Norges teknisk-naturvitenskapelige universitet
Institutt for telematikk

EKSAMENSOPPGAVE I TTM4130 – EXAM IN TTM4130 SOLUTION
[text added in brackets is not required for obtaining full score]
TTM4130 - Tjenesteintelligens og mobilitet
TTM4130 – Service intelligence and mobility

Faglig kontakt under eksamen:	Lill Kristiansen
Tlf.:	97 72 72 27
Eksamensdato / Date:	4 juni 2009 / June 4th 2009
Eksamenstid /Time:	09:00-13:00 / 9:00 am – 1:00 pm
Vekttall / Credits :	7,5 SP
Examination aids:	**D:** No written and handwritten examination support materials.
	A specified, simple calculator is permitted.
Tillatte hjelpemidler/	**D:** Ingen trykte eller håndskrevne hjelpemidler tillatt
	Bestemt, enkel kalkulator tillatt
Språkform / language:	**English** English is the master text (authorative)
	(Norwegian text is for information only)
	Answer can be in nynorsk, bokmål or English
Number of pages in English:	4 (pages 2-5)
Antall sider bokmål:	4 (sidene 6-9)
Antall sider nynorsk:	0
Appendix (in English):	7 (pages 10- 16 with text)
Sheets for drawings	2 sheets which may be handed in
Sensurdato[1]:	**25. juni 2009**

[1] Merk! Studentene må primært gjøre seg kjent med sensur ved å oppsøke sensuroppslagene. Evt. telefoner om sensur må rettes til sensurtelefonene. Eksamenskontoret vil ikke kunne svare på slike telefoner.

You should **start by reading through all the material** and then decide which sequence you want to use when answering the exercises. In some places there are some dependencies that are listed, but it is possible to start e.g. with exercise 3, 4, 5 or 6 if you do not want to start with SIP. 2 sheets with MSC diagrams to be filled in by the canditate may be used to save some drawing and are attached at the end. **Short answers are requested.**

Make your own assumptions if the text is unclear, or information is missing.

Exercise 1. (26 %) About SIP (SIP proper as defined by IETF)

a) (8 %) List 4 of the main entities in the SIP architecture and describe the main tasks of each of the entities.(UA-C + UA-S = UA, this counts as one entity). Do not list DNS

lillk 6/4/09 11:56 AM
Deleted: s

***0) UA User Agent** in the user's terminal handles both outgoing and incoming calls (tutorial states: "UA Client (originates calls) UA Server (listens for incoming calls)" which is OK, but not the whole truth). UAC and UAS is also responsible for call states, timeouts etc. UAC is responsible for sending method ACK as appropriate. UAC is also responsible for registering with the network*

Tutorial and IMS book differs a bit on registrar and loc.server. The tutorial seems to view this as one entity, while book handles this as two different (both answers will we honored)
***1*) SIP Registrar** (according to tutorial)*

– accept registration requests from users

– maintains user's whereabouts at a Location Server (like GSM HLR)

(Thus is seems that loc.server is 'a part of' registrar)

IMS book list 4 servers and list loc. and reg. as two different servers.

***1) Location server** -maintains loc. of users*

***2) Registrar server** - accept registration requests from users*

***3) Proxy server** - forwards SIP messages see also answer to 1.c)*

- tutorial: They glue SIP components such as phones, gateways, applications and other domains by implementing some routing logic

(not required but one may add: A proxy may fork a request to multiple destinations, be responsible for various services, security etc.)

***4) Redirect server -** redirects callers to other servers*

– Used rather rarely as operators appreciate staying path. May be used to achieve very scalable load distribution (hence maybe less natural to list, but a natural part of the endpoint centric view in SIP)

***5) B2B UA** may also be listed*

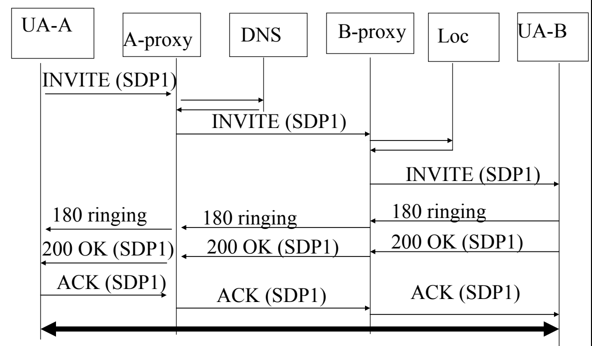
- behaving as a UA in 'both directions'. May implement additional states and may be responsible for various additional services,

Any 4 of these will be honored (but not listing 1 and 1) and 2) of course). (Other entities may also be honored but not entities like S-CSCF etc from IMS)*

b) (9 %)
Explain the role of SDP in SIP.
SDP is used for media negotiation. May add, but not needed: SDP is sent as payload in SIP (in INVITE and sent also in 200 OK and in ACK).
List also other major protocols to be used with SIP and explain how they complement the functionality in SIP.
RTP+RTCP for media streaming and control, *Diameter for AAA, some protocol for QoS negotiation ++ (Any 2 protocols with functionality will be OK)*
Explain how SIP is similar to HTTP and explain also some major differences
Based on http and is a text based protocol and with same use of 1xx, 2xx and 4xx etc for responses. Differently because in telephony the endpoint may receive an incoming call hence the UAS (server) is introduced. We asked for differences in plural, which was maybe not so wise. Real time aspects and dependability req. may also be said to be a difference.180 ringing is introduced in SIP and may be said to be a (minor) difference. It is true that SIP is for signaling, and that this is different from http. However: SIP allows jpeg to be sent in INVITE ((picture caller-id). In IP all signaling is transported in transport network. GPRS operators are not happy with jpeg) as signaling.

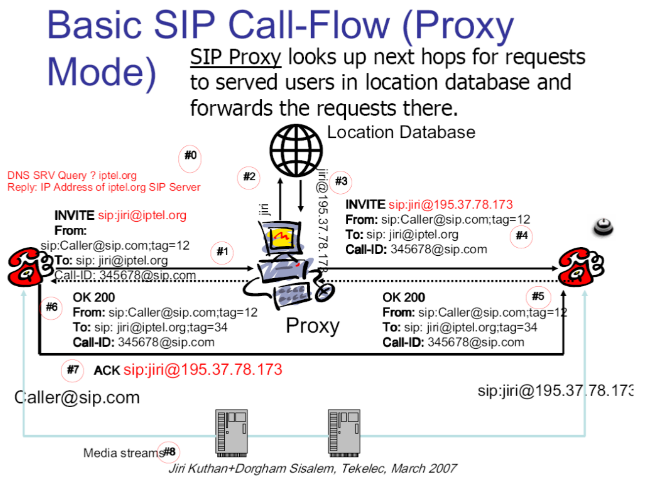
c) (6 %)
Show a call flow for call/session establishment between Alice (caller) and Bob (callee/ called party) until the media flow is established.
- You may use an MSC, or you might use a 'free' drawing showing a call flow with message numbers You may use the "SIP trapezoid" . You may assume SDP1 is a voice proposal and that this will be accepted by B.
- You need *not* include any re-negotiation of SDP. You need *not* include forking
- You *shall include* methods (like INVITE and more) and response messages (like 180, 200) etc. all the way until the media flow is established.

