

- 1 -

AN INTEGRATED ACCESS CONTROL AND IDENTITY MANAGEMENT SYSTEM5 Field of the Invention

The present invention relates to an integrated access control system for controlling access to at least an IT resource by a person, and to a method of controlling
10 access to at least an IT resource by a person.

Background of the Invention

It is known to provide a system for monitoring and
15 controlling physical access to an area so that access is restricted to authorised persons only. In one such system, access by persons through any one of a plurality of doors is controlled by providing each door with a credential reader for gathering one or more credentials
20 from a person, such as a pin number, biometric information or an ID number stored on a card, and verifying the gathered credentials with reference credentials stored in a back end system.

25 It is also known to provide a system for monitoring and controlling access to an IT resource, for example including software applications and data, so that only authorised personnel are able to use the software and/or access the data. Such IT access control may be
30 implemented by each user operable computing device associated with the IT resource, or may be implemented at least in part using a separate gateway device that operates to control access and to grant or deny access

- 2 -

based on the user's credentials.

However, such conventional IT access control systems are relatively unsophisticated and as a result do not provide effective access control.

Summary of the Invention

In accordance with a first aspect of the present invention, there is provided an access control system comprising:

an IT access control unit arranged to monitor attempts to access an IT resource by a person; and stored access criteria defining access rights for each user associated with the system;

the IT access control unit arranged to determine whether and the extent to which access should be granted to a user based on the stored access criteria;

wherein the stored access criteria are arranged such that an identity criterion indicative of the identity of the user able to access the IT resource, a location criterion indicative of the location from which the user is allowed to access the IT resource, a time criterion indicative of the time at which the user is allowed to access the IT resource, a type criterion indicative of the type of IT resource that the user is allowed to access, and/or an access level criterion indicative of the level of access authority given to the user are definable in the stored access criteria.

In one embodiment, the system comprises a physical access control unit arranged to monitor attempts to physically access an area by a person.

- 3 -

In one embodiment, the system comprises an access information storage device, the system being arranged to store in the access information storage device access information indicative of access attempts monitored by the IT and physical access control units.

In one embodiment, the identity criterion, the location criterion, the time criterion, the type criterion, and the access level criterion are all defined in the stored access criteria for at least one user associated with the system.

In one embodiment, the IT resource comprises at least one software application and/or data stored in at least one data storage device.

In one embodiment, the time criterion is indicative of the duration of time during which a user is allowed to access the IT resource.

In one embodiment, the type criterion is indicative of one or more storage locations that the user is allowed to access, and/or one or more software applications that the user is allowed to access, and/or one or more data types that the user is allowed to access.

In one embodiment, the type criterion is a trust level criterion indicative of the maximum level of sensitivity of data the user is allowed to access.

In one embodiment, the access level criterion is selected from a group including administrator, supervisor, view only, and no access.

- 4 -

In one embodiment, the system is arranged to associate tag information with the access information and to store the tag information in the access information storage device, the tag information including information usable to make a determination as to whether a first access attempt monitored by the physical access control unit is related to a second access attempt monitored by the IT access control unit.

10 In one embodiment, the identity of a user is determined based on credentials gathered from the person.

The credential information may include biometric information associated with the person, identification information gathered from an identification card carried by the person, a PIN number provided by the person, or any other identification information.

In one embodiment, the tag information includes location information indicative of the location of the access attempt associated with the tag information.

In one embodiment, the tag information includes credential information indicative of at least one credential gathered from a person attempting to access an area or resource.

In one embodiment, the tag information includes date and/or time information.

30 In one embodiment, the tag information is in the form of metadata added to the access information.

- 5 -

In one embodiment, the system comprises an integrated access control and identity management station in communication with the first and second access control units, the integrated access control and identity management station receiving the access information and tag information from the first and second access control units, and the integrated access control and identity management station arranged such that the access information and tag information is accessible through the integrated access control and identity management station.

The integrated access control and identity management station may be arranged so as to facilitate searching by a user through access information and/or tag information.

The integrated access control and identity management station may be accessed locally or remotely, and may be accessed through a communications network such as the Internet.

