

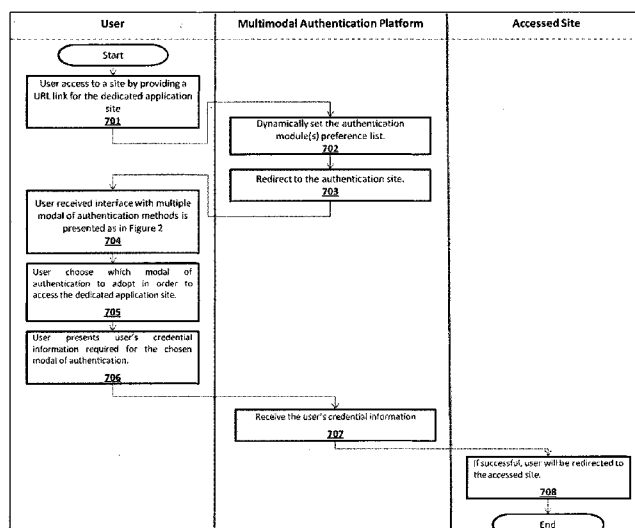


- (51) **International Patent Classification:**
H04L 29/06 (2006.01)
- (21) **International Application Number:**
PCT/MY2013/000124
- (22) **International Filing Date:**
5 July 2013 (05.07.2013)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
PI 2012003211 13 July 2012 (13.07.2012) MY
- (71) **Applicant:** MIMOS BERHAD [MY/MY]; Technology Park Malaysia, 57000 Kuala Lumpur (MY).
- (72) **Inventors:** NG, Kang Siong; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). GALOH, Rashidah Haron; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). WONG, Hon Loon; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). DHARMADHARSHNI, Maniam; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). SEA, Chong Seak; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). NOR, Izyani Daud; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY).
- (74) **Agent:** MIRANDAH, Patrick; Patrick Mirandah Co. (malaysia) SDN BHD, Suite 3B-19-3 Plaza Sentral, Jalan Stesen Sentral 5, 50470 Kuala Lumpur (MY).
- (81) **Designated States** (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) **Designated States** (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) **Title:** A SYSTEM AND METHOD FOR MULTIMODAL AUTHENTICATION PLATFORM

700



(57) **Abstract:** The system and method of the present invention provides multimodal authentication platform as a front channel (100, 300) for user to access a particular application site with security intact. The system of the present invention comprising at least one user (101); at least one authentication gateway (105) and at least one authentication server (102). The at least one authentication server (102) comprising at least one user registration module (302); at least one user profile module (303); at least one manage authentication module (301); and at least one authentication database interface (304). The methodology of the present invention comprises steps of accessing application site by providing URL link (701); setting authentication module (s) for user access based on authentication module (s) preference list (702); redirecting user to authentication site (703); providing interface with multimodal authentication platform (704); selecting modal of authentication to access application site (705); presenting user credential information required for selected modal of authentication (706); authenticating user based on user credentials (707); and granting user access to application site upon successful authentication (708).

**Declarations under Rule 4.17:**

- | | |
|--|--|
| — as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) | — before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h)) |
|--|--|

Published:

- with international search report (Art. 21(3))

A SYSTEM AND METHOD FOR MULTIMODAL AUTHENTICATION PLATFORM

FIELD OF INVENTION

- 5 The present invention relates to a system and method for authentication by providing multimodal authentication platform as a front channel for user to access a particular application site with security intact.

BACKGROUND ART

10

Multiple authentication methods are available, for example username and password, certificate and biometric. The similarity between these authentication methods is the capability in providing a unique identity to represent user, as such only the user is indeed, the user claims to be. Traditionally, system will present a challenge for user authentication. The challenge may involve one or more factors of authentication as user will need to provide a valid respond to have access to the system.

15

At present, current authentication issues arises wherein user has to handle multiple authentications and identities in order to access different applications. Authentication method is handled solely by the application. Application 'A' is using '1' type of authentication method and application 'B' is using another, '2' type of authentication method. In result, different authentication methods are adapted in order to login to various applications. In addition, user is unable to select user's preferred authentication method for specific application in accordance to its security intensity.

20 Authentication method is fixed by the application. Application 'A' is using '1' type of authentication method. But user insists in using '2' type of authentication method. In result, user is forced to use '1' type of authentication method in order to access the application.

25

30 User is also unable to select user's preferred dynamic authentication method in accessing an application. Authentication method is fixed by the application. In case where capability of multi level and factors authentication method is turned on for the application, the next level of authentication method is fixed by the application. In result, to re-authenticate a user, user is forced to use a fixed authentication method.

