3GPP TSG-SA WG3 Meeting S3#36
Shenzen, PRC, November 23-26, 2004

Tdoc ⌘S3-041093

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.222** **CR** **010** ⌘ **rev** **1** ⌘ 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:	⌘	Authorization flag transfer between AP and AS
Source:	⌘	SA WG3
Work item code:	⌘	GBA-SSC
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:	⌘	Editor's note on transfer of user profile from AP to AS is no longer needed, since the identities of the user are transferred in the HTTP header from the AP to the AS. In case the AS resides behind the AP, the AS would need to obtain the authorization flags to make a decision on the user authorization (based on the flags).
Summary of change:	⌘	1. Removal of editor's note in 6.4.2 and correcting wrong reference number 2. Removal of editor's note in 6.5.2 3. Addition in 6.5.2.3 to transfer the authorization profile flags in the HTTP header of message from AP to AS.
Consequences if not approved:	⌘	The editor's notes will indicate open issues and the AS that resides behind the AP will not be able to make an authorization decision that is based on authorization flags.

Clauses affected:	⌘	6.4.2, 6.5.2, 6.5.2.3

		Y	N			
Other specs affected:	⌘	X		Other core specifications	⌘	TS 24.109
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	

===== BEGIN CHANGE =====

6.4.2 AP-AS reference point

The HTTP protocol is run over the AP-AS reference point.

Confidentiality and integrity protection can be provided for the reference point between the AP and the AS using NDS/IP mechanisms as specified in TS 33.210 [~~12~~13]. For traffic between different security domains, the Za reference point shall be operated. For traffic inside a security domain, it is up to the operator to decide whether to deploy the Zb reference point. As AP terminates the TLS tunnel from UE, also a TLS tunnel is possible.

The AP shall support the transfer of an identity of the UE authenticated by the AP from AP to AS in a standardised format. The format of this information element in the HTTP request header is left to stage 3 specifications.

~~Editor's Note: If further information elements from the application specific user profile are transferred in standardised format to AS is ffs.~~

===== BEGIN NEXT CHANGE =====

6.5.2 Transfer of Asserted Identity from AP to AS

The AP is configured per AS to perform authentication and access control according to one of the following subclauses: if required in the subclause, the user identity is transferred to AS in every HTTP request proxied to AS.

~~Editor's Note: It is ffs if further information elements from application specific user profile may be transferred to AS.~~

===== BEGIN NEXT CHANGE =====

6.5.2.3 Authorised User of Application with Transferred Identity asserted to AS

The AP checks that the UE is an authorised user of the application. The user identity (or user identities) received from the BSF shall be transferred to AS. Based on AS-specific configuration of the AP, any authorization flags existing in application-specfic user security settings shall also be transferred to AS.

Depending on the application specific user security setting and the AS-specific configuration of the AP, the transferred user identity (or identities) may be the private user identity (IMPI), or may be taken from the application specific user security setting (e.g. an IMPU), or may be a pseudonym chosen by AP (e.g. Random, B-TID).

This case may be supported by AP.

NOTE 1: If the AP is configured to transfer a pseudonym to AS, any binding of this pseudonym to the user identity (e.g. for charging purposes by AS) is out of scope of this specification.

NOTE 2: If the AP is configured not to request an application specific user security setting from BSF, only the private user identity (IMPI) or a pseudonym may be transferred to AS. In this case any authorised participant of GBA is supposed to be an authorised user of the application.

===== END CHANGE =====