In accordance with a second aspect of the present invention, there is provided a method of controlling access to an IT resource by a person, the method comprising:

monitoring attempts to access an IT resource by a person; and

storing access criteria defining access rights for each user associated with the system;

determining whether and the extent to which access should be granted to a user based on the stored access criteria;

wherein the stored access criteria are arranged such that an identity criterion indicative of the identity

- 6 -

of the user able to access the IT resource, a location criterion indicative of the location from which the user is allowed to access the IT resource, a time criterion indicative of the time at which the user is allowed to access the IT resource, a type criterion indicative of the type of IT resource that the user is allowed to access, and/or an access level criterion indicative of the level of access authority given to the user are definable in the stored access criteria.

10 Brief Description of the Drawings

The present invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

15 Figure 1 which is a diagrammatic representation of an access control system in accordance with an embodiment of the present invention;

Figure 2 is a diagrammatic representation of components of the access control system shown in Figure 1; and

20 Figure 3 shows an access matrix of the access control system shown in Figures 1 and 2.

Description of an Embodiment of the Invention

25 Referring to Figure 1, an embodiment of an access control system 10 that is arranged to control physical access to an area and IT access to a resource is shown. In this example, the access control system 10 also facilitates monitoring of access attempts by recording historical access event information associated with a user in an access information storage device and facilitating access to the historical access event information by an operator

- 7 -

of the system.

In this example, the IT resource may comprise one or more software applications and/or data stored in one or more
5 folders in one or more data storage devices.

An access event includes positive identification of a person and consequent granting of access by the person, either physically to at least part of an area or
10 electronically to at least part of an application or data of an IT resource; negative identification wherein a player attempts to gain access but the identity of the person is not verified and consequently access by the person is denied; and otherwise unauthorised physical or
15 electronic access to an area or IT resource, such as forced entry through a controlled access door or physical disconnection of a computing device from the IT resource.

The system 10 includes a physical access control
20 arrangement 12 and an IT access control arrangement 14, each of which in this example communicates with an access information storage device in the form of an integrated access control and identity management station 16 that may be located remotely relative to the physical and IT access
25 control arrangements 12, 14, for example in communication with the physical and IT access control arrangements 12, 14 through the Internet. In this example, the physical and IT access control arrangements 12, 14 are disposed at the same location or in close proximity to each other.

30

The physical access control arrangement 12 is arranged to control physical access to an area, and to determine whether an undesirable access event has occurred, such as

- 8 -

a failed physical access attempt based on gathered user credentials or an attempt to forcibly gain physical access. Similarly, the IT access control arrangement 14 is arranged to control access to an IT resource, including a software application and/or data, and to determine whether an undesirable access event has occurred, such as a failed IT access attempt based on gathered user credentials, an access attempt outside of a defined access period or that exceeds a defined access duration, an attempt to access data for which the user is not authorised, an access attempt from a location that is not authorised, or an attempt to forcibly gain access to software or data.

In this example, information indicative of access attempts is sent to the integrated access control and identity management station 16 by the physical access control arrangement 12 and the IT access control arrangement 14, and relevant tag information is added to the access information by each of the access control arrangements 12, 14. The tag information includes information usable to associate access events with each other, for example information indicative of location, information indicative of the gathered user credential data, date and/or time information, and so on.

Since access control events that are likely to be related to each other can be linked with each other by virtue of the tag information, it is possible for an operator to easily identify potentially related physical and IT access control events by searching for particular tag information.

- 9 -

In the example shown in Figure 1, the physical access arrangement 12 includes a physical access control unit 20 arranged to control physical access control attempts, and in particular to gather credentials from users seeking to gain physical access to an area, compare the gathered credentials with reference credentials, and grant or deny access based on the comparison.

In this example, the physical access control unit 20 is connected to at least one camera 22 arranged to gather video information from the surrounding area, at least one access point 24, such as a door, and at least one credential reader 26.

Each access point 24 has an associated door lock 25 that in this example is controlled by a respective physical access control unit 20 such that the door lock 25 may be caused to enable or prevent opening of the access point 24 in response to an appropriate signal from the physical access control unit 20.

