3GPP TSG SA WG3 Security — S3#21b **S3z020027**

31st January - 1st February, 2002

Antwerp, Belgium

Source: **Hutchison 3G UK**

Title: **Need for section 7.3.3**

Document for: **Discussion/Decision**

Agenda Item: **IMS-8**

The change of having only one SA between a UE and P-CSCF makes the need for Section 7.3.3 Authenticated re-registration less necessary. This is because there is no real difference between an authenticated registration of a further IMPU and an authenticated re-registartion. This is because for both of them there already exists an SA and they will both negotiate a new SA. Put another way as there is now one SA per IMPI and it is the IMPI that is authenticated, every register after the first is effectively the same process.

An examination of the sections in 7.3.3 reveals that only 7.3.3.1 and 7.3.3.2 contain any significant information that is not in other sections. These are both about the handling of SAs and could be contained in standalone sections. Section 7.3.3.3 contains no more information than is contained in sections 7.3.1.1, 7.3.1.2 and 7.3.1.3, except perhaps the need not to set security associations. Section 7.3.3.4 contains the same information as 7.3.2.

The only changes needed in earlier sections by removing the unnecessary sections of 7.3.3 are to make some sections apply to re-registrations as well as registrations.

This contribution proposes some changes to TS 33.203 given in the attached document.

SA3 is asked to approve this changes to TS 33.203.

********** FIRST MODIFIED SECTION **********

6.1 Authentication and key agreement

The scheme for authentication and key agreement in the IMS is called IMS AKA. The IMS AKA achieves mutual authentication between the ISIM and the HN, cf. Figure 3. The identity used for authenticating a subscriber is the private identity, IMPI, which has the form of a NAI, cf. [3]. The HSS and the ISIM share a long-term key associated with the IMPI.

For the IMS the ISIM and the HSS keeps track of the counters SQN_{ISIM} and SQN_{HSS}~~,~~ respectively. The handling of the SQN can be as in [1]. The HN shall choose the IMS AKA scheme for authenticating an IM subscriber accessing through UMTS. The security parameters e.g. keys generated by the IMS AKA scheme are transported by SIP and embedded in EAP, cf. [7]-[9].

[Editors Note: Shall the HN choose EAP AKA for 3GPP-access or is it to be an option for the HN to choose either EAP AKA or perhaps any other mechanism e.g. HTTP digest depending on policy?]

The generation of the authentication vector AV that includes RAND, XRES, CK, IK and AUTN shall be done in the same way as specified in [1]. For each user it is the HSS that keeps track of the counter SQN_{HSS}. The requirements on the SQN handling both in the Home Network i.e. the HSS and the ISIM are specified in [1]. The AMF field can be used in the same way as in [1].

Furthermore a security association is established between the UE and the P-CSCF. The subscriber may have several IMPUs associated with one IMPI. These can ~~and~~ belong to the same or different service profiles. Only one SA shall be active between the UE and the P-CSCF. This single SA shall be updated when a new successful authenticated registration or re-registration has occurred, cf. section 7.~~3.3~~4.1. It is the policy of the HN that decides if an authentication shall take place for the registration of different IMPUs e.g. belonging to same or different service profiles.

6.1.1 Registration 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 3, which will perform the authentication of the user. The same flows are used for re-registrations.

