

USER AUTHENTICATION METHOD FOR ENHANCING INTEGRITY AND SECURITY

ABSTRACT OF THE DISCLOSURE

Disclosed is a user authentication method having an enhanced integrity and
5 an enhanced security. The user authentication method includes (1) if a procedure for
registration of a user, performing a primary conversion to generate a first common
authentication key and performing a secondary conversion to provide an encrypted
first common authentication key, by a user terminal, and registering the encrypted
first common authentication key, by the authentication server; (2) generating a first
10 server authentication key, and performing an OTP operation on the first server
authentication key to generate first server authentication information; (3) if an
authentication procedure is started, performing a primary conversion to generate a
second common authentication key, performing a secondary conversion to generate
an encrypted second common authentication key, generating a first user
15 authentication key, and performing an OTP operation on the first user authentication
key to generate first user authentication information; and (4) performing a user
authentication or an authentication of the authentication server for determining a
genuineness of the authentication server, based on coincidence of the first server
authentication information and the first user authentication information.

20 Fig. 2