During use, the credential reader 26 gathers at least one user credential from a person desiring to pass through the access point 24, and the physical access control unit 20 compares the gathered user credentials with stored reference user credentials and makes a decision as to whether to grant or deny access. If access is granted, the physical access control unit 20 sends a signal to the door lock 25 to dispose the door lock 25 in an unlocked state and thereby allow the person to pass through the access point 24 and access the area. If access is not granted, the physical access control unit 20 does not send a signal to the door lock 25 and the door lock 25

- 10 -

therefore remains in a locked state, thereby preventing the person from passing through the access point 24 and into the area. The decision whether to grant or deny access may also be based on the time and/or date that the access attempt occurred. For example, users may be allocated different dates and/or times when access is permitted, and the physical access control unit 20 arranged to allow access only at the allocated dates/times.

10

In this example, the credential reader 26 is in the form of a biometric reader arranged to gather biometric data from a person, such as fingerprint data, although it will be understood that other types of credential reader are envisaged, such as a card reader arranged to read a personal identification card carried by a person, a keypad for enabling a person to enter a PIN number, or any other device arranged to determine the identity of a person.

20 While in this example the access point 24 is a door, it will be appreciated that other types of access point are envisaged, such as an elevator door, turnstile, parking gate, or any other physical barrier.

25 In this example, the access point 24 has associated sensors 27, in this example for detecting whether the access point 24 is open or closed. Any suitable sensor for this purpose is envisaged, and in this example magnetic-type proximity sensors are used.

30

The sensors 27 are connected to the physical access control unit 20, and the physical access control unit 20 monitors the sensors 27 and generates a warning signal

- 11 -

when the access point 24 is open. The warning may be used to trigger an alarm, for example in the event that a sensor 27 indicates that the physical access point 24 is open but that no valid credential verification has occurred.

An access attempt, and in particular an attempted unauthorised access event or an actual unauthorised access event, may also be determined using the camera 22, for example by automatically analysing video and/or images captured by the camera 22 at the physical access control unit 20.

In this example, the physical access control unit 20 also includes a tagging application 28 arranged to add the tag information 29 to the access information sent to the integrated access control and identity management station 16. In this example, the tag information 29 includes information indicative of the location of the physical access control arrangement 12, the date and time that the access attempt occurred, biometric information gathered from the person desiring to pass through the access point 24, and any/or other relevant information.

The tagging application 28 may source the tag information from the credential reader, from location and/or identification information stored at the access control unit 20, from location information derived from respective electronic identifiers, such as IP addresses, associated with the access control unit 20, or from any other source capable of providing tag information usable to link a physical access attempt with another access attempt. In this example, the physical access control arrangement 12 includes a location application 31 arranged to determine

- 12 -

the location of the physical access control unit 20, for example using a determined IP address related to the current location of the access control unit 20.

5 The access information indicative of the physical access attempt and associated tag information received at the integrated access control and identity management station 16 is stored in a data storage device in communication with the integrated access control and identity management
10 station 16, in this example in the form of a database 40. The database 40 includes a plurality of records 42, each of which relates to an access attempt.

The tag information is used to enable an operator to link
15 a physical access attempt with an IT access attempt.

It will be understood that the physical access control unit 20 may be implemented by a computing device, for example as a software application implemented by the
20 computing device.

The IT access control arrangement 14 includes an IT access control unit 30 arranged to control access attempts to an IT resource, gather credentials from users seeking to gain
25 access to the IT resource, compare the gathered credentials with reference credentials, grant or deny access based on the comparison and, if access is granted, determine the extent to which access should be granted.

30 The IT access control arrangement 14 is capable of receiving access attempts directly from one or more locally disposed computing devices 32, for example connected to the IT access control unit 30 through a LAN,

- 13 -

or from one or more remotely located computing devices 33 that for example connect to the IT access control unit 30 through the Internet.

