3GPP TSG SA WG3 S3#19265 Tdoc S3-010xxxx0210xxx590367
Newbury,Oxford UK
4th July – 6th July19-22 November, 20021

Agenda Item: IMS7.2TBD

Source: Ericsson

Title: Re-use and re-transmission of RAND and AUTN Security needs: Evaluation of UTRAN IP transport interfacesOn registering several public identities in IM CN SS

Document for: InformationDiscussion/Decision

---

1 GeneralScope and objectives

At the SA3 meeting in Munich, Ericsson presented a CR in Tdoc S3-020548 on the "Re-use and retransmission of RAND and AUTN". We proposed to delete an editor note based on the findings in the reason for change. There were comments during the meeting that some of the conclusion in the Reason for change could be lifted into the CR to 33.203 as requirements. Ericsson presented a new version of the CR in Tdoc S3-020560, in the same meeting.

As no conclusion could be reached on S3-020560, as some companies felt that they needed more time to sort out what requirements actually already is included in the standard SIP specifications, Ericsson started an e-mail discussion in order to be able to agree a new version of the CR at the SA3#26 meeting.

The following PPT slides with comments from Ericsson and also a new version of the CR in Tdoc S3-020590 was sent out:


Re-use and re-transmission of ...


S3-020590_CR-Ericsson-Retransm...

During the e-mail discussion we received comments from Adrian Escott at Hutchinson on the S3 reflector:

"From your analysis, it seems as though an AV should only re-transmitted by the S-CSCF as part of the normal SIP re-transmissions in the transaction layer. Hence there are very clear and definite circumstances for a re-transmission. This does not seem well reflected in the last sentence added by the CR, which states that in general AVs are not re-tranmitted.

It seems to me better to replace the last sentence of the CR "In general therefore the S-CSCF shall use a quintet only once. " with something along the lines of the following: "Therefore there shall be no re-transmission of AVs, except as part of the normal SIP transaction layer re-tranmission procedures".

I also think there was some dicussion about not using quintet at the Munich meeting. Finally, it might be alright to include the paragraph as a direct replacement for the editor's note rather than at the end, as it only short and does not in my opinion affect the flow of the section."

The new version of the CR presented in this meeting, has been updated with Adrians comments - slightly modified.

This paper discusses the enhancement of NDS/IP specification to cover the control plane of IP UTRAN as proposed in [9].

Ericsson proposes:

SA3 should consider updating the WID for Release 6, cf. [10], to include a link to the work in SA1 on Network Sharing

SA3 should investigate if a new Security Domain should be defined in TS33.210 to capture the Network Sharing Scenarios which potentially can affect the security requirements for the Iu interface

SA3 should investigate if UTRAN can be defined as a Security Domain in particular it is not clear if the protection of e.g. Iub and Iur should be regarded as Zb interfaces

The scope for this contribution is to discuss different requirements needed and different alternatives on how to register several public identities in IM CN SS.

Ericsson proposes that the UE and the P-CSCF shall have one SA for each registered IMPU (IM Public Identity) due to the requirement with additional S-CSCFs for future releases. This means that each REGISTER message with the aim of registering an IMPU should be authenticated.

2 Background

The proposal in [9], to encrypt and integrity protect the control plane over the IP based Iu interface, seems to be a sensible recommendation considering the sensitivity of the conveyed information (e.g. the session keys for the air link, the control to set on/off the encryption on the air link). NDS extension as Zb interface could be the right choice. However SA1 is currently working on Requirements for Network Sharing cf. [7] that was not included in the discussion in [9] but should be considered in the work on enhancing NDS for Release 6. In [8] a number of scenarios have been identified e.g. a scenario called 'Common Spectrum Network Sharing'. In this scenario a multiple number of Iu interfaces belonging to different Operators are connected to one UTRAN. Ericsson believes that the enhancement of TS33.210 should include an investigation if a new Security Domain is required for defining a new Za interface i.e. a SEG concept between UTRAN and CN. However the protection of the other interfaces in UTRAN should require further investigation. Threats and trust models validating the need of security on such interfaces should be investigated and weighed towards the implications that adding security would bring.