MSC based on 'SIP trapezoid IMS book p.301) (DNS may be skipped)
(note some similarity with MSC in Figure 3 *from PSTN)*
If no proxy is shown that should be explained, 2 proxies is the most natural choice
As a minimum INVITE, 200 OK and ACK shall be listed but parameters wanted



100 trying may be listed, but not needed
SDP1 should be visible in the diagram at least in INVITE
(preferrably also in OK and ACK)
To, From etc. not needed

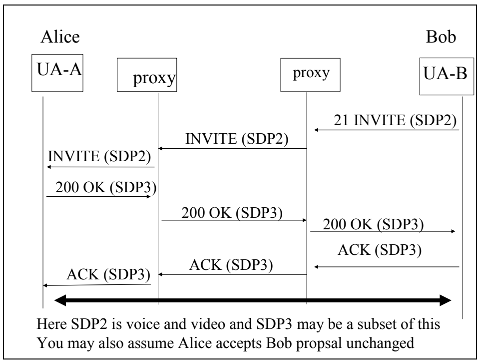
Alternative figure is p. 29 in Sip tutorial



This figure shows only one proxy (better to show inbound and outbound as two separate. The figure is rather messy, but may be redrawn to an MSC. Names should be Alice and Bob of course)

d) (3 %)
Show how Bob propose new media types and how this proposal is accepted by Alice. You may let SDP2 represent this new voice+video proposal. This message exchange shall take place after the call flow in c) is successfully carried out.

- *Note:* To ease the sensors reading of this call flow you shall number the first message now as message 21 (regardless of how many messages you actually used in c).
- You *should not* "crash" the new messages onto the drawing used in c) in a manner that makes it unreadable. (A small MSC where each message follows in a timely fashion should do the job here.)



Since this drawing is an MSC the message numbers are not really needed (unless you want to refer to a message in your text). In a 'free' drawing numbers are needed (to illustrate the sequence of course)

You should indicate that SDP2 is carried in 21 (re-)INVITE, and that some SDP (SDP2 or SDP3) is carried also in OK (SDP in ACK is not required) (may be stated in text as well)

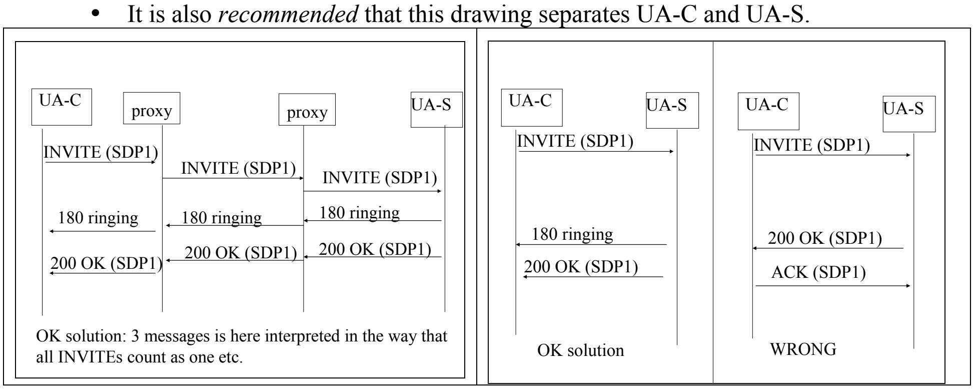
Exercise 2 (9 %) SIP protocol details (SIP proper)

a) (6 %) Call-ID is one header field in the INVITE method.
Task: List *4 other header fields* used in INVITE . For each of the chosen header fields you shall explain briefly how they are used (i.e. what meaning they have)

- You should preferably include header fields that you find most important (though all header fields are of course important in different ways). Try *not* to include header fields that are specific for IMS.
- *A natural selection is this (from tutorial p. 76)*
    - ***Via:** for routing replies back along the same path. via is very natural to list*
    - ***From:** SIP address of request originator*
    - ***Contact:** SIP address of originator's equipment*
    - ***Content-type:** type of message payload*
- *Other field such as **Content-Length** or **CSeq** may also be listed, as they are important as well. **Subject** may also be of relevance for the end-user, and maybe for some value added services (but maybe not so natural to list this, it is free text)*
- *The teacher believed that **P-Preferred-Identity** (from appendix material was IMS specific), however this is no so (it is listed in tutorial), so in fact you were given (unintended) help here.*

b) (3%) Illustrate a SIP transaction which starts with INVITE and contains 3 messages. You may make a new example or re-use a part of a call flow from exercise 1.
*Comment: There were many questions on this formulation. The term **transaction** is what is important here, you should not list 'just any' MSC with 3 messages starting with INVITE. A transaction has a natural ending (ref. buying stuff, and paying for it)*

- *Please make a new drawing* to ease the reading for the sensors.
- It is also *recommended* that this drawing separates UA-C and UA-S.



Since I have reused electronically the answer from 1, I have kept 2 proxies (1 is OK as well)

It is fully acceptable to have only UA-C and UA-S (0 proxies). In fact this might be the most natural interpretation of "3 messages". NB: ACK shall not be included, ACK is a separate method. One transaction contains exactly one METHOD (typically from UA-C with one or more responses (from UA-S). In fact the term transaction was used is the example questions listed at the end of the learning goals.

Exercise 3 (15 %)

a) Explain Mobile IP (M-IP). Explain the main entities involved and the basics of how M-IP works.

Mobile IP uses two IP addresses: a) a fixed home address and b) a care-of address that changes at each new point of attachment. FA and HA are the major entities involved

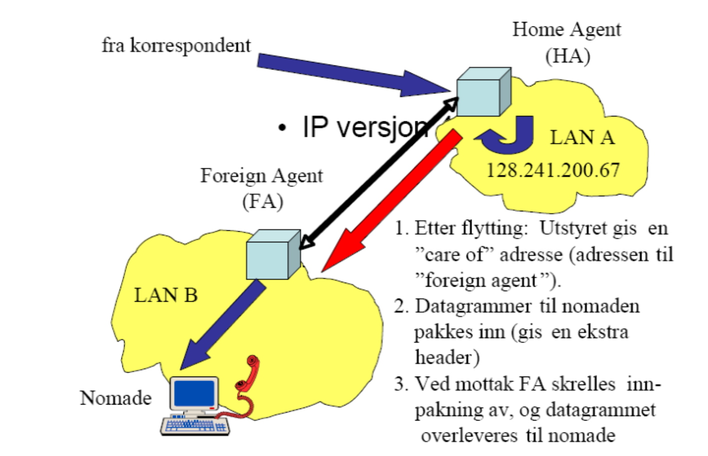
"Mobile IP, then, is best understood as the cooperation of three separable mechanisms: 1) Discovering the care-of address; 2) Registering the care-of address; 3)Tunneling to the care-of address." (From Perkin's tutorial) You are not required to state this as crystal clear as he does)

(CN: Corresponding node MN: Mobile node or 'nomade')

***FA**: Foreign agent – somewhat like a VLR mapping MN to FA via c/o address*

***HA**: Home agent – somewhat like an HLR responsible for knowing the current (care of, c/o) IP address of EP, However different from HLR: All traffic (packets) will be forwarded by HA (tunneled)*

Optional figure: MN finds FA and registers home to HA. CN starts sending packets (via HA to FA (tunneled), 'detunneled' in FA which sends to MN (in some cases MN may act also as FA according to LN)



Translation:

1: After move equipment [MN] is given a care of address

2: packets to [MN] is given an extra header [tunneling]

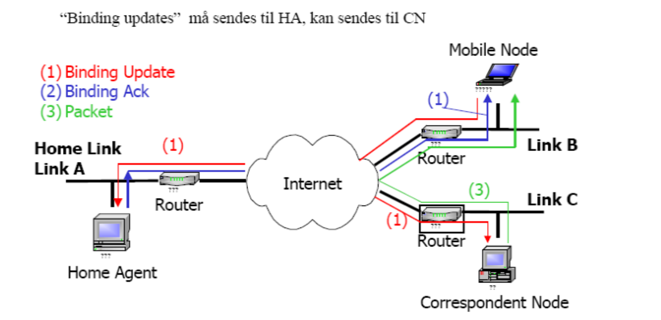
3: At the FA the extra header is removed (detunneled) and packet is sent to [MN]

from LN fig. 8.2 also from slides 06_Chapt8.pdf

b) Explain how route optimization in M-IP works when using IPv6.

