3GPP TSG SA WG3 #21bis NDS/MAP ad hoc **Tdoc S3z020045**

Tdoc S3z020040

Antwerp, Belgium
31st January – 1st February 2002

Source: **SA WG3**

To: **CN1, CN4**

Title: **~~Draft~~ LS on "Transport of IMS-AKA Material"**

Contact: **David Castellanos-Zamora**

Email: **david.castellanos-zamora@era.ericsson.se**

As defined in TS 33.203, IMS-AKA is a corner~~-~~stone for the IMS security architecture. This procedure, based on concepts and techniques already developed for UMTS, provides means for mutual authentication and session key establishment between the end user and the IMS CN SS. The execution of IMS-AKA implies that IMS-AKA material (i.e. RAND, AUTN and XRES for authentication and CK and IK for key agreement) is transported and used all over the IMS CN SS infrastructure and UE.

It has been SA3´s working assumption that IMS-AKA material shall be encapsulated into the framework of the Extensible Authentication Protocol (EAP). That requires new internet drafts that allows the use of AKA as a new authentication scheme into the EAP framework [1] and the use of EAP formats into the SIP protocol [2]. As indicated by SA3 CN1 and CN4 have been also working under this assumption.

Reasonably good discussions related to these I-Ds took place during the last IETF meeting, and it was expected to continue forward as planned. However, there have been since then several discussions between the IETF ADs, Ileana Leuca, Stephen Hayes (CN chair), various IETF WG chairs, editors and experts regarding the SIP security area. In particular, the IETF co-ordination meeting that took place January 25, 2002 brought up IETF opinions ~~clearly~~ and as a conclusion they recommended 3GPP to change some of the~~our plans~~working assumptions~~ on some parts~~. The results from this meeting have been already reported by CN chairman [3] and can be summarized as follows:

1. Requirements from draft-garcia-sipping-3gpp-reqs-03.txt need to be broken away and submitted as small independent drafts. In particular the following shall be submitted as independent requirement I-Ds:
    - AKA authentication in SIP
    - Secure algorithm agreement
    - Key transport
2. IMS-AKA in SIP should be provided through an extension of Digest, not through EAP.
3. Key transport can not be provided as an additional feature of digest or EAP, as earlier suggested by CN1 [4].

On a positive note, the IETF ADs and WG chairs are now behind the new approach and it seemed to be the general feeling that this plan can be completed in time. Such support is necessary to make progress in IETF.

This information from IETF was raised and discussed during SA3's ad-hoc meeting on IMS security (Jan 31st – Feb 1st, 2002) and SA3 would like to inform CN1 and CN4 groups of the agreements reached that affects the work in progress~~ at these groups~~:

- SA3 ad-hoc agreed to follow the IETF recommendation to encapsulate IMS-AKA material into http-digest rather than within EAP as previously assumed by SA3. TS 33.203 will be updated accordingly and references to EAP will be removed.

  CN1 specifications shall also be based on this new assumption for handling of IMS-AKA material within the SIP protocol.

SA3 ad-hoc also concluded that it would be wise ~~to~~ also to modify the working assumption in CN4 specifications for the handling of IMS-AKA material over the DIAMETER protocol at Cx interface (IMS-AKA authentication challenges/responses and synchronisation failures would be encapsulated within the corresponding DIAMETER http-digest AVPs while session keys would be transported in DIAMETER NAS-Session-Key AVPs, for example).This would be also required in terms of consistency of our architecture and avoid potential delays the definition of AKA within the EAP framework may suffer at IETF.

- SA3 ad-hoc agreed to follow the IETF recommendation to provide Key transport as a separate function of authentication. Despite the IETF goal~~wish~~ to have an application layer mechanism be used to protect key transport, 3GPP IMS security architecture will still ~~relay in~~rely on NDS/IP measures to ensure the secure transport of information (including session keys) over the IMS CN SS infrastructure. Therefore, the hop-by-hop approach to secure IMS session key transport still applies.

  CN1 and CN4 specifications shall provide means for the IMS-AKA session keys to be transported over the IMS CN SS infrastructure in a way that fulfills SA3´s new working assumption.

  In particular, CN1 is asked to evaluate the suitability to encapsulate IMS session keys within the 3GPP XML SIP message body, which is being specified by CN1.

Actions to CN1 and CN4:

- CN1 and CN4 are asked to adopt the new recommendations from IETF and latest agreements at SA3 for the handling of IMS-AKA material.
- CN1 and CN4 are also asked to find and develop suitable solutions in their specifications that suits the new working assumptions.
- ~~Finally,~~ CN1 and CN4 are kindly asked to raise any concern that the adoption of these new working assumptions may cause to the specification work in progress.

References:

[1] IETF Draft (2001) “draft-arkko-pppext-eap-aka-01.txt“

[2] IETF Draft (2001) “draft-torvinen-http-eap-01.txt“

[3] “Results from the recent IETF coordination meeting”.
Stephen Hayes’ e-mail to SA3 (forwarded).

~~-~~[4] LS on transportation of SIP session keys from S-CSCF to P-CSCF N1-020154)

Date of Next SA3 Meetings:

SA3_22	25th – 28th February 2002	Bristol, UK
SA3_23	14th – 16th May 2002	Victoria Island, Canada