3GPP TSG-SA WG3 Meeting #37
Sophia Antipolis, France 21-25 February 2005

Tdoc ⌘S3-050042

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.222**	**CR**	**016**	⌘**rev**	**-**	⌘	Current version:	**6.2.0** ⌘

*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:	⌘	Clarification to TS 33.222		
Source:	⌘	Ericsson		
Work item code:	⌘	SEC1-SC	***Date:*** ⌘	14/02/2005
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:* *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:	⌘	It is proposed to add a note to TS 33.222 to clarify that there are situations when UE and AP may end-up having parallel TLS connections, e.g. if two applications in the UE are not able to share the same TLS connection. This is to align TS 33.222 with TS 33.220, which states in chapter 4.1.3: NOTE 1: If it is not desired by the UE to use the same Ks for the selected UICC application to derive more than one Ks_NAF then the UE should agree on a new key Ks with the BSF over the reference point Ub, and then proceed to derive Ks_NAF;
Summary of change:	⌘	A new note is added to chapter 6.2 to align TS 33.222 with TS 33.220.
Consequences if not approved:	⌘	TS 33.222 is not aligned with TS 33.220.

Clauses affected:	⌘	6.2				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

***** Begin of Change *****

6 Use of Authentication Proxy

An Authentication Proxy (AP) is an HTTP proxy which takes the role of a NAF for the UE. It handles the TLS security relation with the UE and relieves the application server (AS) of this task. Based on GBA the AP can assure the ASs that the request is coming from an authorized subscriber of the MNO.

6.1 Architectural view

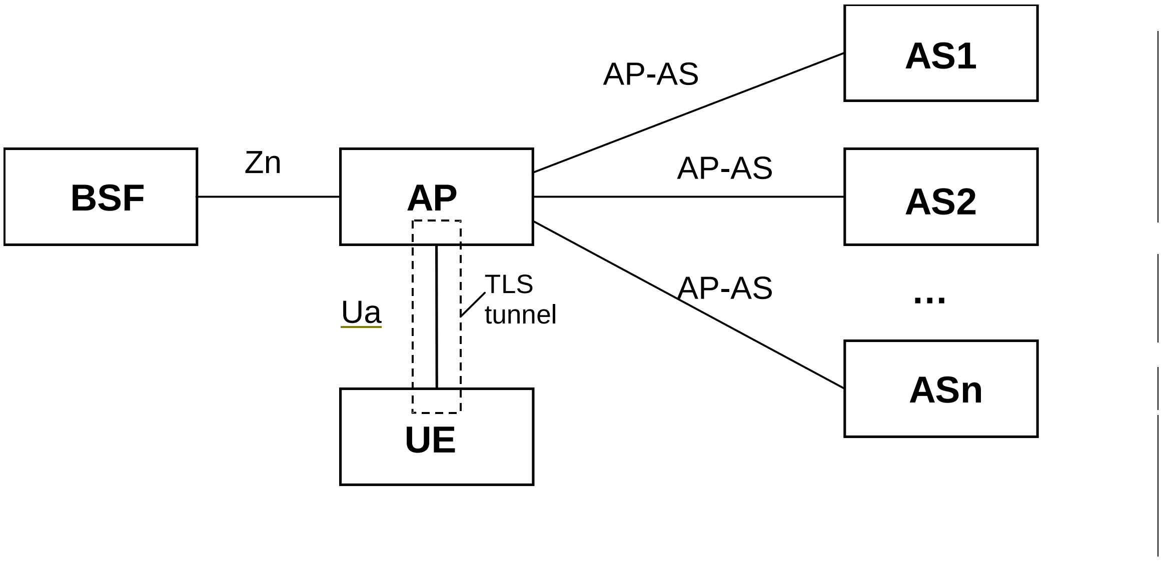

Figure 2: Environment and reference points of AP

The use of an authentication proxy (AP) is fully compatible with the architecture specified in TS 33.220 [3] and in clauses 4 and 5 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 (AS) behind an AP, the AP terminates the TLS tunnel and performs UE authentication. The AP proxies the HTTP requests received from UE to one or many application servers. The AP may add an assertion of identity of the subscriber for use by the AS, when the AP forwards the request from the UE to the AS.