In fact it is probably not important that IPv6 is mentioned here.

*One problem in a) is 'triangulation' (all packets send from CN **via HA** to FA and MN). Route optimization avoids this by allowing MN to inform CN about the c/o address. This is done by having the binding updates from MN routed directly to CN (as well as to HA). Later packets are then sent directly (i.e. route optimal)*



Comment: FA is not shown here

It may be that FA and MN is the same entity orthat FA is an entity 'close' to MN

From LN Figur 8.5 (p. 73) as well as from slides 06_Chapt8.pdf

c) Explain two major issues if M-IP is to be used with realtime multimedia streams. You shall not cover the route optimization from b)
Hint: Think of how GSM handles mobility in the visited network
Hint: IETF has a proposal using 'Hierarchical M-IP' (HMIP) and using a Mobility Anchor Point (MAP) in the network visited by the mobile node

***A)Packet loss** during 'handover': M-IP is well suited for TCP connections and nomadic type of mobility (i.e. for non-realtime). For TCP packets may be retransmitted and the TCP connection may be preserved. This may work even in cases where a MN such as a lap top is unplugged and re-plugged into a new (fixed) nw point of attachment. Retransmission after a longer time is not tolerable in real time media streams (as VoIP) VoIP has requirement <= 100 ms) (this number is not requsted). To have a local entity in visited nw handle the'local' handover is needed to avoid too much packet loss and too much latency. (Handling 'double' streams may also be an option)(Shorter avswers will be fully honored)*

***B) Mobility updates:** If every minor update is sent to HA this will cause a lot of 'signaling traffic'. The hierarchical approach HMIP with MAP (mentioned above and below) will act somewhat similar to the MSC/VLR in GSM. Changes in BS and BSC will only affect the VLR/MSC and not the HLR. Here one may notice that IPv6 will probably handle issue B) relatively well, since the IP-address may be kept when changing radio attachment point*

BTW: LectureNotes mention an (old) version of mipshop charter in IETF (http://www.ietf.org/html.charters/mipshop-charter.html: and quotes:
*"HMIPv6 deals with reducing the amount and latency of signaling ..by introducing the Mobility Anchor Point (MAP) (a special node located in the network visited by the mobile node). The MAP acts somewhat like a **local home agent** for the visiting mobile node ..." (my emphasis)*

Comment: It would seem more natural to compare MAP with BSC in GSM (and/or with the MSC). Maybe IETF folks do not know the GSM architecture or at least do not want to talk about it (?!)

Exercise 4 (24 %) Miscellaneous

a) (3 %) What is this?
The question is 'what', not the 'meaning behind' the text. A short answer is requested.

```
v=0
o=Alice 2790844676 2867892807 IN IP4 192.0.0.1
s=Let's talk about swimming techniques
c=IN IP4 192.0.0.1
t=0 0
m=audio 20000 RTP/AVP 0
a=sendrecv
m=video 20002 RTP/AVP 31
a=sendrecv
```

The simple answer is: "This is SDP".

The longer answer is SDP with a proposal to use audio and video to discuss swimming techniques (subject), but his was not what we asked for

b) (6 %)
Explain briefly some business considerations behind Parlay/OSA.
How are business considerations in Parlay/OSA similar and different from IN?

Parlay/OSA aims at reaching ***general programmers*** *outside of the telco environment. It is believed that this will speed up service production in terms of creativity as well as with respect to "time-to-market" Parlay/OSA (i.e. the trad. operators in 3GPP) also want to allow* ***3rd parties*** *to create (and operate) various valued added services (VAS) , which may need network resources (such as QoS enabled streams), or which may utilize nw based charging (similar to CPA content provider access as used e.g. in SMS). [Parlay claims this is a win-win, but currently they have not really managed to attract the huge amount of general programmers and 3*rd *parties.]*

IN *also aimed to decrease time-to-market, but was different in two aspects: IN assumed 'programming' via Service creation environments (SCE)* ***using propriatary tools/languages*** *such as SIB etc. IN was created from within telcos. Hence they did not reach out to general programmers (and did not get the best of all programming and SW competence to build their concepts either).* ***IN assumed (mostly) that VAS was offered by the telco itself*** *(Telenor created a separate department Telenor Link, but the story about Teletopia and its IN fights with Telenor shows that really independent 3rd parties was not welcome...)*

(Shorter answers will be fully honored, but ***3 of the bolded words should be touched upon*** *in a full answer)*

c) (15 %) Answer the following questions with yes or no: (Guessing gives no credit)

Understanding the implications of the statement of ”Guessing gives no credit”, should make you realize that it might be equally good to have 3 right and 6 blank, than guessing on the 6 last ones, which may typically (statistically) result in 6 right and 3 wrong. Wrong will be deducted if it look like guessing (many wrong answers).

Comment: This statement does not imply that a reason is requested, though you may add an explanation if you feel that is relevant

1. The entity in IN conceptual model called SCF is a logical entity.
   ***Yes** explanation: F = function = logical, saying "No it is a functional entity" is wrong*
2. The entity in IMS called S-CSCF is a physical entity.
   ***No** S-CSCF and e.g. I-CSCF may be implemented in same physical entity*
3. The framework (FW) in OSA is a Java Framework allowing 3rd party programmers to write program code to be run on the HW owned by the network operator owning the FW.
   ***No** see also see slide 13 (attached at the end) for info on FW*
   No1: OSA is a kind of 'service broker' offering control of access to the network-integrity management - discovery of network functionality
   No2: OSA allows programmers to use any programming language
   No3: OSA assumes that the application servers by the 3rd party is run outside of their own network (not on their own HW)
4. In IMS the HSS is the entity where service execution of value added (or supplementary) services takes place (An example of such a service is some kind of call forwarding)
   No
   explanation: Note the work EXECUTION. HSS is a DB (S-CSCF or Appl.Nodes or similar (B2B UA etc) may do service execution)
5. Mobile IP was initially designed to be used for nomadic users, but has later turned out to be an optimal protocol to handle mobility for VoIP.
   ***No**, see further explained in exercise 3.c (and 3.b)*
6. In IN SS7 is used for the signalling between SSP-SCP
   Yes
   Explanation/comment: In some figures an STP is listed between SSP and SCP. STP is an SS7 router, so saying "No, because an STP is between" is wrong.
7. When a voice-menu is used in IN (press 1 for English etc.) then a voice-connection will be established towards the SCP.
   ***No**, the voice stream will be connected to an "IP" (and entity 'down' in the network) The SCP will only **control** the IP, See exam2003 for details of how voice menus and IP and voice connection.*
8. Parlay/OSA standardizes the interactions (interfaces) between a 3rd party and the network via so-called SCS (Service Capability Servers)
   ***Yes**, see slide 13 (attached at the end)*
9. Parlay/OSA standardizes the interactions (interfaces) between so-called SCS (Service Capability Servers) and nodes like S-CSCF and HLR
   ***No,** see slide 13 (attached at the end)*

Exercise 5 (14%) Value added services, service management and IN.

