**3GPP TSG-SA3 Meeting #103-e *S3-211855-r1***

**e-meeting, 17 - 28 May 2021** Revision of S3-20xxxx

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.203** | **CR** | **Draft** | **rev** | **-** | **Current version:** | **16.1.0** |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Recommendation of SHA256 in SIP digest | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei; HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eCryptPr | | | | |  | ***Date:*** | | | 2021-05-17 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | B |  | | | | | ***Release:*** | | | Rel-17 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change 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](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) Rel-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | The SIP digest makes use of MD5 which is weak and no longer recommended to use. This contribution propose to add recommended algorithm (i.e., SHA256) in SIP digest. However, to maintain backwards compatibility, the MD5 algorithm is still supported but not recommended. It should be noted that SIP Digest authentication and the requirements shall not apply to access networks defined in 3GPP specifications. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The HSS shall calculated two hashes based on both SHA256 and MD5 and send them to S-CSCF.  S-CSCF shall send Auth\_Challenge with SHA256 and MD5, which are in order of preference, starting with the most preferred algorithm, followed by the less preferred algorithm.  UE shall select and use the first algorithm it supports and send back it to S-CSCF. Then, S-CSCF shall behave based on the received algorithm. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Weak and unsecure algorithm used in IMS. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2；N | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

**\*\*\*\* Start of 1st Changes \*\*\*\***

# 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*.

[x] IETF RFC 7616 (2015) " HTTP Digest Access Authentication ".

**\*\*\*\* Start of 2nd Changes \*\*\*\***

Annex N (normative):  
Enhancements to the access security to enable SIP Digest

# N.1 SIP Digest

SIP Digest authentication and the requirements in this Annex shall not apply to access networks defined in 3GPP specifications. The P-CSCF can enforce this condition by identifying REGISTER requests relating to SIP Digest according to the rules in Annex P.3 of the present document and discarding them when received over an access network defined in 3GPP specifications.

The provisions in Annex N are optional for implementation. The provisions in Annex N are optional for use. However, the use of one of the authentication mechanisms in the present document is mandated.

SIP Digest shall not be used in conjunction with IPsec.

NOTE 1: The use of SIP Digest in conjunction with IPsec, as specified in the main body and in Annex N of this specification, is technically impossible because SIP Digest does not generate session keys for use with IPsec security associations.

An additional scheme for authentication is SIP Digest as specified in RFC 3261 [6]. SIP Digest achieves mutual authentication between the UE and the HN, and is based on HTTP Digest as specified in RFC 7616 [x]. The identity used for authenticating a subscriber is the private identity, IMPI, which has the form of a NAI. The HSS and the UE share a preset secret (e.g., a password) associated with the IMPI. The generation of the authentication challenge shall be done in the same way as specified in RFC 7616 [x] and the present document.

It is the policy of the HN that decides if an authentication shall take place for the registration of an additional IMPU that is not part of the already registered set of IMPUs associated with the same IMPI.

If a UE supports SIP Digest as well as further authentication methods, the UE shall proceed as follows:

- If the access network is of a type defined in 3GPP specifications then the UE shall not select SIP Digest, in accordance with the requirement at the start of this clause.

NOTE 2: The rules listed in Annex T of this specification say how a UE can select between IMS AKA and GIBA.

- If the access network is of a type not defined in 3GPP specifications then

- if both the UE and network support IMS AKA according to the main body or Annex M of this specification, as determined by the use of sip-sec-agree RFC 3329 [21], the authentication method shall be IMS AKA;

- otherwise the authentication method shall be SIP Digest as specified in Annex N of this specification.

# N.2 Authentication

## N.2.1 Authentication Requirements

### N.2.1.1 Authentication Requirements for Registrations

For the purposes of this subclause, the name "authentication" is used synonymously with "entity authentication".

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, i.e. the S‑CSCF, cf. figure N.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.

