3GPP TSG SA WG3 Security — S3#34 **S3-040652**
July 6 - 9, 2004
Acapulco, Mexico

Title: LS on Authentication Proxy
Response to: Tdoc N1-041313 = S3-040472
Release: Rel 6
Work Item: SSC-GBA, Presence

Source: SA3
To: CN1
Cc: -

Contact Person:
Name: **Günther Horn, Siemens**
Tel. Number: **+49 89 63641494**
E-mail Address: guenther.horn@siemens.com

Attachments: none

---

1. Question by CN1: WG CN1 seeks advice from SA3 on where in the IMS architecture a separate authentication proxy exists (home network or visited network, inside trusted domain or outside the trusted domain).

Answer by SA3: an authentication proxy (AP) is a NAF in the sense of TS 33.220. NAFs can exist in the home network or visited network. But, so far, a need for NAFs in the visited network has only been discovered for MBMS, where a BM-SC can be a NAF. So, the Zn reference point (BSF - NAF) can be inter-domain or intra-domain. But, for IMS, so far no requirement has been identified for the BSF and the NAF to reside in different security domains,

Regarding the AP-AS reference point, TS 33.222 und 33.141 also permit both cases, authentication proxy (AP) and application server (AS) may reside in the same or in different domains, cf. section 6.4.2 of 33.222:
"The HTTP protocol is run over the AP-AS reference point.
Confidentiality and integrity protection can be provided for the reference point between the AP and the AS using NDS/IP mechanisms as specified in TS 33.210 [12]. For traffic between different security domains, the Za reference point shall be operated. For traffic inside a security domain, it is up to the operator to decide whether to deploy the Zb reference point. As AP terminates the TLS tunnel from UE, also a TLS tunnel is possible."
But, so far, no requirement has been identified for the AP and the AS to reside in different security domains, or in different networks. If this creates problems, then, at least for Release 6, it could be required for the AP and the AS to reside in the same security domain or network.

2. Question by CN1: Is such a separate authentication proxy discovered by the UE?

Answer by SA3: No, the UE addresses the application server, and DNS returns the IP address of the AP, irrespective of whether the AP is an independent entity or not. The UE is not aware of the existence of an AP. Cf. section 6.2 of TS 33.222: "The use of an authentication proxy should be such that there is no need to manage the authentication proxy configuration in the UE.
NOTE 2: This requirement implies that the authentication proxy should be a reverse proxy in the following sense: A reverse proxy is a web server system that is capable of serving web pages sourced from other web servers - in addition to web pages on disk or generated dynamically by CGI - making these pages look like they originated at the reverse proxy."

3. Date of Next TSG SA WG 3 Meetings:

TSG-SA3 Meeting #35	5-8 October 2004	Malta
TSG-SA3 Meeting #36	23-26 November 2004	Shenzhen, Chia