

---

**Source:** SA WG3  
**Title:** CR to 33.203: ISIM related parameters (Rel-5)  
**Document for:** Approval  
**Agenda Item:** 7.3.3

---

SA doc#	Spec	CR	R	Phase	Subject	Cat	Current Version	WI	SA WG3 doc#
SP-020346	33.203	003		Rel-5	ISIM related parameters	F	5.1.0	IMS-ASEC	S3-020226

# CHANGE REQUEST

⌘ **33.203 CR 003** ⌘ rev      ⌘ Current version: **5.1.0** ⌘

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

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

<b>Title:</b>	⌘ ISIM related parameters		
<b>Source:</b>	⌘ SA WG3		
<b>Work item code:</b>	⌘ IMS-ASEC	<b>Date:</b>	⌘ 06/05/2002
<b>Category:</b>	⌘ <b>F</b>	<b>Release:</b>	⌘ Rel-5
	Use <u>one</u> of the following categories: <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		Use <u>one</u> 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)

**Reason for change:** ⌘ Remove some editors notes in TS33.203. Clarify how that the SAs shall be deleted at power off and no storage of SA is required in the ISIM.

**Summary of change:** ⌘ In IMS plastic roaming is not required and R'99 parameters like e.g. START, TRHESHOLD and HFN are not applicable in IMS

**Consequences if not approved:** ⌘ Open issues are kept in TS33.203 and other specifications cannot be progressed

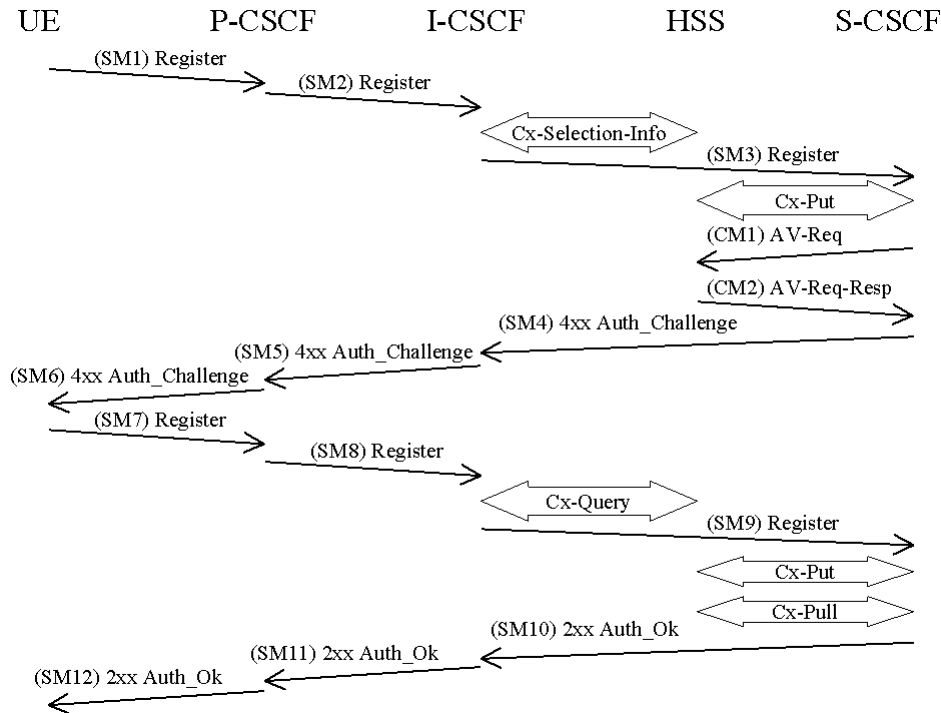
**Clauses affected:** ⌘ 6.1.1, 8.1

**Other specs affected:** ⌘  Other core specifications ⌘       
 Test specifications  
 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.



**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.

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. 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 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 only if required by CN4.]

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.

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<sub>1</sub>||AUTN<sub>1</sub>||XRES<sub>1</sub>||CK<sub>1</sub>||IK<sub>1</sub>,..., RAND<sub>n</sub>||AUTN<sub>n</sub>||XRES<sub>n</sub>||CK<sub>n</sub>||IK<sub>n</sub>)

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 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).

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 in an unprotected message 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). The P-CSCF shall forward the unprotected REGISTER to S-CSCF with an indication that the existing SA is not applied. As a consequence, the S-CSCF shall trigger a new authentication procedure. 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 based on two scenarios.

- If the re-registration is successful, the registration status keeps registered and timer for next registration is refreshed in the S-CSCF.
- The IMS subscriber remains registered after unsuccessful re-registration until timer set for next re-registration is expired. Before that the registration flag is kept in the HSS to the value *registered* even if the authentication was unsuccessful. The S-CSCF shall not remove the data about subscriber's registration and the P-CSCF shall keep the existing SA.

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

\*\*\*\*\* NEXT CHANGED SECTION \*\*\*\*\*

## 8.1 Requirements on the ISIM application

This section identifies requirements on the ISIM application to support IMS access security. It does not identify any data or functions that may be required on the ISIM application for non-security purposes.

The ISIM shall include:

- The IMPI
- At least one IMPU
- Home Network Domain Name
- Support for sequence number checking in the context of the IMS Domain
- The same framework for algorithms as specified for the USIM applies for the ISIM
- An authentication Key

The ISIM shall deliver the CK to the UE although it is not required that SIP signaling is confidentiality protected.

At UE power off the existing SAs in the MT shall be deleted. The session keys and related information in the SA shall never be stored on the ISIM.

~~{Editors Note: It is FFS if a KSI, data equivalent to the START parameter, AMF related data, storage for CK and IK is needed or not.}~~

~~{Editors Note: It is FFS if an IMS subscriber shall be de-registered at power off}~~