3GPP TSG SA WG3 Security — S3#19 **S3-010402**

4 - 6 July, 2001

Newbury, UK

Source: **TSG-SA WG3**

To: **SA2, CN4**

Cc: **SA1, CN1**

Title: **Requirements related to private and public identities in IMS**

Contact: Krister Boman, Ericsson
Email: krister.boman@emw.ericsson.se

Attachments: S3-010328, S3-010367

This liaison raises some issues concerning the handling of Private and Public Identities at registrations in the IM CN SS. In particular the following topics are covered:

- Registration of several Public User Identities
- Validation of Public User Identity at Registration.

Registration of several public identities

1. SA3 is currently defining the authentication schemes for the IM CN SS. The current understanding in SA3 is that an IM subscriber will have one IM Private user identity (IMPI) and at least one IM Public user identity (IMPU), which are issued by the operator. A subscriber may have additional IMPUs associated with the IMPI and the understanding that SA3 has is that all IMPUs associated with the IMPI will be stored in the HSS. In 23.228 v500 in section 4.3.3.4 it is stated that

   "The home network operator is responsible for the assignment of the private user identifier, and public user identifiers; other identities that are not defined by the operator may also exist. "

   It would be very helpful if SA2 could clarify what identities, in relation with the IMPI and the IMPU that can be defined without the interaction of the operator.

2. For several reasons SA3 has adopted the working assumption that an IMPU, IMPU1 say, which has been registered in an S-CSCF will be re-registered in the same S-CSCF. Furthermore SA3 has the working assumption that when a subscriber registers a second IMPU, IMPU2 say, then IMPU2 will be registered in the same S-CSCF as IMPU1.

   In 23.228-v500 section 5.2.2.1 it is said that:

"A Serving-CSCF is assigned at registration, this does not preclude additional Serving-CSCFs or change of CSCF at a later date. Procedures for use of additional CSCFs are not standardized in this release."

This requirement seems not to be aligned with the current working assumptions that SA3 currently have. In the attached document, S3-010367, this issue is analyzed. It is specifically mentioned in S3-010367 that one solution with additional S-CSCFs is to introduce an SA, Security Association, for each IMPU that is being registered. This adds complexity to the UE and increases the signaling in the network.

However there might exist other secure solutions than having several SAs such that any S-CSCF can deduce that the IMPI has been appropriately authenticated in any other S-CSCF or if a re-authentication shall take place. Currently no such other secure solution has been addressed in SA3. Before further analysis takes place and decisions are taken it is very important that SA3 understands the requirements correctly.