Supplementary services are often standardized, but an interesting issue is to allow rapid introduction of new value added services *without* needing to standardize the service description or add new parameters (e.g. to the Establish method).

One example of such a service may be Personal-DND service. Such a service may be realized in different ways and have various service logics and associated data. See appendix section 3 for more description of some Personal-DND services.

Some of the description will also use the term malicious call. See appendix section 2.4

We will follow Alice and Carl during a time where Carl and Alice starts dating:

- Alice has 2 different phone subscriptions (one on PSTN and one on GSM).
- Carl has the personal-DND service as described in Appendix section 3.1
- At Time T1 Carl wants Alice to pass through his Personal-DND service.
  Comment added to the solution: This means that Carl wants Alice on his White-list, but she may still be subject to screening because of 'personal state' set to 'occupied'. 'Pass through' should thus be interpreted as : "Being connected trough with voice connection to Carl's phone whenever Carl is not in state occupied"
- Later Alice is threatened by her ex-boyfriend David. She finds out that she needs to change to new phone numbers.
- At time T3 Alice gets new phone numbers that are 'non-listed' (but not strictly secret). This means that her new phone numbers will not be searchable on 1881.no or similar yellow/white pages services. She chooses to keep the CLIP supplementary service.
- After some more time Alice realizes that some of her friends have leaked her mobile phone number to David and she is getting threatening calls at night.
- At time T4 she is changing phone numbers again, still opting for 'non-listed' numbers and this time she is determined to subscribe to CLIR (Calling Line Identity Restriction) on both her PSTN and GSM numbers

a) (6 %)

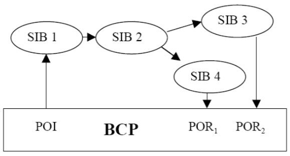
- **Subtask:** Explain briefly what actions Carl must do at/after time T1 in his private 'service management system' on his answering machine. (This service management system is probably manual)
  2 phone number for Alice must be added to Carl's white-list (other entries may have to be kicked out). It is important that you realize that Alice is 1 person, having 2 phone numbers, and this relates no names/addresses) [Hint bottom p. 17
- **Subtask:** Explain briefly what actions Carl will need to take at/after time T3 on his answering machine in order for his personal-DND service to work properly (i.e. letting Alice through).
  Carl must update the two entries for Alice according to her two new numbers
- **Subtask:** Explain what difficulties Carls enters into at Time T4. Is it enough to update with the new phone numbers of Alice? How can the service from Tele-Harmonia described in appendix section 0 serve Carl under these new conditions in a way different from the endpoint centric version
  The service logic on answering machine is relying on CLIP, but now Alice has CLIR, hence overruling CLIP feature. Hence updating as after T2 will not solve the problem this time. However Tele-Harmonia will know CLId since we assume that it is a trusted party to the network operators.

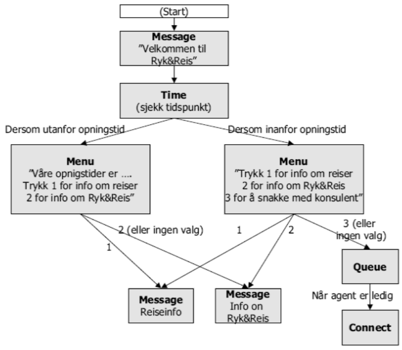
b) (8 %)

Explain briefly how the PSTN/ISDN network operator may create/build/realize some Personal-DND service via IN. You may choose to describe *either* the ”global functional plane” (using BCSM and SIBs) or the details of the physical realization (using SSP, SCP, IP etc) in the so-called ”Physical Plane”

- It is requested that you describe *only one* of these two planes (of your own choice)
- It is not expected that you remember names of SIBs. You may uses SIBs named MESSAGE, CONNECT and RELEASE and optional other SIBs of your choice.

***Alternative 1**: Solution using global functional plane (GFP).*
This should look somewhat like the following (generic illustration of GFP). However the IN-exercise in 2003 uses a slightly different format in their illustration (to the right), and both are acceptable.





BCP= Basic Call Process, same ting as BCSM= Basic Call State Modell

```
Service logic (for the Answering machine AM):
IF <CLId not present>  THEN ...
ELSEIF <CLId on Black_list> THEN ...
ELSEIF <CLId on White_list) and personal_state = 'occupied'>  THEN ...
ELSEIF <CLId on White_list> and personal_state = 'free'
      THEN <answer call on the phone>;
```

In a networked solution almost the same logic may be used, but there should be some changes: `<CLId not present>` *should now be replaced with p-bit = 1, and Alice should be accepted on White list even in this case. I.e. the sequence of the tests must change. Anyone not on white-list with p-bit = 1 should be banned. In addition "some Personal-DND service" was requested, not a service exactly as before, so presence is removed(i.e. offering less functionality than the service from Tele-Harmonia and this is OK as this service is describes as being offered by the telco)*

IN **`Service logic (networked solution without 'presence')`**

```
COMMENT: Alice must through even though she has CLIR (p-bit = 1) hence the
sequence ofthe tests must change ENDCOMM
IF <CLId on White_list> THEN <connect trough>
ELSEIF p-bit = 1  THEN
BEGIN <answer using Message1 ("stupid idiot!")>; <hang up> END
ELSEIF <CLId on Black_list> THEN
BEGIN <answer use Message1 ("stupid idiot!")>; <hang up> END
ELSE <connect trough>
COMMENT: ordinary callers willing to show CLId and not explicitly black
listed are let through here ENDCOMM;
```

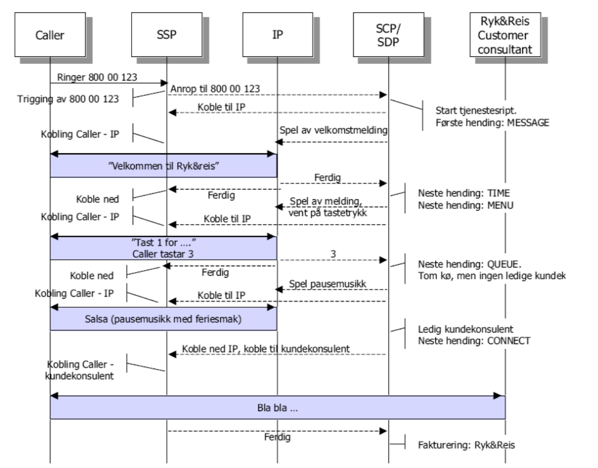
We need the following SIBs to represent this service logic in any of the formats shown above:

```
SIB representing <testing whether p-bit = 1>.
SIB MESSAGE representing <answer using Message1 (”stupid idiot!”)> (and
keeping the control with the SIB, a likely next SIB is any of the next:)
SIB RELEASE representing <hang up>  return to BCP
SIB CONNECT representing connecting through i.e. also returning to BCP
```