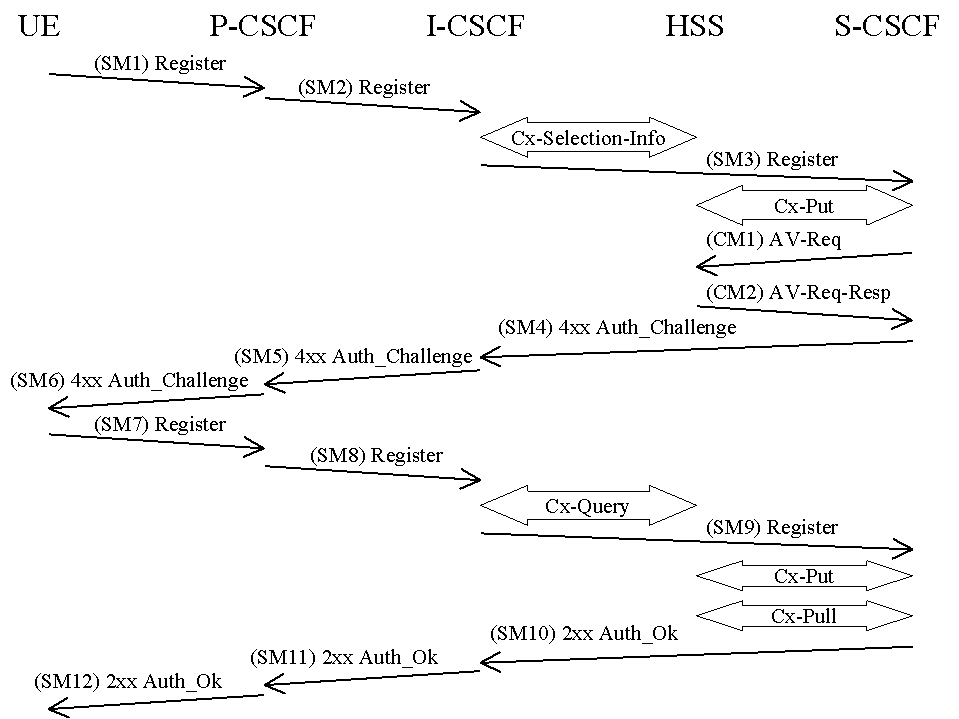


Figure N.1: The IMS Authentication using SIP Digest for an unregistered IM subscriber and successful mutual authentication

The detailed registration procedures are defined in TS 24.229 [8].

The NAT traversal procedures in RFC 5626  [32] and in TS 24.229 [8] clause K.4 shall apply.

NOTE 1: It is recognized that RFC 5626 [32] can be useful for capabilities beyond NAT traversal (e.g. multiple registrations) however this annex does not consider such capabilities at this time.

The UE should include an indication of support for managing client-initiated connections as defined in RFC 5626 [32] in all REGISTER requests. Per RFC 5626 [32], the P-CSCF shall be able to accept registration request with or without an indication of support for managing client-initiated connections. However, the P-CSCF should only accept a register request without support for managing client-initiated connections if it can determine that no NAT is present in the signaling path between the UE and the P-CSCF.

NOTE 2: It is left to stage 3 specifications how a P-CSCF can determine whether the conditions in the preceding paragraph are met. An operator may configure all UEs and P-CSCFs in his network not to use support for managing client-initiated connections (provided there is no roaming). Cf. also the implications of the indication of support for managing client-initiated connections for the P-CSCF procedures after receiving SM11.

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) |

“IMPI\*” in SM1 means that the inclusion of the IMPI is optional in SM1.

NOTE 2a: When a registering UE omits the IMPI from the REGISTER request, the IMPI for the registration is derived from the registering IMPU. Since there can be only one registered instance of an IMPI at any point in time, the registering IMPU in this case cannot be shared across multiple UEs.

In SM2 and SM3 the P‑CSCF and the I‑CSCF respectively forwards the SIP REGISTER towards the S‑CSCF. If SM1 does not contain an IMPI, the P-CSCF shall behave according to Annex P.3 and forward the message as SM2 to the I-CSCF.

NOTE 2b: Annex P.3 formulates conditions depending on the presence of an Authorization header. Note that, if SM1 does not contain an IMPI, then SM1 does not contain an Authorization header.

The I-CSCF queries the HSS to find the address of the S‑CSCF. If SM2 does not contain an IMPI the I-CSCF shall derive the IMPI from the IMPU in the REGISTER request as described in 3GPP TS 24.229 [8]. Then the I-CSCF forwards the message as SM3 to 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 UE 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.

The S-CSCF shall determine the type of authentication based on the rules in Annex P. If SM3 does not contain an IMPI the S-CSCF shall derive the IMPI from the IMPU in the REGISTER request as described in 3GPP TS 24.229 [8]. If the IMS registration request is related to SIP Digest, then the procedures below apply.

Upon receiving the SIP REGISTER the S‑CSCF shall use a SIP Digest Authentication Vector (SD-AV) for authenticating the user. If the S‑CSCF has no valid SD-AV for the specific IMPI, then the S‑CSCF shall send a request for SD-AV(s) to the HSS in CM1 where the number m of SD-AVs wanted is equal to 1.

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

Upon receipt of a request from the S‑CSCF, the HSS sends one SD-AV to the S‑CSCF using CM2. The SD-AV consists of the qop (quality of protection) value, the authentication algorithm including SHA256 and MD5, realm, and two hashes, called H(A1)\_256 and H(A1), of the IMPI, realm, and password. The H(A1)\_SHA256 is calculated based on SHA256 while the H(A1) is calculated based on MD5. Refer to RFC 7616 [x] for additional information on the values in the authentication vector for SIP Digest based authentication.