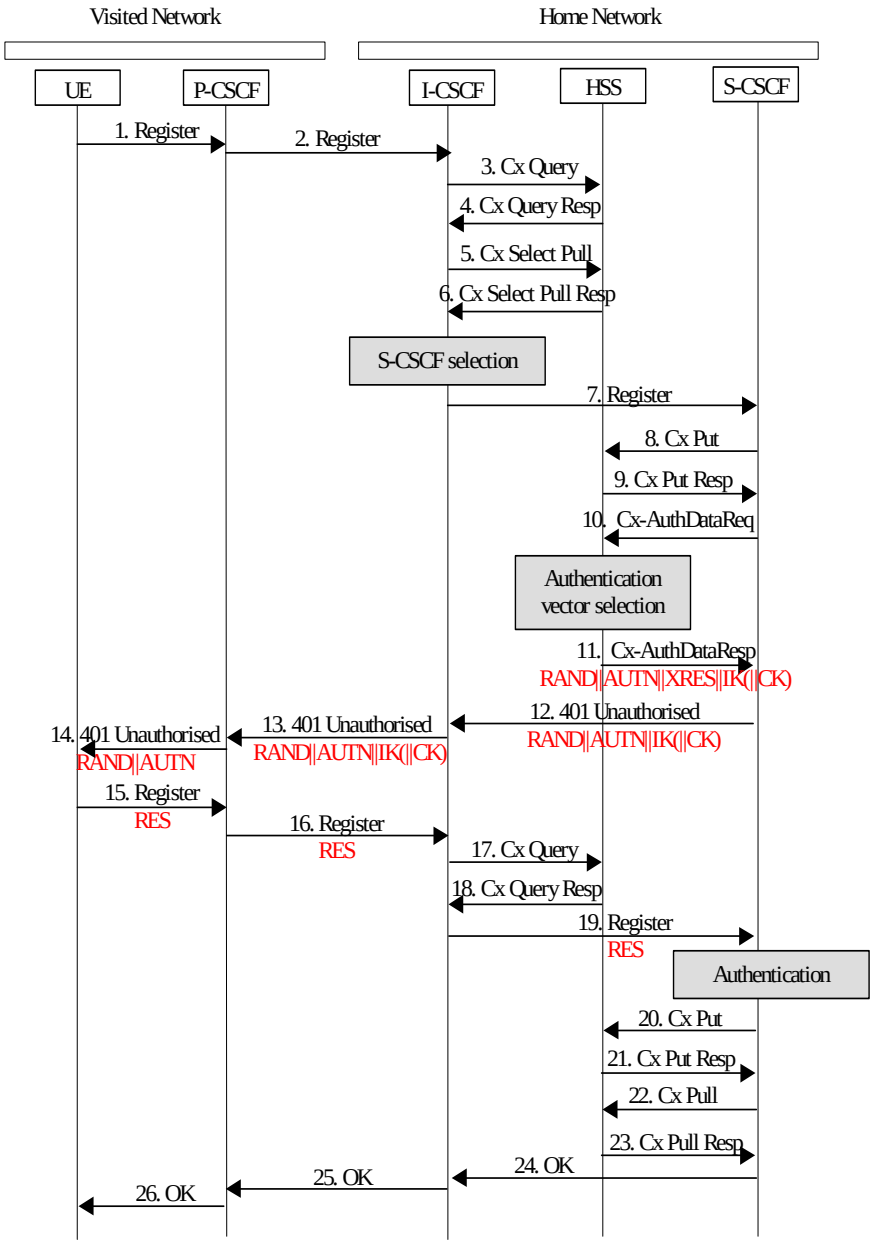
- SA3 would be happy if SA2 could clarify the requirements.
- SA3 kindly asks if SA2 can agree on the appropriateness of the working assumptions that SA3 currently have

Validation of Public User Identity at Registration

TSG SA WG3 would also like to inform TSG SA WG2 that during S3#19 another issue was discussed regarding "Validation of Public User Identity during Registration". This was originally presented and discussed at S2 (S2-011634), cf. the attachment S3-010328.

S3 recognizes the fact that there is no security relation between the IMPI and the IMPU. This requires that the IMPU that is being registered needs to be validated i.e. the network shall check that the IMPU has a relation with the IMPI in the HSS.

S3 will accommodate the validation of the IMPUs within the authentication flows that have just been agreed by S3 and that are included in this liaison for information:



Authenticated registration, authentication successful

1. SA3 recognizes that the IMPI could be first authenticated and then the IMPU could be validated. One solution is that all IMPUs should be downloaded to the S-CSCF during Cx-Pull (22 & 23) and the S-CSCF performs this check.

2. SA3 also recognizes that another solution would be to do the check during the Cx-Query procedures.

3. There may be other solutions.

Before any decision is taken, SA3 needs to know if scenario 1, which means that all IMPUs are downloaded to the S-CSCF, is acceptable by SA2 and CN4 or not.

3GPP TSG SA WG3 Security — S3#19 **S3-010328**
3 - 6 July, 2001, Newbury, UK

Agenda Item: 7.3

Source: Ericsson

Title: Validation of public user identity in registration

Document for: Discussion and decision

---

1. Scope and objectives

During last S2 meeting (25th – 29th June), Ericsson presented a contribution that tried to solve a potential problem when Public Identities are misused at User Registration.

Since this was considered by S2 as having too many security implications and there were not time enough to draft a LS to S3, Ericcson was asked to raise this issue in S3 directly.

S2 contribution and CR to 23.228 below introduces the problem and proposes a solution. This shall be discussed now by S3#19 in order to provide guidance as requested by S2.

It shall be also noted that this issue shall be dealt with along with other discussions regarding the correct handling of Private and Public User Identities in IMS.

