

METHODS AND SYSTEMS FOR TRUSTED WEB AUTHENTICATION

TECHNICAL FIELD

The presently disclosed subject matter relates to methods and systems for enabling trusted authentication, in particular to cloud-based services and/or websites.

BACKGROUND

In the web, users need to be authenticated when attempting to access various cloud-based services and/or websites, such as emailing websites, bank accounts, health records, etc.

Most websites still use a username and password to authenticate users. Some websites use physical devices or two-factor authentication (using token and/or mobile phones).

Each method has disadvantages: passwords can be stolen, physical devices are not convenient, and two-factor authentication does not prevent the creation of fake identities, since a one-time SIM card can be used.

Another issue is that one (physical) person may have many unrelated (virtual) identities: several email addresses (private and business), phone numbers and profiles in different social networks. It may also be legitimate to use multiple profiles for business purposes, advertisement and promotional activities. The problem is that illegal activists abuse the web openness and create fake identities to hide their activities.

There is now a need to provide new methods and systems for enabling trusted authentication, in particular to cloud-based services and/or websites.

GENERAL DESCRIPTION

In accordance with certain aspects of the presently disclosed subject matter, there is provided an identification method, comprising:

providing at least one database storing, for each of a plurality of users, user data comprising:

- o biometric data representative of biometric features of the user,