- 5 Any of the computing devices 32, 33 may be connected to a credential reader 34 that enables at least one user credential to be gathered from a person desiring to gain access to the IT resource.
- 10 The credential reader may include a biometric reader arranged to gather biometric data from a person, such as fingerprint data. It will be understood, however, that other types of authentication device arranged to determine the identity of a person are envisaged, such as a card
15 reader arranged to read a personal identification card carried by a person, a keypad for enabling a person to enter a PIN number, or a conventional username/password arrangement.
- 20 The decision whether to grant or deny access and the extent to which access is granted is determined by comparing defined IT access criteria with current access criteria that may include any one or more of the gathered user credentials, the time and/or date that the access
25 attempt occurred, the duration of access, the location of the person attempting to gain access, and/or the type of data that the user desires to access. The IT access control arrangement 14 is therefore able to grant, deny or limit access to an IT resource based on who the user is,
30 where the user is, when the user attempts to gain access and what the user is attempting to access, and in this way the IT access control arrangement 14 is capable of providing a high degree of access control.

- 14 -

For example, users may be allocated different dates and/or times, or defined access time durations, when access is permitted, and the IT access control unit 30 arranged to allow access only at the allocated dates/times and/or only
5 for the defined duration.

The level of access may be determined based on the location of the person attempting to gain access, for example whether a computing device associated with the
10 person is connected to the IT access control unit 30 through a local LAN or whether the user's computing device is connected to the IT access control unit 30 through the Internet. In one embodiment, location information may be derived from the physical access control arrangement 12,
15 for example the credential reader 26, such that by gaining positive authentication using the credential reader 26, the location of the person at the physical access control unit is confirmed.

20 The level of access may be determined based on user identity information derived from credential information gathered from the user.

The level of access may be determined based on whether the
25 user has been given the authority to access particular types of data, or to access data stored in a particular location. For example, a user holding a senior position in an organisation may be authorised to access all data associated with the organisation, and a user holding a
30 junior position in the organisation may be authorised to access only data that is directly relevant to the user, for example that is stored in a folder associated with the user.

- 15 -

It will be appreciated that in the present embodiment, the physical and IT access control units 20, 30 are interfaced with each other so that information gathered by the physical access control unit 20, such as credential
5 information, may be used by the IT access control unit 30, and/or information gathered by the IT access control unit 30 may be used by the physical access control unit 20.

It will be appreciated that the access control system 10
10 is arranged such that the above access criteria are customisable such that the access criteria applicable for a user are modifiable and thereby the degree of security applied to the user is modifiable.

15 The IT access control unit 30 in this example is also arranged to add tag information 37 to the access information indicative of an access attempt that is sent to the integrated access control and identity management station 16 by the IT surveillance arrangement 14. In this
20 example, the tag information 37 includes information indicative of the location of the IT surveillance arrangement 14, the date and time that the access attempt occurred, identity information, such as biometric information, gathered from the person desiring to gain
25 access to the IT system, and/or any other relevant information.

In this example, the IT access control unit 30 also includes a tagging application 36 arranged to add the tag
30 information 37 to the access information sent to the integrated access control and identity management station 16. The tagging application may source the tag information from credential reader 26, 34, from location

- 16 -

and/or identification information stored at the IT access control unit 30, from location information derived from an electronic identifier, such as an IP address, associated with the IT access control unit 30, or from any other source capable of providing tag information usable to link the IT access attempt with another access attempt record 42.

In this example, the IT access control unit 30 may include a location application 38 arranged to determine the location of a computing device 32, 33 desiring to gain access, for example using an IP address related to the current location of the computing device 32, 33. Based on the determined location, access may be granted when the computing device 32 is in a specified area, but denied when the computing device is not in the specified area. Similarly, access may be granted or denied based on whether the location of the computing device 32, 33 is verified or not, for example based on whether the computing device 33 is connecting to the IT access control unit 30 through the Internet and whether the location of the computing device can be ascertained and the location authorised as safe.

It will be understood that the IT access control unit 30 may be implemented using a computing device, for example at least in part as a software application.

In this example, the access information indicative of the IT access attempt and associated tag information received at the integrated access control and identity management station 16 is stored in a record 42 in the database 40.

- 17 -

In this example, the physical and IT access control arrangements 12, 14 include suitable functional components to enable determinations to be made as to whether and to what extent to grant or deny access by a person based on the relevant criteria defined for a user. For this purpose, the functional components may include a processor and memory arranged to implement one or more software applications. In this example, access criteria are stored at the physical and IT access control arrangements 12, 14 and the credentials used to determine whether to grant or deny access. It will however be understood that other implementations are envisaged. For example, the access criteria may be stored and determinations as to whether to grant or deny access may be made remotely from the physical and IT access control arrangements, such as at the integrated access control and identity management station 16.