2 instances of a SIB LIST to check white and black list is also needed

I have assumed that personal presence occupied/free is not implemented in this IN solution, but that can be added, requiring a few more data elements, as well as a phone-based solution for the end user to signal busy vs free (clumsy on PSTN, ref. the GUI for UPT which was a real ’show stopper’ and this is partly why I removed it)

***Alt 2: Physical plane** What is requested is primarily to show where the voice connection is physically attached (IP) and that this is different from the SCP. You need not show a detailed ‘MSC-look-alike’ as below Solution to exam 2003 offer the following illustration in the case of a travel agency named R&R having menus + attendants ++*



Some explanation:

(‘disconnect is a natural translation of koble ned)

HOWEVER:‘koble ned’ after ‘Welcome to R&R’ is disconnecting the ‘half leg’ towards the IP only

The other ‘half leg’ (from caller to SSP is still established, and waiting at SSP on either:

- further connection to IP,
- connecting to B
- disconnecting the whole call (with all connection parts) (e.g. due to timeout or other events or a build in service logic)

In our case we need a few simple changes if we base our description on this figure:

1) The sequence will now be much simpler, since no complicated” reestablishment” of voice connections (or half legs) needs to be done.

2) Callers (Alice and others) are dialing Carl’s ordinary number (not an IN-specific number). SSP must trigger on Carl’s number and the SCP will be activated.

Someone dial Carls number and ssp detects IN triggering
SCP/SDP must locate service logic and data for Carl.
Then first action (hending as states in figure in nynorsk) will be the forked if-statement
In case of CONNECT:
a voice stream to B (now Carl) will be establish (and SCP not involved any more)
In case a message is played:
’ferdig’ (ready) will be sent to both SSP and SCP. SSP will ‘koble ned’ (disconnect) the half leg towards IP. Next instruction from SCP will be release call. (Such details are not expected)

Exercise 6 (12%) Service mobility

Assume in this exercise that Alice and Bob subscribes to a standardized supplementary service SS1. In order to be a bit more concrete you may assume that SS1 is either:

- CLIR (Calling Line Identity Restriction) (subscribed to by Alice) or
- CFNR (Call Forwarding on No Reply) (subscribed to by Bob)

You may choose between CFNR and CLIR as you find most appropriate depending on your knowledge from the syllabus and your ability to find useful information in the appendixes. Note that CLIR in GSM is briefly explained at the end of Appendix section 2.2.

Assume also that Bob is currently roaming into a foreign domain and is assigned an MSC in this domain. Assume also that Alice is a GSM subscriber.

a) (4 %) Explain the role of the HLR for service profile for the service SS1 and how the HLR interact with other entities in order to realize SS1.

- I.e. explain how SS1 (either CLIR or CFNR) in realized in GSM, by using Alice and Bob as concrete examples. Alice is at home (in GSM) calling Bob.
- Hint 1: You may look at Figure 1, (but change the originating side a bit since now Alice is on GSM). Before this call takes place Bob has registered and you should find out the call flow (sequence diagram) for Bob registering at this location. Since this registration naturally involves the HLR the answer to the question lies here.
- Hint 2: It might be useful to recall how HSS in involved in an IMS registration for service profile data and S-CSCF selection, *though the procedures are not exactly the same in GSM.*
- Hint 3: Unless you remember how CFNR in realized in GSM, you may want to look at how CLIR is realized in PSTN in appendix section 2.2.

HRL sends the service profile data to the VLR during registration. In this way the MSC will know which SS which are active for any user.
See edtails in http://www.item.ntnu.no/~lillk/presentations/GSM-UMTS-rel5-rev0.7-animert.ppt slide 18

This short description is true irrespectively of the service being CLIR or CFNR or any other standard service defined with a standard service profile in GSM. One will get full score both for such a generic description as well as for a more concrete description talking about Alice and CLIR etc. We asked about a concrete example because we believed that to be simpler for the candidates.

May be added: The MSC will then perform CLIP, CLIR and CFNR similar to an ordinary Local Exch. (LE) according to the data received from HLR as stored in VLR. (MSC/VLR are (almost always) co-located and have huge similarities with an LE in fixed network)

[Triggering data for IN/camel services will also be moved to VLR/MSC during registration, but we did not ask for that]

The following definitions of service mobility are given is the various syllabus material.

Def.1 (from Lecture Notes (LN) translated to English): Service mobility (alternative names: program mobility / software mobility or actor mobility) will allow SW modules / actors (like code, objects and processes) to be moved from one machine to another machine

Def. 2 (from ETSI T TR 180001, Tispan, NGN release definition): **Service mobility**: mobility, applied for a specific Service

- NOTE: I.e. the ability of a user to use the particular (subscribed) service irrespective of the location of the user and the terminal that is used for that purpose.

b) (4 %) Does GSM offer service mobility for CFNR and CLIR according to Def.2? Make a sensible (short) discussion in addition to answering yes or no.

- Hint: You may find some useful information in a correct answer to 6.a)

Def. 2 implicitly assumes that user mobility is already in place, (because of the statement "irrespective of (...) the terminal that is used"). One may say that GSM offers user mobility in the sense that a SIMcard can be moved between various GSM-terminals (as long as the user is on GSM. (This level of fine discussion (termed 'flisespikkeri' in Norwegian) is not expected in order to obtain full score on this point)

The following argument is a bit on the far side: "User mobility is not supported because the user cannot use a tree in the wood as a terminal".

A full score will be given to any of the following explanations:

***Yes**, service mobility of CFNR according to def. 2 is also supported in GSM: B can activate this service from everywhere, and the service will always be executed 'in a location near you' (i.e. an MSC) upon incoming calls with NoReply condition (as this condition is standardized in GSM) (B must however be on GSM equipment, this last comment is not needed)*

***Yes,** GSM offer service mobility for SS CLIR according to def. 2: A's wish to withdraw CLId is handled regardless of the location of both A and B. (in fact the argument for CLIR is more complicated than the argument for CFNR since you should ideally mention both A and B in this case)*
[2 comments not needed for full score: a) A must however be on GSM equipment using her own SIMcard, b) In fact Alice may also use the following "work-around" which also offer some kind of CLId restriction: She may borrow a foreign GSM phone, since in this case her own CLId will not be revealed.

c) (4 %) Does GSM use service mobility according to Def.1 for a service like CLIR (Calling Line Identity Restriction) or CFNR (Call Forwarding on No Reply). Make a sensible (short) discussion in addition to answering yes or no.

- Hint: You may find some useful information in a correct answer to 6.a)

*The only 'thing' that is moved from HRL to VLR/MSC is service profile data. One may call this 'data object', but it is certainly not program code. [One of the problematic issues with code is that is may be arbitrarily long, not so with a simple well defined service profile data such as <CFNR active: yes, forwarding number xxx xxxxx> Code may also be short but occupy 'arbitrarily' much execution resources which is also problematic in telecom systems]. Hence it is most sensible to say that GSM does **not** use service mobility as given in def. 1*

The SIMcard may be moved from one machine/ terminal to another, but the SIMcard is not directly involved in SS like CLIR/CFNR. Even in case the SIM card is executing code, I would not call this 'program mobility'. The SIM card is better viewed as a separate piece of HW (machine)

***Comment for 6.b and 6.c:** Any sensible discussion of the two definitions will be honored according to how sensible the censor finds the definition. (This may even imply that a very good argument for the opposite conclusion may be fully honored)*

One may also say that GSM does not offer user mobility because PCs (and fixed phones cannot be used, hence user mobility id not offered. If this argument is used, then the answer becomes different.

