Title: A TASK COMPLETION AUTHENTICATION SYSTEM AND METHOD

Figure 1

Abstract: A method of authenticating the completion of a task includes receiving data including contextual data, user identification data and task completion data including information about a task that has been completed. A memory is accessed and retrieving previously stored contextual data and user identification data and the received contextual data and user identification data is stored with the previously stored contextual data and user identification data for future authenticating that the task described in the task completion data has been complete if required.
Published:
— without international search report and to be republished upon receipt of that report (Rule 48.2(g))
A TASK COMPLETION AUTHENTICATION SYSTEM AND METHOD

BACKGROUND OF THE INVENTION

This patent application relates to a system and method of authenticating the completion of a task.

When users are allowed to use any device and/or platform application to update and execute tasks, it becomes increasingly important to the business process requesting the execution of the task to ensure that the intended task operator is indeed the one who executed or operated on the task. Since devices can be lost, stolen, misused and fraudulently accessed, a mechanism is required for authenticating the completion of the task including the user at the point where the task is released with an update or outcome back to the task issuer.

This patent application addresses these issues.
SUMMARY OF THE INVENTION

According to a first aspect of the invention there is provided a method of authenticating the completion of a task, the method comprising:

- receiving data from a device, the data including contextual data, user identification data and task completion data including information about a task that has been completed;
- accessing a memory; and
- storing in the memory the received contextual data, user identification data and task completion data for future authenticating that the task described in the task completion data has been complete if required.

The contextual data may include one or more of an identification of an electronic device used to complete the task, the location of the electronic device at the time of the task completion, and the date and time from the electronic device at the time of the task completion or any available information on the electronic device that may be used to uniquely identify it.

The user identification data may include one or more of a fingerprint, an electronic signature, a palm print, a photograph, a voice recording, a one-time-pin and an iris scan or any biometric information that may be obtained from a person that completed the task.

According to a second aspect of the invention there is provided a system for managing tasks, the system comprising:

- a communications module for receiving data from a device, the data including contextual data, user identification data and task completion data, the data being the data used in the method described in the first aspect of the invention;
completion data including information about a task that has been completed;

a memory; and

an authentication processor for accessing the memory and storing the received contextual data and user identification data with the task completion data for future authenticating that the task described in the task completion data has been complete if required.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows a schematic drawing of a system in accordance with an example embodiment;

Figure 2 shows a schematic drawing of the task proxy of Figure 1 in greater detail;

Figure 3 shows a flow diagram of a method in accordance with an example embodiment; and

Figure 4 shows a schematic structure of a data file stored in a memory.

DESCRIPTION OF PREFERRED EMBODIMENTS

in the following description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of an embodiment of the present disclosure. It will be evident, however, to one skilled in the art that the present disclosure may be practiced without these specific details.
Referring to the accompanying Figures an example system for authenticating the completion of a task is generally indicated by reference numeral 10.

The task to be completed will typically be sent to an electronic device 12 of a person to complete the task.

It will be appreciated that in Figure 1 there is illustrated a single user with three electronic devices 12, however, the system is able to cater for any number of users each having one or more devices 12.

in any event, the devices 12 are electronic data communication devices such as a computer 12a, tablet 12b and mobile telephone 12c to name but a few examples.

There are many ways in which the task could be created and transmitted to the electronic device 12 and the methodology of the present invention could work with all of these.

in one example embodiment, the task is created and transmitted to the device 12.

The user who will complete the task does so and then uploads data using the electronic device 12 by means of which the completion of the task by the correct individual can be authenticated.

In order to accomplish this, the system includes an authentication processor 14.

Associated with the authentication processor 14 is a communications module 16 for receiving data including contextual data, user identification data and task completion data including information about a task that has been complete.
In this regard, "module" in the context of the specification will be understood
to include an identifiable portion of code, computational or executable
instructions, data, or computational object to achieve a particular function,
operation, processing, or procedure. It follows that a module need not be
implemented in software; a module may be implemented in software,
hardware, or a combination of software and hardware. Further, the
modules need not necessarily be consolidated into one device but may be
spread across a plurality of devices.

In one example embodiment the contextual data includes one or more of an
identification of an electronic device used to complete the task, the location
of the electronic device at the time of the task completion, and the date and
time from the electronic device at the time of the task completion.

This information is captured by one or more executable applications
running on the device that access existing device hardware and software,
such as a GPS module, to obtain this information.

The user identification data may include one or more of a fingerprint, an
electronic signature, a palm print, a photograph, a video recording, a voice
recording and an iris scan from a person that completed the task or taking a
photo and/or voice recording of the subject in question using the device.
This type of data is biometric type data used to identify the user.

This information is also captured by one or more executable applications
running on the device that accesses existing device hardware and
software. For example, many smart phones include a fingerprint sensor
and the user's fingerprint can be read at the time of task completion. In
another example, almost all mobile phones and tablets include a camera
and the user can take an appropriate photograph at the time of task
completion.