Currently Ericsson believes that a compelling investigation including threats and risks are missing and it is believed that the cost issue can be overwhelming. In particular on the Iub interface where a low cost solution for the Node B:s may be wanted by the operator. Extending the NDS security to Node B:s means requiring both IPsec and IKE etc. Key management appears to be a troublesome issue due to the immense number of involved nodes (the UTRAN network is complex and comprises tens of thousands of nodes). There is a need for a simple key management solution and it should be further investigated what solution is the right choice.In [23.228] it is a requirement that a user shall have one IM private identity (IMPI) and several IM public identities (IMPU(s)). The IMPI and at least one IMPU is stored in the ISIM, IM SIM. It is the private identity, i.e the IMPI, which is used for authenticating the subscriber. The user sends a SIP REGISTER towards the registrar, which is the S-CSCF, and the registrar performs the authentication. The registrar sends a challenge to the user, which in turns sends, a response back that is checked by the S-CSCF.

The REGISTER sent by the user towards the registrar:

REGISTER sip: ---

Via: ---

From: IMPI

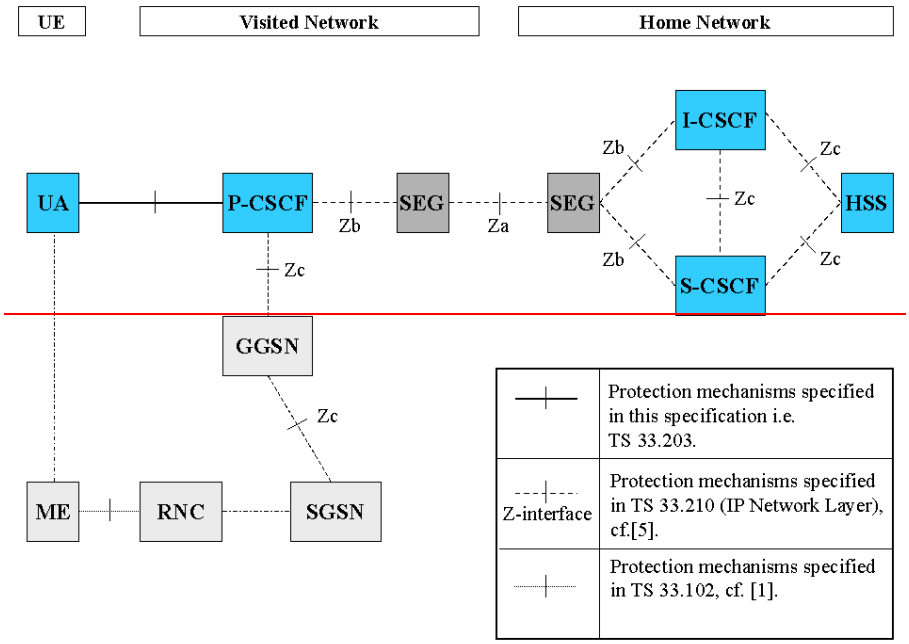
To: IMPU

Call-ID: ---

Cseq: 1 REGISTER

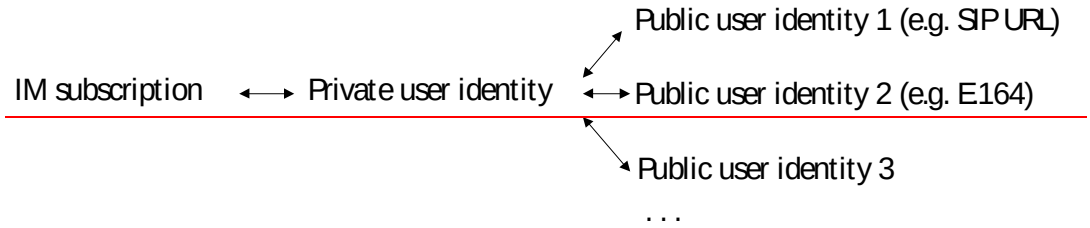
Content-Length: 0

The S-CSCF gets the Authentication vector from the HSS, which includes the challenge, and the key(s), IK and optionally the CK.



