serving that UE. Whilst there appears to be confusion surrounding this assumption, it is based on the current stage 2 specification, 23.228- Can CN1 or SA2 confirm the accuracy of our assumption?

11. A WI exists within SA3 for network hiding. With regard to hiding the host and/or domain name of CSCFs and hiding the number of CSCFs within one operator's network, there is a contribution to this meeting (S3-010323) and a companion liaison to SA2 in S3-010398.

SA3 note that the decision on whether or not the standardisation of key distribution is needed is dependent on which nodes perform the encryption/decryption. This decision should be made in SA3. It is currently assumed by SA3 that the I-CSCF (THIG) that is doing the encryption could potentially be different to the node that is doing the decryption.

SA3 has up until now not considered the requirement to provide different levels of privacy, i.e. full, name, URI or off or none, and we seek justification for such a requirement.

12. The hiding of IP addresses associated with the user plane media has not been considered by SA3. Should such an IP address be given to the UE at the far end? This IP address is used by the UE for the entire duration of the (SIP signalling) PDP context. The far end UE could use the IP address to establish a session directly to that IP address, thus bypassing the IMS nodes. There may be security/fraud implications with this and SA3 will study this further.

13. Regarding session transfer, SA3 has sent a liaison statement (S3-010383) to the GSM association seeking their opinion on the fraud potential of the service and asking for guidance on this issue. SA3 would like to see the complete charging model from SA5 for this service before the work on the security aspects is progressed. SA3 note that the LS from CN1 on this issue was also sent to SA5, and are aware that SA5 are working on this already.

    Looking closely at slide number 24 in S3-010339 ("UE1 -> UE2; UE2 transfers session to UE3"), SA3 can not see how legal intercept would work in UE2's network. It was also highlighted that it is desirable to limit the number of parallel sessions in the network that can be initiated by any one terminal. In addition, it should be possible for UE2's network to release a transferred session at any time.

14. With regard to the future progression of the IMS work between SA3 and CN1, the following can be reported:

    SA3 asked for a volunteer to attend the CN1 #18 meeting in Dresden, to present the current status of the SA3 work on the IP Multimedia core network subsystem. **Krister Boman, Ericsson, agreed to do this on Wednesday 11 July**.

    SA3 agrees to the proposal in S3-010339 to create an annex in the stage 2 specification 33.203. This annex will be used to maintain a list of open issues requiring discussion/resolution. SA3 encourages e-mail discussion to progress the work between meetings. The Tdocs relating to IP Multimedia core network subsystem work from SA3 #19 and the report of the meeting will be provided on the CN1 e-mail reflector. The editor of 33.203 has kindly offered to create the new annex based on the issues raised in S3-010339.

    It was noted that there is a discrepancy between the projected timescales for the stage 2 and stage 3 IP Multimedia core network subsystem work, between CN1 and SA3. The current work plan in SA3 indicates March 2002 for the approval of the stage 2 specification, 33.203.

IM CN SS (Security) CN1 perspective

Presented by
John O'Hare (Motorola)

Note: Some of the material in this presentation has been provided with the kind permission of Keith Drage (Lucent) and Gabor Bajko (Nokia)

Agenda

- **SIP Security**

1. **Introduction / Objective**
2. **Overview of IM CN subsystem**
3. **Current list of Security issues**
4. **Process for incorporating security updates in 24.228?**
5. **Reference Material**
6. **Questions**
7. **Backup Slides**

Introduction

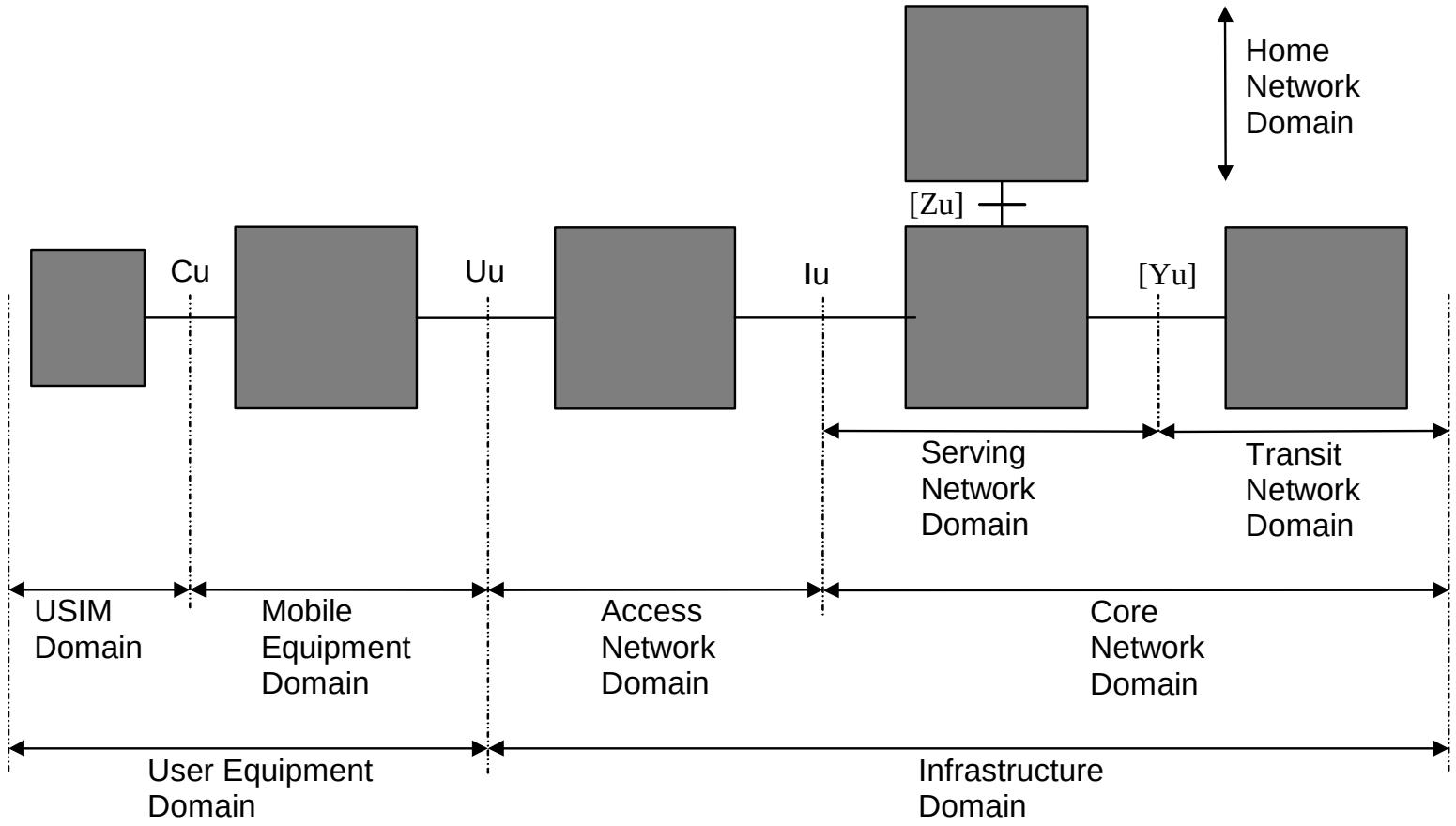
- **Presentation given based on acceptance (S3-010291) of offer (N1-010588/S3-010152) made by CN1.**
- **Objective is to**
  - **Give a brief overview of the Rel5 SIP work in CN1**
  - **Ensure we have a comprehensive list and understanding of all the SIP security issues as pertains to the 3GPP Rel5 IP Multimedia implementation**
  - **Try gain a common understanding of solutions to these issues**
  - **Give introduction to 24.228 to help SA3 determine what security information needs to be included**
- **Convey that CN1 would also like SA3 delegate(s) to attend one of the CN1 SIP meetings and to give presentation highlighting the issues and solutions for the IM CN subsystem from an SA3 perspective.**
  - **Upcoming CN1 meetings:**
    - CN1#18 (July 10-12 Dresden)
    - CN1#19 (Aug 27-31 Helsinki)

