3GPP TSG SA WG3 Security#31 **S3-030745**
18-21 November, 2003
Munich, Germany

Agenda Item: **6.9 (GAA) and 6.18 (Presence)**

Source: **Siemens**

Title: **Technical solutions for access to application servers via Authentication Proxy and HTTPS - Pseudo-CRs to TSs on GAA/HTTPS and Presence Security**

Document for: **Discussion and decision**

Abstract

As a consequence of the discussion on S3-030553 "Difficulties in using one TLS tunnel to access different servers behind an authentication proxy", TS ab. cde (GAA/HTTPS) and TS 33.141 (presence security) should be amended by an annex discussing technical solutions for Authentication Proxy – NAF elements accessed via HTTPS, so as to help avoid misconfigurations.

1. Pseudo-CRs to TSs on GAA/HTTPS and Presence Security

Based on the discussion on S3-030553 "Difficulties in using one TLS tunnel to access different servers behind an authentication proxy" it is proposed to include the following text as informative annexes to TS ab.cde v011 (GAA/HTTPS, S3-030665) and to TS 33.141 v020 (Presence Security):

" *Annex <y> (informative): Technical solutions for access to application servers via Authentication Proxy and HTTPS*

This annex gives some guidance on the technical solution for authentication proxies so as to help avoid misconfigurations. An authentication proxy acts as reverse proxy which serves web pages (and other content) sourced from other web servers (AS) making these pages look like they originated at the proxy.

To access different hosts with different DNS names on one server (in this case the proxy) the concept of virtual hosts was created.

One solution when running HTTPS is to associate each host name with a different IP address (IP based virtual hosts). This can be achieved by the machine having several physical network connections, or by use of virtual interfaces which are supported by most modern operating systems (frequently called "ip aliases"). This solution uses up one IP address per AS and it does not allow the notion of "one TLS tunnel from UE to AP-NAF" for all applications behind a NAF together.

If it is desired to use one IP address only or if "one TLS tunnel for all" is required, only the concept of name-based virtual hosts is applicable. Together with HTTPS, however, this creates problems, necessitating workarounds which may deviate from standard behaviour of proxies and/or browsers. Workarounds, which affect the UE and are not generally supported by browsers, may cause interoperability problems. Other workarounds may impose restrictions on the attached application servers."

It is proposed to include this informative annex in both draft TSs, as it is currently unclear whether both TSs will be completed within the Release 6 timeframe. If both TSs are completed in time, SA3 may decide later that all material on authentication proxies is to be contained in TS ab.cde (GAA/HTTPS), and that TS 33.141 (Presence Security) only is to make reference to TS ab.cde (GAA/HTTPS).