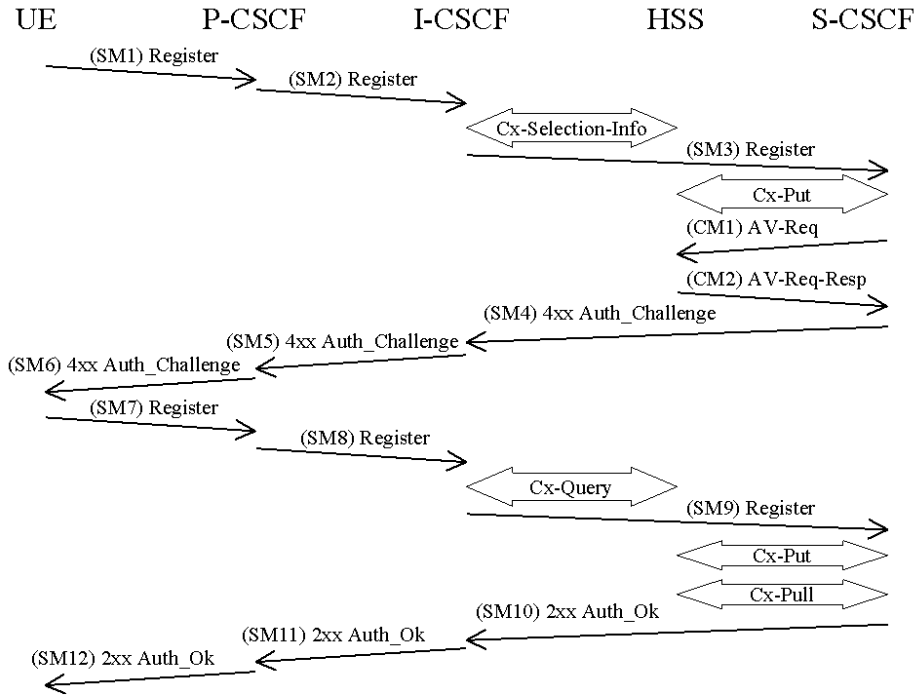

Figure 3: The IMS Authentication and Key Agreement for an unregistered IM subscriber and successful mutual authentication with no synchronization error.

The flows in more detail (for clarification: TS 24.229, cf. [13], specifies complete registration flows)

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

SM1:

REGISTER sip: ----

Authorization-EAP(IMPI)

[Editor's note: This example covers the case when only one public identity is registered. It is still FFS how to treat the case when the subscriber registers several public identities or those IMPUs are implicitly registered.]

The P-CSCF and the I-CSCF forwards the SIP REGISTER towards the S-CSCF and adds a Via header with their addresses included, i.e. SM2 and SM3.

In order to handle mobile terminated calls while the initial registration is in progress and not successfully completed the S-CSCF shall send a registration flag to the HSS. The registration flag shall be stored in the HSS together with the S-CSCF name. The aim of the registration flag is 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 HSS receives the information about this state (together with the S-CSCF name and the user identity) from the S-CSCF with which (re-) registration of the user is carried out only when a Cx-Put message is sent from the S-CSCF to the HSS. The registration flag shall be set to *initial registration pending* at the Cx-Put procedure after SM3 has been received by the S-CSCF.

Upon receiving the SIP REGISTER the S-CSCF will need one AV which includes the challenge. As an option the S-CSCF can require more than one AVs. If the S-CSCF has no valid AV then the S-CSCF shall send a request for the AV(s) to the HSS in CM1 together with the number n of AVs wanted where n is at least one but less than or equal to nmax.

[Editor's note: The maximum value of n i.e. nmax has not been defined.]

[Editor's note: Potential failure scenarios and potential extra requirements needed for the handling several AV(s) in the S-CSCF are left FFS.]

CM1:

Cx-AV-Req(IMPI, IMPU, n)

If the HSS has no pre-computed AVs the HSS creates the needed AVs on demand for that user and sends it to the S-CSCF in CM2.

CM2:

Cx-AV-Req-Resp(IMPI, IMPU,n,$RAND_1$||$AUTN_1$||$XRES_1$||CK_1||IK_1,….,$RAND_n$||$AUTN_n$||$XRES_n$||CK_n||IK_n)

The S-CSCF sends a SIP 4xx Auth_Challenge i.e. an authentication challenge to the UE including the challenge RAND, the authentication token AUTN in SM4 and the integrity key IK and optionally the cipher key CK.

[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.]

SM4:

SIP/2.0 4xx Auth_Challenge

WWW-Authenticate-EAP(*IMPI, RAND, AUTN)* Key parameters(*IK, (CK))*

[Editor's note: The use of KSI i.e. Key Set Identifier for IMS is FFS.]

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:

SIP/2.0 4xx Auth_Challenge

WWW-Authenticate-EAP*(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. It should be noted that the UE at this stage also computes the session keys CK and IK.

