3GPP TSG WG3 S3#20 **Tdoc S3-010495**
Sydney, Australia
16th October – 19th October, 2001

Agenda Item: 7.3

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.

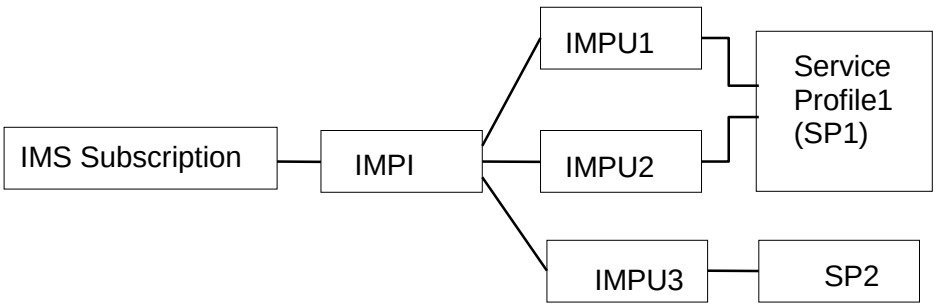
Ericsson proposes that the UE and the P-CSCF shall establish just one SA through which all the SIP signalling between the UE and the P-CSCF is carried.

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

The current assumption has been that all IMPU(s) will be registered in the same S-CSCF. This however is not the general scenario adopted by SA2. It is left FFS how the current solutions need to be adapted to the general scope as shown in the figure:



According to the SA1 requirement this is the scenario that should be supported by the IMS in Release 5. All public user identities that are associated with the same service profile should have the same set of services. Public user identities that are associated with a different service profiles could have a different set of services. All the identities belonging to one service profile will be registered in the same S-CSCF. Identities belonging to different service profiles may be assigned to different S-CSCF.

According to chapter 4.3.3.2 in [TS 23.228] it shall be possible to implicitly register several public identities through one single UE register request:

> "It shall be possible to register globally (i.e. through one single UE request) a subscriber that has more than one public identity via a mechanism within the IP multimedia CN subsystem. This shall not preclude the user from registering individually some of his/her public identities if needed."

The confidentiality and integrity protection for SIP-signalling is provided in a hop-by-hop fashion. The first hop i.e. between the UE and the P-CSCF shall provide integrity protection and may provide confidentiality protection. The other hops, inter-domain and intra-domain are specified in [33.210].

In the IM CN SS, authentication of users is performed during registration. Subsequent signalling communications in this session between the P-CSCF and the UE will be integrity and optionally confidentiality protected based on the keys derived during the authentication process.

3 Issues

This section handles different alternatives for registering multiple IMPU(s) belonging to an IM-subscriber. The different implications on user authentication and SA handling are discussed.

3.1 Independent handling of IMPU(s)

The first alternative is to handle the registration of the IMPU(s) independently. In this case, the registration of each IMPU is handled as defined in [33.203]. Each registration is authenticated and as a result a separate SA is established for each IMPU.

Let's assume a user registers first IMPU1. Since it is the first registration 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.

In a 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, since the existing SA between the UE and the P-CSCF is not used.

This means that the S-CSCF (may be the same S-CSCF or a different one) will perform a new authentication and a new SA is derived for IMPU3.

This approach does not optimise the usage of resources and is not scalable either in the UE or in the P-CSCF, since as many SA as registered IMPU(s) will be active. On the other hand, this approach simplifies P-CSCF behaviour since all registrations will be handled in the same way, regardless whether they correspond to the same UE or not.

3.2 Integrated handling of IMPU(s)

A second alternative is to handle the registration of new IMPU(s) in the same way it is defined for re-registrations in [33.203]. Therefore, there will only be one SA between the UE and the P-CSCF.

Let's assume a user registers first IMPU1. Since it is the first registration 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.

In a second message the user wants to register IMPU3. The REGISTER message is protected with the existing SA. The S-CSCF (may be the same S-CSCF or a different one) will perform a new authentication and a new SA is derived. From that point on, the new SA will protect SIP signalling messages between the UE and the P-CSCF.