NOTE: To maintain backwards compatibility with RFC2617 [12], the MD5 algorithm is still supported but NOT RECOMMENDED.

The qop value shall be set to "auth" since SIP Digest, as used in IMS, can only provide authentication, not message integrity.

|  |  |
| --- | --- |
| CM2:  Cx-AV-Req-Resp(IMPI, realm, algorithms, qop, H(A1)\_SHA256 and H(A1) ) |  |

The S-CSCF generates a random nonce, stores H(A1)\_SHA256 and H(A1) and the nonce against the IMPI, and then sends a SIP 401 Auth\_Challenge i.e., an authentication challenge towards the UE including the nonce in SM4. It also includes the realm, qop and algorithm parameters including SHA256 and MD5, which are in order of preference, starting with SHA256, followed by MD5. RFC 7616 [x] specifies how to populate the parameters of a 401 Auth\_Challenge.

|  |
| --- |
| SM4:  401 Auth\_Challenge(IMPI, realm, nonce, qop, algorithms) |

The I-CSCF forwards the SIP 4xx Auth\_Challenge message towards the P-CSCF as SM5.

When the P-CSCF receives SM5 it shall forward the message to the UE.

|  |
| --- |
| SM6:  401 Auth\_Challenge(IMPI, realm, nonce, qop, algorithms) |

Upon receiving the challenge, SM6, the UE generates a cnonce. It then selects the first algorithm it supports and uses the cnonce as well as parameters provided in the SM6 such as nonce and qop to calculate an authentication response according to RFC 7617 [x]. This response and other parameters are put into the Authorization header and sent back towards the network in SM7. The inclusion of the IMPI, the selected algorithm and an Authorization header in SM7 are mandatory.

|  |
| --- |
| SM7:  REGISTER(IMPI, realm, nonce, response, cnonce, qop, nonce-count, algorithm, digest-uri) |

NOTE 3: As specified in RFC 3261 [6], when the P-CSCF receives a SIP request from the UE, the P-CSCF checks the IP address in the "sent-by" parameter of the Via header field provided by the UE. If the "sent-by" parameter contains a domain name, or if it contains an IP address that differs from the packet source IP address, the P-CSCF adds a "received" parameter to that Via header field value. This parameter contains the source IP address from which the packet was received.

The P‑CSCF forwards the authentication response 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 authentication response to the S‑CSCF.

Upon receiving SM9 containing the response, the S-CSCF selects the stored H(A1) based on the received algorithm selected by UE and calculates the expected response using the received algorithm selected by UE and the selected H(A1) and stored nonce together with other parameters contained in SM9 (e.g., cnonce, nonce-count, qop, as specified in RFC 7616 [x]) and uses this to check against the response sent by the UE. 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.

NOTE 4: Depending on its local security policy, the S-CSCF may delete H(A1) immediately after checking the Digest response, but this may then lead to an increased exposure of H(A1) on the Cx-interface as H(A1) would then have to be fetched from the HSS more often.

It shall be possible to implicitly register IMPU(s) (see clause 4.3.3.4 in TS 23.228 [3]). 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 of 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.

If the user has been successfully authenticated, the S‑CSCF sends a SM10 SIP 2xx Auth\_OK message to the I-CSCF indicating that the registration was successful. The 2xx Auth\_OK message contains the Authentication-Info header with a response digest as specified in RFC 7616 [x]. The response digest allows the UE to authenticate the HN.

In SM11 the I‑CSCF forwards the SIP 2xx Auth\_OK towards the P-CSCF.

The P-CSCF associates the UE's packet source IP address along with the "sent-by" parameter of the Via header, cf. RFC 3261 [6], of the REGISTER message with the IMPI and all the successfully registered IMPUs related to that IMPI. If managing of client-initiated connections as defined in RFC 5626 [32] is used then the P-CSCF shall also include the UE's packet source port of the REGISTER message as part of the association. The P-CSCF stores the associated parameters in an IP address check table. If managing of client-initiated connections is not used then the P-CSCF shall overwrite any existing entry in the IP address check table which has the same IP address, but a different IMPI. If managing of client-initiated connections is used then the P-CSCF shall overwrite any existing entry in the IP address check table which has the same (IP address, port) pair, but a different IMPI.

The P-CSCF forwards the SIP 2xx AUTH\_OK towards the UE.

NOTE 5: If a P-CSCF associated the port with the IMPI even when managing of client-initiated connections was not used then the UE would be unnecessarily restricted in opening new connections during a registration. The restriction is unavoidable in the presence of NAT.

Upon receiving SM12, the UE shall calculate the expected response from the HN as described in RFC 7616 [x]. To authenticate the HN, the UE shall compare its expected response to the response provided by the HN. If the comparison fails the UE shall abort the communication.