~~Figure: An overview of the security architecture for the IM CN SS and its relationship to NDS i.e. TS 33.210.~~

~~The relationship between the IMPI and the IMPUs are specified in [23.228] as:~~



~~In [23.228] it is specified that the HN operator is responsible for the assignment of the IMPI and IMPUs. Furthermore it is also said in [23.228] that identities that are not defined by the operator may exist, cf. chapter 4.3.3.4. Regarding the assignment of an S-CSCF for a user it is specified that an S-CSCF is assigned at registrations however for future releases it should not be precluded that additional S-CSCFs might be assigned, see chapter 5.2.2.1.~~

~~A registration will last for some specified time which can be included in the "expire" and the registrar can increase or decrease this time depending on the policy, cf. [SIP] chapter 7.4. If the user does not include the "expire" then he will by default be registered for one hour, cf. SIP chapter 7.4. It is possible for a user to de-register all identities by sending a REGISTER with a wildcard "*" in the Contact with an expire header with value 0, cf. [SIP] in chapter 7.6.~~

~~In [33.203] it is mentioned in an editor's note that it is optional to implement confidentiality protection and it should be applied at the same level as the integrity protection. This means that neither the IMPI nor the IMPU should be used as an SPI since both of these could be encrypted. Hence the P-CSCF needs some other SPI to do that. Here we assume that such an SPI is in place but so far this SPI is not specified in [33.203]. It could however be based on what is included in the From: field but then this field may not be encrypted.~~

~~3 Issues~~

~~In this section different alternatives for registering an IM-subscriber and its IMPUs in the S-CSCF. Also the different security implications are discussed and its compliance with [23.228].~~

~~3.1 One SA Alternative 1~~

In this alternative the subscriber registers several IMPUs at the same time in one S-CSCF.

REGISTER sip: ---

Via: ---

From: IMPI

To: IMPU1, IMPU2, IMPU3

Call-ID: ---

Cseq: 1 REGISTER

Content-Length: 0

The major drawback with this alternative is that it is not compliant with SIP since it needs an extension making it possible to include several identities in the To: field.

There will only be one SA between the UE and the P-CSCF. All subsequent SIP messages can be protected by the defined SA and negotiated algorithms except when a new REGISTER is sent from a user. Then it is assumed that if the authentication is successful that all current IMPUs are released in the S-CSCF. Note that the identities are all registered in one and the same S-CSCF.

An advantage with this alternative is that all IMPUs that the user wants to register are registered with performing only one authentication. The handling of the validity of the SA is also simple since a new SA is only derived at expiration or when the user wants to register new IMPUs. It is assumed that the user can only register a limited number of IMPUs such that the limited bandwidth over the radio channel is taken into account.

3.2 One SA-Alternative 2

In this alternative the subscriber registers one IMPU at the time i.e. first the UE sends

REGISTER sip: ---

Via: ---

From: IMPI

To: IMPU1

Call-ID: ---

Cseq: 1 REGISTER

Content-Length: 0

And then the UE after some time sends e.g.

REGISTER sip: ---

Via: ---

From: IMPI

To: IMPU3

Call-ID: ---

Cseq: 1 REGISTER

Content-Length: 0

Assuming that when the user registers IMPU1 the user has not yet been registered and that the REGISTER message is unprotected and hence there exist no SA between the UE and the P-CSCF. The S-CSCF will send a challenge to the user and when the user has been authenticated and received the 200 OK message the SA will be in place and it could be based on an SPI.

After some unknown time the user might want to REGISTER IMPU3 and then the UE could apply the keys derived with the first REGISTER message. This means that there must be a mechanism in place such that the UE treats the REGISTER messages differently. The solution to this is that the UE checks that it has a valid SA and uses that. The S-CSCF not only has to keep the IMPUs that are registered but also the corresponding IMPI.

When receiving the REGISTER(IMPU3) message the S-CSCF might not have to perform an authentication. The

S-CSCF checks that the IMPI is registered and that the registration has not expired. Let us assume that the subscriber wanted to register IMPU3 1800s after IMPU1 was registered. This means that the S-CSCF has to decide weather to decrease the wanted expire time of 3600 s to 1800 s for IMPU3 or accept the 3600 s and perform an authentication in order to define a new SA. This new SA should then be used for all IMPUs registered thus far. Furthermore IMPU1 should be de-registered or re-registered after about another 1800 s. Whether authentication was performed or not the S-CSCF sends a 200 OK back to the UE.