The tag information may take any suitable form, and in this example the tag information is added to the access information as metadata.

Referring to Figure 2, components of the IT access control arrangement 14 are shown. The IT access control unit 30 in this example controls access to one or more software applications 50 and/or data stored on one or more storage devices 54 by one or more user computing devices 32 disposed locally and connected to the IT access control unit 30 through a wired or wireless LAN, or one or more user computing devices 33 disposed remotely and connected to the IT access control unit 30 through the Internet 52.

In this example, the IT access control unit 30 is arranged

- 18 -

to use access criteria stored in an access matrix 56 to determine whether to grant or deny access and the extent to which access should be granted. An example access matrix 56 is shown in Figure 3 and includes user
5 information 58 indicative of the users associated with the system 10, location criteria 60 that defines the locations that are allowed for each user to access the system 10, time criteria 62 that defines the allowed times, dates, and/or durations of access for each user, trust level
10 criteria 64 that defines the type of data that the user is allowed to access in terms of the degree of sensitivity of data that the user is allowed to access, and an access level criterion 66 that defines the level of access authority granted to each user.

15

In the present example, User A is allowed to access data up to a high level of sensitivity, to access the data only when the user is located at either Secure Location A or Secure Location B, and to only access the data during
20 office hours. In addition, when User A is located at Secure Location A, the user is assigned administrator access level that provides the user with a high level of access authority. In contrast, when User A is located at Secure Location B, the user is assigned supervisor access
25 level that provides the user with a reduced level of access authority.

In the present embodiment, administrator access level provides a user with full and complete access to data such
30 that the user is able to read, write and modify data, and the user is able to execute all applications and carry out all functions with full system privileges. Supervisor access level provides a user with partial authority

- 19 -

depending on the role of the user and functions that the user is required to perform. Typically a supervisor is only able to read and write data, and sometimes is able to modify data.

5

It will be understood that since User A is allowed to access an IT resource only when the user is located at Secure Location A or Secure Location B, if an attempt to access the IT resource occurs but the location of the user is not verified, for example by confirming user credentials using a credentials reader at Secure Location A or Secure Location B, then access to the data will be denied.

10

15

Also in the present example, User C is assigned different access rights (view only, supervisory or no access) depending on whether the location of the user is verified, for example by verifying the location of the computing device associated with the user, and depending on the time of day.

20

25

It will be understood that the access matrix 56 may be arranged so that trust level criterion 64 alternatively or in addition specifically defines the type of data that the user can access in terms of the location of the data, for example the storage devices and/or data folders that the user is able to access.

30

In this example, all access attempts, both physical and IT related, are stored in the database 40 associated with the integrated access control and identity management station 16, and in this way a single accessible source is provided for information relating to all access attempts.

- 20 -

It will be understood that in this example for each access attempt, information indicative of the user attempting to access an area or resource, of the date and time that the access attempt occurred, the duration of access granted, the location of the user, and the area(s) and/or resource(s) accessed by the user are recorded in the database 40 and can therefore be used to monitor, trace and/or audit user access activities. For example, if a person attempts to access an IT resource from a particular unverified location, such as a cyber cafe, multiple times, the system 10 may be arranged to generate an alert to an operator.

In addition, the system may be arranged to modify any one or more of the access criteria defined in the access matrix 56 in response to a potential access risk situation determined from the access information stored in the database 40. For example in the above example wherein multiple access attempts occur from an unverified location, the system 10 may be arranged to modify the trust level 64 specified for the user in the access matrix 56 to a lower level, such as No Access.

In order to facilitate searching through the records 42 in the database 40, the system may include a terminal 44, for example in the form of a personal computer, tablet computer or smartphone. For this purpose, the integrated access control and identity management station 16 is arranged to allow a user terminal 44 to search records 42 relating to both physical and IT related access attempts based on potentially common variables so that related physical and IT access attempts can be identified when a physical access attempt is also accompanied by an IT

- 21 -

access attempt. In this example, the integrated access control and identity management station 16 is accessible on-line, for example through the Internet.

