

Abstract

Embodiments of the invention relate to authentication of user equipment and core network with at least an asymmetric key in USIM/eUICC as authentication
5 credentials to prevent man-in-the-middle attacks. Embodiments of the invention further relate to use of asymmetric key in combination with any of a symmetric key, another pair of asymmetric keys and Diffie-Hellman (DH) procedure in authentication and/or key generation procedure.

10 (Figure 4)