

AUTHENTICATION METHOD AND COMMUNICATION APPARATUS

ABSTRACT

This application provides an authentication method and a communication apparatus, and
5 relates to the field of communication technologies, to authenticate terminal devices that support
different security algorithms. The method includes: A terminal device sends a first registration
request message to a serving call session control function network element. The first registration
request message carries information about security algorithms that can be supported by the
terminal device. The terminal device receives an authentication challenge message from the
10 serving call session control function network element. The authentication challenge message
includes information about a third security algorithm, and the third security algorithm is one of the
security algorithms that can be supported by the terminal device. The terminal device calculates a
hash value of a security parameter based on the third security algorithm, and the terminal device
calculates an authentication response based on the third security algorithm and the hash value. The
15 terminal device sends a second registration request message to the serving call session control
function network element. The second registration request message carries the authentication
response, and the authentication response is used to authenticate the terminal device.

(Fig.3)