Agenda

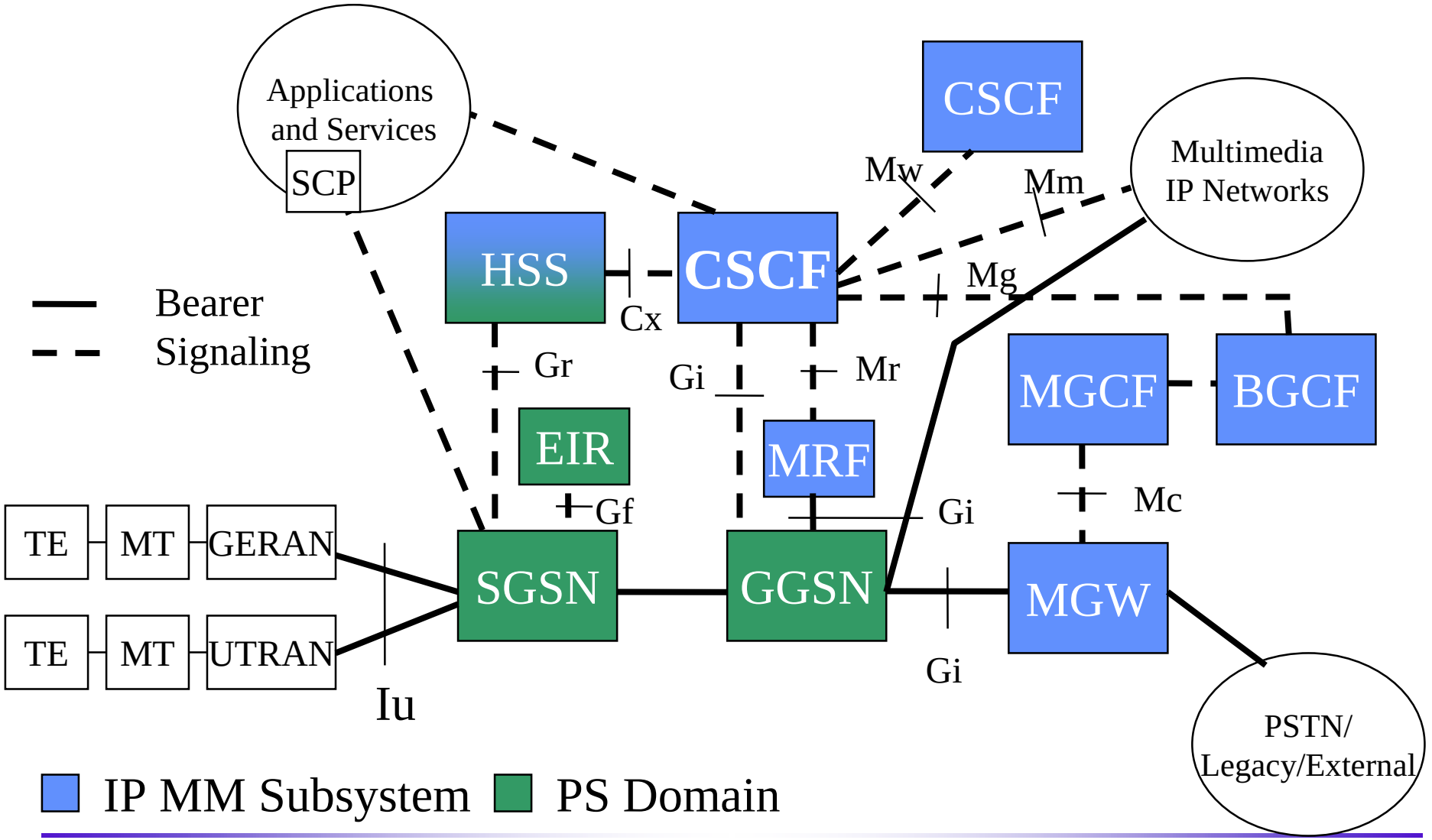
- **SIP Security**

1. Introduction / Objective
2. Overview of IM CN subsystem
3. Current list of Security issues
4. Process for incorporating security updates in 24.228?
5. Reference Material
6. Questions
7. Backup Slides

