3GPP TSG SA WG3 Security — S3#23 **S3-020218**

14 - 18, May 2002

Victoria, Canada

Source: **Nokia**
Title: **Reference of HTTP Digest AKA in TS 33.203**
Document for: Approval
Agenda: **TBD**

Discussion

TS 33.203 version 5.1.0 uses term IMS AKA referring AKA for accessing IMS. The embodiment is specified in the Internet-Draft HTTP Digest Authentication using AKA (draft-ietf-sip-digest-aka-01) as Digest AKA. It is necessary to refer this draft in TS 33.203 in section 6, for further concrete placement of parameters and algorithms.

The detailed specification of IMS AKA is seen as stage 3 work to be specified in CN1 WG.

Proposal

The author suggests endorsement to the CR from this meeting.

(The CR is attached below.)

CR-Form-v4

CHANGE REQUEST

⌘	**33.203**	**CR**		⌘ ev	**-**	⌘ 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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	**Reference of HTTP Digest AKA in TS 33.203**	
Source:	⌘	Nokia	
Work item code:	⌘		***Date:*** ⌘
Category:	⌘	**B**	***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)*

Reason for change:	⌘	To refer Digest AKA work in TS33.203.
Summary of change:	⌘	The reference is added as well as a couple of text editorial to refer the further detail found in the Internet-Draft.
Consequences if not approved:	⌘	Inconsequent definitions and reference may lead to misunderstandings.

Clauses affected:	⌘	
Other specs affected:	⌘	[X] 24.228 [X] 24.229 [ ]
Other comments:	⌘	

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".

[2] 3GPP TS 22.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service Requirements for the IP Multimedia Core Network".

[3] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia (IM) Subsystem".

[4] 3GPP TS 21.133: "3rd Generation Partnership Project; T Technical Specification Group Services and System Aspects; Security Threats and Requirements ".

[5] 3GPP TS 33.210: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network domain security; IP network layer security".

[6] IETF RFC 3261 "SIP: Session Initiation Protocol".

[7] 3GPP TS 21.905: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects; Vocabulary for 3GPP specifications".

[8] 3GPP TS 24.229: "3rd Generation Partnership Project: Technical Specification Group Core Network; IP Multimedia Call Control Protocol based on SIP and SDP".

[9] 3GPP TS 23.002: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects, Network Architecture".

[10] 3GPP TS 23.060: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects, General Packet Radio Service (GPRS); Service Description".

[11] 3GPP TS 24.228: "3rd Generation Partnership Project: Technical Specification Group Core Network; Signalling flows for the IP multimedia call control based on SIP and SDP".

[12] IETF RFC 2617 (1999) "HTTP Authentication: Basic and Digest Access Authentication".

[13] Draft-ietf-sip-digest-aka-01 : “HTTP Digest Authentication Using AKA”. April, 2002.

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 1. 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.

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} respectively. The requirements on the handling of the counters and mechanisms for sequence number management 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 may 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 authentication of the subscriber 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 cf. [3].

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.

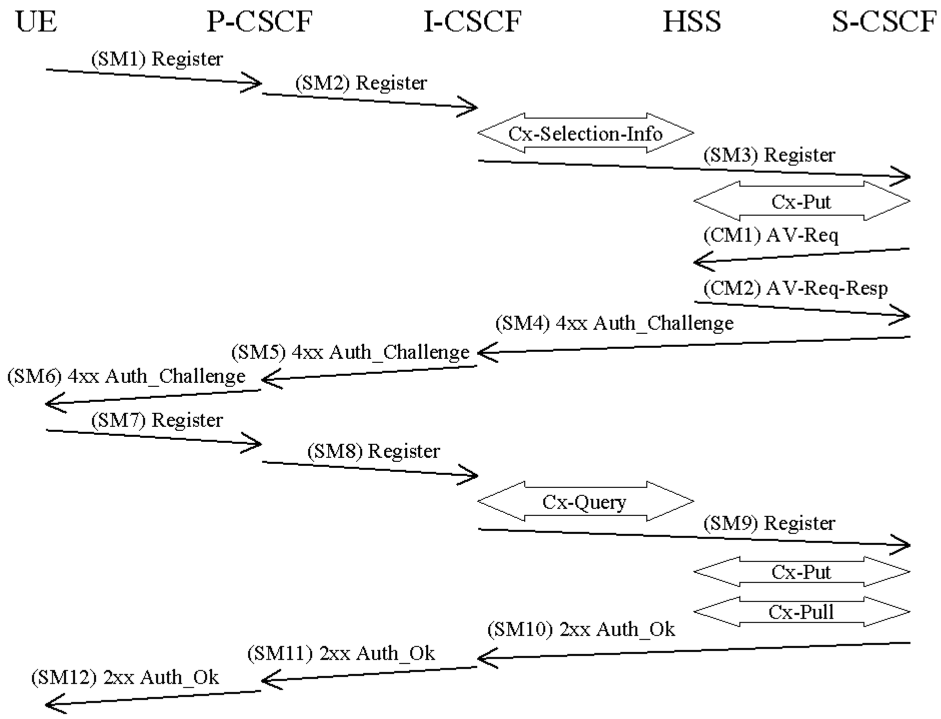


Figure 4: The IMS Authentication and Key Agreement for an unregistered IM subscriber and successful mutual authentication with no synchronization error

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 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,$RAND_1$||$AUTN_1$||$XRES_1$||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 towards the UE including the challenge RAND, the authentication token AUTN in SM4 and the integrity key IK and optionally the cipher key CK. [13] 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.]

