3GPP TSG SA WG3 Security — S3#32 **S3-040069**
09 - 13 February 2004, Edinburgh, Scotland, UK

CR-Form-v7

CHANGE REQUEST

⌘ **TS 33.222** **CR** **CRNum** ⌘ **rev** ⌘ Current version: 0.2.0 ⌘

*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:	⌘	The virtual hosts identity
Source:	⌘	Nokia
Work item code:	⌘	GBA and Support for subcriber certificates
Date:	⌘	29/1/2004
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:

2	*(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)*

Reason for change:	⌘	There are several standardised means to identify the intended virtual host to that the UE intends to connect.
Summary of change:	⌘	The two methods are described in section 5.2; The references are added; The Annex A is removed.
Consequences if not approved:	⌘	The improper text would mislead the audience.

Clauses affected:	⌘	2, 5.2, Annex A

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	

--- START OF CHANGE ---

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[<seq>] <doctype> <#>[([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: “<Title>”.

[1] 3GPP TR 41.001: “GSM Release specifications”.

[2] 3GPP TR 21 912 (V3.1.0): “Example 2, using fixed text”.

[3] IETF RFC 3546 (2003) “Transport Layer Security (TLS) Extensions”.

[4] IETF RFC 2818 (2000) “HTTP Over TLS ”.

--- NEXT CHANGE ---

5.2 Authentication proxy architecture

<include figure y here>

The use of an authentication proxy (AP) is fully compatible with the architecture specified in [TS33.220] and in section 4 of this specification. When an AP is used in this architecture, the AP takes the role of a NAF. When an https request is destined towards an application server behind an authentication proxy (AP), the AP terminates the TLS tunnel and performs UE authentication. The AP proxies the http request to the application server.

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 specifed in RFC 3546 [3]. This RFC supports the UE to indicate a virtual host that it intends to connect in the very initial TLS handshaking message;

- 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 [4].

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

~~Annex A contains further guidance on technical solutions for authentication proxies.~~

--- NEXT CHANGE ---

~~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.~~

~~Editors' note: The text in this informative annex may need to be revisited if changes in the main body of the text are made.~~

--- END OF CHANGE ---