Appendix

The appendix contains some material from the syllabus (LN, other reading material) as well as some material from new sources (not listed on the syllabus).

Some of the material given here is refered to in a specific exercise in the exam, while other material is given for your convienience.

All material listed here may be refered to in your answers.

1. GSM related information

The following figure is given in http://www.m-indya.com/gsm/gsmntaspects.htm (from the English syllabus). Note a small error in this figure.

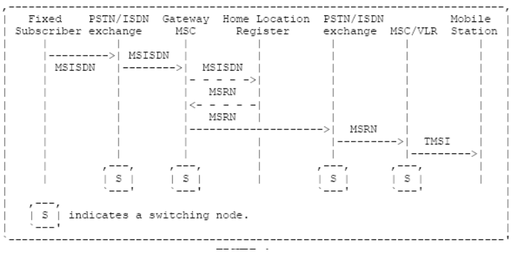


Figure 1 GSM call flow with location look up. Note a minor error

A **correct figure of call establishment in GSM** is as follows:

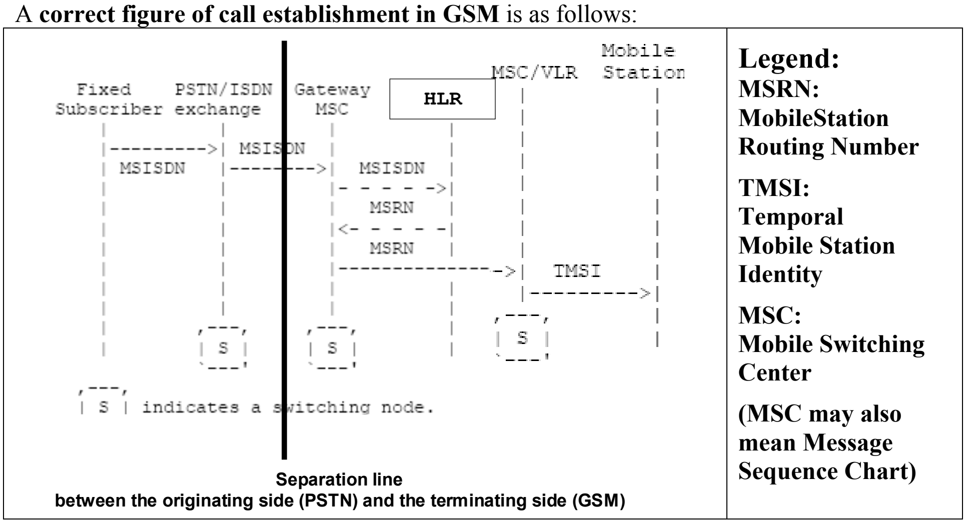


Figure 2 GSM call flow)or MSC) from PSTN to GSM with location look up (correction). Fat line is added

The message names are not shown on these figures, instead it is the most important parameters related to addressing that are indicated. Also note that the details of BSC and BS are not shown on these figures.

Relating to PSTN material in Figure 3 (page 16), the name of the message between PSTN and GW-MSC will be Establish (with parameter diallednumber being the MSISDN of the B party as detailed in Figure 4). (The message Establish is also called ’call setup’ or similar).

2. PSTN related information

We will start by showing an ordinary call flow in PSTN (the names of the messages are 'abstract' (and not according to the real names in ISUP signaling). The names follow the material from Prof. Audestad (given here as Figure 5). It is recommended that you read 2.1 and 2.2 first and treat 2.3 as optional material.

2.1. PSTN (a simplified version)

Here we will show a high level view of how call setup work in PSTN. We have chosen to use 'abstract' names, and these names are in line with the names used by Audestad (see 2.3 for details).

In line with GSM we will use the term TE for the phone. We also find it useful to separate the phone from the human end user.

Note that in the general case there are more switches involved (and hence a longer chain of NNI interfaces), but this simple example shows the necessary details.

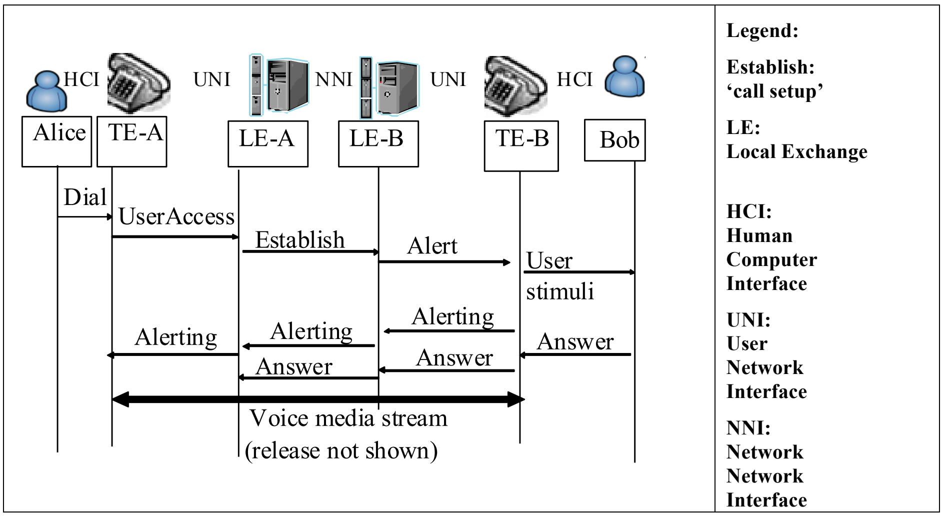


Figure 3 High level illustration of PSTN call setup (simplified case). Some parameters shown in Figure 4

This figure illustrates a call flow in PSTN and you should be able to compare this with the material given for GSM in Appendix section 1 and with SIP related material from the syllabus. In the latter case UserAccess, Establish and Alert will all correspond to INVITE.

Note that in PSTN there is no call and connection separation. The establishment of the connection (bearer) is performed by the Switches (LE-A and LE-B in this simplified example) as the call is progressing. (This is of course different from SIP) The details of the switching (connection establishment) is shown in 2.3, but these details can be ignored in this exam.

Important parameters in the message Establish are: diallednumber, CLId and the p-bit. The latter serves as a privacy indication.
(p-bit = 1 indicates that the privacy restriction apply as described in the next section 2.2)

2.2. CLIP and CLIR as two Supplementary Services (SS) in PSTN

CLId = Calling Line Identity (A-nummer på norsk)
CLIP = CLId Presentation (A-nummer-visning på norsk)
CLIR = CLId (presentation) Restriction
p-bit = privacy bit (indicating whether CLId shall be presented or not to the called party)

CLIR is a SS related to the calling party (A), and it allows calling party (A) to determine[2] that his/her own CLId shall not be presented towards the called party (B). Part of this SS execution takes place in the local exchange of the called party (B) as will be explained below.

CLIP is a SS related to the called party (in the old days B was charged for this SS). CLIP is relying on CLId to be passed in the network from LE of A towards the LE of B. LE of B is then responsible to check the p-bit and remove the CLId if so indicated.

