3GPP TSG SA WG3 #22bis aSIP ad hoc **Tdoc S3z020051**
Fort Lauderdale, Florida USA
8th April 2002

Source: Ericsson and Nokia

Title: IETF-53: AKA in SIP

Agenda item: TBD

Document for: Information

---

1 Scope and objectives

This document gives a summary on the status of Digest AKA Internet-Draft discussed in SIP and SIPPING Working Groups in IETF-53, Minneapolis, March 17th –22nd, 2002.

2 AKA in SIP

The work on AKA relates to the authentication between the UE and the S-CSCF. This authentication takes place through SIP protocol extensions. It is important to note that the UE – S-CSCF protection is separate from the UE – P-CSCF protection. Mechanisms proposed for these two tasks are also different.

The Internet Draft [Digest-AKA] describes the use of AKA as an algorithm under the HTTP Digest framework. This approach had earlier this year been suggested to us by the IETF Area Directors and security experts as an alternative to EAP which could not meet 3GPP time plan. The draft specifies the use of AKA in the SIP headers carrying HTTP authentication, and the use of AKA RES to perform the authentication in the normal Digest manner.

Requirements related to AKA were submitted to SIPPING WG as a separate draft [SIPPING-AKA].

The solution draft [Digest-AKA] and the open issues were presented ~~in Minneapolis~~ at IETF#53 in SIP Working Group. The draft was approved as a working group item. Private discussions with the ADs and WG chairs indicate that the draft can progress fast.

There has recently been discussion in the SA3 mailing list about whether the Digest approach (which uses also MD5 and not just AKA) or a more direct use of AKA would be appropriate. In view of this, we asked the IETF about their view on this. The view presented in the meeting was clearly that the Digest approach ~~has to~~should be followed. This can perhaps be best explained by noting that the IETF designs protocols for general use, and does not wish to have many different special cases for particular user groups, hence new extensions should fit under existing frameworks such as Digest.

Furthermore, the SIP WG has earlier had a strong consensus that a cleartext password mechanism HTTP Basic is no longer satisfactory, even when used with one-time passwords. Due to this, Basic is no longer allowed in SIP. Direct use of AKA RES would essentially bring back Basic functionality, which would likely be viewed in a negative manner. A private discussion with SIP WG chair and CN1 delegate Dean Willis confirmed the IETF view in the Digest matter and the likelihood of negative responses for Basic-like functionality. Furthermore, both Dean Willis and SIP experts at the contributing companies have confirmed that the use of P-headers for security related tasks is not be possible. As even P-headers need to be entered to IETF review as Internet Drafts, this prevents the use of P-headers to carry plain AKA authentication. Former experience has also shown that any security related Internet Drafts are difficult and time-consuming to get accepted in SIP/SIPPING Working Groups.

Note that as in the regular Digest framework, integrity protection is optional and controlled by the qop parameter. (A specific formula is still employed to calculate the authentication response even if no integrity protection is employed.)

The security properties of Digest AKA approach are discussed in a separate contribution. Note, however, that the primary observation is that any attacks that can be performed using exhaustive search of to find out RES are trivially performed if the RES is in the clear. Furthermore, even if 3GPP does not currently need integrity protection for the home authentication, other users could still benefit from the ability to not just guarantee authentication but also verify integrity of the request accompanying the authentication headers.

The current Internet Draft does not necessarily require approval from the SIP/SIPPING Working Groups because it does not change HTTP Digest framework or introduces any SIP extensions. Alternative standardisation paths would require formal approval from these groups. As already mentioned above, any security related Internet Drafts are difficult and time-consuming to get accepted in SIP/SIPPING Working Groups. This includes the use of P-headers and XML bodies for security.

Contributing companies do agree that the transportation of AKA parameters in clear would have been the most straightforward solution from 3GPP perspective. However, companies do not believe that such solution would meet the Release 5 timeframe. In order to fulfil the time schedules and complete the IETF process for getting an RFC number, the existing solution draft needs to be updated and IETF Last Call started within few weeks. It is recommended that 3GPP adopt the approach currently introduced in draft-niemi-sipping-digest-aka-00.txt as a working assumption.

3 References

[Digest-AKA] Niemi et al, “HTTP Digest Authentication Using AKA”, IETF, Work in progress, February 2002, draft-niemi-sipping-digest-aka-00.txt.

[SIPPING-AKA] Arkko et al, "3GPP Requirements for SIP Authentication", IETF, Work in progress, February 2002, draft-uusitalo-sipping-authentication-00.txt.