User is unable to select user's preferred dynamic authentication method in accessing an application. Authentication method is fixed by the application. The adaptive authentication method is fixed by the application where capability of adaptive authentication is turned on for the application.

5

The present invention proposes a system and method to allow users to access a particular application site with multiple modal of authentication methods as valid user's access accounts is proposed. User will be presented with a centralized multimodal authentication as a front channel in accessing any application site. The method
10 includes presenting the multimodal authentication interface to user before accessing any application site; receiving user credentials and authenticates the user and granting user access to the application site, provided that the authentication is successful. The present invention allows and re-enforce security in selection of authentication mechanism by allowing system preference of multi modal
15 authentication to precede the user preference.

The subject matter claimed herein is not limited to embodiments that solve any disadvantages or that operate only in environments such as those described above. Rather, this background is only provided to illustrate one exemplary technology area
20 where some embodiments described herein may be practice.

SUMMARY OF INVENTION

The present invention provides a system and method for authentication by providing multiple multimodal authentication platform (100,300) as a front channel for user to access a particular application site with at least one user (101); at least one authentication gateway (105) and at least one authentication server (102). The at least one authentication server (102) comprising at least one user registration module (302); at least one user profile module (303); at least one manage authentication module (301); and at least one authentication database interface (304).

Another aspect of the present invention provides for at least one authentication gateway (105) wherein said authentication page and framework (100, 300) having means for providing multimodal authentication method for accessing a particular application site; presenting selected authentication module (s) as a front channel in accessing a protected application site; supporting multiple level and factors of authentication based on available methods; providing method to request additional authentication method; providing method to add user registration module; providing method to add user profiling module; and providing method to maintain user account module.

A further aspect of the present invention provides for at least one authentication gateway (105) wherein said authentication server (102) further comprises of at least one interface; said interface having means for displaying multiple iconic interfaces set in accordance to either user or system preference. The at least one interface is user configurable in which user can dynamically select any multiple authentication method set to user preference. Further, the at least one interface is system configurable in which system can presets user selection of multiple authentication method.

A further aspect of the present invention provides for at least one user registration module (302) wherein said user registration module further comprises of at least one interface. The at least one interface having means for selecting default authentication method based on user preference for user registration; submitting user identification; entering any unique identification based on chosen authentication method; re-entering unique identification for verification; confirming registration for validation; and storing user registration information.

Another aspect of the present invention provides for at least one user profile module (303) wherein said user profile module further comprises of at least one interface. The at least one interface having means for selecting default authentication method based on user preference for authentication; selecting only or multiple authentication method (s) based on user preference for authentication; selecting order of authentication method based on user preference for authentication; submitting Media Access Control (MAC) address of machines used to trigger another level of authentication; submitting any unique user information used to trigger another level of authentication; and storing user profile information.

A further aspect of the present invention provides for at least one manage authentication module (301) wherein said manage authentication module further comprises of at least one interface. The at least one interface having means for updating each of available authentication method (s) that associates to user account; and storing user authentication maintenance information. Further, the present invention provides for at least one authentication database interface (304) having means for user registration, profile and maintenance of user account.

Another aspect of the present invention provides for a method for authentication by providing multimodal authentication platform as a front channel to access a particular application site. The method comprising steps of accessing application site by providing URL link (701); setting authentication module (s) for user access based on authentication module (s) preference list (702); redirecting user to authentication site (703); providing interface with multimodal authentication platform (704); selecting modal of authentication to access application site (705); presenting user credential information required for selected modal of authentication (706); authenticating user based on user credentials (707); and granting user access to application site upon successful authentication (708).

A further aspect of the present invention provides the methodology for setting authentication module (s) for user access based on authentication module (s) preference list. The said method comprises steps of extracting authentication module (s) provided by application site (802); grouping and ranking extracted authentication module (s) based on its security intensity (804); setting current authentication module (s) as L1, S1

(806); checking availability of any authentication module (s) set by authentication server (808); removing authentication module (s) in L1, S1 against any risk factor when no authentication module is set by authentication server (810); adding unlisted authentication module (s) in L1, S1 for any known risk factor (812); setting current authentication module (s) as L2, S2 (814); checking availability of any flag to adopt user profiles for the adaptive or next level of authentication (816); adding elements of user profiles in L2, S2 when there are flags to adopt user profiles for the adaptive or next level of authentication (818); setting current authentication module (s) as L3, S3 (820); checking availability of authentication module (s) set by user (822); grouping and ranking extracted authentication module (s) set by user based on security intensity (824); ranking extracted authentication module (s) against L3, S3 by group (826); ranking extracted authentication module (s) against L3, S3 by sub group (828); setting current authentication module (s) as L4, S4 (830); and presenting selected authentication module (s) as a front channel in accessing a protected application site (832).

