3GPP TSG-SA WG3 Meeting #36
Shenzhen, China, November 23-26, 2004

Tdoc ⌘S3-041026

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.222**	**CR 014**	⌘ **rev -** ⌘	Current version:	**6.1.0** ⌘

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:	⌘ Visited AS using subscriber certificates		
Source:	⌘ Nokia		
Work item code:	⌘ SEC1-SC	***Date:***	⌘ 16/11/2004
Category:	⌘ **C**	***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:	⌘ Clarification is added how a visited AS can use subscriber certificates to authenticate the subscriber.
Summary of change:	⌘ When the AS resides in the visited network, the visited network can decide to trust the home operator's CA certificate as trusted root certificate. Therfore, the editor's note is not needed.
Consequences if not approved:	⌘

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

==== ***BEGIN CHANGE*** ====

Annex B (informative): Guidance on Certificate-based mutual authentication between UE and application server

This section explains how subscriber certificates (see TS 33.221 [16]) are used in certificate-based mutual authentication between a UE and an application server. The certificate-based mutual authentication between a UE and an application server shall be based TLS as specified in IETF RFC 2246 [6] and IETF RFC 3546 [8].

When a UE and an application server (AS) want to mutually authenticate each other based on certificates, the UE has previously enrolled a subscriber certificate as specified in TS 33.221 [16]. After UE is in the possession of the subscriber certificate it may establish a TLS tunnel with the AS as specified in RFC 2246 [6] and RFC 3546 [8].

The AS may indicate to the UE, that it supports client certificate-based authentication by sending a CertificateRequest message as specified in section 7.4.4 of IETF RFC 2246 [6] during the TLS handshake. This message includes a list of certificate types and a list of acceptable certificate authorities. The AS may indicate to the UE that it supports subscriber certificate-based authentication if the list of acceptable certificate authorities includes the certification authority of the subscriber certificate (i.e. the operator's CA certificate).

The UE may continue with the subscriber certificate-based authentication if the list of acceptable certificate authorities includes the certification authority of the subscriber certificate. This is done by sending the subscriber certificate as the Certificate message as specified in sections 7.4.6 and 7.4.2 of IETF RFC 2246 [6] during the TLS handshake. If the list of acceptable certificate authorities does not include the certification authority of the subscriber certificate, then UE shall send a Certificate message that does not contain any certificates.

NOTE 1: Due to the short lifetime of the subscriber certificate, the usage of the subscriber certificate does not require on-line interaction between the AS and the PKI portal that issued the certificate.

If the AS receives a Certificate message that does not contain any certificates, it can continue the TLS handshake in two ways:

- if subscriber certificate-based authentication is mandatory according to the AS's security policy, it shall response with a fatal handshake failure alert as specified in IETF RFC 2246 [6], or
- if subscriber certificate-based authentication is optional according to AS's security policy, AS shall continue with TLS handshake as specified in IETF RFC 2246 [6].

In the latter case, if the AS has NAF functionality, the NAF may authenticate the UE as specified in clause 5.3 of the present specification, where after establishing the server-authenticated TLS tunnel, the procedure continues from step 4.

NOTE 2: In order to successfully establish a TLS tunnel between the UE and the AS using certificates for mutual authentication, the UE must have the root certificate of the AS's certificate in the UE's certificate store, and the AS must have the root certificate of the UE's subscriber certificate (i.e. operator's CA certificate) in the AS's certificate store. The root certificate is the root of the certification path, and should be marked trusted in the UE and the AS.

~~Editor's note: The support of accessing an AS in the visited network is FFS in future Release.~~

NOTE 3: In order to enable access to an AS in a visited network with subscriber certificates requires that the AS has the CA certificate of subscriber's home operator and it is marked trusted in the visited AS. The procedure to do this is outside the scope of this specification.

==== ***END CHANGE*** ====