ABSTRACT

When an entrustor entrusts an outsourcer with the supply of a service for members, member information managed by the entrustor is kept secret from the outsourcer, and users can receive the service without communicating with the entrustor. For using the service, user apparatus 3 sends group signature data to outsourcer apparatus 2. Outsourcer apparatus 2 authenticates the group signature data using public information of entrustor apparatus 1. When the group signature data passes the authentication, confirming that user apparatus 3 is a member of entrustor apparatus 1, outsourcer apparatus 2 provides the service to user apparatus 3.