

ABSTRACT

METHOD AND TERMINAL FOR ESTABLISHING SECURITY INFRASTRUCTURE AND
DEVICE

A method and terminal for establishing a security infrastructure and a device, comprising: an intermediate service organization receives an organization secret key sent by a third-party service organization (S101); the intermediate service organization employs a first encryption means to encrypt the organization secret key and sends the encrypted organization secret key to a security storage region of a terminal (S102); the intermediate service organization receives a first terminal public key encrypted by the terminal using a second encryption means (S103); and the intermediate service organization sends the first terminal public key obtained by decryption to the third-party service organization (S104). The organization secret key of the third-party service organization may be sent to the terminal by means of the intermediate service organization, and the first terminal public key of the terminal may be sent to the third-party service organization, thus a universal security infrastructure and a technical frame work having good openness may be provided by the intermediate service organization.

Fig. 1