

Abstract

Embodiments of the invention provide key generation and authentication methods that dynamically generate device credentials e.g. device key, at the core network during authentication procedure, and thereby eliminating the need to store device credentials, e.g. device key, at the core network. Particularly, at a core network node, e.g. HSS, upon receiving an authentication message which at least includes a device identifier and a service identifier, the core network node generates a device key based at least on the device identifier and a service key which is stored at the core network node and associated with the service identifier; and uses the generated device key to authenticate a device associated with the device identifier.

(Figure 2)