Technical Specification Group Services and System Aspects
Meeting #18, New Orleans, USA, 9-12 December 2002

**TSGS#18(02)0714**

**Source:** **SA WG3**

**Title:** **1 CR to 33.203 (Rel-5): Re-use and re-transmission of RAND and AUTN**

**Document for:** **Approval**

**Agenda Item:** **7.3.3**

| SA doc# | Spec | CR | R | Phase | Subject | Cat | Current Version | WI | SA WG3 doc# |
|---|---|---|---|---|---|---|---|---|---|
| SP-020714 | 33.203 | 028 | | Rel-5 | Re-use and re-transmission of RAND and AUTN | F | 5.3.0 | IMS-ASEC | S3-020680 |
| | | | | | | | | | |

**3GPP TSG-SA3 Meeting #26**
**Oxford, UK, 19-22 November 2002**

***Tdoc ⌘S3-020680***

*CR-Form-v7*

# CHANGE REQUEST

⌘ **33.203** **CR** **028** ⌘ **rev** **-** ⌘ Current version: **5.3.0** ⌘

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

***Proposed change affects:*** UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

| | | | | |
|---|---|---|---|---|
| ***Title:*** | ⌘ | Re-use and re-transmission of RAND and AUTN | | |
| ***Source:*** | ⌘ | SA WG3 | | |
| ***Work item code:*** | ⌘ | IMS-ASEC | ***Date:*** ⌘ | 11/11/2002 |
| ***Category:*** | ⌘ | **F** | ***Release:*** ⌘ | Rel-5 |

*Use one of the following categories:*
***F*** *(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)*
*Rel-6* *(Release 6)*

***Reason for change:*** ⌘

An outstanding editor note remains in the TS 33.203 which states that it is FFS if re-use and retransmissions of the same RAND and AUTN is allowed

Either UDP or TCP will be used for IMS. In the case when UDP is used, the transaction layer in SIP will handle the retransmissions.

Already in UMTS R99 it was acknowledged that reception of two consecutive authentication challenges with the same RAND and AUTN by the USIM application, would cause a synchronization failure on the USIM application. This problem applies to the ISIM as well.

In IMS the UE will handle the retransmission of the (SM1) REGISTER message in the case the UE does not receive any response (e.g. authentication challenge) from the network to a previously issued (SM1) REGISTER message. A retransmitted (SM1) REGISTER message from the UE will contain the same sequnce number as in the previous issued one, so from the S-CSCF point of view, the (SM1) REGISTER will not look as a new Register procedure. The transaction layer in SIP in the S-CSCF will retransmit the same authentication challenge with the same RAND and AUTN as used in the previous issued authentication challenge.

If the UE issues a new Register procedure then a new sequence number will be used, and the S-CSCF is then able to distinguish this as a new Register procedure.

Conclusions:

-In the case when the UE issues a new Register procedure with a new sequence number, then the S-CSCF has to select a new RAND and AUTN (i.e. a new quintet). Therefore a S-CSCF shall use a quintet only once.

- The S-CSCF is allowed to re-use the same RAND and AUTN (i.e. the same quintet) in

| | | |
|---|---|---|
| | | the case it receives a retransmitted (SM1) Register message from the UE i.e. with the same sequence number and call-id as in the previous received (SM1) Register message from the UE. For UDP, this is handled in the transaction layer in SIP according to RFC 3261. But as soon as the S-CSCF receives a response message to an authentication challenge then no further re-transmissions of the same RAND and AUTN are allowed.<br><br>- It does not seem likely that the USIM or ISIM can receive two consecutive authentication challenges with the same RAND and AUTN (which would create a synchronisation failure on the USIM and ISIM). The transaction layer in SIP in the UE will discard a received Authentication Challenge with the same RAND, AUTN and sequence number as a previously received Authentication Challenge from the network, and not forward it to the upper layer in SIP. In addition, if the UE receives an authentication challenge as a response to an issued (SM1) Register message, then the UE would not issue any further re-transmissions of the same (SM1) Register message. |
| ***Summary of change:*** | ⌘ | It is proposed that the editor note is removed.<br><br>In addition it's proposed to add that the S-CSCF shall use a quintet only once. |
| ***Consequences if not approved:*** | ⌘ | The Editor Note remains in TS33.203, which may lead the reader to belive that this issue is unresolved. |

| | | | | | |
|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 6.1.1 | | | |
| ***Other specs affected:*** | ⌘ | **Y** | **N** | | ⌘ |
| | | | **X** | Other core specifications | |
| | | | **X** | Test specifications | |
| | | | **X** | O&M Specifications | |
| ***Other comments:*** | ⌘ | | | | |

## 6.1.1 Authentication 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 1, which will perform the authentication of the user. The message flows are the same regardless of whether the user has an IMPU already registered or not.

