Technical Specification Group Services and System Aspects **TSGS#27(05) 0264**
Meeting #28, Quebec, Canada, 6-8 June 2005

Source: **SA3**

Title: **CR to 33.222 to Remove editor's note in Generic Authentication Architecture (Rel-6)**

Document for: **Approval**

Agenda Item: **7.3.3**

Meeting	SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers. Current	Vers New	SA1 Doc
SP-28	SP-050264	33.222	019	-	Rel-6	F	Removal of editor's note	6.3.0	6.4.0	S3-050301

3GPP TSG-SA WG3 Meeting S3#38
Geneva, Switzerland, 26-29 April, 2005

Tdoc ⌘S3-050301

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.222**	**CR**	**019**	⌘**rev**	**-**	⌘	Current version:	**6.3.0**	⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects:	UICC apps⌘ □	ME □	Radio Access Network □	Core Network ☒

Title:	⌘	Removal of editor's note		
Source:	⌘	SA3 (Nokia, Ericsson)		
Work item code:	⌘	SEC1-SC	***Date:*** ⌘	27/4/2005
Category:	⌘	**F**	***Release:*** ⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	Removal of left-over editors note. The current specification already covers the case and the editor's note would mark the task as not handled. The name of the AS (NAF_Id) comes in ServerName field of the TLS client extension, the B-TID comes in the PSK identity field in the ClientKeyExchange message. The AP obtains the Ks_NAF from the BSF. The editor's note could lead to interoperability problems.
Summary of change:	⌘	Deleting of editor's note.
Consequences if not approved:	⌘	Misleading information left in the TS.

Clauses affected:	⌘	Annex A				
		Y	**N**			
Other specs Affected:	⌘		**N**	Other core specifications	⌘	
			N	Test specifications		
			N	O&M Specifications		
Other comments:	⌘					

Annex A (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.

To access virtual hosts where different servers with different DNS names are co-located on AP, either of the solutions could be used to identify the host during the handshaking phase:

- Extension of TLS is specified in RFC 3546 [8]. This RFC supports the UE to indicate a virtual host that it intends to connect in the very initial TLS handshaking message (see clause 5.3.1);
- The other alternative is to issue a multiple-identities certificate for the AP. The certificate will contain identities of AP as well as each server that rely on AP's proxy function. The verification of this type of certificate is specified in RFC 2818 [9].

Either approach may be chosen by the operator who operates the authentication proxy.

~~Editor's note: The shared-key TLS based authentication does not require server's certificate, but the possession of the key for authentication. The procedure is ffs.~~