3GPP TSG SA WG3 Security — S3#14 **S3-000456**

2-4 August, 2000

Oslo, Norway

Source: **Nokia**

Title: **UMTS AKA in SIP**

Document for: **Discussion/ Decision**

Agenda Item:

BACKGROUND

SIP has been selected as the protocol over the UNI (Mt reference point) for UMTS R00 IM CN subsystem. A natural option is to standardize the current UMTS AKA as the authentication mechanism for the UMTS R00 IM CN domain also; but the SIP RFC (RFC 2543) does not define the appropriate messages to perform a UMTS AKA procedure.

Therefore a way to carry the necessary UMTS AKA parameters need to be defined.

SOLUTIONS

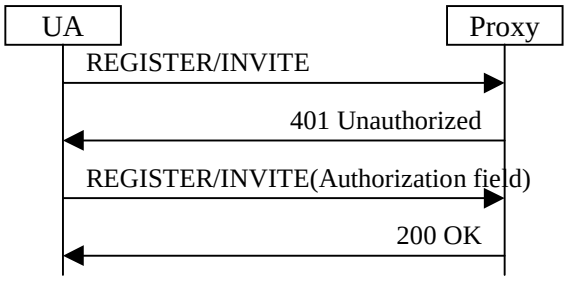
Actually, there are two ways to perform a UMTS AKA through SIP Protocol :

- Since three different authentication mechanisms (HTTP basic mode, HTTP digest mode, PGP) have already been defined for SIP, a new authentication mode, a UMTS AKA mode, with the necessary fields, could be defined.
- Or since it may be difficult to have a new SIP message standardized in IETF, the existing modes can be reused and adapted in order to perform a UMTS AKA procedure.

Procedure

According to the security policies, when an UMTS AKA needs to be performed (e.g. at a call set up, or at registration), the User Agent - UA sends a REGISTER or INVITE request to the proxy; the SIP proxy then asks for an authentication with a 401 Unauthorised response. This 401 response includes the WWW-Authenticate response header field which contains the UMTS AKA authentication vectors i.e. the random challenge (RAND) and the authentication token (AUTN).

After a 401 response, the UA sends a new REGISTER or INVITE request which should contain the appropriate authentication information in the Authorisation header field: the authentication response (RES), the synchronisation failure parameter (AUTS) or an error code.



For a call set-up, the 407 Proxy Authentication Required Response can also be used to carry the UMTS AKA Parameters.

Solution 1 : Definition of a new authentication mode

This solution introduces a new authentication mode. It tries to keep the headers as short as possible since the SIP messages are going through the air interface.

WWW-Authenticate response header

The WWW-Authenticate response header in the case of UMTS AKA mechanism must be able to carry the random challenge (RAND) and the authentication token (AUTN). The following simple format can be used:

WWW-Authenticate = " WWW-Authenticate" ":" "UMTS" RAND AUTN
RAND = "RAND" "=" RAND-value
AUTN = "AUTN" "=" AUTN-value

The hexadecimal format is proposed for the AUTN and RAND value.

Authorization header

The Authorization header in the case of UMTS AKA mechanism must be able to carry the user authentication response (RES) value or the authentication synchronization parameter (AUTS) value. The following simple format can enough for this purpose:

Authorization = "Authorization" ":" "UMTS" RES | AUTS | AUTH-REJECT
RES = "RES" "=" RES-value
AUTS = "AUTS" "=" AUTS-value
AUTH-REJECT = " AUTH-REJECT" "=" error-code

The hexadecimal format is proposed for the RES and AUTS value. The possible value of the error-code is FFS.

Pros :

Specific to UMTS AKA

necessary fields can be present (format, length)

Cons :

Difficult to have a new mode defined in IETF

Solution 2 : UMTS AKA via existing SIP messages

Adapted HTTP's basic and digest authentication mechanisms are supported in SIP implementations; the digest can be used to carry the UMTS AKA parameters:

The "nonce" field will carry the concatenated RAND and AUTN value in hexadecimal format. Since the content of this nonce is implementation dependant, the length should be large enough to carry the

RAND and AUTN. But if it is not the case, the "opaque" field can be used to carry part of the parameters.

The "response" field will be used for the RES. In the case of synchronization error the AUTS will be included in the response "field". The first character of the "response" can indicate that the response includes the RES, the AUTS or an error code; the RES and the AUTS can be included in hexadecimal format.

In authentication with digest mode, an "algorithm" field can specify which algorithm to use to compute the digest (MD5 is used by default), actually this field can be used to inform the receiver that this is a UMTS AKA procedure, and in that way, the MS will understand that the nonce actually carry the RAND and the AUTN.

At present a PGP Authentication scheme had been defined for SIP. As an alternative this mode can also be re-used to carry the UMTS AKA parameters :

The "nonce" will carry the RAND and AUTN values

The "pgp=algorithm" will inform the receiver that it is a UMTS AKA procedure

And the result will be included in the "pgp-signature". Since this field can be more than 200 bits long, some first bits can be used to specify the type of result : RES, AUTS or error code.

Pros :

No modification to the existing SIP protocol except a new algorithm name.

Cons:

Slight "misuse" of some fields.