

ABSTRACT

According to an embodiment, a key management device includes a first acquisition unit, a storage unit, a first authentication unit, a generation unit, a second acquisition unit, and a second authentication unit. The first acquisition unit acquires pre-authentication information including a user ID, authentication information and encrypted authentication information. The storage unit stores a DB key securely. The first authentication unit decrypts the encrypted authentication information using the DB key and performs authentication using the decrypted authentication information and the authentication information. The generation unit generates a ticket associated with the user ID based on a result of the authentication and generates a pre-authentication response including the ticket. The second acquisition unit which acquires session information including the ticket. The second authentication unit which authenticates the session information based on the ticket included in the session information and generates a cryptographic key corresponding to the ticket.