INTERCEPTION-PROOF AUTHENTICATION AND ENCRYPTION SYSTEM AND METHOD

Abstract

An interception-proof authentication and encryption system and method is provided that utilizes passcodes with individual pins that are made up of symbols from a set of symbols, and tokens that contain at least two symbols from the set of symbols used for the passcode. Multiple tokens (a token set) are presented to a user, with some or all of a users pre-selected pins (symbols) randomly inserted into some or all of the tokens. The user selects a token from the token set for each pin position in the passcode. The user is authenticated based on the selected tokens. Because each selected token may or may not contain one of the pre-selected pins in the users passcode, and also contains other randomly generated symbols that are not one of the pre-selected pins in the users passcode, someone that observes which tokens the user has chosen cannot determine what the users actual passcode is.

Fig. 15A