3GPP TSG-SA WG3 Meeting S3#34
Acapulco, Mexico, July 6-9, 2004

Tdoc ⌘S3-040~~530~~640

CR-Form-v7

CHANGE REQUEST

⌘ **33.919** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **1.2.1** ⌘

*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 **X**

Title:	⌘	Application guidelines to use GAA
Source:	⌘	Alcatel , BT , Nokia
Work item code:	⌘	GAA
Date:	⌘	29/06/2004
Category:	⌘	**B**
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:	⌘	Providing text for section 7. It was agreed to have a section 7 with application guidelines to use GAA but there was no text proposed yet for this section.
Summary of change:	⌘	Proposed text for section 7 is added.
Consequences if not approved:	⌘	Section 7 is empty.

Clauses affected:	⌘	7

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

Other comments:	⌘	

7 Application guidelines to use GAA

GAA provides different alternatives to an AS or an AP to perform user authentication (i.e. force the UE to run AKA with the BSF as specified in TS 33.220 or use a mechanism based on subscriber certificates). Also under GAA, an AS may understand that the user request is already authenticated by an Authentication Proxy.

GAA as described in this TR has not the intention to impose any one authentication mechanism onto applications . It is rather aimed to be a tool at developers disposal which they can use to their benefit. Application developers may save development time by using GAA instead of designing and implementing application-specific authentication mechanisms. An additional advantage of the mechanisms of GAA is that they can provide global coverage, inherited from the GSM/UMTS coverage.

Depending on network configuration and policies of the operator, an AS or an AP will be able to use any of the alternatives provided by GAA or even any other user authentication mechanisms specified outside of 3GPP if such mechanisms are at their disposal. It is therefore assumed that an AS and an AP should be able to take the decision what parts of GAA shall be used if any.

This section tries to give an overview of arguments that can play a role in the choice of authentication mechanism. The authentication mechanism selected will be dependent on

1. Requirements/policies relating to the user/server/application/device that needs authentication. This may be in both directions (mutual authentication), but the usual emphasis is user to server authentication.

2. Device and service characteristics, user capabilities and preferences as defined in the user profile

3. Policies of the network or networks providing the transport service and the service providers of the applications

Requirements/policies relating to authentication will depend on whether there is a need for:

a) **Device authentication:** The device is genuine and not a clone i.e. Authentication of a (U)SIM by challenge response

b) **Integrity protection:** An example is signalling protection in UTRAN access A weakness in GSM is that it is very easy for a man in the middle to manipulate signalling message e.g. cipher mode command and a way to prevent it being compromised is to use device authentication **and** integrity protection via a keyed MAC (Message Authentication Code) on the specific signalling messages

c) **Application authentication:** It will often be necessary to check the authenticity of the application software by checking its digital signature. An example is Open Service Access (OSA) Application Programming Interface (API) Part 3: Framework (Parlay 4) ETSI ES 202 915-3 V1.2.1 . Application authentication is however out of the scope of GAA. This is more the domain of code signing and will not be further discussed in this section.

d) **User authentication:**. This refers to authentication of the end user, the person who is using the end user device. One way of doing this is to make the USIM availability to devices/protocols/applications dependent, logically, by user PIN input or physically, by a policy of removal and insertion. The entry of a PIN may also be required before access is allowed to a specific application

e) **Transaction authentication and non-repudiation:** For some business transactions that are carried out using the mobile device it is necessary to digitally sign the transaction with a users private key, specifically where there is a need for non repudiation i.e. to prevent:

- The False Denial of the: SENDING of the Message "I never sent it!"
- CONTENT of the Message i.e. "I said you should sell, not buy!"
- The TIME of the Message "I sent it a different time!"

Note that many authentication techniques such as 3GPP AKA are based on a single key which is shared between the network and the user - this is OK for authentication between sender and recipient, but non repudiation provable to a third party may require the use of public key technique where the private key is only held by the sender

Figure 5 below shows how device and service characteristics can impact the choice of a particular technique from the Spectrum of Authentication Mechanisms.

	authentication type		
client (device) charateristics	device (client) auth	server auth	transaction auth
PIN/password	stored PIN/password	signature	x
GAA: subscriber certificate	client private key, signature	signature	private key, signature
GAA: GBA at UE	shared secret (GBA), keyd MAC	shared secret (GBA), keyd MAC OR server private key, signature	x

Figure 5: Authentication characteristics comparison

X = client characteristics do not allow authentication requirement to be met

~~GAA provides different alternatives to an AS or an AP to perform user authentication (i.e. force the UE to run AKA with the BSF as specified in TS 33.220 or use a mechanism based on subscriber certificates using TS 33.221). Also under GAA, an AS may understand that the user request is already authenticated by an Authentication Proxy.~~

7.1 Use of shared secrets and GBA

Some examples of where shared secrets from the innovation of GBA can be used are

- Distribution of symmetric ciphering and Integrity keys for securing applications running between the UE and a server in he network. Example protocols that can be used to secure an application and that require a shared secret include HTTP Digest, shared secret TLS and IPsec.
- Distribution of passwords and PIN for third party applications
- For protecting the distribution of certificates between the UE and the certificate authority
- ~~For user authentication when subscriber certificates are not available~~
- In situations where the mobile device has very limited processing capabilities and public/private key operations are considered to be too heavy.

7.2 Use of certificates

Some examples of where certificates can be used for authentication are

- When it is necessary to check the identity of the end user
- When the application security protocol works smoothly with (public, private) key pair authentication and subscriber certificates are available (e.g. normal TLS).

Where there is a need for non-repudiation and where the user is required to digitally sign the transaction with a user's private key as many authentication techniques such as 3GPP AKA are based on a single key, which is shared between the network and the user. Non repudiation provable to a third party may require the use of public key technique where the private key is only held by the sender