With this scenario it is only possible to register a user in one S-CSCF since only one S-CSCF should keep track of the validity of the SA, i.e. the expiration time related with the registration, between the UE and the P-CSCF. This does not seem to be compliant with the requirement of additional S-CSCFs in future releases.

When the UE de-registers one or all IMPUs the S-CSCF could rely on the existing SA and implicitly rely on that it received an authentic de-register otherwise it could send a challenge towards the user.

3.3 Several SAs -Alternative 3

When sending the first REGISTER the IMPU1 is registered in the S-CSCF as in alternative 2.

In the second message the user wants to register IMPU3. With this alternative the REGISTER message is treated in the same way as for the case when the user REGISTERed IMPU1 i.e. the REGISTER message is not assumed to implicitly be protected i.e. a valid SA exist between the UE and the P-CSCF.

This means that the S-CSCF will perform a new authentication and a new SA is derived for IMPU3. This would mean that the UE has to keep track on several SAs as well as the P-CSCF, one SA for each registered IMPU. This solution does not exclude the scenario that different S-CSCFs, based on e.g. the profile related to the IMPU, are used when registering different IMPUs.

This gives more freedom in treating e.g. the expiration time since it would be set individually for each IMPU. Probably the SQN would anyway be related to the IMPI such that the ISIM does not have to keep track on several SQNs for each public identity. This model is more complicated from the number of SAs point of view. However from a security point of view this model means that different S-CSCFs can take care of different SAs and IMPUs and expiration times related to the SA. Furthermore this alternative is compliant with the requirement for additional S-CSCFs. This requirement seems to make it difficult to use the optimization with sending several AVs to the S-CSCFs. It is an issue that should be further analyzed.

For each mobile originated de-registration the S-CSCF could implicitly rely on the existing SA also in this alternative. It could also be possible to authenticate de-registrations as well in order to reduce the threat for DoS attacks. The S-CSCFs has to keep track on the expiration times individually for each IMPU.

3 4 Conclusions

As a conclusion, encryption and integrity protection of the control plane over the Iu interface seems reasonable i.e. as suggested in [9]. An extension to TS 33.210 NDS/IP is recommended, potentially by implementing Zb interface. However the work on Network Sharing in SA1 needs to be considered. In particular it is not clear whether a new security domain needs to be defined when considering securing the communication between the CN and UTRAN.

The contribution from Nokia, cf. [9], recommends integrity protection (with low priority) of the control plane over other IP-based interfaces (i.e. Iur, Iub, Iupc, Iur-g and Iu-BC). Ericsson recommends SA3 to request further study of threats and trust models for such interfaces considering not only the risks but also the cost aspects should security on those interfaces be included in TS33.210. Ericsson proposes that security for those interfaces is introduced at a later stage only if proven necessary.This contribution has presented three different alternatives for registering a subscriber and his/hers IMPUs. Two alternatives that defined only one SA between the UE and the P-CSCF. And one alternative with several SAs, one for each registered IMPU, was also described.

It seems that Alternative 3 is the only one that is compliant with the requirements in [23.228]. Also each new REGISTER message has to be authenticated. It is the understanding of Ericsson that Alternative 3, reflecting the requirements above, is the alternative that should be adopted by SA3. This means that the proposal with sending several AVs to the S-CSCFs should be analysed further for this scenario.

Furthermore it is not clear what "…. identities that are not defined by the operator may exist" imply, cf. [23.228] section 4.3.3.4. Does this mean that the subscriber could actually define his own IMPUs?

It has also been defined that IMPI and IMPU cannot be used as identifier, i.e. if they are encrypted, and a more general SPI should in that case be used. One other possibility would be to let the From field to be un-protected, i.e. not the whole SIP message is encrypted. Anyway from a general SIP perspective To: and Via: fields can not be encrypted end to end. This issue has not yet been discussed in SA3.

One further requirement that has to be defined by SA3 is whether de-registrations should be authenticated in the S-CSCF or if the HN in should rely on the hop-by-hop security.