3GPP TSG-SA WG2 drafting
25-29 June, 2001
Dallas (US)

Tdoc S2-011634

Agenda item: 4

Source: Ericsson

Title: Validation of public user identity in registration

Document for: discussion and decision

---

1. Introduction

In SA2 # 17, the role of the identifiers in IMS was defined. A description of the usage of public and private user identities is shown in TS 23.228 in section 4.3.3 Identification of users. The following statements are captured from this section:

- *The Private User Identity is authenticated only during registration of the subscriber, (including re-registration and de-registration).*
- *Public User Identities are not authenticated by the network during registration.*

The current assumption is that the REGISTER message contains both identities, the private user identity to authenticate the user and the public user identity for the registration process itself. According to the discussions in last SA3-SA2 joint meeting held in Madrid, there is no security relation between both user identities. Therefore, the validation of the private user identity through the user authentication procedure does not preclude the fraudulent usage of the public user identity, above all during an initial registration when no integrity protection is provided yet.

---

2. Discussion

The fact that there is no security relation between the private user identity and the public user identities, brings up the need of validating the public user identity that the end user is trying to use to register in the IMS. This means that the network shall check that the public user identity intending to register is included in the list of public user identities subscribed for that user.

The HSS is the network entity that owns the subscription of the user. This subscription contains the list of valid public user identities for a given private user identity (user). Therefore, it is proposed that the HSS checks the validity of a public user identity during the registration process. It is considered that the sooner this check is done the better, so the allocation of resources to a user that might not have a valid identifier is avoided. It is proposed that the HSS performs this check when a Cx- Query is received from the I-CSCF. This Cx-Query message shall contain both user identities sent in the REGISTER message.

---

3. Proposal

The following CR contains the proposed modifications in the registration information flows of 23.228 (section 5.2.2.3).

CR-Form-v3

CHANGE REQUEST

⌘ 23.228 CR 57 ⌘ rev - ⌘ Current version: 5.0.0 ⌘

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

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

Title:	⌘	Validation of public user identity in registration
Source:	⌘	Ericsson
Work item code:	⌘	IMS-CCR
Date:	⌘	2001-06-20
Category:	⌘	**B**
Release:	⌘	REL-5

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

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change:	⌘	User authentication procedures only authenticate the private user identity. There is no security relation between the private user identity and the public user identity, therefore, the network shall ensure that a valid public user identity is being used for registering the IMS.
Summary of change:	⌘	During the registration process, the HSS checks that the public user identity is valid according to the subscription information.
Consequences if not approved:	⌘	Fraudulent usage of public identities. This may cause security problems and MT routing problems.

Clauses affected:	⌘			
Other specs affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	
Other comments:	⌘			

First Change

5.2.2.3 Registration information flow – User not registered

The application level registration can be initiated after the registration to the access is performed, and after IP connectivity for the signalling has been gained from the access network. For the purpose of the registration information flows, the subscriber is considered to be always roaming. For subscribers roaming in their home network, the home network shall perform the role of the visited network elements and the home network elements.

