ABSTRACT

For group signature data capable of keeping anonymity, it is possible to efficiently determine whether the user having created the group signature data is a valid member of the group. When a message and group signature data are received, the verification unit 3 authenticates the data and inquires, of the member status response unit 4, whether the user of the signature unit 2 having created the group signature data is a valid member of the group. In response to the inquiry, the response unit 4 determines the member status of the user having created the group signature data, according to a member revocation list notified from the group management unit 1. The response unit 4 then transmits a judge result of the member status to the verification unit 3.