References

[23.228] 3G TS 23.228 (v500): "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; IP Multimedia (IM) Subsystem".

[33.203] 3G TS 33.203 (v040): "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA3; Access Security for IP-based services".

[SIP] IETF RFC 2543bis-03 (2001) "SIP: Session Initiation Protocol"[1] 3GPP TS 25.412 UTRAN Iu interface signalling transport

[2] 3GPP TS 25.422 UTRAN Iur interface signalling transport

[3] 3GPP TS 25.432 UTRAN Iub interface: signalling transport

[4] 3GPP TS 25.452 UTRAN Iupc interface signalling transport

[5] 3GPP TS 43.930 Iur-g interface, Stage 2

[6] 3GPP TS 25.419 UTRAN Iu-BC interface: Service Area Broadcast Protocol (SABP)

[7] TSG SA, TSGS#14(01)739, Proposed WID: Service Requirements for Network Sharing,

[8] 3GPP TR 22.951v1.0.0 Service Aspects and Requirements for Network Sharing

[9] SA3-020536, Security need evaluation of UTRAN and GERAN IP transport interfaces, Nokia

[10] TSGS#17(02)0513, Work Item Description, Network Domain Security; IP network layer security (NDS/IP) for Release 6

CR-Form-v7

CHANGE REQUEST

⌘ **33.203** CR **CRNum** ⌘rev **-** ⌘ Current version: **5.3.0** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Re-use and re-transmission of RAND and AUTN
Source:	⌘	Ericsson
Work item code:	⌘	IMS
Date:	⌘	11/11/2002
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)*
Rel-6	*(Release 6)*

Reason for change: ⌘ An outstanding editor note remains in the TS 33.203 which states that it is FFS if re-use and retransmissions of the same RAND and AUTN is allowed

Either UDP or TCP will be used for IMS. In the case when UDP is used, the transaction layer in SIP will handle the retransmissions.

Already in UMTS R99 it was acknowledged that reception of two consecutive authentication challenges with the same RAND and AUTN by the USIM application, would cause a synchronization failure on the USIM application. It's the author's (of this CR) understanding that this problem apply to the ISIM as well.

In IMS the UE will handle the retransmission of the (SM1) REGISTER message in the case the UE does not receive any response (e.g. authentication challenge) from the network to a previously issued (SM1) REGISTER message. A retransmitted (SM1) REGISTER message from the UE will contain the same sequnce number as in the previous issued one, so from the S-CSCF point of view, the (SM1) REGISTER will not look as a new Register procedure. The transaction layer in SIP in the S-CSCF will retransmit the same authentication challenge with the same RAND and AUTN as used in the previous issued authentication challenge.

If the UE issues a new Register procedure then a new sequence number will be used, and the S-CSCF is then able to distinguish this as a new Register procedure.

Conclusions:

-In the case when the UE issues a new Register procedure with a new sequence number, then the S-CSCF has to select a new RAND and AUTN (i.e. a new quintet). Therefore a S-CSCF shall use a quintet only once.

- The S-CSCF is allowed to re-use the same RAND and AUTN (i.e. the same quintet) in the case it receives a retransmitted (SM1) Register message from the UE i.e. with the same sequence number and call-id as in the previous received (SM1) Register message from the

	UE. For UDP, this is handled in the transaction layer in SIP according to RFC 3261. But as soon as the S-CSCF receives a response message to an authentication challenge then no further re-transmissions of the same RAND and AUTN are allowed. - It does not seem likely that the USIM or ISIM can receive two consecutive authentication challenges with the same RAND and AUTN (which would create a synchronisation failure on the USIM and ISIM). The transaction layer in SIP in the UE will discard a received Authentication Challenge with the same RAND, AUTN and sequence number as a previously received Authentication Challenge from the network, and not forward it to the upper layer in SIP. In addition, if the UE receives an authentication challenge as a response to an issued (SM1) Register message, then the UE would not issue any further re-transmissions of the same (SM1) Register message.
Summary of change: ⌘	It is proposed that the editor note is removed. In addition it's proposed to add that the S-CSCF shall use a quintet only once.
Consequences if not approved: ⌘	The Editor Note remains in TS33.203, which may lead the reader to belive that this issue is unresolved.

