3GPP TSG SA WG3 Security — S3#22 **S3-020110**

25 - 28 February 2002

Bristol, UK

Source: Vodafone

Title: Proposed editorial clarifications to 33.203 v1.1.0

Document for: Approval

Agenda Item:

Some editorial clarifications to 33.203 are proposed.

Section 5.1.1: A reference to the detailed specification in section 6 is added. This is in-line with the other sub-sections in section 5. A minor editorial clarification is also made.

Section 6.1: Some text on the management of sequence numbers is moved to improve readability. Some text on AV handling is updated to allow an editor's note to be removed. A new editor's note is added since it is not clear what the S-CSCF behaviour should be when it cannot fetch new AVs from the HSS.

5 Security features

5.1 Secure access to IMS

5.1.1 Authentication of the subscriber and the network

Authentication between the subscriber and the network shall be performed as specified in section 6.1.

An IM-subscriber will have its subscriber profile located in the HSS in the Home Network. The subscriber profile will contain information on the subscriber that may not be revealed to an external partner, cf. [3]. At registration an S-CSCF is assigned to the subscriber by the I-CSCF. The subscriber profile will be downloaded to the S-CSCF over the Cx-reference point from the HSS (Cx-Pull). When a subscriber requests an IM-service the S-CSCF will check, by matching the request with the subscriber profile, if the subscriber is allowed to continue with the request or not i.e. Home Control (Authorization of IM-services).

All SIP-signaling will take place over the PS-domain in the user plane i.e. IM-services are essentially an overlay to the PS-domain. Hence the Visited Network will have control of all the subscribers in the PS-domain i.e. Visited Control (Authorization of bearer resources) since the Visited Network provides with a transport service and QoS.

For IM-services a new security association is required between the mobile and the IMS before access is granted to IM-services. The Home Network or a 3rd party even (which does not have to be an UMTS operator) provides the user with the IM-services.

The mechanism for mutual authentication in UMTS is called UMTS AKA. It is a challenge response protocol and the AuC in the Home Stratum derives the challenge. A Quintet containing the challenge is sent from the Home Stratum to the Serving Network. The Quintet contains the expected response XRES and also a message authentication code MAC. The Serving Network compares the response from the UE with the XRES and if they match the UE has been authenticated. The UE calculates an expected MAC, XMAC, and compares this with the received MAC and if they match the UE has authenticated the Serving Network.

The AKA-protocol is a secure protocol developed for UMTS and the same concept/principles will be reused for IM-services and then called IMS AKA.

The Home Network authenticates the subscriber ~~via~~ during registrations or re-registrations only.

6 Security mechanisms

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$_{HSS}$. 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.

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]. The ISIM and the HSS keep track of counters SQN$_{ISIM}$ and SQN$_{HSS}$. The requirements on the handling of the counters and mechanisms for sequence number management ~~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 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 re-registration has occurred, cf. section 7.3.3.

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. Regarding the definition of service profiles and implicit registrations cf. [3].

6.1.1 Authentication procedure

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.

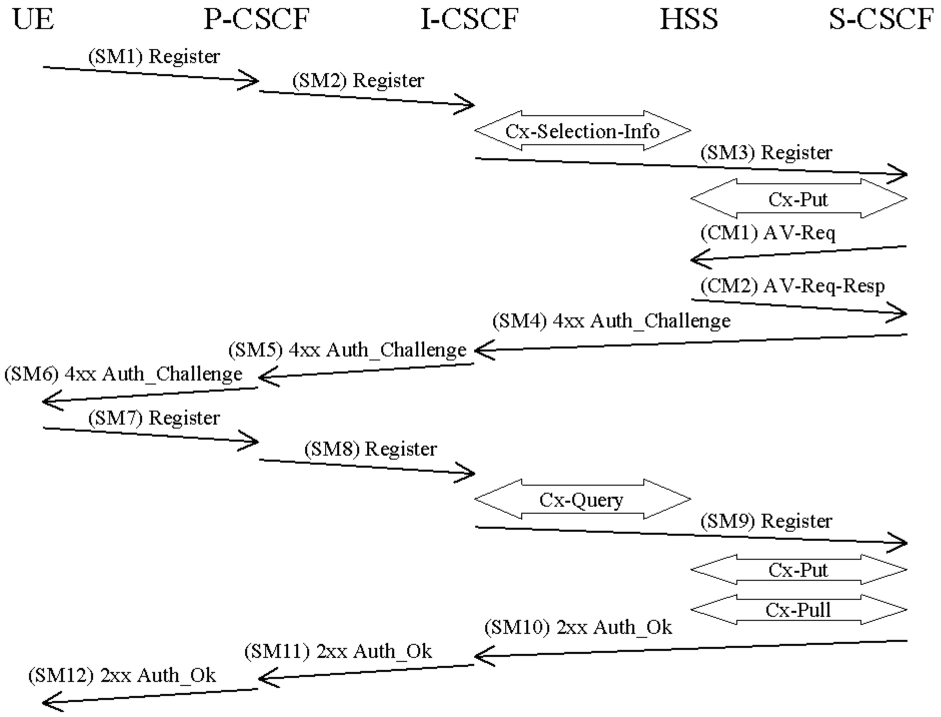

Figure 3: The IMS Authentication and Key Agreement for an unregistered IM subscriber and successful mutual authentication with no synchronization error.

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)

[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.]

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

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 shall use an Authentication Vector (AV) for authenticating and agreeing a key with the user ~~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 will be defined only if required by CN4~~has not been defined~~.]

Upon receipt of a request from the S-CSCF, the HSS sends an ordered array of *n* authentication vectors to the S-CSCF. 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.

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

[Editor's note: Should a S-CSCF be able to use an old cipher and integrity key when it cannot fetch new AVs from the HSS and the S-CSCF has no valid authentication vectors remaining?]

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

At this stage the HSS has performed a check that the IMPI and the IMPU belong to the same user.

CM1:

Cx-AV-Req(IMPI, 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, 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:

4xx Auth_Challenge(IMPI, RAND, AUTN, 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:

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. 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 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].