Another aspect of the present invention provides for checking availability of any authentication module (s) set by authentication server (808) which further comprises of directly setting current authentication module (s) as L2, S2 when no authentication module (s) are set by authentication server (814) while checking availability of any flag to adopt user profiles for the adaptive or next level of authentication (816) further comprises directly setting current authentication module (s) as L3, S3 when there is no flag to adopt user profiles for the adaptive or next level of authentication (820) and checking availability of authentication module (s) set by user (822) further comprises directly setting current authentication module (s) as L4, S4 when no authentication module (s) are set by user (830).

The present invention consists of features and a combination of parts hereinafter fully described and illustrated in the accompanying drawings, it being understood that various changes in the details may be made without departing from the scope of the invention or sacrificing any of the advantages of the present invention.

BRIEF DESCRIPTION OF ACCOMPANYING DRAWINGS

To further clarify various aspects of some embodiments of the present invention, a more particular description of the invention will be rendered by references to specific
5 embodiments thereof, which are illustrated in the appended drawings. It is appreciated that these drawings depict only typical embodiments of the invention and are therefore not to be considered limiting of its scope. The invention will be described and explained with additional specificity and detail through the accompanying drawings in which:

10 FIG. 1.0 illustrates the integration module of the present invention.

FIG. 2.0 illustrates the authentication interface as a Front Channel of the present invention.

15 FIG. 3.0 illustrates the integrated modules in Authentication Server.

FIG. 4.0 illustrates the determining factors of multimodal authentication.

FIG. 5.0 illustrates the ranking of authentication module(s).

20

FIG. 6.0 illustrates the example flow of authentication module(s) list of preference.

FIG. 7.0 is a flowchart illustrating user authenticates to the Application Site Flow.

25 FIG. 8.0 is a flowchart illustrating the setting up authentication module(s) for user access.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention provides a system and method for authentication by providing multiple multimodal authentication platform as a front channel for user to access a particular application site. Hereinafter, this specification will describe the present invention according to the preferred embodiments. It is to be understood that limiting the description to the preferred embodiments of the invention is merely to facilitate discussion of the present invention and it is envisioned without departing from the scope of the appended claims.

Reference is first being made to FIG. 1.0 and FIG. 2.0 respectively. FIG. 1.0 illustrates the integration module of the present invention while FIG. 2.0 illustrates the authentication interface as a Front Channel of the present invention. As illustrated in FIG. 1.0, (101), represents a user. A user is accessing an Application Site #1.....Site n, (106), commonly via web browser. The Authentication Gateway (105) shall forward user's access request to Authentication Server (102) in order to access to the Application Site #1 (106), which is the secure content. The Authentication Gateway (105) will communicate with the Authentication Server (102) regarding user authenticity information. If the user has not been authenticated, the Authentication Server (102) will perform user authentication and present an authentication site interface as illustrated in FIG. 2.0. If the user has been authenticated, Authentication Gateway (105) will received user authentication information and proceeds with the authorization process. Authentication database (103) is the database to store user information with the following support authentication module. Authentication module (104) is an example to identify user with the authentication module supported to access the Application Site #1.....Site n (106).

As illustrated in FIG. 2.0, (201) represents the multimodal authentication platform. The interface will consist of at least a display of multiple authentication method that is available to user. The interface preferably consists of multiple iconic interfaces where one iconic interface represents one authentication method. (202) is a link for user to register as a new user which may also exist by its own dedicated interface while (203) is for user to manage the account, which include setting for the default for authentication module and setting for user information and profile. The interface may also exist by its

own dedicated interface. (204) is an optional interface where a user can scroll to the left and to the right, to browse the entire series of available authentication module. In adding a new module of authentication, it will create one new icon in the series of authentication module.

5

Reference is now being made to FIG. 3.0. FIG. 3.0 illustrates the integrated modules in Authentication Server of the present invention. The present invention provides a system (100, 300) for authentication by providing multimodal authentication platform as a front channel to access a particular application site (106) with at least one user (101); at least one authentication gateway (105) and at least one authentication server (102). The at least one authentication server (102) comprising at least one user registration module (302); at least one user profile module (303); at least one manage authentication module (301); and at least one authentication database interface (304). The at least one manage authentication module (304) provides a direct communication interface to the Authentication Database (103).