Figure 3 presents an architectural view of using Authentication Proxy, for example, for IMS SIP based services. The UE shall manipulate own data such as groups, through the Ua/Ut reference point. The reference point Ut specified in TS 23.002 [1] shall be applicable to data manipulation of IMS based SIP services, such as Presence, Messaging and Conferencing services. The stage 1 requirements are specified in TS 22.250 [2].

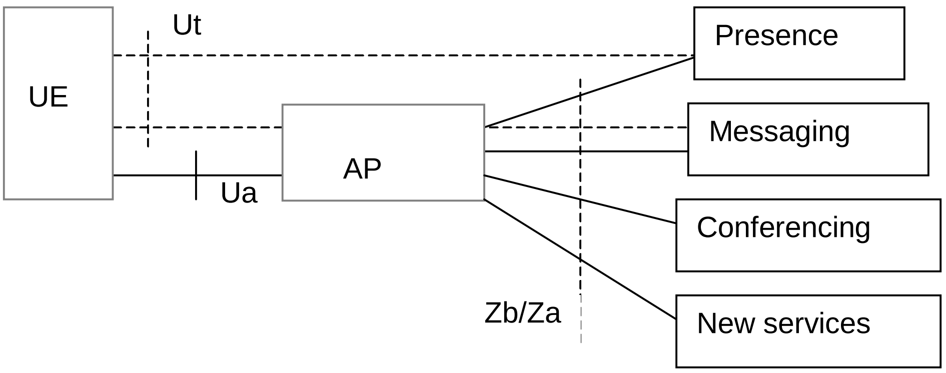

Figure 3: The architectural view using Authentication Proxy for IMS SIP based services

Management of UE identities is described in clause 6.5.

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

6.2 Requirements and principles

The authentication proxy may reside between the UE and the NAF as depicted in figure 2. The usefulness of an Authentication Proxy may be to reduce the consumption of authentication vectors and/or to minimize SQN synchronization failures. Also the AP relieves the AS of security tasks.

The following requirements apply for the use of an Authentication Proxy:

- authentication proxy shall be able to authenticate the UE using the means of Generic Bootstrapping Architecture, as specified in TS 33.220 [3];
- if the application server requires an authenticated identity of the UE the authentication proxy shall send it to the application server belonging to the trust domain with every HTTP request;
- if required, the authentication proxy may not reveal the authenticated identity of the UE to the application server not belonging to the trust domain;
- the authenticated identity management mechanism shall not prevent the application server to use an appropriate session management mechanisms with the client;
- the UE shall be able to create multiple parallel HTTP sessions via the authentication proxy towards different application servers;

NOTE 1: The used session management mechanism is out of the scope of 3GPP specifications.

NOTE 2: One motivation for having AP between UE and AS's is to minimize the number of TLS connections. However, there are situations when UE and AP may end-up having parallel TLS connections, e.g. if two applications in the UE are not able to share the same TLS connection.

- implementation of check of asserted user identity in the AS is optional;
- activation of transfer of asserted user identity shall be configurable in the AP on a per AS basis.

The use of an authentication proxy should be such that there is no need to manage the authentication proxy configuration in the UE.

NOTE 3~~2~~: This requirement implies that the authentication proxy should be a reverse proxy in the following sense: A reverse proxy is a web server system that is capable of serving web pages sourced from other web servers - in addition to web pages on disk or generated dynamically by CGI - making these pages look like they originated at the reverse proxy.

6.4 Reference points

6.4.1 Ua reference point

The Ua reference point is standardised in specification TS 33.220 [3] and in clauses 4 and 5 of this specification.

NOTE: The optional introduction of an AP has advantages which are stated elsewhere. However, the following consequences should be taken into account to decide whether an AP is to be used:

- The AP terminates TLS and HTTP digest. This relieves the AS of the burden to handle TLS and HTTP digest, but it should be noted that then the UE is not able to establish an additional end-to-end TLS tunnel to the AS, nor can the UE additionally authenticates itself to AS by use of client authentication within TLS. Furthermore, if GBA authentication uses HTTP Digest Authentication, then the UE cannot use Basic or Digest Authentication directly with AS.