Clauses affected:	⌘	6.1.1			
Other specs affected:	⌘	**Y**	**N**		⌘
			X	Other core specifications	
			X	Test specifications	
			X	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/specs/CR.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.

6.1.1 Authentication of an IM-subscriber

Before a user can get access to the IM services at least one IMPU needs to be registered and the IMPI authenticated in the IMS at application level. In order to get registered the UE sends a SIP REGISTER message towards the SIP registrar server i.e. the S-CSCF, cf. Figure 1, which will perform the authentication of the user. The message flows are the same regardless of whether the user has an IMPU already registered or not.

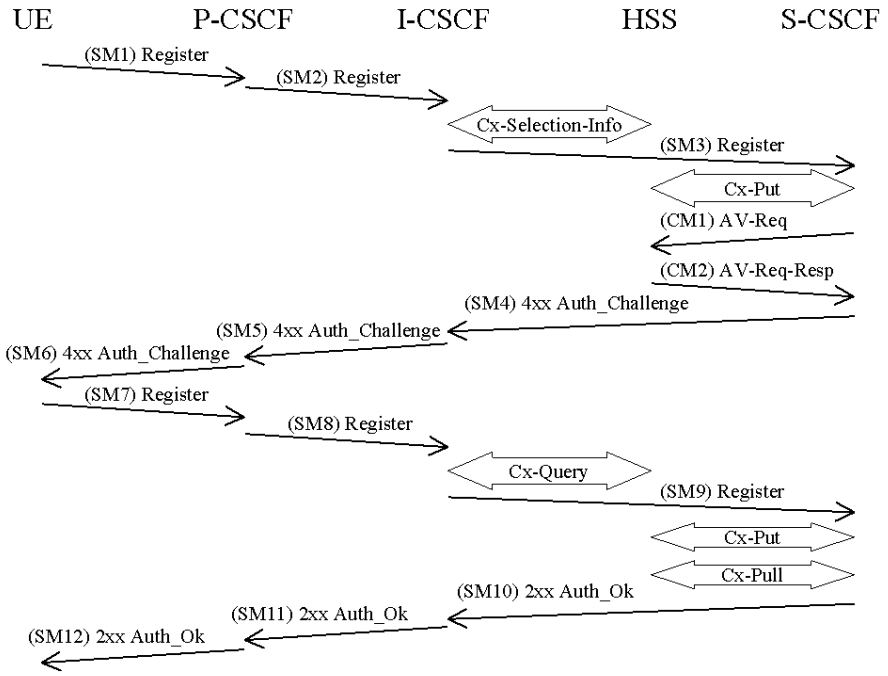


Figure 4: The IMS Authentication and Key Agreement for an unregistered IM subscriber and successful mutual authentication with no synchronization error

The detailed requirements and complete registration flows are defined in [8] and [11].

SMn stands for SIP Message n and CMm stands for Cx message m which has a relation to the authentication process:

SM1:
REGISTER(IMPI, IMPU)

In SM2 and SM3 the P-CSCF and the I-CSCF respectively forwards the SIP REGISTER towards the S-CSCF.

After receiving SM3, if the IMPU is not currently registered at the S-CSCF, the S-CSCF needs to set the registration flag at the HSS to initial registration pending. This is done in order to handle mobile terminated calls while the initial registration is in progress and not successfully completed. The registration flag is stored in the HSS together with the S-CSCF name and user identity, and is used to indicate whether a particular IMPU of the user is unregistered or registered at a particular S-CSCF or if the initial registration at a particular S-CSCF is pending. The registration flag is set by the S-CSCF sending a Cx-Put to the HSS. If the IMPU is currently registered, the S-CSCF shall leave the registration flag set to *registered*. At this stage the HSS has performed a check that the IMPI and the IMPU belong to the same user.

Upon receiving the SIP REGISTER the S-CSCF CSCF shall use an Authentication Vector (AV) for authenticating and agreeing a key with the user. If the S-CSCF has no valid AV then the S-CSCF shall send a request for AV(s) to the HSS in CM1 together with the number m of AVs wanted where m is at least one.