This means that the UE checks that it has a valid SA and uses that. The P-CSCF needs to associate the SA to the UE and not to a particular IMPU. A new SA is derived when the user wants to register new IMPU(s) or may also be derived due to any subsequent registration initiated by the UE.

3.3 Single Authentication

The two alternatives presented above share a major drawback. Even if the user registers several IMPU(s) consecutively, the system will authenticate each of the registrations. This is a result of the fact that the SA is terminated in the visited environment, and therefore, the Home Environment, which takes the decision whether a new authentication shall be performed or not is not aware of whether a valid SA is currently in use.

In addition, [23.228] currently states that it shall be possible to register through one single UE request a subscriber that that has more than one public identity. A need for a possibility to implicitly register several IMPU(s) with the same Service Profile or by another service is discussed in chapter 3.3.2.

3.3.1 Indication to S-CSCF that a valid SA is currently in use

A possible solution to make the S-CSCF aware of whether a valid SA is currently in use or not would be to define a flag in the communication between the P-CSCF and the S-CSCF. The flag would make it possible for the P-CSCF to indicate to the S-CSCF that a valid SA has been used by the UE for sending the SIP message.

The S-CSCF would keep track of the validity of the SA. As long as the SA is valid, the S-CSCF will not require authentication for those messages sent by the UE through the appropriated SA. In this case the Home Environment is trusting the Serving Environment since it has no means to verify that the P-CSCF is using the SA flag in a proper way. Even in the case when the user registers several IMPU(s) implicitly in the Home Environment, the S-CSCF do not have to require authentication for those messages sent by the UE through the appropriate SA.

This solution may require the definition of a new SIP header to carry the flag between the P-CSCF and the S-CSCF. The actual format of the flag and the mapping to the SIP headers is left for further study.

This solution is applicable only to the alternative presented in 3.2, since in the alternative in 3.1 authentication is necessary to derive the new SA(s), one per IMPU.

This solution will reduce the number of user authentication required due to the registration of several IMPU.

Using this solution, for each mobile originated de-registration the S-CSCF could implicitly rely on the existing SA. So it would not be necessary to authenticate de-registrations.

3.3.2 Authenticate once per Service Profile (SP)

Another way of optimising the number of times the authentication is performed could be to use the Service Profile concept (or another type of service in the IM CN SS) to implicitly register all Public ID's belonging to the same Service Profile. The S-CSCF would then authenticate the user once for each Service Profile.

For example, the user first registers IMPU1. Since it is the first registration 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. As IMPU1 belong to SP1, IMPU2 is also implicitly registered.

In a second message the user wants to register IMPU3, which belong to SP2. The REGISTER message is protected with the existing SA. The S-CSCF (may be the same S-CSCF or a different one) will perform a new authentication and a new SA is derived. From that point on, the new SA will protect SIP signalling messages between the UE and the P-CSCF.

This solution is only applicable to the alternative presented in 3.2, since the alternative in 3.1 authentication is necessary to derive the new SA(s), one per IMPU.

This solution assumes that the S-CSCF knows which IMPU(s) that are implicitly registered, e.g. the Cx interface may be impacted.

4 Conclusions

This contribution has presented two different alternatives for registering a subscriber and his/hers IMPU(s). The first one handles the IMPU in an independent manner, and creates one SA per IMPU. The second alternative re-uses a single SA between the UE and the P-CSCF for all the SIP messages, regardless the IMPU they are related to. The contribution has also presented two possible ways of optimising the solution proposed in chapter 3.2.

Considering the drawbacks with the solution described in chapter 3.1, it is proposed that SA3 take the working assumption that there exist only one SA between the UE and the P-CSCF and that the latest SA applies.

In addition, it is proposed that further discussions are needed to decide on the needed optimisations. It is assumed that the optimisations in chapter 3.3.1 and 3.3.2 could be used in combination or separately.

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 (v060): "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”