

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.

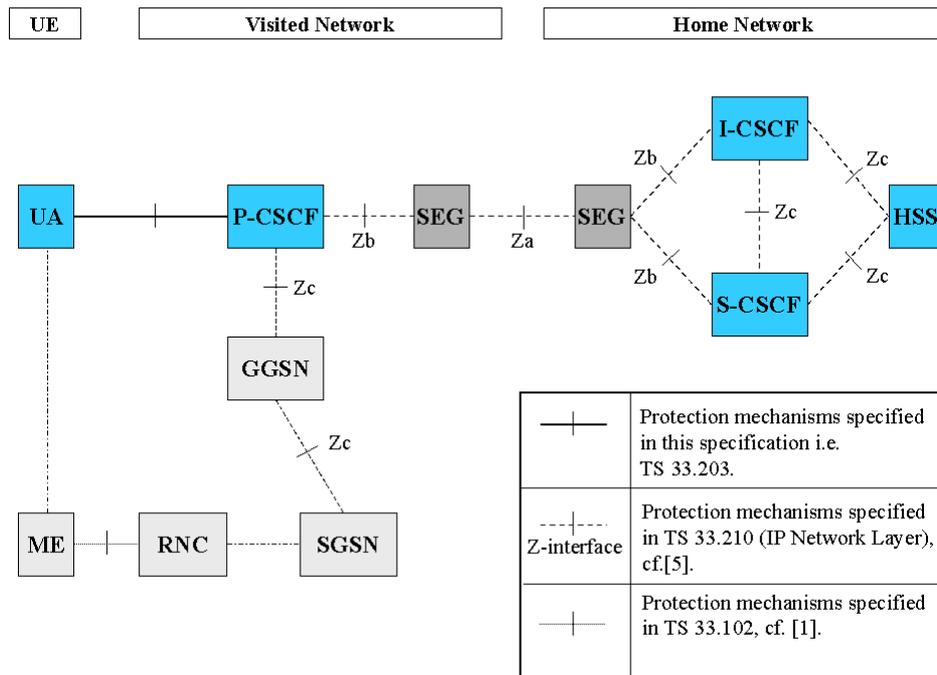
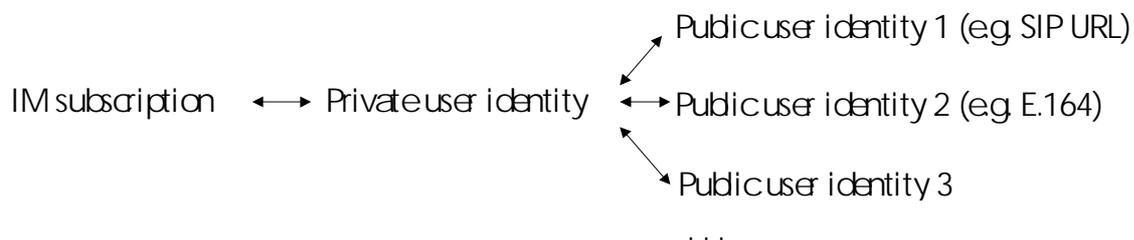


Figure: An overview of the security architecture for the IM CN SS and its relationship to NDS i.e. TS 33.210.

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 whether 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"