CLAIMS

1. A method of user identification by keystroke dynamics, the method performing using a computing device, the method comprising:

registering one or more user credentials in the system;

assigning an identifier, appropriate to the credentials, to a user;

pre-dividing one or more keys of a keyboard into two or more keyboarding operation areas;

training a classifier to identify the user, wherein, during training, the user entering credentials into the system from the keyboard a specified number of times, wherein during each input:

measuring a time each key is held down,

measuring an interval between the time of pressing each key and each of pressing all the other keys that are used by the user when entering credentials,

measuring an interval between the time of releasing each key and each of releasing all the other keys that are used by the user when entering credentials,

measuring an interval between the time of pressing each key and each of releasing all the other keys that are used by the user when entering credentials,

measuring an interval between the time of releasing each key and each of pressing all the other keys that are used by the user when entering credentials,

multiplying each of the measured intervals by a predetermined factor, wherein a respective predetermined factor is pre-set and assigned for the keys from each area of the keyboard,

generating a user data set, based on the measured time and multiplied intervals, and the identifier associated with the corresponding user,

saving the generated user data set in a database,

selecting a data set from the database having the measured time and the multiplied intervals with the least variance using a selection algorithm, and

training the classifier on the basis of the selected data set to identify the user when entering credentials into the system.

2. The method of claim 1, further comprising using the trained classifier to confirm the identity of the user who entered the credentials at login, on whose data sets the classifier was trained.

3. The method of claim 2, wherein using the trained classifier further comprising, selecting a threshold value, the excess of which indicates the identity of the user who enters the credentials is the user on whose data sets the classifier was trained.

4. The method of claim 3, wherein using the trained classifier further comprising, wherein when a trained classifier response that is numerically smaller than the selected threshold is received, an alert is generated that an access to the credentials by an unidentified user is unauthorized.

5. The method of any preceding claim, wherein when typing in the credentials, the presses of the non-character keys are additionally recorded.

6. The method of any preceding claim, wherein the classifier is trained by a method of machine learning.

7. The method of any preceding claim, wherein a pre-set number of measured time or measured intervals that have the greatest variance in the data sets of the corresponding user are not used for the selection algorithm.

8. The method of any preceding claim, wherein the user identification includes identification of a pre-set group of persons using the same account.

9. A system of user identification by keystroke dynamics, the system comprising:

the keyboard;

a unit configured for registration of the user credentials in the system;

a system clock configured to determine the pressing time and the release time of the keys;

a long-term memory configured to store the database;

the computing device configured to perform the method according to any of claims 1 to 8.

10. A remote banking service system comprising the system of claim 9.

11. A website, which involves user authorization comprising the system of claim 9.