15

The at least one authentication page and framework (100, 300) having means for providing multimodal authentication method for accessing a particular application site; presenting selected authentication module (s) as a front channel in accessing a protected application site; supporting multiple level and factors of authentication based on available methods; providing method to request additional authentication method; providing method to add user registration module; providing method to add user profiling module; and providing method to maintain user account module. The at least one authentication server (102) further comprises of at least one interface; said interface having means for displaying multiple iconic interfaces set in accordance to either user or system preference and the at least one interface is user configurable in which user can dynamically select any multiple authentication method set to user preference. The at least one interface is also system configurable in which system can presets user selection of multiple authentication method.

20

25

30

Further, as illustrated in FIG. 3.0, the at least one user registration module (302) further comprises of at least one interface. The said interface having means for selecting default authentication method based on user preference for user registration; submitting user identification; entering any unique identification based on chosen authentication method;

re-entering unique identification for verification; confirming registration for validation; and storing user registration information.

5 The at least one user profile module (303) further comprises of at least one interface wherein said interface having means for selecting default authentication method based on user preference for authentication; selecting only or multiple authentication method (s) based on user preference for authentication; selecting order of authentication method based on user preference for authentication; submitting Media Access Control (MAC) address of machines used to trigger another level of authentication; submitting any
10 unique user information used to trigger another level of authentication; and storing user profile information.

The at least one manage authentication module (301) further comprises of at least one interface having means for updating each of available authentication method (s) that
15 associates to user account; and storing user authentication maintenance information. In addition, the at least one authentication database interface (304) having means for user registration, profile and maintenance of user account.

Reference is now being made to FIG. 4.0 and FIG. 5.0 respectively. FIG. 4.0 illustrates
20 the determining factors of multimodal authentication while FIG. 5.0 illustrates the ranking of authentication module(s). User shall be presented with multimodal authentication interface and have access to the numbers of authentication methods. The authentication methods available to user are set by user's preferences to be authenticated. In addition, the number of authentication methods presented to a user can be controlled by the
25 determining factors as illustrated in FIG. 4.0.

As illustrated in FIG. 4.0, the Application Site (401) is the first determining factor in setting up the list of authentication methods and its sequence order (L1, S1). The application site will determine its authentication methods for application site that has high
30 security risk and demand for high security requirement which will adopt a high authentication method(s). For example, a financial site will require high authentication method. The financial site will set a policy that it will not support username and password for its authentication method. In this case, (L1, S1) is preferably to be biometric, certificate, and short message service (SMS) mobile, as its authentication method.

The module authentication gateway (105) shall be configured to accept the (L1, S1). If the list is empty, the application site will adopt authentication methods that are determined by the next factor (i.e. the Risk Factor (402)).

- 5 The second determining factor (i.e. the Risk Factor (402)) in setting up the list of authentication methods and its sequence order (L2, S2) will include security risk that is based on security event or knowledge base. For example, for security event, if the HTTP request is coming from the internet protocol address or location that is a victim of hacking activities, it will immediately stop the request. For the knowledge base example,
- 10 if the authentication method contains unavoidable security breach, then the authentication method will be discarded in the list. In this case, from the value of (L1, S1) above, if the certificate has been compromised either by its signing algorithm or any other factor, (L2, S2) the value is biometric and short message service (SMS) mobile as its authentication method. The module authentication server (102) shall be configured to
- 15 accept the (L2, S2) updating the previous list of authentication method and its sequence order (L1, S1). The next factor, (i.e. User Profile (403)) will determine the authentication method(s) if the list is empty.

- User Profile (403) is the third determining factor in setting up the list of authentication
- 20 methods and its sequence order (L3, S3). It is based on user usage history of the authentication system. It automates the collection of user information and creates user profiles for each user. This will includes user internet protocol address, the time of login and etc. The user profiles information will contributes to the adaptive authentication method. The module authentication server (102) shall be configured to accept the (L3,
- 25 S3) updating the previous list of authentication method and its sequence order (L2, S2). The next factor, user preference (404) will determine the authentication method(s) if the list is empty.

- The final determining factor lies in the User Preference (404) in setting up the list of
- 30 authentication methods and its sequence order (L4, S4) which is based on user preference of the authentication system. User will have an option to select user's preferred authentication mechanism. If user's preferred authentication mechanism is not listed in L4, then user preference is discarded. If user set the user's preference than comparison should be made to the current list of preference set in L3, S3. The decision
- 35 of ranking is based on the strength of authentication module(s) as illustrated in FIG. 5.0.

The module authentication server (102) shall be configured to accept the (L4, S4). If the list is empty, the authentication can adopt any available method to the user.