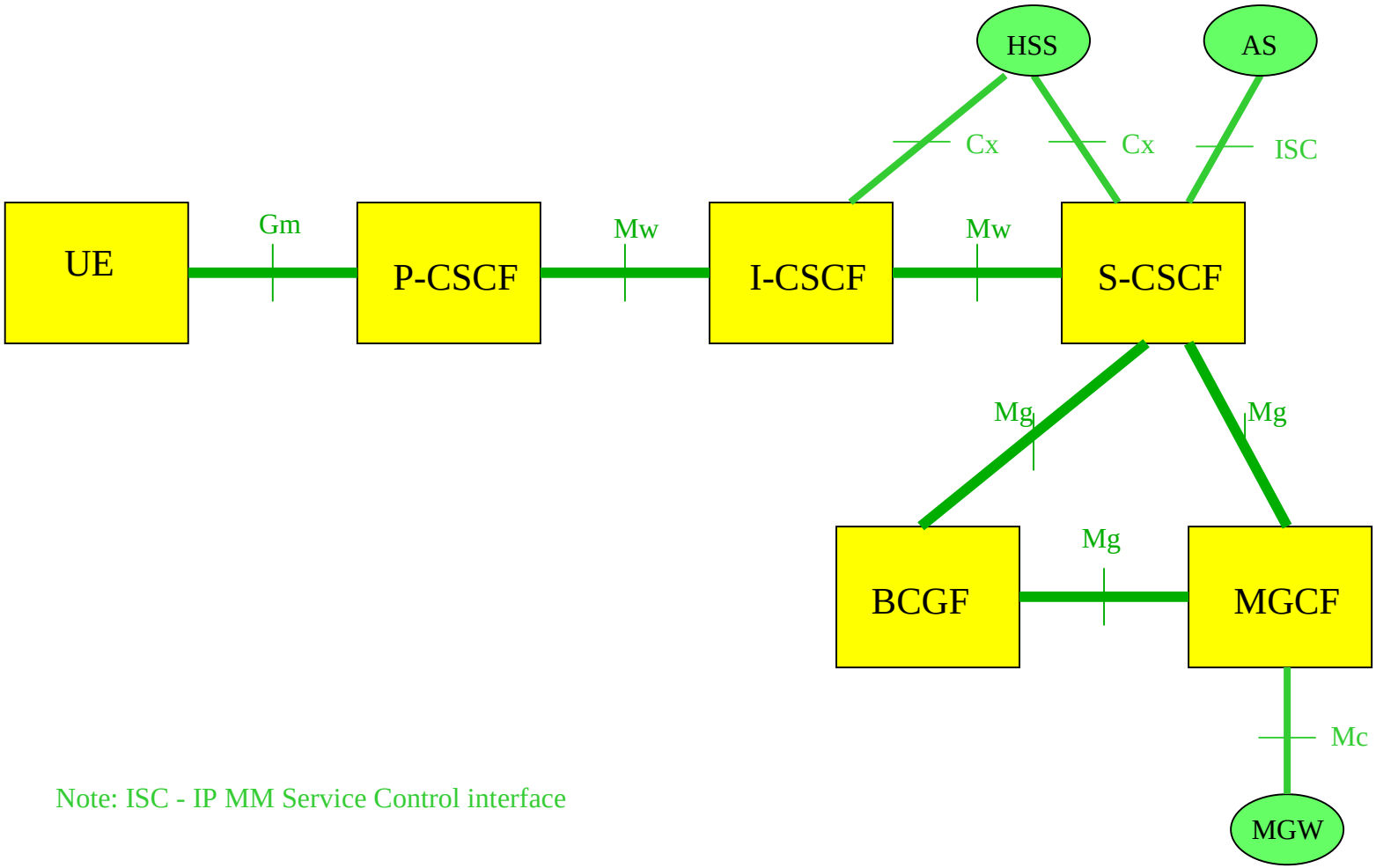
3G Reference Architecture



Rel 5 IM CN and PS Ref Architecture



Functional Architecture

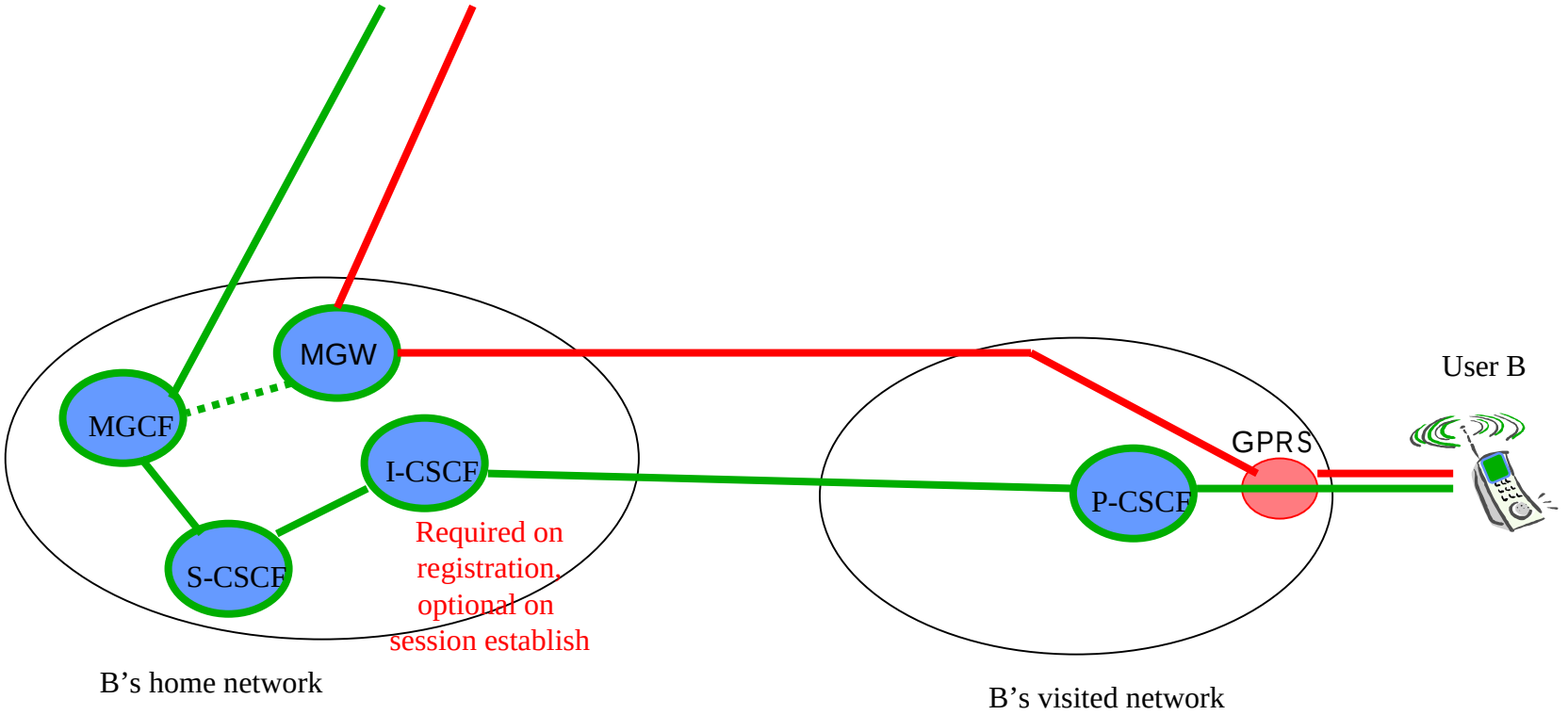


Note: ISC - IP MM Service Control interface

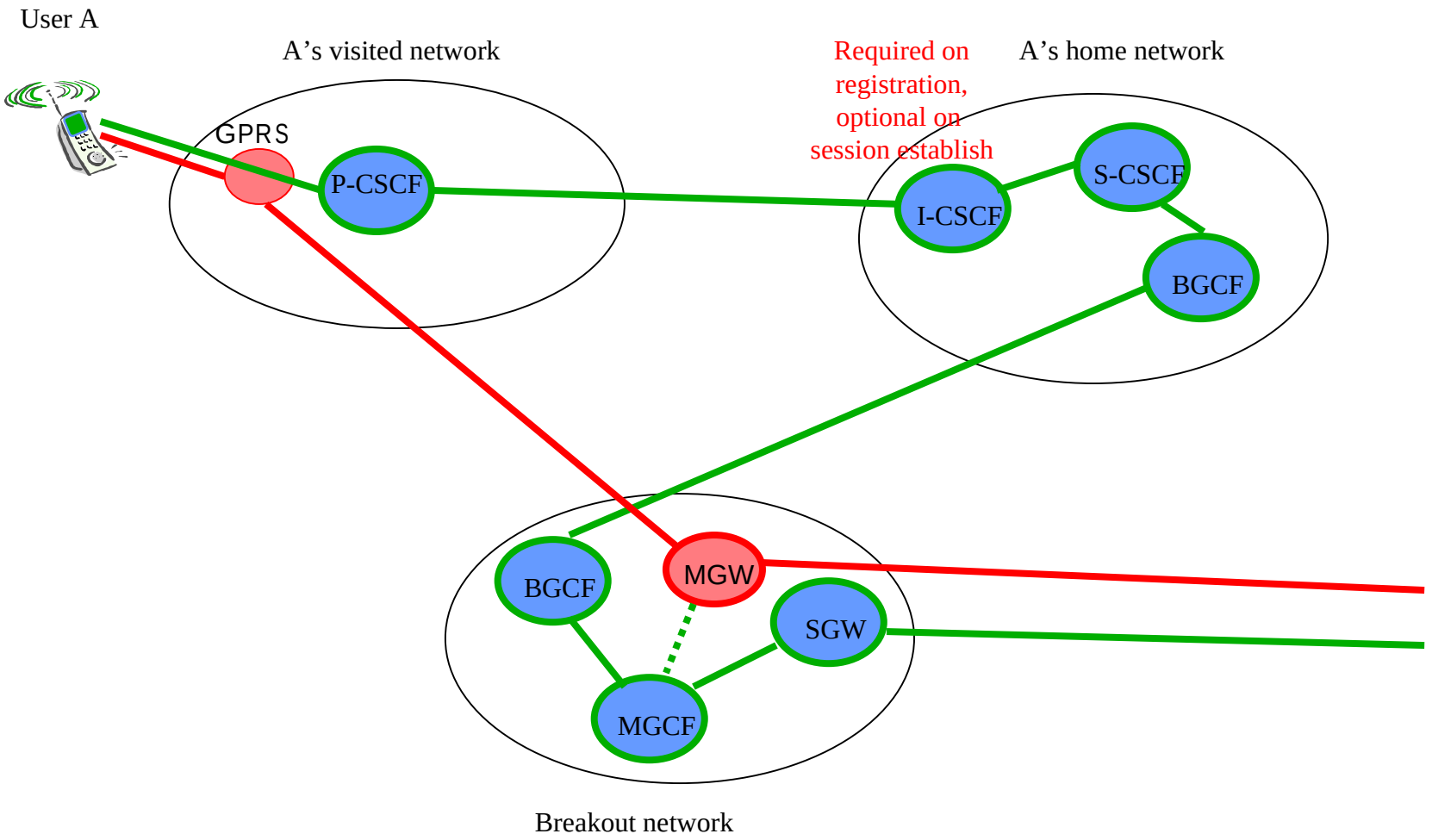
Rel5 Architecture Functional Entities

- Home Subscriber Server (HSS) - extension of the HLR to include the data pertaining to the IP Multimedia Subsystem
  - access from the CSCF will be based on IETF protocols
  - to the PS and CS domains this entity will functionally be the HLR
- Call State Control Function (CSCF) - provides the call control for a multimedia session. Has several roles:
  - serving CSCF - supports the Call state machine and provides service triggers for a session
  - proxy CSCF - proxies messages between the UE and the serving CSCF (acts on behalf of the UE within the IMS). Also performs QoS authorization i.e Policy Control Function.
  - Interrogating CSCF - used to allocate or determine the S-CSCF. May also perform a network hiding function.

