ABSTRACT

Public-key cryptography is realized by means of PKI in which biometrics data, in which biological information of users is converted to numerical values, are used to authenticate users that transmit and receive data, and based on the biometrics data, identical secret keys (common secret keys) are generated in each of the user terminal devices that are used by the users without releasing the secret keys onto the network.