Source:	Nokia
Title:	**Using SSC as optional in Presence service TS33.141**
Document for:	Discussion/Decision
Agenda Item:	GBA

This is a short companion contribution to TS 33.141, section 6, to conform the general cases specified in TS 33.222.

6 Security Mechanisms

The UE and the AP/Presence Server shall support the TLS version as specified in RFC 2246 [6] and WAP-219-TLS [13] or higher. Earlier versions are not allowed.

Editors Note: It is FFS if it is possible to base the Presence Security on TLSv1.1 [14], which is currently in draft status in IETF.

Note 1: The management of Root Certificates is out of scope for this Technical Specification

6.1 Authentication and key agreement

6.1.1 Authentication of the Subscriber

From a TLS point of view the UE shall be considered as un-authenticated, cf. RFC 2246 [6].
The authentication of the UE may take place in either the Authentication Proxy or the Server. However the AP or the Server may given the policy of the operator conclude that the AP/Presence Server shall not authenticate the UE using GBA i.e. the UE is considered as authenticated already or the UE is authenticated by other means.

Otherwise if the AP/Presence Server concludes that the authentication shall take place in the AP/Presence Server then the UE may be authenticated as specified in TS 33.220 [11] (where the Ua interface is between the UE and the AP/Presence Server).

The AP/Presence Server may also authenticate the UE based on subscriber's certificates that is specified in TS 33.222 [x], if the AP/Presence Server supports such capability.

It shall be possible for the operator at any time to request a re-authentication of an active UE.
Editors Note: A clean up what item is used for authentication purposes might be needed i.e. User, Subscriber and UE.