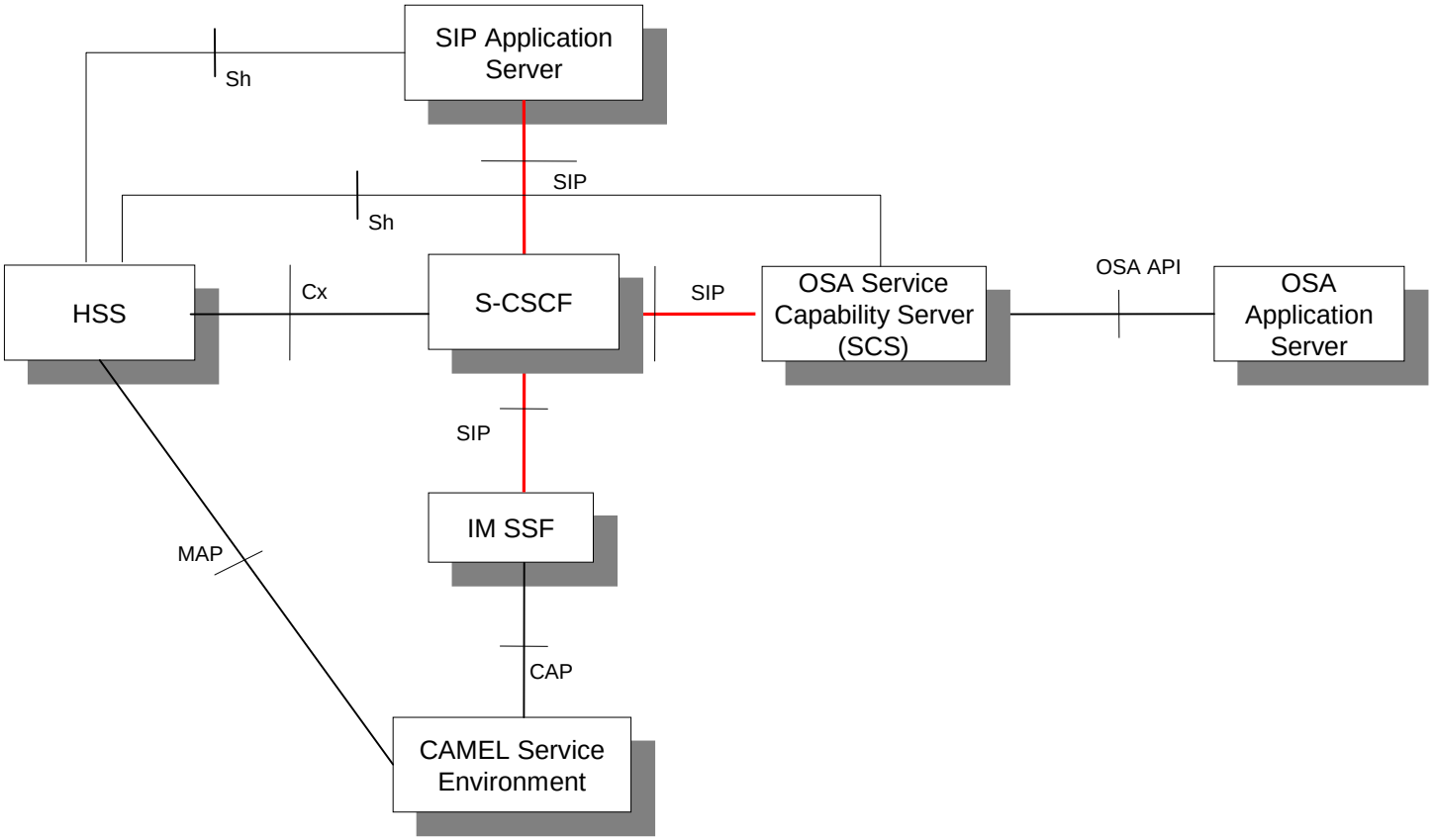
Example 1 – PSTN to UE session



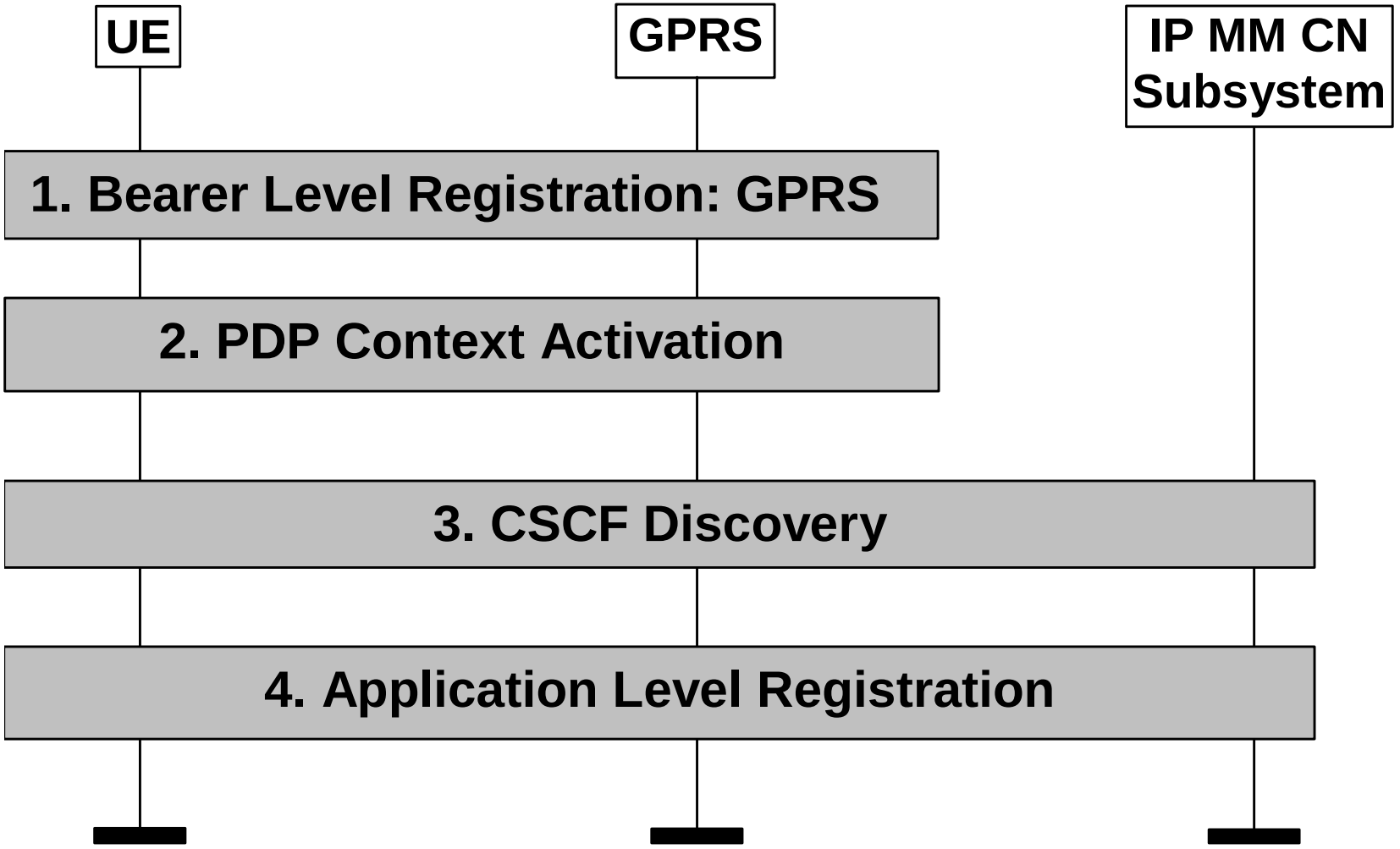
Example 2 – UE to PSTN session



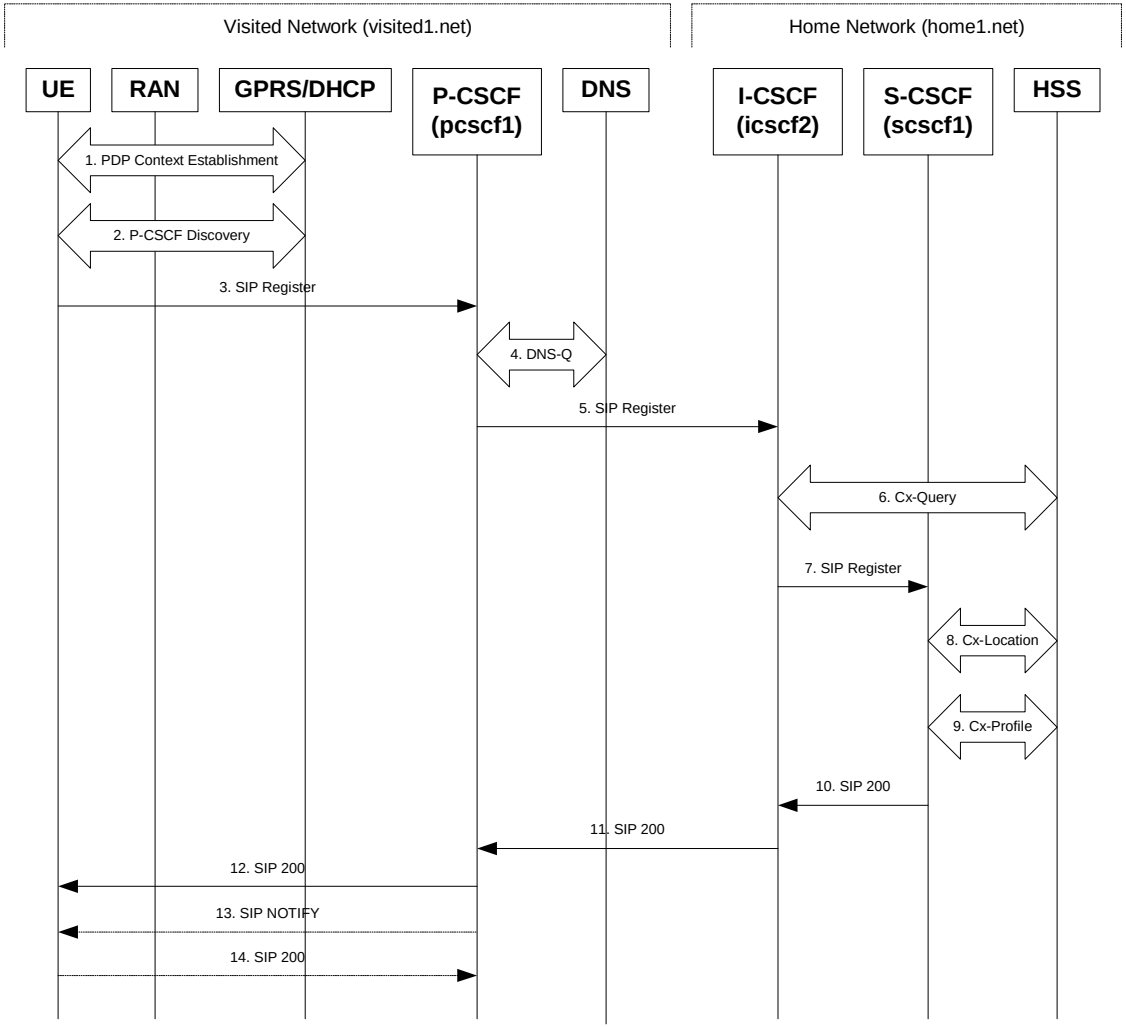
Provision of Services



Registration Overview



Registration Example 24228-110 7.1



Note: Alternatives to SIP Notify and 200 OK are currently being studied in CN1

24.228 7.1-3. Register

Table 7.1-3 SIP 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@home1.net>
To: <sip:user1@home1.net>
Contact: <Sip:[5555::aaa:bbb:ccc:ddd]>
Call-ID: 123456789@[5555::aaa:bbb:ccc:ddd]
CSeq: 1 REGISTER
Expires: 7200