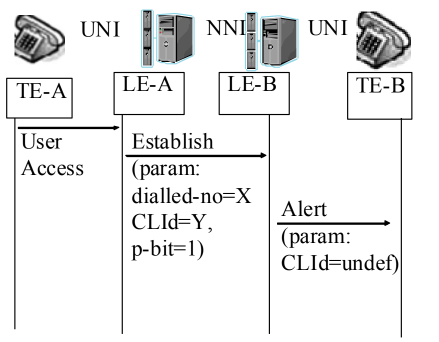
The behavior of LE-A on the originating side is partly described as follows:

```
IF <SS CLIR is active for A>
      THEN <include CLId in Establish and use p-bit=1>
      ELSE <include CLId in  Establish and use p-bit=0>;
```

The behavior of LE-B on the terminating side is partly described as follows:

```
IF <callerID is emergency number> THEN  <include CLId in Alert message>;
COMMENT overrule p-bit for emergency services ENDcomment;
ELSE IF p-bit = 1
      THEN <withhold CLId from Alert message>
      ELSE <include CLId in Alert message>;
```

In short: This means that CLId is sent within the network[3] also in case that calling party does not want the CLId to be presented to the enduser. CLId is then withheld by the LE before the alert message (also known as 'call setup' or similar) is sent over the UNI to the called party. In real life an exception apply for the emergency services 911/113 etc. and thus this is described above (as explained by the `COMMENT`).



Explanation:

Diallednumber = X, where X = 22 22 33 44 which is the public phone number of Bob in Oslo

CLId (Calling line Identity) = Y, where Y=73 73 74 75 which is the public phone number of Alice in Trondheim

Figure 4 A subscribes to CLIR and B subscribes to CLIP. Details of some parameters shown

The services CLIP and CLIR exist in GSM and then CLIR is realized as follows: In GSM B's MSC will handle the CLIR (p-bit) at the terminating side. *Note* that in GSM it is not really the CLId that is presented, but an identity representing the *user* (not the access *line*). However the term CLIR is still used in GSM.

---

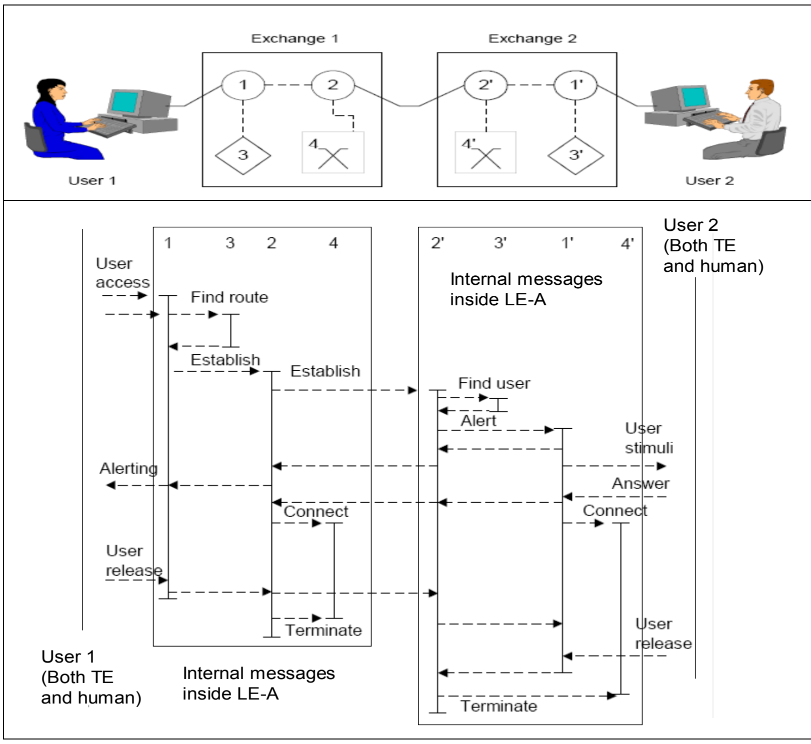
[2] The selection may be done per call via e.g. *28# (or other more or less user friendly actions)

[3] Via the so-called NNI interface(/s)

2.3. Two figures from Prof. Audestad showing PSTN connections ++

These two figures are given here as supplementary information.

You should be able to manage with only the material from 2.1 and 2.2. However if you are already familiar with Audestad's material (from the syllabus) you will probably have interest in comparing these figures with the figures in 2.1 and 2.2.



Legend:

4 and 4' represent the actual switching of circuits.

3 and 3' represent some number analysis

1,2 1' and 2' represent some process states with a longer duration

Figure 5 Two figures based on material from prof. Audestad.

Note that User 1 here is both TE and human user, while TE and human is separated in the figures in 2.1 and 2.2 (indicating UNI and HCI as two different interfaces). Because of this difference the message 'Alert' is shown as an internal message here while 'Alert' and 'user stimuli' are used on the UNI and HCI interfaces in Figure 3.

The details between UNI and TE and human user are better illustrated in Figure 3. While the inner parts of the LE is better shown in Figure 5.

In case you wonder why CLId is sometimes not shown on international calls even if you subscribe to CLIP you may see this footnote[4]

[4] There are several versions of NNI and on the international NNI interface the national operator might chose to withhold the CLId in case he does not trust that the other operator will respect the privacy bit (p-bit). See also Appendix section 4 is you wonder how IMS handles this issue.

2.4. MCID (Malicious[5] Call Identification) as defined by ETSI (Teddi database) (valid for PSTN)

”The MCID supplementary service is a [standarized] service that enables an incoming call to be identified and registered. The following call information is registered: - called party number; - calling party number; - local time and date of the invocation in the network serving the called user; and - as a service provider option: calling party sub-address (if provided by the calling user). The information is not available to the terminal equipment under the control of the called user nor the calling user. The information is stored at a location(s) under the control of the network operator. The MCID supplementary service can either be invoked during the active phase of the call, or after the active phase for a limited period […]”

A registration via MCID may be a first step leading to a criminal investigation at a later point.

3. “Personal-DND” Service descriptions

The ’Personal-do-not-disturb’ (P-DND) is a not standardized service which can be realized in several ways.

Two very different ways to realize such as service can be the described as the endpoint centric way and the network centric way. These two approaches will be described below.

It might be useful to read appendix 2.4 on MCID before reading this material.

3.1. The endpoint centric realization of Personal-DND:

Carl has bought a PSTN answering machine (AM) of the type that is located in his own home. This AM is programmable[6] to a certain extent. The AM also contains a button where Carl can register his personal-state as being ’occupied’. Every second push will change his personal-state from ’occupied’ to ’free’ and vice versa and a lamp on the AM will change from red to green accordingly.

Carl has programmed his AM as follows (sketch of service data and service logic)

```
Data:
Black_list: <Up to 10 phone numbers on E.164 format >
COMMENT I do NOT want to talk to these under any circomstances ENDcomment;

White_lists: <Up to 10 phone numbers on E.164 format >
COMMENT I may want to talk to these under certain conditions ENDcomment;

Personal_state: <binary value: ’occupied’ or ’free’>

Service logic:
IF <CLId not present>
       THEN <answer on AM using Message1 (”stupid idiot!”)>
ELSEIF <CLId on Black_list>
       THEN <answer on AM using Message1  (”stupid idiot!”)>
ELSEIF <CLId on White_list) and personal_state = ’occupied’>
       THEN <answer on AM using Message 3 (”leave a message”)>
ELSEIF <CLId on White_list> and personal_state = ’free’
       THEN <answer call on the phone>;
```

Comment: Some student pointed out that this service logic does not state what to do with an ’ordinary caller’ (having CLId and not being on nether black list or white list). This flaw should not really make any difference for the candidates’ ability to answer the exercise.

