

ABSTRACT

AUTHENTICATION AND VALIDATION PROCEDURE FOR IMPROVED SECURITY IN COMMUNICATIONS SYSTEMS

5

A client communications device and method for generating a user message comprising an assertion for verification by a remote server device is described. Payload data for the user message as generated by a secure application resident on the communications device is received. Biometric authentication of the user is performed as a first level security mechanism. If biometric authentication of the user is successful, a digital signature is generated based on the message payload as a second level security mechanism. The digital signature is generated using a private signature key stored in a secure element of the client device. A third level security mechanism is applied by authenticating the user message using a secure application-specific key. In implementations, the digital signature is generated in a secure environment of the client device which has sole access to the secure element after successful biometric authentication. The user message comprising the message payload and the digital signature is generated for sending to the remote server device. The verification may be required during a financial transaction. A corresponding server communications device and method is also described.

10

15

20

(Fig. 2)

25