### N.2.1.2 Authentication Requirements for Non-registration Messages

For the purposes of this subsection, the name "authentication" is used synonymously with "message origin authentication".

The IP address check table (cf. subclause N.2.1.1) shall be used by the P-CSCF to identify the initiator of subsequent requests as follows: one of the public user identities associated with the packet IP address (and port if applicable) is selected and asserted to the S-CSCF according to the rules in TS 24.229 [8], subclause 5.2.6.3.

In addition, subsequent requests (e.g. INVITE) may be authenticated with SIP Digest, as described in the following:

NOTE 1: The assertion of IMPUs based on checks of IP address (and ports if applicable) provides a reasonable level of security only in environments where the risk from source IP address and port spoofing or from IP address re-assignment unnoticed by the SIP application is sufficiently low. If the environment does not fulfill this condition then it is recommended to use SIP Digest in conjunction with either TLS, as specified in Annex O of this specification, or with the SIP Digest proxy authentication mechanism as specified in this subclause. It is not part of this specification to determine which environments fulfill the conditions in this NOTE. This is left to specifications, possibly maintained by standardization bodies other than 3GPP, describing these environments. More details on the usage of the authentication mechanisms for non-registration messages are provided in Annex Q (informative).

When the S-CSCF receives a SIP request with a method other than the REGISTER method from the UE, the S-CSCF may perform authentication on the SIP request according to the operator's policy and according to the following procedures.

* If the request does not contain a Proxy-Authorization header or the Proxy-Authorization header does not contain a digest response the S-CSCF shall send a 407 (Proxy Authentication Required) response to challenge the UE. The 407 response shall contain digest challenge parameters in a Proxy-Authenticate header as defined by RFC 7616 [x]. The challenge parameters, with the exception of the nonce, shall be taken from the same SD-AV as used for the last successful registration or re-registration message of the UE. The nonce shall be generated freshly by the S-CSCF. Upon receiving the challenge the UE shall extract digest challenge parameters from the Proxy-Authenticate header field and calculate a digest response as indicated in RFC 7616[x]. The UE should store the received digest challenge. The UE then sends a new request to the network containing a Proxy-Authorization header in which the header fields are populated as described in RFC 7616 [x] using the calculated digest response. Upon receiving the new request which contains a digest response, the S-CSCF verifies the user’s identity by validating the digest response information (e.g. the nonce-count) contained in the Proxy-Authorization header field against the expected information based on the same SD-AV as used for generating the challenge;

NOTE 1a: Authorization (used for registration messages, cf. sub-clause N.2.1.1) and Proxy-Authorization (used for non-registration messages, this sub-clause) are handled by logically separated protocol engines and thus each mechanism has its own nonce, cnonce and nonce-count parameters.

NOTE 1b: The usage of the same SD-AV for authentication of non-registration messages and of registration messages requires the storage of the SD-AV in S-CSCF during the authentication of registration messages (cf. subclause N.2.1.1), as retrieval of AVs from HSS is only specified for handling of registration messages. In case of dynamic password change (cf. clause N.2.5), the SD-AV (or SD-AVs) used for generating the challenge(s) are specified in clause N.2.5.

* If the check is successful then the request has been authenticated, and the S-CSCF sends a 2xx AUTH\_OK towards the UE;
* If the check fails, based on local policy the S-CSCF may choose to re-challenge the user by using the same procedure described in this subclause, or reject the request by sending a 403 response.

When the UE is to send a non-REGISTER SIP request it should first check whether it has a digest challenge stored which was previously received in a Proxy-Authenticate header. If such a digest challenge is available in the UE the UE should use it together with the nonce-count mechanism as specified in RFC 7616 [x] to calculate a digest response, include the digest response in a Proxy-Authorization header and send this header together with the non-REGISTER SIP request.

NOTE 2: According to RFC 7616 [x], the S-CSCF may send a 407 (Proxy Authentication Required) as a response to any non-REGISTER request, indicating that the nonce is stale and the digest response shall be recomputed using the fresh challenge sent in the same 407 message.

When the S-CSCF has successfully used the SIP Digest proxy authentication mechanism it shall check if the public user identity asserted by the P-CSCF belongs to the implicit registration set (i.e. the public user identities associated with the authenticated user). If the check is not successful the S-CSCF shall reject the non-registration request.

NOTE 3: Such a rejection may occur when one of the conditions mentioned in NOTE 1 is not fulfilled.

NOTE 4: When TLS according to Annex O is used, or when IPsec according to the main body or Annex M is used, then the failure conditions mentioned in NOTE 1 and Annex Q.3 cannot occur, and the public user identity asserted by the P-CSCF is reliable.

**\*\*\*\* End of Changes \*\*\*\***