---

[5] The word *malicious* is derived from *malice* which means ’desire to harm others’ (according to Webster’s)

[6] This is an imaginary description. I am not aware of any real Answering machine product aiming for the private market offering this features. However within SIP one may easily assume a SIP B2B UA which could be programmable and behave like this.

3.2. The network centric way to realize Personal-DND:

The company Tele-Harmonia is a networked 3rd party service provider and uses Parlay/OSA call control. It might be that Tele-Harmonia also uses some User interaction in Parlay/OSA and maybe also some User Status features.

Tele-Harmonia offers a similar service to Carl's original service, but Tele-Harmonia is offering several additional features:

- Similar to Carl's programmable answering machine both a personal black list and a personal white list are offered. However the size of each list is now much bigger.
- Tele-Harmonia offers a common black list of telephony sellers (to avoid phone spam).
- Via Parlay/OSA Call Control Tele-Harmonia has access to CLId of all incoming calls related to Carl. In this way Tele-Harmonia will be able to let Alice through and still keep telephony sellers using CLIR away from Carl's phone and home.[This will require some changes in the logic given in section 3.1]
- Tele-Harmonia is also integrating a presence server into their Personal-DND service. Hence Carl has now many options to choose from such as "occupied", "free", "lunch", "rather busy" etc. and the number of voice messages is increased accordingly. The message "stupid idiot" may of course be replaced with an immediate release of the call (if wanted)
- Tele-Harmonia also offers Carl an additional feature which we may call 'personal-malicious-call-barring' which is included in the personal-DND service. Each time Carl has received what he perceives as a 'malicious call' he may not only report it as a Malicious call (as explained in 2.4), but he might also *automatically add this phone number to his/her personal black-list*.
  This is done via a menu on the (programmable) phone.
  It can also be done via a webpage where all calls from the last X minutes are listed anonymously without CLId visible to Carl. In this way Tele-Harmonia respect the p-bit of the caller, and keep the trust of the network providers. (Even though the caller is perceived malicious s/he deserves some privacy.)
  It can also be done via an action such as dialing *27# while the other party is still active in call, or within Y sec. after the other party has hung up in a way more similar to the way it is realized in PSTN on dumb endpoints. (In the latter case Tele-Harmonia would need to get an indication of this interaction over Parlay/OSA).

4. IMS handling of "caller-ID" and "caller-ID restriction"

It *might* be that the following material can be useful for you. It is up to each candidate to make use of this material.

This description is for IMS (not for SIP proper as defined by IETF).

The various caller-IDs and the privacy handling (a kind of caller-ID restriction) are described in the IMS book (in chapter 10.12), and a short version follows here.

In IMS there are **several caller identities** as illustrated by the following:

```
INVITE sip:Theresa@home2.hu SIP2.0
From: "Your brother" <sip:tobi@brother.com>; tag=veli
To: "My beloved sister" <sip:therera@sister.com>;
P-Preferred-Identity: <sip:tobias@home1.fr>
Privacy: None
```

The P-Preferred-Identity is inserted by the UE (UE of Tobias in this case). But the **originating P-CSCF** will check this identity, by asserting that it is received over a valid IPSec SA (Security Association) and matching with the previous registration. If the originating P-CSCF finds the P-Preferred-Identity to be asserted, it will use this Id, but this time as P-Asserted-Identity.

The SIP message will then be sent to the S-CSCF on the originating side. It may look as follows:

```
INVITE sip:Theresa@home2.hu SIP2.0
From: "Your brother" <sip:tobi@brother.com>; tag=veli
To: "My beloved sister" <sip:therera@sister.com>;
P-Asserted-Identity: <sip:tobias@home1.fr>
Privacy: None
```

In case privacy is "id" the originating S-CSCF must then check whether Theresa's home network is within the same trust domain. If not the P-Asserted-Identity must be removed.

The **terminating side** must check the P-Asserted-Identity and the privacy header value. In case the value is set to "id", the P-Asserted-Identity shall not be sent to Theresa's UE.

However in this case no privacy restriction applies. Thus the "real name" of Theresa's caller (i.e. <sip:tobias@home1.fr>) will be sent to her UA.

You should notice how the header Privacy has two values "None" and "id" is similar to the p-bit 0 and 1 as explained for PSTN in appendix 2.2

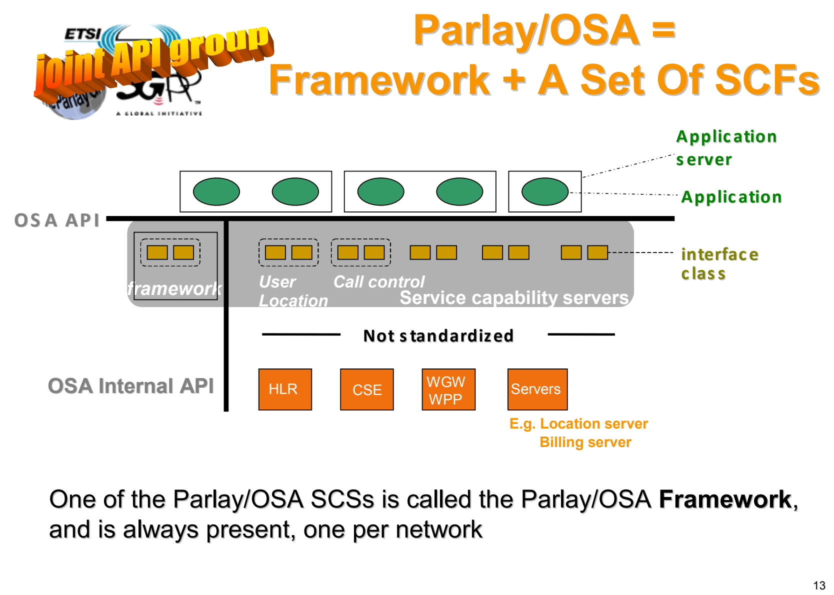
4.1. The call flow resulting from this description is as follows

The call flow can be briefly illustrated as follows (only the initial messages are shown and only the parameters affecting caller-ID is shown). The actions on the way at the CSCFs are indicated in < >-brackets:

```
UE --> INVITE (P-Preferred-Identity: <sip:tobias@home1.fr>) --> P-CSCF
<P-CSCF checks P-Preferred-Identity with prev. Reg. via IPSec SA>
P-CSCF --> INVITE (P-Asserted-Identity:<sip:tobias@home1.fr>) --> S-CSCF
<S-CSCF checks trust relationship with terminating side>
S-CSCF --> INVITE(P-Asserted-Identity:<sip:tobias@home1.fr>) --> I-CSCF
<I-CSCF interacts with HSS and S_CSCF>
S-CSCF --> INVITE(with P-Asserted-Ident.:<sip:tobias@home1.fr>) --> P-CSCF
<P-CSCF checks privacy header not set to "id" >
P-CSCF --> INVITE (with P-Asserted-Identity: <sip:tobias@home1.fr>) --> UE
```

In this call flow it is assumed that the outcome at each check is 'yes'. If last check results in 'no' the P-Asserted-Identity will be withheld.

Added in the solution, not part of the exercise description:



Slide 13 from 16_Chapt15_AllAboutParlayOSA.ppt (originally from a meeting in ”Joint API group”)