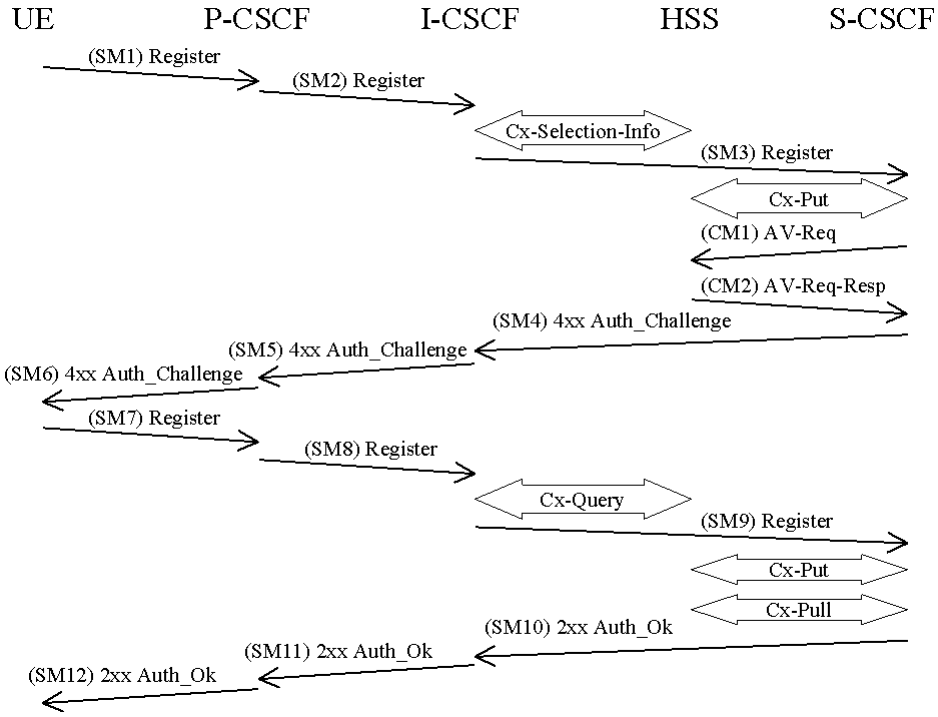


**Figure 4: The IMS Authentication and Key Agreement for an unregistered IM subscriber and successful mutual authentication with no synchronization error**

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, IMPU)

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

After receiving SM3, if the IMPU is not currently registered at the S-CSCF, the S-CSCF needs to set the registration flag at the HSS to initial registration pending. This is done in order to handle mobile terminated calls while the initial registration is in progress and not successfully completed. The registration flag is stored in the HSS together with the S-CSCF name and user identity, and is used 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 registration flag is set by the S-CSCF sending a Cx-Put to the HSS. If the IMPU is currently registered, the S-CSCF shall leave the registration flag set to *registered*. At this stage the HSS has performed a check that the IMPI and the IMPU belong to the same user.

Upon receiving the SIP REGISTER the S-CSCF CSCF shall use an Authentication Vector (AV) for authenticating and agreeing a key with the user. If the S-CSCF has no valid AV then the S-CSCF shall send a request for AV(s) to the HSS in CM1 together with the number m of AVs wanted where m is at least one.

CM1:
Cx-AV-Req(IMPI, m)

Upon receipt of a request from the S-CSCF, the HSS sends an ordered array of *n* authentication vectors to the S-CSCF using CM2. 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.

CM2:
Cx-AV-Req-Resp(IMPI, RAND1||AUTN1||XRES1||CK1||IK1,….,RANDn||AUTNn||XRESn||CKn||IKn)

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

The S-CSCF sends a SIP 4xx Auth_Challenge i.e. an authentication challenge towards the UE including the challenge RAND, the authentication token AUTN in SM4. It also includes the integrity key IK and the cipher key CK for the P-CSCF. Draft-ietf-sip-digest-aka-01 [17] specifies the fields to populate corresponding parameters of authenticate challenge.

~~[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.]~~

The verification of the SQN by the USIM and ISIM will cause the UE to reject an attempt by the S-CSCF to re-use a AV. Therefore no AV shall be sent more than once.

NOTE: This does not preclude the use of the normal SIP transaction layer re-transmission procedures.

SM4:
4xx Auth_Challenge(IMPI, RAND, AUTN, IK, CK)

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. Draft-ietf-sip-digest-aka-01 [17] specifies the fields to populate corresponding parameters of the response. 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 SM9 containing the response, the S-CSCF retrieves the active XRES for that user and uses this to check the response sent by the UE as described in Draft-ietf-sip-digest-aka-01 [17]. If the check is successful then the user has been authenticated and the IMPU is registered in the S-CSCF. If the IMPU was not currently registered, the S-CSCF shall send a Cx-Put to update the registration-flag to *registered*. If the IMPU was currently registered the registration-flag is not altered.

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 and subsequently to the P-CSCF. The S-CSCF shall regard all implicitly registered IMPU(s) as registered IMPU(s).

When an IMPU 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. A successful registration of a

previously registered IMPU (including implicitly registered IMPUs) means the expiry time of the registration is refreshed.

It should be noted that the UE initiated re-registration opens up a potential denial-of-service attack. That is, an attacker could try to register an already registered IMPU and respond with the wrong RES and in order to make the HN de-register the IMPU. For this reason a subscriber should not be de-registered if it fails an authentication. It shall be defined by the policy of the operator when successfully registered IMPU(s) are to be de-registered.

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