3GPP TSG SA WG3 Security **S3-040989**

November 23 – 26, 2004

Shenzhen, P.R.China

Agenda Item: 5.2 (Reports and Liaisons from other groups; IETF)

Source: Ericsson

Title: IETF status report on HTTP Digest AKAv2

Document for: Information

1. IETF status

Ericsson has been working on a new algorithm version for HTTP Digest AKA in IETF. This work was initiated because the current algorithm version [RFC 3310] is vulnerable to certain man-in-the-middle/interleaving attacks, especially if used with TLS. Furthermore, the passwords generated by [RFC 3310] are limited to one time use only. The new algorithm version intends to fix both of these problems, i.e. AKAv2 can be used with TLS, and the passwords can be re-used for subsequent authentication.

Previous version of the draft (version –01) has been queuing for Expert / IESG review for long time, and it was finally taken to review last summer. A new version of the draft [Digest-aka-v2-02] has been published in IETF I-D directory based on the IESG comments. Comments were mostly editorial, and are publicly available in [I-D-status].

It is expected that the draft will receive RFC status in the near future. SA3 should see AKAv2 as a new building block that can be used in future standards.

2. References

[Digest-aka-v2-02] Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA) Version-2, IETF, draft-torvinen-http-digest-aka-v2-02.txt.

[I-D-status] IETF Draft Tracker, https://datatracker.ietf.org/public/pidtracker.cgi.

[RFC 3310] Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA), IETF, RFC 3310.