Allow-Events: org.3gpp.nwinitdereg
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 routeing 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.

…

24.228 7.1-5. Register

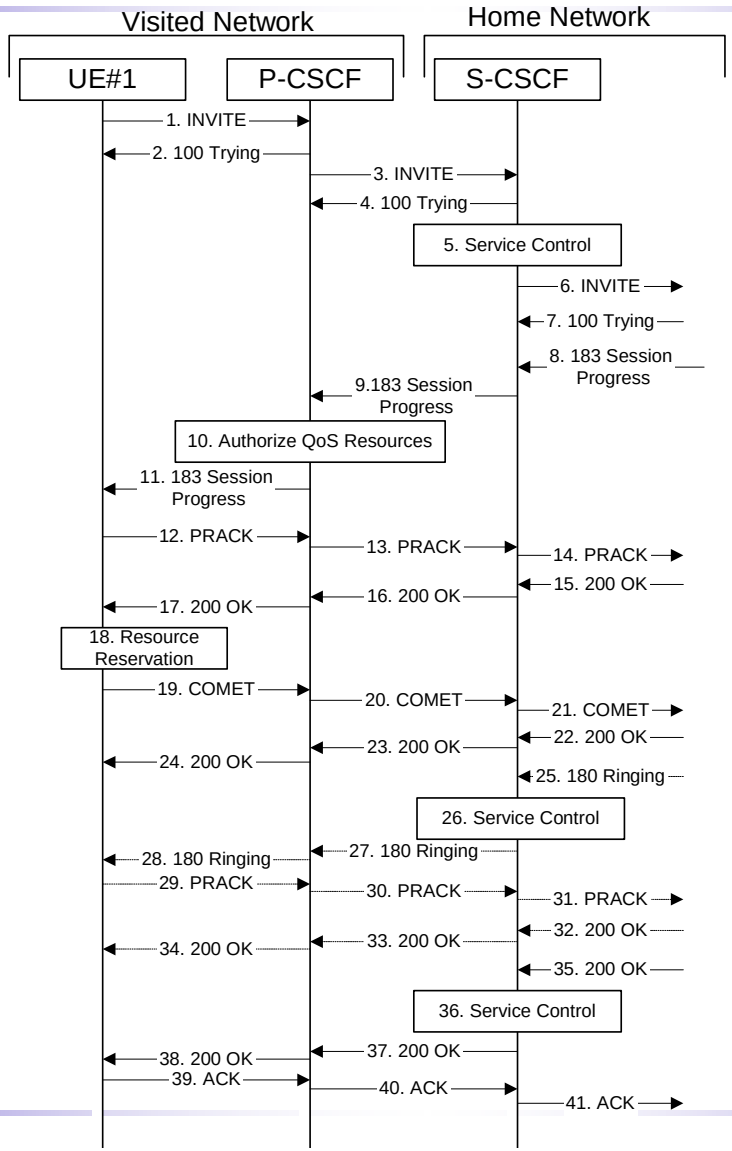
Table 7.1-3 SIP REGISTER request (UE to P-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
        Via: SIP/2.0/UDP pcscf1.visited1.net, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]
Path: <sip:pcscf1.visited1.net>
Proxy-require: path
Require: path
From:
To:
Contact: <sip:user1%40home1.net@pcscf1.visited1.net>
Call-ID:
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.
…

…..