Alternatively or in addition, the user identification could be performed by
requesting a username/password or any other credential from the user,
sending the subject a One Time Pin challenge response, requesting a certificate or token of the subject or any other authentication mechanism not mentioned that can be used to identify the user.

it will be appreciated that other forms of contextual data and user identification data may be used.

The authentication processor 14 stores the received contextual data and user identification data with the previously stored contextual data and user identification data in the memory 18 for use at a later date if authenticating is required at the later date that the task described in the task completion data has been complete.

Since the device 12 may have different capabilities for authenticating users, in one example embodiment, authentications are classified and grouped according to levels. Interactions that require level 3 authentication for example may use any of the level 3 grouped authentication mechanisms that are available to the specific device/platform application.

This means that if a level 3 authentication is required on one kind of tablet this could mean taking the biometrics of a handwritten signature. On another tablet device this mechanism may be unavailable and an acceptable level 3 authentication replacement would be to take a photograph of the user in combination with their GPS position. Thus if level 3 authentication is required the devices pick from their available level 3 authentication mechanisms then enforce those.

It will be appreciated that using the method described above, the task authentication history can be read back by a forensic investigator for auditing purposes and it can be proved that they have not been altered in any way.

Referring to Figure 4, a schematic of the stored data is shown.
The stored data, which for convenience can be referred to as a task container, is composed of the task information data, device contextual data and user authentication data. Thus the task container also contains the context and information of the human task as it is not sufficient to rely on a link between the human task and the task unit alone. The task container must be able to represent the entire task context, data, outcome and authentication token as a single unit that may not be unpicked or separated.

This ensures the validity of the task container to the process and is sufficient proof of the identity of the user who invoked or executed an action upon a specific task. Such containers may be (but are not limited to) a PDF document for example. The container may also take the form of a proprietary machine readable object or document or any other secure non-divisible container of information.

In one example, this is achieved by the authentication processor algorithmically "signing" information as in PKI certificate signing. The authentication token, data and context data is combined into a file. Next a checksum of the file is calculated and hashed using SHA-2 and a certificate that is then attached to the signed package.

The data that composes the container must not be transmitted or stored separately requiring a processor to compile the container and secure it in one action on the device/platform application at the time of authentication.

Thus it will be appreciated that by tying together the task information, user information and device information in one indivisible unit, this provides all of the necessary components to allow a task to be authenticated at a later date.
CLAIMS:

1. A method of authenticating the completion of a task, the method comprising:

   receiving data from a device, the data including contextual data, user identification data and task completion data including information about a task that has been completed;

   accessing a memory; and

   storing in the memory the received contextual data, user identification data and task completion data for future authenticating that the task described in the task completion data has been complete if required.

2. The method of claim 1 wherein the contextual data includes one or more of an identification of an electronic device used to complete the task, the location of the electronic device at the time of the task completion, and the date and time from the electronic device at the time of the task completion or any available information on the electronic device that may be used to uniquely identify it.

3. The method of claim 1 wherein the user identification data includes one or more of a fingerprint, an electronic signature, a palm print, a photograph, a voice recording, a one-time-pin and an iris scan or any biometric information that may be obtained from a person that completed the task.

4. A method according to claim 1 wherein the contextual data, user identification data and task completion data is stored in the memory in a combined data file or task container.
5. A method according to claim 4 wherein the combined data file is signed by attaching a data certificate and digital checksum to the combined file.

6. A system for managing tasks, the system comprising:

   - a communications module for receiving data from a device, the data including contextual data, user identification data and task completion data including information about a task that has been completed;

   - a memory; and

   - an authentication processor for accessing the memory and storing the received contextual data and user identification data with the task completion data for future authenticating that the task described in the task completion data has been complete if required.

7. The system of claim 6 wherein the contextual data includes one or more of an identification of an electronic device used to complete the task, the location of the electronic device at the time of the task completion, and the date and time from the electronic device at the time of the task completion or any available information on the electronic device that may be used to uniquely identify it.

8. The system of claim 6 wherein the user identification data includes one or more of a fingerprint, an electronic signature, a palm print, a photograph, a voice recording, a one-time-pin and an iris scan or any biometric information that may be obtained from a person that completed the task.

9. A system according to claim 6 wherein the contextual data, user identification data and task completion data are secured and stored in the memory in a combined data file.
10. A system according to claim 9 wherein the authentication processor signs the combined data file by attaching a data certificate and digital checksum to the combined file.
START

RECEIVE DATA INCLUDING CONTEXTUAL DATA, USER IDENTIFICATION DATA AND TASK COMPLETION DATA INCLUDING INFORMATION ABOUT A TASK THAT HAS BEEN COMPLETED

ACCESS A MEMORY AND RETRIEVING PREVIOUSLY STORED CONTEXTUAL DATA AND USER IDENTIFICATION DATA

STORE THE RECEIVED CONTEXTUAL DATA AND USER IDENTIFICATION DATA WITH THE PREVIOUSLY STORED CONTEXTUAL DATA AND USER IDENTIFICATION DATA FOR FUTURE AUTHENTICATING THAT THE TASK DESCRIBED IN THE TASK COMPLETION DATA HAS BEEN COMPLETE IF REQUIRED

END

FIGURE 3