SM7:

REGISTER sip: ----

Authorization-EAP*(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 the response, RES, the S-CSCF retrieves the active XRES for that user and checks if XRES=RES. If the check is successful then the user has been authenticated and the IMPU is registered in the S-CSCF. To ensure that the S-CSCF is able to take the decision whether a subsequent registration shall trigger a new authentication and to be able to check that all INVITE messages will be sent to/from an authorized subscriber 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. The S-CSCF shall regard all implicitly registered IMPU(s) as registered IMPU(s).

[Editor's note: Since implicitly registered IMPUs are not available in the P-CSCF this functionality opens up a weakness in the IMS security architecture. Requirements that closes this weakness needs to be defined and is left FFS.]

At this stage the S-CSCF shall send in the Cx-Put after receiving SM9 an update of the registration-flag. If the authentication of the subscriber is successful the registration flag shall take the value *registered.* When the authentication is unsuccessful the registration flag shall be set to *unregistered*.

When a subscriber 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. The UE initiated re-registration opens up a potential denial-of-service attack in the sense that an attacker could re-register a subscriber and respond with the wrong RES and the HN could then de-register the subscriber. It shall be defined by the policy of the operator when successfully registered IMPU(s) are to be de-registered.

The authenticated re-registration looks the same as the initial registration except that CM1 and CM2 can be omitted as long as the S-CSCF has valid AV(s). At a re-registration the registration flag has already the value *registered.* The policy of the home provider states whether the flag shall be changed at a re-registration. There are two cases:

- The IMS subscriber is de-registered after unsuccessful registration. In this case the registration flag shall be set to *unregistered* and an error message shall be sent to from the S-CSCF to the HSS.
- The IMS subscriber remains registered after unsuccessful re-registration. In this case the registration flag is kept in the HSS to the value *registered* even if the authentication was unsuccessful.

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

********** NEXT MODIFIED SECTION **********

7.3.1.1 User authentication failure

In this case the authentication of the user fails in the network due an incorrect RES. The S-CSCF will send a 4xx Auth_Failure message SM7, which will pass through the already established SA to the UE as SM8. Afterwards both the UE and the P-CSCF delete the new SAs.

Note, that this failure will already occur in SM5, when the UE does not use the correct integrity key IK. In this situation, the P-CSCF will receive protected packets that cannot be verified.

It may seem from the above discussion that there is no requirement to check the RES at the S-CSCF since a false RES sent by a UE will never reach the S-CSCF. However, it is still necessary to check RES at the S-CSCF since this prevents a P-CSCF from registering a UE without performing user authentication. It therefore reduces S-CSCF trust in the P-CSCF.

7.3.1.2 Network authentication failure

If the UE is not able to successfully authenticate the network, the UE ~~is~~ does not ~~able to~~ create ~~the key IK and therefore~~ the SA. ~~with the P-CSCF, such that it is not possible to send SM5 in a protected way~~. Since the P-CSCF already expects SIP messages from the UE to be protected, and is not already aware of any errors, the P-CSCF shall accept such REGISTER messages indicating network authentication failure in the clear although the UE can protect the message with a previously established SA.

So the UE sends a new register message SM5, indicating a network authentication failure, to the P-CSCF, without protection. SM5 should not contain the security-setup line of the first message. The P-CSCF deletes the new SA after receiving this message.

7.3.1.3 Synchronisation failure

In this situation, the UE observes that the AUTN sent by the network in SM4 contains an out-of-range sequence number. The UE does not set-up an SA and shall send~~s~~ a new register message SM5 to the P-CSCF ~~in the clear~~, possibly protected with a previously established SA, indicating the synchronization failure. SM5 should not contain the Security-Setup line of the first message, and the P-CSCF shall keep the security-setup state created after receiving SM1 from the UE. The P-CSCF deletes the new SA after receiving this message.