Session Establishment (UE to S-CSCF)



Agenda

- **SIP Security**

1. Introduction / Objective
2. Overview of IM CN subsystem
3. Current list of Security issues
4. Process for incorporating security updates in 24.228?
5. Reference Material
6. Questions
7. Backup Slides

Security related categories

- **Security related categories**
  - **Authentication**
  - **Encryption**
  - **Hiding (Network Configuration)**
  - **Session (Call) Transfer**
  - **Security Mode Setup**
- **Related contributions to-date:**
  - **N1-010588 (S3-010152) LS on "Security for IM SIP session Signalling" and S2-010757 (S3-010160) Proposed Reply LS for "IM User Identities"**
    - S3-010291 Response LS (from SA3 to CN1 and SA2 on N1-010588 and S2-010757
  - **S3z-010035 – SIP Headers and Messages for Security in 24.228 flows**
  - **N1-010890 (S3-010249) LS on the IM Call Transfer Service**
    - N1-010706 – Detailed Flows for Call Transfer Service
    - S3-010292 – Response to LS on the IM Call Transfer Service

S3-010291 Response LS to N1-010588 and S2-010757

- *"SIP Header Parameter modification by I-CSCF"*
  This is possible because integrity protection is done in a hop-by-hop fashion.

- *"Via and Record Route Header Hiding by I-CSCF"*
  A new work item on hiding mechanisms has been created by S3 at S3#18 *which was approved at SA#12.* The S3 work on this new work item is expected to be completed by July 2001?

- *"Contact header modification by P-CSCF"*
  This is possible because integrity protection is done in a hop-by-hop fashion.

- *"Useage of the User Private Identity"*
  S3 sees no security problem with the current working assumption by S2 and N1 "that the Registration flow is definitely the only time the Private User Identity is sent to the network in SIP signalling messages".

- *"Authentication of Invite and other SIP session signalling messages"*
  It is the current working assumption of S3 that authentication is only required for registration and re-registration.

- *"Integrity protection of SIP signalling messages (especially the first message that is sent)"*
  The mechanism for integrity protection of SIP signalling messages between the UE and the P-CSCF is still under study by S3, the mechanism for integrity protection of SIP signalling messages between other IMS entities is IPSec (ESP). The first message that is sent (REGISTER) cannot be integrity protected as no integrity key establishment has yet taken place. However, when REGISTER is sent a second time it can be integrity-protected. The precise mechanism for this is still under discussion in S3.

- *"Requirement for SIP signaling to support Key exchange for encryption of bearer"*
  S3 understands that " encryption of bearer" refers to end-to-end encryption of user data. S3 would like to inform N1 and S2 that an S3 work item relating to end-to-end security in UMTS exists. S3 can confirm that SIP signalling messages will be required to support key exchange for IMS end-to-end encryption. However, no solutions are currently available.

Authentication

- **CN1 documents do not yet, contain any flows for authentication**
- **Working assumption: authentication is done during registration and re-registration**
  - (S2-011317)
- **CN1 waits for other requirements regarding authentication:**
  - **Should the system be able to authenticate INVITEs in MO calls (authenticate the caller) and/or MT calls (authenticate the callee)?**
  - **Should the system be able to authenticate any of the parties during a (long) call?**
  - **Should CN1 develop a mechanism for authentication which is not bound to the Registration procedure? (Document 33.203 only provides IMS Authentication and Key Agreement example with Register Request)**
  - **Network initiated registrations and de-registrations**

Encryption

- **Signalling**
  - **Assuming hop-by-hop, at what layer does encryption take place?**
- **Bearer**
  - **End-to end encryption to be assumed?**
  - **Are keys to be transported in SDP information?**

Hiding -1-

- **CN1 incorporates the following hiding requirements into Rel5:**
  - **Hiding the host and/or domain name of CSCFs**
  - **Hiding the number of CSCFs within one operator's network**
    - For this purpose a new functionality is defined in CN1: THIG (Topology Hiding Internetwork Gateway)
    - THIG encrypts/tokenizes entries in the Via, Path, Record Route headers. Is there a difference between encrypt and tokenize?
    - A key_distribution_mechanism/database_synchronization_mechanism is needed between THIGs for the implementation of this requirement (encryption/tokenization). Can CN1 take as a working assumption that such a mechanism will exist in Rel5?
  - **Hiding the caller's public-ID: privacy**
    - Different levels of privacy: full | name | URI | off
      - Full privacy: display name and the address URL must be hidden.
      - Name privacy: The Display name has to be hidden.
      - URI privacy: The address URL has to be hidden.
      - Off: Indicates that lack of privacy is explicitly requested.
    - For this purpose a new SIP header was defined in the IETF SIP privacy draft: Remote-Party-ID header field, which carries the public-ID of the caller
    - The Remote_Party_ID header field is encrypted by the caller's S-CSCF and decrypted by the same S-CSCF

Hiding -2-

- **Hiding the caller's IP address: anonymity**
  - User requires IP address privacy. All the IP addresses that reveal user identity should be hidden, including SDP (it requires an Anonymiser for the media part of SIP message)
  - A new header, Anonymity is defined to implement this requirement
  - Is this a real requirement in an environment where the IP addresses are dynamically assigned to mobile terminals?
  - Does the network operator require, not to expose IP addresses to called part?

Session (call) Transfer

- UE1 -> UE2; UE2 transfers session to UE3
  - UE3's public_ID is contained in the Refer-To header
  - UE3's public_ID can optionally be encrypted (being represented by a "token"). The encrypted string must reflect the encryptor's name.
  - When that happens 3 networks will be involved in the new session setup path:
    - UE1's, UE2's and UE3's
- Request SA3's guidance based on the GSM Call Transfer Feature re:
  - Should UE1's network be aware of the real destination being represented by the "token" it is calling? Are there any security implications?
  - Should UE2's network be able to do legal interception on the media flow between UE1 and UE3?
  - Should UE2's network be able to limit the number of parallel calls UE2 can transfer?
  - If UE2 is a prepaid customer, and assuming UE2 pays for the transferred session, then is a mechanism is required where UE2's network may terminate the call should UE2's credit expire (during a session)?

Security Mode Setup

- Purpose of this procedure is to agree on the used encryption /integrity protection algorithm and to signal the start of the cryptographic protection for the traffic
- Details of this negotiation need to be worked out.

Agenda

- **SIP Security**

1. Introduction / Objective
2. Overview of IM CN subsystem
3. Current list of Security issues
4. Process for incorporating security updates in 24.228?
5. Reference Material
6. Questions
7. Backup Slides

Process for incorporating security updates in 24.228?

- **The End Objective:**
  - **24.228 needs to include example flows showing authentication, encryption, hiding details etc. to the same level of detail as shown on Slides 14 and 15 of this presentation.**
  - **Protocol and call model impacts to be captured in 24.229 and 23.218 respectively**
- **Both CN1 and SA3 will need to work in close co-operation:**
  - **Security requirements**
    - SA3 captures all agreed requirements in 33.203?
  - **Stage 2 flows**
    - Should these be incorporated in to 23.228 or 33.203?
  - **Stage 3 flows (i.e. 24.228)**
    - Need for joint SA3/CN1 meeting, close co-operation between SA3 and CN1 delegates?
- **Suggestion:**
  - **SA3 to send LS to CN1 (and SA2?) detailing the groups understanding on the process for incorporating security related aspects into 24.228**
  - **SA3 requested to send delegate(s) to present IMS security workings to CN1?**
  - **Add an Annex to 33.203 as a temporary holding ground for these types of questions/issues from CN1?**
    - Contributions to the Annex would consist of questions from CN1 and answers from SA3☺
    - Annex removed before spec goes for approval.