CM1:
Cx-AV-Req(IMPI, m)

Upon receipt of a request from the S-CSCF, the HSS sends an ordered array of *n* authentication vectors to the S-CSCF using CM2. The authentication vectors are ordered based on sequence number. Each authentication vector consists of

the following components: a random number RAND, an expected response XRES, a cipher key CK, an integrity key IK and an authentication token AUTN. Each authentication vector is good for one authentication and key agreement between the S-CSCF and the IMS user.

CM2:
Cx-AV-Req-Resp(IMPI, RAND1||AUTN1||XRES1||CK1||IK1,….,RANDn||AUTNn||XRESn||CKn||IKn)

When the S-CSCF needs to send an authentication challenge to the user, it selects the next authentication vector from the ordered array, i.e. authentication vectors in a particular S-CSCF are used on a first-in / first-out basis.

The S-CSCF sends a SIP 4xx Auth_Challenge i.e. an authentication challenge towards the UE including the challenge RAND, the authentication token AUTN in SM4. It also includes the integrity key IK and the cipher key CK for the P-CSCF. Draft-ietf-sip-digest-aka-01 [17] specifies the fields to populate corresponding parameters of authenticate challenge.

~~[Editor's note: It is FFS if re-use and re-transmission of RAND and AUTN is allowed. If allowed the mechanisms have to be defined.]~~

The verification of the SQN by the USIM and ISIM will cause the UE to reject an attempt by the S-CSCF to re-use a AV. Therefore no AV shall be sent more than once.

NOTE: This does not preclude the use of the normal SIP transaction layer re-transmission procedures.

SM4:
4xx Auth_Challenge(IMPI, RAND, AUTN, IK, CK)

When the P-CSCF receives SM5 it shall store the key(s) and remove that information and forward the rest of the message to the UE i.e.

SM6:
4xx Auth_Challenge(IMPI, RAND, AUTN)

Upon receiving the challenge, SM6, the UE takes the AUTN, which includes a MAC and the SQN. The UE calculates the XMAC and checks that XMAC=MAC and that the SQN is in the correct range as in [1]. If both these checks are successful the UE calculates the response, RES, puts it into the Authorization header and sends it back to the registrar in SM7. Draft-ietf-sip-digest-aka-01 [17] specifies the fields to populate corresponding parameters of the response. It should be noted that the UE at this stage also computes the session keys CK and IK.

SM7:
REGISTER(IMPI, RES)

The P-CSCF forwards the RES in SM8 to the I-CSCF, which queries the HSS to find the address of the S-CSCF. In SM9 the I-CSCF forwards the RES to the S-CSCF.

Upon receiving SM9 containing the response, the S-CSCF retrieves the active XRES for that user and uses this to check the response sent by the UE as described in Draft-ietf-sip-digest-aka-01 [17]. If the check is successful then the user has been authenticated and the IMPU is registered in the S-CSCF. If the IMPU was not currently registered, the S-CSCF shall send a Cx-Put to update the registration-flag to *registered.* If the IMPU was currently registered the registration-flag is not altered.

It shall be possible to implicitly register IMPU(s). The implicitly registered IMPU(s) all belong to the same Service Profile. All the IMPU(s) being implicitly registered shall be delivered by the HSS to the S-CSCF and subsequently to the P-CSCF. The S-CSCF shall regard all implicitly registered IMPU(s) as registered IMPU(s).

When an IMPU has been registered this registration will be valid for some period of time. Both the UE and the S-CSCF will keep track on a timer for this purpose but the expiration time in the UE is smaller than the one in the S-CSCF in order to make it possible for the UE to be registered and reachable without interruptions. A successful registration of a

previously registered IMPU (including implicitly registered IMPUs) means the expiry time of the registration is refreshed.

It should be noted that the UE initiated re-registration opens up a potential denial-of-service attack. That is, an attacker could try to register an already registered IMPU and respond with the wrong RES and in order to make the HN de-register the IMPU. For this reason a subscriber should not be de-registered if it fails an authentication. It shall be defined by the policy of the operator when successfully registered IMPU(s) are to be de-registered.

The lengths of the IMS AKA parameters are specified in chapter 6.3.7 in [1].