Abstract of the Disclosure

An Authentication System

A method for authenticating a user for accessing secure data, the method comprising:

transmitting user identification information for identifying the user, from the user to an authentication server;

generating a session key for associating the user with the server in a session, the session key being transmitted from the server to the user; and

transmitting an authorisation key for authenticating the user to the server in the session, the authorisation key being transmitted from the user to the server;

wherein the authorisation key is formed by performing a predetermined operation on the session key, the predetermined operation being defined by a private key of the user; and

whereby if the authorisation key transmitted by the user matches a corresponding authorisation key generated by the server, access to the secure data is granted.

Fig. 2