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. [13] 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 the response, ~~RES,~~ the S-CSCF retrieves the active XRES for that user and uses this to check the response sent by the UE as described in [13]. ~~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.

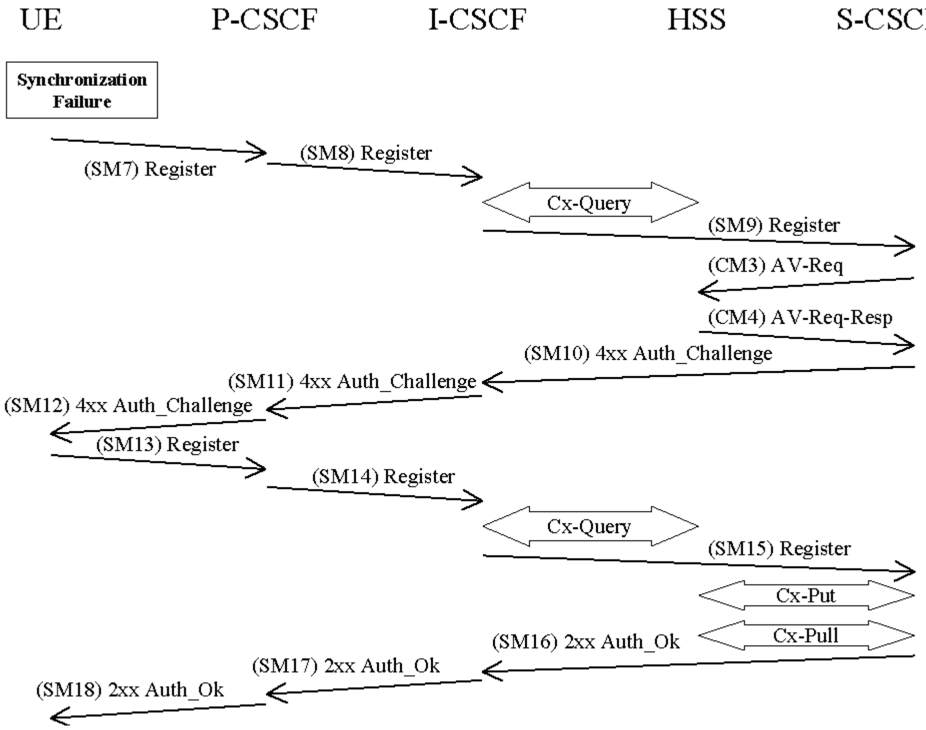
- The IMS subscriber remains registered after unsuccessful re-registration until timer set for next re-registration is expired. Before that the registration flag is kept in the HSS to the value *registered* even if the authentication was unsuccessful. The S-CSCF shall not remove the data about subscriber's 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].

6.1.3 Synchronization failure

[Editor's note: This subsection shall deal with the requirements for the case when the SQNs in the ISIM and the HSS are not in synch.]

In this section the case of an authenticated registration with synchronization failure is described. After re-synchronization, authentication may be successfully completed, but it may also happen that in subsequent attempts other failure conditions (i.e. user authentication failure, network authentication failure) occur. In below only the case of synchronization failure with subsequent successful authentication is shown. The other cases can be derived by combination with the flows for the other failure conditions.



The flow equals the flow in 6.1.1 up to SM6. When the UE receives SM6 it detects that the SQN is out of range and sends a synchronization failure back to the S-CSCF in SM7. [13] describes the fields to populate corresponding parameters of synchronization failure.

SM7:
REGISTER(Failure = *Synchronization Failure,* AUTS, IMPI*)*

Upon receiving the *Synchronization Failure* and the AUTS the S-CSCF sends an Av-Req to the HSS in CM3 including the required number of Avs, n.

CM3:
Cx-AV-Req(IMPI, RAND,AUTS, n)

The HSS checks the AUTS as in section 6.3.5 in [1]. If the check is successful and potentially after updating the SQN the HSS creates and sends new AVs to the S-CSCF in CM4.

CM4:
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 rest of the messages i.e. SM10-SM18 including the Cx messages are exactly the same as SM4-SM12 and the corresponding Cx messages in 6.1.1.