

ABSTRACT

METHOD AND TERMINAL FOR ESTABLISHING SECURITY INFRASTRUCTURE AND
DEVICE

A method, terminal and device for establishing security infrastructure, comprising: an intermediate service organization receives an organization secret key sent by a third-party service organization; the intermediate service organization encrypts the organization secret key by a first encryption means and sends the encrypted organization secret key to a security storage region of a terminal; the intermediate service organization receives a first terminal public key encrypted by the terminal using a second encryption means; and the intermediate service organization sends the first terminal public key obtained by decryption to the third-party service organization. The organization secret key of the third-party service organization may be sent to the terminal through 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