Abstract

For digital signature processing using a public key cryptosystem, there is provided a convenient digital signature system which facilitates control of a private key. Based on an "ID" supplied by a user, the dynamic signature encryption key control section 16 obtains registered dynamic signature data and a private key from a control database 12. The registered dynamic signature data is compared with authentication dynamic signature data sent by the user in the dynamic signature verifying section 14. When it is determined that they are identical signature data, the dynamic signature encryption key control section 16 supplies message data sent from the user, and the private key to the encryption operation section 18. The encryption operation section 18 encrypts the message data using the private key, and sends the encrypted message data to the dynamic signature encryption key control section 16. The dynamic signature encryption control section 16 returns signed, i.e. encrypted, message data or the like to the user. The user need not control his own private key.