5. Reference Material

- **3GPP**
  - **TS 23.228: "3rd GPP; Technical Specification Group Services and System Aspects; IP Multimedia (IM) Subsystem - Stage 2".**
  - **TS 24.228: "3rd GPP; Technical Specification Group Core Network; Signalling flows for the IP multimedia call control based on SIP and SDP".**
  - **TS 24.229: "3rd GPP; Technical Specification Group Core Network; IP Multimedia Call Control Protocol based on SIP and SDP".**
  - **TS 23.218: "3rd GPP; Technical Specification Group Core Network; IP Multimedia (IM) Session Handling; IP Multimedia (IM) call model"**
  - **TS 33.203: "3rd Generation Partnership Project; Technical Specification Group SA3; Access security for IP-based services"**
- **IETF**
  - **draft-ietf-sip-rfc2543bis**
  - **draft-sip-manyfolks-resource**
  - **draft-ietf-sip-100rel**
  - **draft-ietf-sip-privacy**
  - **draft-ietf-sip-call-auth**
  - **draft-roach-sip-subscribe-notify**

Agenda

- **SIP Security**

1. Introduction / Objective
2. Overview of IM CN subsystem
3. Current list of Security issues
4. Process for incorporating security updates in 24.228?
5. Reference Material
6. Questions
7. Backup Slides

Agenda

- **SIP Security**

1. Introduction / Objective
2. Overview of IM CN subsystem
3. Current list of Security issues
4. Process for incorporating security updates in 24.228?
5. Reference Material
6. Questions
7. Backup Slides

(1) Example IMS Services

- **Web Voice Response Unit Replacement (ATT)**
  - **a) 3G subscriber calls a Service Center**
    - Terminal indicates ability to display Web response in setup request
    - CS based calls get routed to a VRU
  - **b) Service Center responds with a Web page containing a list of possible 'destinations.' Possible destinations include, for example:-**
    - Continue with web interaction for online ordering.
    - Click to dial a human customer service representative.
    - Click to send a text message requesting more information, along with optional attachments
      - (e.g., scanned bar code from newspaper along with customer contact information from SIM card).
  - **c) List is presented to the caller, caller chooses preferred destination**
  - **d) Session continues in preferred media**

(1) Example IMS Services

- **Web access to voice mail (ATT)**
  Phone browser displays list of current voice mail messages

1. Terminal application downloads list of voicemail messages from voicemail server
2. Terminal offers the list to the user
   - Random access to messages
3. “Click to dial” connection to voice mail server

Rel5 could support this as an integrated service in the IM domain, whereas R99 might allow only a combination of CS and PS domain applications. This would need to be coordinated by complex service logic in the terminal.

(1) Example IMS Services

- **Integration of audio+data sessions (ATT)**
  - *Download caller picture /company logo during call setup*

  1. **User sets up a regular voice call and passes a bitmap image (or URL) in the setup message**
  2. **Callee is presented with calling number of caller + provided image**

(1) Example IMS Services

- **Integration of audio+data sessions (ATT)**
  Private chat session during audio conference call

  1. User attaches to audio conference session
  2. Receives back a list of participants
  3. User is presented with the list and can initiate a chat session to any of the other participants from this (menu) interface.

- *Rel5 could support this as an integrated service in the IM domain, whereas R99 might allow only a combination of CS and PS domain applications, coordinated by complex service logic in the terminal.*

(2) SIP - Features

- **User location:**
  determination of the end system to be used for communication;
- **User capabilities:**
  determination of the media and media parameters to be used;
- **User availability:**
  determination of the willingness of the called party to engage in communications;
- **Session setup:**
  “ringing”, establishment of call parameters at both called and calling party;
- **Session handling:**
  including transfer and termination of calls.

(2) SIP – What it does not provide

- Application services
  - e.g. phone, email
  - applications that manage the bearer path
- Application control
  - Traditional Call Control and Supplementary Services
- Bearer Path Security and QoS Setup
- Lots of other things people want SIP to provide

(2) SIP - Advantages

- Services
  - SIP is independent of application or service
  - SIP can be used to set up most applications or services
- Scalability
  - Fast and Simple inside the network
  - Edge devices do most of the work
- Extensibility
  - SIP is independent of applications and services
  - Based of extensible concepts - MIME, HTTP, URL
- Flexibility
  - SIP does not define complete system
  - Does not mandate architecture, usage patterns, deployment, ...

(2) SIP – Basic Messages (Request or Response)

- **Methods**
  - **INVITE** — **Invite target to join a session**
  - **ACK** — **Confirms final response to an INVITE**
  - **OPTIONS** — **Asks server about its capabilities**
  - **BYE** — **Terminate or leave a session**
  - **CANCEL** — **Cancel pending Request**
  - **REGISTER** — **Register with SIP location Services**
- **Responses**
  - **1xx** — **Informational (e.g. Trying, Ringing)**
  - **200** — **Success (200 OK)**
  - **3xx** — **Redirection**
  - **4xx** — **Client Error (e.g. Bad Request, Unauthorized)**
  - **5xx** — **Server Error (e.g Bad Gateway, Version Not Supported)**
  - **6xx** — **Global Failure (Busy Everywhere, Does Not Exist anywhere)**

(2) SIP - Terminology

- **User Agent Client** — **Application that sends INVITE**
- **User Agent Server** — **Application that receives INVITE**
- **User Agent** — **Application that sends and receives INVITE**
- **Proxy**
  - **Intermediary program that makes requests on behalf of other clients.**
- **Registrar**
  - **Server that accepts REGISTER requests and updates location server**
- **Location Server**
  - **Used to obtain information about a callee's possible location(s).**
- **Session**
  - **A set of multimedia senders and receivers and the data streams flowing from senders to receivers. (e.g. a multimedia conference)**

(3) Rel5 Architecture
Application of SIP to 3GPP

- **User Agent Client** — **Allocated to UE**
- **User Agent Server** — **Allocated to UE**
- **User Agent** — **Allocated to UE**
- **Proxy** — **Allocated to CSCF**
- **Registrar** — **Allocated to Serving CSCF (S-CSCF)**
- **Location Server** — **Allocated to HSS**
- **Session**
  - **A set of multimedia senders and receivers and the data streams flowing from senders to receivers. (e.g. a multimedia conference)**

(5) UE-to-UE Session: Both Roaming and Home Served