- 5 It will be appreciated that the tag information also allows an operator to trace back to a person associated with a physical or IT access event.

It will be appreciated that system enables administrators
10 to control access to an IT resource based on who the user is, where the user is, when the user attempts to gain access and what the user is attempting to access. The access control system provides a high degree of access control, and minimizes the possibility of an impersonation
15 attack (for example through a compromised machine or spoofing).

It will also be appreciated that unlike conventional electronic access control systems, the present access
20 control system provides the ability to control access based on the location of the user, for example using location from a physical access control system.

The present integrated access control system can be viewed
25 as a system that removes data ubiquity or enables data ubiquity to an organization. The system is able to remove ubiquity to classified data which requires stricter access control, and at the same time is able to enable ubiquity to unclassified data.

30

Modification and variations as would be apparent to a skilled addressee are deemed to be within the scope of the present invention.

- 22 -

Claims:

1. An access control system comprising:

an IT access control unit arranged to monitor
5 attempts to access an IT resource by a person; and
stored access criteria defining access rights for
each user associated with the system;
the IT access control unit arranged to determine
whether and the extent to which access should be granted
10 to a user based on the stored access criteria;
wherein the stored access criteria are arranged such
that an identity criterion indicative of the identity of
the user able to access the IT resource, a location
criterion indicative of the location from which the user
15 is allowed to access the IT resource, a time criterion
indicative of the time at which the user is allowed to
access the IT resource, a type criterion indicative of the
type of IT resource that the user is allowed to access,
and/or an access level criterion indicative of the level
20 of access authority given to the user are definable in the
stored access criteria.

2. An access control system as claimed in claim 1,
wherein the identity criterion, the location criterion,
25 the time criterion, the type criterion, and the access
level criterion are all defined in the stored access
criteria for at least one user associated with the system.

3. An access control system as claimed in claim 1 or
30 claim 2, wherein the IT resource comprises at least one
software application and/or data stored in at least one
data storage device.

- 23 -

4. An access control system as claimed in any one of claims 1 to 3, wherein the time criterion is indicative of the duration of time during which a user allowed to access the IT resource.

5

5. An access control system as claimed in any one of the preceding claims, wherein the type criterion is indicative of one or more storage locations that the user is allowed to access, and/or one or more software applications that the user is allowed to access, and/or one or more data types that the user is allowed to access.

10

6. An access control system as claimed in any one of the preceding claims, wherein the type criterion is a trust level criterion indicative of the maximum level of sensitivity of data the user is allowed to access.

15

7. An access control system as claimed in any one of the preceding claims, wherein the access level criterion is selected from a group including administrator, supervisor, view only, and no access.

20

8. An access control system as claimed in any one of the preceding claims, comprising a physical access control unit arranged to monitor attempts to access an area by a person.

25

9. An access control system as claimed in any one of the preceding claims, wherein the identity of a user is determined based on credentials gathered from the person.

30

10. An access control system as claimed in claim 9, wherein the credential information includes biometric

- 24 -

information associated with the person, identification information gathered from an identification card carried by the person, a PIN number provided by the person, or any other identification information.

5

11. An access control system as claimed in claim 8, comprising an access information storage device, the system being arranged to store in the access information storage device access information indicative of access
10 attempts monitored by the IT and physical access control units.

12. An access control system as claimed in any one of the preceding claims, wherein the system is arranged to
15 associate tag information with the access information and to store the tag information in the access information storage device, the tag information including information usable to make a determination as to whether a first access attempt monitored by the physical access control
20 unit is related to a second access attempt monitored by the IT access control unit.

13. An access control system as claimed in claim 12, wherein the tag information includes location information
25 indicative of the location of the access attempt associated with the tag information.

14. An access control system as claimed in claim 12 or claim 13, wherein the tag information includes credential
30 information indicative of at least one credential gathered from a person attempting to access an area or resource.

- 25 -

15. An access control system as claimed in any one of claims 12 to 14, wherein the tag information includes date and/or time information.

5 16. An access control system as claimed in any one of claims 12 to 15, wherein the tag information is in the form of metadata added to the access information.