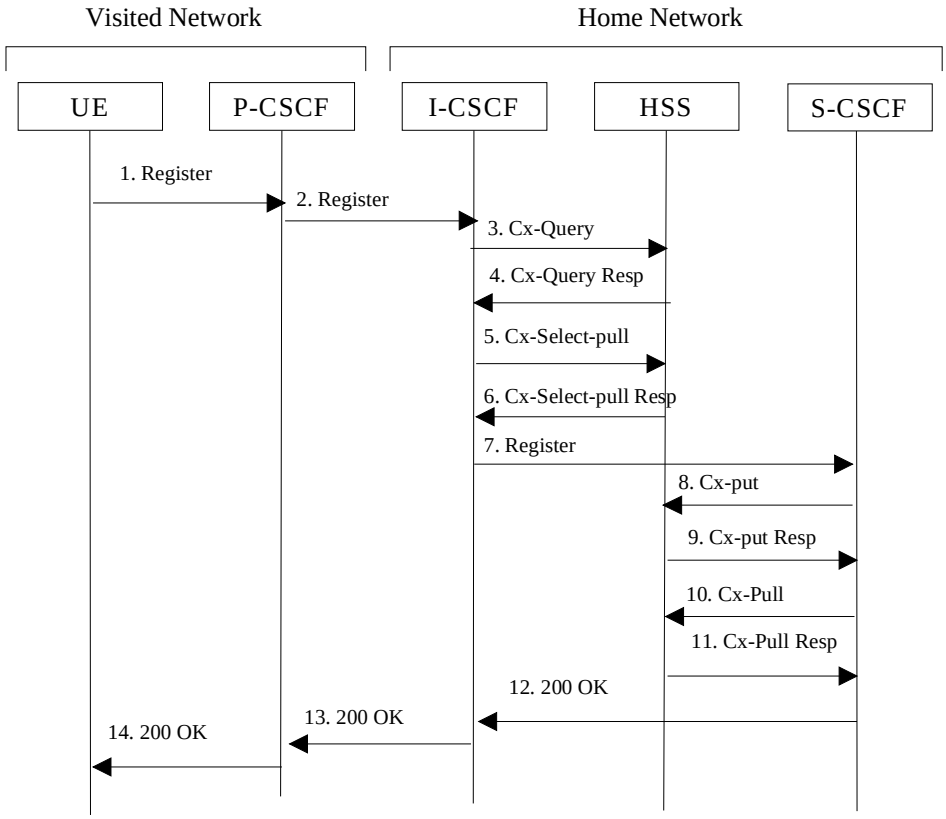


Figure 5.1: Registration – User not registered

1. After the UE has obtained a signalling channel through the access network, it can perform the IM registration. To do so, the UE sends the Register information flow to the proxy (private user identity, public user identity,~~subscriber identity,~~ home networks domain name).

2. Upon receipt of the register information flow, it shall examine the "home domain name" to discover the entry point to the home network (i.e. the I-CSCF). The proxy shall send the Register information flow to the I-CSCF (P-CSCFs "name" in the contact header, private user identity, public user identity,~~subscriber identity,~~ visited network contact name). A name-address resolution mechanism is utilised in order to determine the address of the home network from the home domain name. When the I-CSCF receives the registration information flow from the proxy, it shall examine the subscriber identity and the home domain name, and employ the services of a name-address resolution mechanism, to determine the HSS address to contact.

3. The I-CSCF shall send the Cx-Query information flow to the HSS (P-CSCF name, ~~subscriber identity~~private user identity, public user identity, home domain name, visited network contact name). The P-CSCF name is the contact name that the operator wishes to use for future contact to that P- CSCF.

Editors Note: It is FFS whether the terminal name, or proxy name, or both is included within this and subsequent register messages.

The Cx-query (P-CSCF name, ~~subscriber identity~~private user identity, public user identity, home domain name, visited network contact name) information flow is sent to the HSS. The HSS shall check whether the user is registered already. The HSS shall indicate whether the user is allowed to register in that visited network according to the User subscription and operator limitations/restrictions if any. The HSS shall validate the public user identity according to the subscription information.

4. Cx-Query Resp is sent from the HSS to the I-CSCF. If the checking in HSS was not successful the Cx-Query Resp shall reject the registration attempt.

5. At this stage, it is assumed that the authentication of the user has been completed (although it may have been determined at an earlier point in the information flows). The I-CSCF shall send Cx-Select-Pull (serving network indication, subscriber identity) to the HSS to request the information related to the required S-CSCF capabilities which shall be input into the S-CSCF selection function.

6. The HSS shall send Cx-Select-Pull Resp (required S-CSCF capabilities) to the I-CSCF.

7. The I-CSCF, using the name of the S-CSCF, shall determine the address of the S-CSCF through a name-address resolution mechanism and then shall send the register information flow (P-CSCFs "name" in the contact header, subscriber identity, visited network contact name) to the selected S-CSCF.

8. The S-CSCF shall send Cx-Put (subscriber identity, S-CSCF name) to the HSS. The HSS stores the S-CSCF name for that subscriber.

9. The HSS shall send Cx-Put Resp to the I-CSCF to acknowledge the sending of Cx-Put.

10. On receipt of the Cx-Put Resp information flow, the S-CSCF shall send the Cx-Pull information flow (subscriber identity) to the HSS in order to be able to download the relevant information from the subscriber profile to the S-CSCF. The S-CSCF shall store the P-CSCFs name, as supplied by the visited network. This represents the name that the home network forwards the subsequent terminating session signalling to for the UE.

11. The HSS shall return the information flow Cx-Pull Resp (user information) to the S-CSCF. The user information passed from the HSS to the S-CSCF shall include one or more names/addresses information which can be used to access the platform(s) used for service control while the user is registered at this S-CSCF. The S-CSCF shall store the information for the indicated user. In addition to the names/addresses information, security information may also be sent for use within the S-CSCF.