********** NEXT MODIFIED SECTION **********

~~7.3.3 Authenticated re-registration~~

~~If the registration is a re-registration, a pair of security associations between UE and P-CSCF is already active.~~

~~[Editors Note: It is FFS if these SAs shall protect the first two messages of the authenticated re-registration, i.e. SM1 and SM4.]~~

~~Before SM5 is sent by the UE, both peers shall replace the existing SA by the new SA negotiated during these first two messages.~~

7.3.3.1 Handling of security associations in authenticated re-registrations (successful case)

Before re-registration begins the following SAs exist:

-SA1 from UE to P-CSCF

-SA2 from P-CSCF to UE

The re-registration then is as follows:

1) The UE sends SM1 to re-register with the IMS, using the existing SA1 to the P-CSCF. As in the case of a new registration, a list of parameters to be negotiated in a security association set-up is included.

[Editors Note: It is FFS if the SA1 shall be used for SM1 or not]

2) The P-CSCF waits for the response SM3 from the S-CSCF and then sends SM4 to the UE, using SA2. As in the case of a new registration, the parameters selected for the new security associations are included. The P-CSCF then creates two new security associations, in parallel to the existing ones, in its database:

- SA11 from UE to P-CSCF

- SA12 from P-CSCF to UE

3) If SM4 could be successfully processed by the UE, the UE also creates the new SAs SA11 and SA12 in its database. The UE then sends SM5 to the P-CSCF. As in the case of a new registration, the authentication response and the list of parameters repeated from message 1 are included. SM5 is protected with the new SA11.

4) The P-CSCF waits for the response SM7 from the S-CSCF and then sends SM8 to the UE, using the new SA 12.

5) After the reception of SM8 by the UE, the re-registration is complete.

The UE now uses the new SAs for all subsequent messages. The old (outbound) SA1 is deleted. The old (inbound) SA2 must be kept until a further SIP message protected with the new inbound SA12 is successfully received from the P-CSCF.

The P-CSCF keeps all four SAs with the UE active until a further SIP message protected with the new inbound SA11 is successfully received from the UE. In the meantime, the P-CSCF continues to use the old SA2 for outbound traffic to the UE.

7.3.3.2 Error cases related to authenticated re-registration

Whenever an expected message is not received after a time-out the receiving entity considers the registration to have failed. The receiving entity then deletes any new security associations it may have established and continues to use the old ones if they have not yet expired.

If the registration protocol goes well up to the last message SM8, and SM8 is sent by the P-CSCF, but not received by the UE , then the UE has only the olds SAs available (after the time-out), but the P-CSCF cannot know this. Therefore, the P-CSCF continues to use the old SA2 for outbound traffic to the UE, but keeps both, old and new SAs. The new SAs are deleted when a message is received from the UE which is protected with the old SA, or if a REGISTER message is received on the port where the P-CSCF accepts specific unprotected messages.

7.3.3.3 Error cases related to IMS AKA

User authentication failure

The S-CSCF will send a 4xx Auth_Failure message SM7, which will pass through the already established SA to the UE as SM8. Afterwards, both, the UE and the P-CSCF delete the new SAs.

Network authentication failure

If the UE is not able to successfully authenticate the network, it does not establish a new SA. The UE sends a REGISTER message SM5 indicating a network authentication failure to the P-CSCF, using the already established SA. The P-CSCF deletes the new SAs after receiving this message.

Synchronisation failure

If the UE notices a synchronisation failure it does not establish a new SA. The UE sends a message SM5, indicating the synchronisation failure, to the P-CSCF, using the already established SA. The P-CSCF deletes the new SA after receiving this message.

7.3.3.4 Error cases related to the Security-Setup

Unacceptable proposal set

The message SM4 shall respond to the first REGISTER message SM1 with a 4xx Unacceptable_Proposal, using the already established SA. Neither side establishes a new SA.

The P-CSCF therefore shall modify the message SM2 such that the S-CSCF sends the 4xx Unacceptable_Proposal message back to the UE in SM3/4 and the registration process is finished.

