CR-Form-v7

CHANGE REQUEST

⌘ **33.222** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

*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⌘ [X] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	GBA User Security Settings
Source:	⌘	Nokia, Siemens
Work item code:	⌘	SSC-GBA
Date:	⌘	29/06/2004
Category:	⌘	**D**
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:	⌘	The use of the term GBA User Security Settings (previously termed GAA user profiles) is aligned with TS 33.220.
Summary of change:	⌘	Alignment with TS 33.220.
Consequences if not approved:	⌘	Mismatch of specifications.

Clauses affected:	⌘	6.5

		Y	N			
Other specs affected:	⌘	X		Other core specifications	⌘	TS 29.109
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	-

6.5 Management of UE identity

~~Editor's Note: The changes made to handling of application specific user profiles in TS 33.220 may affect this clause.~~

Different ASs need different kinds of authentication information. To support the requirements of different servers, the AP needs to perform authentication with varying granularity and with varying degree of assertion to the AS. The authentication and the corresponding assertion is therefore AS specific and has to be configured in the AP per AS.

6.5.1 Granularity of Authentication and Access Control by AP

The AP is configured per AS if the particular application or applications served by the AS is in need of an application specific user security setting, cf. TS 33.220 (Definitions)~~profile~~. This user security setting ~~profile~~ may contain the public user identities in the authentication part of the USS. The authorisation part of the USS may contain indications, which of the applications residing on the AP, and the Application Servers behind the AP, a user is allowed to access.

6.5.1.1 Authorised Participant of GBA

The AP checks that the UE is an authorised participant of GBA. Access is granted on success of the basic GBA mechanism, i.e. the UE sends a valid B-TID and performs digest authentication with the Ks_NAF received from BSF.

The AP is configured not to request an application specific user ~~profile~~ security setting from BSF for the AS named in the request. Depending on configuration of BSF the AP may receives the private user identity (IMPI) from BSF.

This case shall be supported by AP.

NOTE: This case may apply when all subscribers of an operator, but no other users, are allowed access to operator defined services. The BSF may not send the IMPI out of privacy considerations or because the AP does not need it. If the BSF does not send the IMPI to the AP, the user remains anonymous towards the AP; or more precisely, the B-TID functions as a temporary user pseudonym.

6.5.1.2 Authorised User of Application

The AP is configured to request an application specific user security setting ~~profile~~ from the BSF. Depending on the policy of the BSF, the AP receives the application specific user security setting ~~profile~~ and the private user identity (IMPI) from the BSF. Access is granted if allowed according to the application specific user security setting ~~profile~~ received from BSF.

The AP may do further checks on user inserted identities in the HTTP request if required according to clause 6.5.2.4.

This case shall be supported by AP.

NOTE: If there is no application specific user security setting ~~profile~~ configured for an application, this case reduces to authentication according to clause 6.5.1.1.

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.

6.5.2.1 Authorised Participant of GBA

The AP checks that the UE is an authorised participant of GBA. If the authentication of the UE by the AP fails, the AP does not forward the request of the UE to the AS.

This case shall be supported by AP.

NOTE: This case simply implies that the NAF checks that the user is known to, and has established a valid key, with the BSF, according to the GBA procedures described in TS 33.220 [3].

6.5.2.2 Authorised User of Application Anonymous to AS

The AP checks that the UE is an authorised user of the application according to application specific user security setting ~~profile~~ received from BSF. No user identity shall be transferred to AS.

This case may be supported by AP.

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.

Depending on the application specific user security setting ~~profile~~ 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 ~~profile~~ (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: 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: If the AP is configured not to request an application specific user security setting ~~profile~~ 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.

6.5.2.4 Authorised User of Application with Transferred Identity asserted to AS and Check of User Inserted Identity

This case resembles clause 6.5.2.3 with the following extension:

Based on the user identity received from BSF, the AP authenticates user related identity information elements as sent from UE. These "user inserted identities" may occur within header fields or within the body of the HTTP request.

Depending on application specific user security setting ~~profile~~ and AS-specific configuration of AP, all user-inserted identities (or a subset thereof) are authenticated by checking against the private user identity (IMPI) or the application specific user security setting~~profile~~.

Depending on the application specific user security setting ~~profile~~ and the AS-specific configuration of AP, the transferred user identity (or identities) may also be selected from the authenticated user inserted identities.

This case may be supported by AP.

NOTE: If AP authenticates certain or all user related identity information elements of a request, and the AS shall rely on the check of these elements, then a corresponding policy between the AP and the AS needs to be in place between the AP and the AS.

NOTE: Any application specific details are beyond the scope of this document and may be specified within the application, e.g. for Presence in TS 33.141 [5]. This specification does not preclude that any other application specific specifications (e.g. Presence) declare this feature as mandatory in their scope.