

KEY MANAGEMENT METHOD, DEVICE, AND SYSTEM

ABSTRACT

This application provides a key management method, a device, and a system, to ensure that a terminal device and an application function network element can still successfully agree on a communication key between the terminal
5 device and the application function network element after re-authentication occurs in an AKMA procedure. The method includes: A terminal device sends a first application session establishment request message to a first application function network element, where the establishment request message carries identification information of a first key, and the first key is an authentication and key management for applications AKMA key. The terminal device receives a first authentication request message in a procedure of the re-authentication. The terminal device sends a
10 response message for the first authentication request message in the procedure of the re-authentication. The terminal device receives a response message for the establishment request message. The terminal device derives a communication key between the terminal device and the first application function network element by using the first key.

15 Fig. 10