SM2:

REGISTER sip: ----

Security-setup*(integrity mechanisms list, [confidentiality mechanisms list], integrity algorithms list, [confidentiality algorithms list], SA_ID_U, [info])*
Authorization-EAP*(IMPI)*
Failure(*NoCommonIntegrityAlgorithm)*

[Editors Note: It is FFS how the exact mechanism shall be for the Unacceptable proposal set case. The editor believes that the S-CSCF is the registrar and hence the P-CSCF should only be able to modify the headers and not send back responses. The failure response should be sent by the S-CSCF. This however has not been agreed.]

Failed consistency check of Security-Set-up lines

This is the case if the Security-Setup line in SM5 from the UE to the P-CSCF cannot be verified, so the Security-Setup line of the unprotected SM1 and the Security-Setup line of the protected SM5 do not match. In this case the P-CSCF shall respond to the UE by sending a 4xx Unacceptable_Proposal message in SM8 using the already established SA. Both sides delete the new SAs.

The P-CSCF therefore shall modify the message SM6 such that the S-CSCF sends the 4xx Unacceptable_Proposal message back to the UE in SM7/8 and the registration process is finished.

~~SM6:~~

~~REGISTER sip: ----~~

~~Security-setup(*integrity mechanisms list, [confidentiality mechanisms list], integrity algorithms list, [confidentiality algorithms list], SA_ID_U, [info]*)~~

~~Authorization-EAP(*IMPI*)~~

~~Failure(*NoCommonIntegrityAlgorithm*)~~

~~*[Editors Note: It is FFS how the exact mechanism shall be for the Unacceptable proposal set case. The editor believes that the S-CSCF is the registrar and hence the P-CSCF should only be able to modify the headers and not send back responses. The failure response should be sent by the S-CSCF. This however has not been agreed.]*~~

********** NEXT MODIFIED SECTION **********

7.4 Management of security associations

7.4.1 Handling of security associations in authenticated registrations and re-registrations (successful case)

Before re-registration begins the following SAs exist:

- SA1 from UE to P-CSCF

- SA2 from P-CSCF to UE

The re-registration then is as follows:

1) The UE sends SM1 to re-register with the IMS, using the existing SA1 to the P-CSCF. As in the case of a new registration, a list of parameters to be negotiated in a security association set-up is included.

[Editors Note: It is FFS if the SA1 shall be used for SM1 or not]

2) The P-CSCF waits for the response SM3 from the S-CSCF and then sends SM4 to the UE, using SA2. As in the case of a new registration, the parameters selected for the new security associations are included. The P-CSCF then creates two new security associations, in parallel to the existing ones, in its database:

- SA11 from UE to P-CSCF

- SA12 from P-CSCF to UE

3) If SM4 could be successfully processed by the UE, the UE also creates the new SAs SA11 and SA12 in its database. The UE then sends SM5 to the P-CSCF. As in the case of a new registration, the authentication response and the list of parameters repeated from message 1 are included. SM5 is protected with the new SA11.

4) The P-CSCF waits for the response SM7 from the S-CSCF and then sends SM8 to the UE, using the new SA 12.

5) After the reception of SM8 by the UE, the re-registration is complete.

The UE now uses the new SAs for all subsequent messages. The old (outbound) SA1 is deleted. The old (inbound) SA2 must be kept until a further SIP message protected with the new inbound SA12 is successfully received from the P-CSCF.

The P-CSCF keeps all four SAs with the UE active until a further SIP message protected with the new inbound SA11 is successfully received from the UE. In the meantime, the P-CSCF continues to use the old SA2 for outbound traffic to the UE.

7.4.2 Error cases related to authenticated registration and re-registration

Whenever an expected message is not received after a time-out the receiving entity considers the registration to have failed. The receiving entity then deletes any new security associations it may have established and continues to use the old ones if they have not yet expired.

If the registration protocol goes well up to the last message SM8, and SM8 is sent by the P-CSCF, but not received by the UE , then the UE has only the olds SAs available (after the time-out), but the P-CSCF cannot know this. Therefore, the P-CSCF continues to use the old SA2 for outbound traffic to the UE, but keeps both, old and new SAs. The new SAs are deleted when a message is received from the UE which is protected with the old SA, or if a REGISTER message is received on the port where the P-CSCF accepts specific unprotected messages.