10 17. An access control system as claimed in any one of claims 12 to 16, wherein the system comprises an integrated access control and identity management station in communication with the first and second access control units, the integrated access control and identity management station receiving the access information and tag information from the first and second access control units, and the integrated access control and identity management station arranged such that the access information and tag information is accessible through the integrated access control and identity management station.

20

18. An access control system as claimed in claim 17, wherein the integrated access control and identity management station is arranged so as to facilitate searching by a user through access information and/or tag information.

25

19. An access control system as claimed in claim 18, wherein the integrated access control and identity management station is accessible locally or remotely, and may be accessed through a communications network such as the Internet.

30

- 26 -

20. A method of controlling access to an IT resource by a person, the method comprising:

monitoring attempts to access an IT resource by a person; and

5 storing access criteria defining access rights for each user associated with the system;

determining whether and the extent to which access should be granted to a user based on the stored access criteria;

10 wherein the stored access criteria are arranged such that an identity criterion indicative of the identity of the user able to access the IT resource, a location criterion indicative of the location from which the user is allowed to access the IT resource, a time criterion
15 indicative of the time at which the user is allowed to access the IT resource, a type criterion indicative of the type of IT resource that the user is allowed to access, and/or an access level criterion indicative of the level of access authority given to the user are definable in the
20 stored access criteria.

21. A method as claimed in claim 20, comprising defining all of the identity criterion, the location criterion, the time criterion, the type criterion, and the access level
25 criterion in the stored access criteria for at least one user associated with the system.

22. A method as claimed in claim 20 or claim 21, wherein the IT resource comprises at least one software
30 application and/or data stored in at least one data storage device.

- 27 -

23. A method as claimed in any one of claims 20 to 22, wherein the time criterion is indicative of the duration of time during which a user allowed to access the IT resource.

5

24. A method as claimed in any one of claims 20 to 23, wherein the type criterion is indicative of one or more storage locations that the user is allowed to access, and/or one or more software applications that the user is
10 allowed to access, and/or one or more data types that the user is allowed to access.

25. A method as claimed in any one of claims 20 to 24, wherein the type criterion is a trust level criterion
15 indicative of the maximum level of sensitivity of data the user is allowed to access.

26. A method as claimed in any one of claims 20 to 25, comprising selecting the access level criterion from a
20 group including administrator, supervisor, view only, and no access.

27. A method system as claimed in any one of claims 20 to 26, comprising monitoring physical attempts to access an
25 area by a person.

28. A method as claimed in any one of claims 20 to 27, comprising determining the identity of a user based on credentials gathered from the person.

30

29. A method as claimed in claim 28, wherein the credential information includes biometric information associated with the person, identification information

- 28 -

gathered from an identification card carried by the person, a PIN number provided by the person, or any other identification information.

5 30. A method as claimed in claim 27, comprising storing access information indicative of access attempts monitored by the IT and physical access control units.

31. A method as claimed in claim 30, comprising
10 associating tag information with the access information and to storing the tag information in the access information storage device, the tag information including information usable to make a determination as to whether a first access attempt monitored by the physical access
15 control unit is related to a second access attempt monitored by the IT access control unit.

32. A method as claimed in claim 31, wherein the tag information includes location information indicative of
20 the location of the access attempt associated with the tag information.

33. A method as claimed in claim 31 or claim 32, wherein the tag information includes credential information
25 indicative of at least one credential gathered from a person attempting to access an area or resource.

34. A method as claimed in any one of claims 31 to 33, wherein the tag information includes date and/or time
30 information.

- 29 -

35. A method as claimed in any one of claims 31 to 34, wherein the tag information is in the form of metadata added to the access information.

5 36. A method as claimed in any one of claims 31 to 35, comprising:

providing an integrated access control and identity management station;

receiving at the integrated access control and
10 identity management station the access information and tag information; and

facilitating access to the access information and tag information through the integrated access control and identity management station.

15

37. A method as claimed in claim 36, comprising facilitating searching by a user through access information and/or tag information.

20 38. A method as claimed in claim 37, comprising facilitating access to the integrated access control and identity management station locally or remotely through a communications network.

25 39. A method as claimed in any one of claims 20 to 38, comprising using the access information and/or the tag information to trace back to a person associated with an access attempt.