12. The S-CSCF shall determine whether the home contact name is the S-CSCF name or an I-CSCF name. If an I-CSCF is chosen as the home contact name, it may be distinct from the I-CSCF that appears in this registration flow. The home contact name will be used by the P-CSCF to forward signalling to the home network. The S-CSCF shall return the 200 OK information flow (serving network contact name, S-CSCF name) to the I-CSCF.

13. The I-CSCF shall send information flow 200 OK (serving network contact name) to the P-CSCF. The I-CSCF shall release all registration information after sending information flow 200 OK.

14. The P-CSCF shall store the serving network contact name, and shall send information flow 200 OK to the UE.

3GPP TSG WG3 S3#19
Newbury, UK
4th July – 6th July, 2001

Tdoc S3-~~010xxxx~~010367

Agenda Item: TBD

Source: Ericsson

Title: On registering several public identities in IM CN SS

Document for: Discussion/Decision

1 Scope and objectives

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

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.

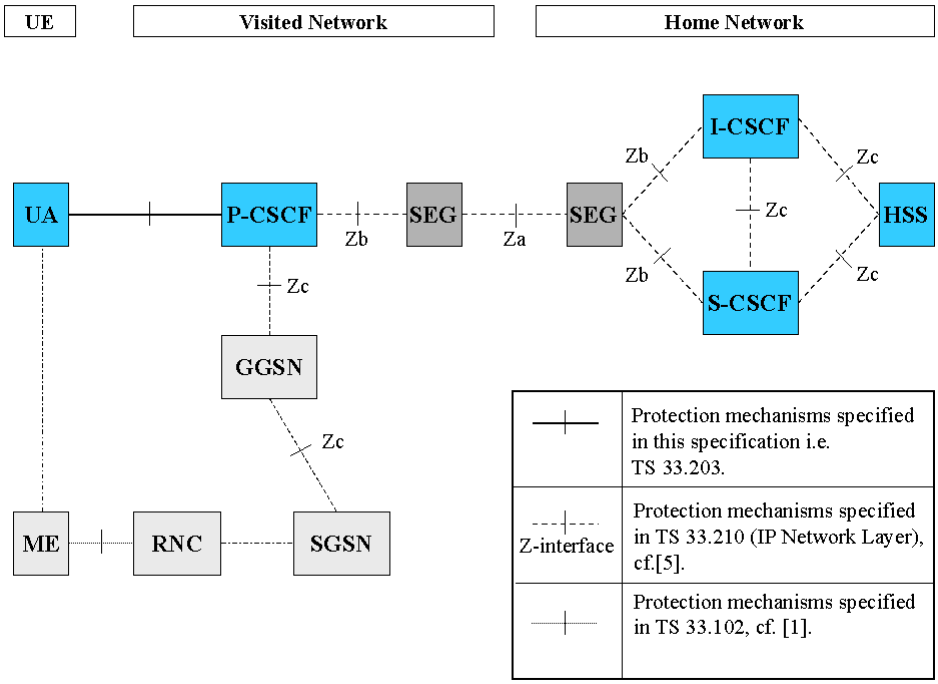
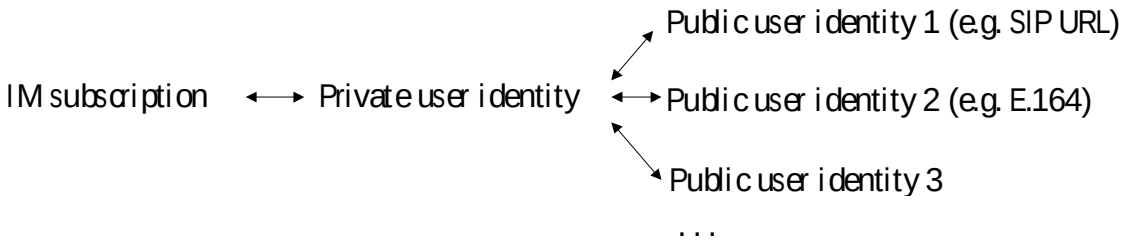


Figure: An overview of the security architecture for the IM CN SS and its relationship to NDS i.e. TS 33.210.

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.

4 Conclusions

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”