As illustrated in FIG. 5.0, the ranking of the authentication module(s) are preferably to be based on measurement of authentication strength. There are two ways ranking is performed. Ranking is performed via group (501) and via subgroup (502). As for ranking via group (501), the group is characterized as Highest, Intermediate, Low and Zero security. Ranking via subgroup (502) will proceed upon completion of ranking via group (501). The example of the subgroup ranking is certificate of key size, username and password.

Reference is now being made to FIG. 6.0. FIG. 6.0 illustrates the example flow of authentication module(s) list of preference. As illustrated in FIG. 6.0, Flow #1 represents a sample flow where user preference of authentication module(s) precedes the system preference while Flow #2, represents a sample flow where system preference of authentication module(s) precedes the user preference.

For Flow #1, Application site does not set any minimum security authentication module(s). Hence, no preference list of authentication modules resides in L1, S1. The next flow is to check whether any risk factors are identified before proceeding to the next action. In this example we have identified that the risk factor is a certificate based authentication with 512 as its key size. The preference list is updated to L2, S2 (¬Certificate 512). Thereafter, the next flow is to check whether the authentication request adopts an adaptive or next level of authentication. The preference list is updated to L3, S3 (¬Certificate 512) if authentication request does not adopt an adaptive or next level of authentication. The final flow is to check whether user has a set of preference list for authentication. In this example, user has set username and password. Thus, the preference list is updated to L4, S4 (¬Certificate 512, username & password).

For Flow #2, Application site does set minimum security authentication module(s). Hence, L1, S1 is set to Certificate, SMS mobile, OTP. For the risk factor, it limits the authentication module to accept certificate based authentication higher than 512 key size, which set up the list to L2, S2 (Certificate > 512, SMS mobile, OTP). For user profiles, it adopts the adaptive authentication which adds checking for IP address for user. The final flow will check the security intensity of the authentication module set by

user and the L3,S3, which results in L4,S3 (Certificate > 512, SMS Mobile, OTP, IP address).

Reference is now being made to FIG. 7.0 and FIG. 8.0 respectively. FIG. 7.0 is a flowchart illustrating authentication of user to the Application Site Flow while FIG. 8.0 is a flowchart illustrating the setting up of authentication module(s) for user access. As illustrated in FIG. 7.0, user access to a site by providing a URL link for the dedicated application site (701). Thereafter, the multimodal authentication platform dynamically sets the authentication module (s) for user access based on authentication module (s) preference list (702) and redirects user to the authentication site (703).

As illustrated in FIG. 8.0, the methodology of setting authentication module (s) for user access based on authentication module (s) preference list (702) further comprises steps of extracting authentication module (s) provided by application site (802); grouping and ranking extracted authentication module (s) based on its security intensity (804); setting current authentication module (s) as L1, S1 (806); and checking availability of any authentication module (s) set by authentication server (808). The authentication module (s) in L1, S1 is removed against any risk factor when no authentication module is set by authentication server (810). Thereafter, unlisted authentication module(s) are added in L1, S1 for any known risk factor (812); and current authentication module(s) are set as L2, S2 (814). The method for checking availability of any authentication module (s) set by authentication server (808) further comprises directly setting current authentication module (s) as L2, S2 when no authentication module (s) are set by authentication server (814).

Thereafter, the said method proceeds by checking the availability of any flag to adopt user profiles for the adaptive or next level of authentication (816) and elements of user profiles are added in L2, S2 when there are flags to adopt user profiles for the adaptive or next level of authentication (818). Current authentication module(s) are set as L3, S3 (820). The method for checking availability of any flag to adopt user profiles for the adaptive or next level of authentication (816) further comprises directly setting current authentication module (s) as L3, S3 when there is no flag to adopt user profiles for the adaptive or next level of authentication (820).

The said method accordingly proceeds by checking the availability of authentication module (s) set by user (822) by grouping and ranking extracted authentication module (s) set by user based on security intensity (824) when authentication module (s) are set by user. Thereafter, the extracted authentication modules (s) are ranked against L3, S3 by group (826) and extracted authentication module (s) are ranked against L3, S3 by sub group (828). Current authentication modules (s) are accordingly set as L4, S4 (830). Alternatively, upon checking the availability of authentication module (s) set by user (822) and it is confirmed that authentication module (s) are not set by user, current authentication module (s) are directly set as L4, S4. Selected authentication module(s) are presented as a front channel in accessing a protected application site (832). The current authentication module(s) are set as per progress. For example L1, S1 is updated with the information from the application site while L2, S2 is updated based on risk factors. L3, S3 is added based on user profile and L4, S4 is updated based on user preference.

Upon redirecting user to authentication site, user receives interface with multimodal authentication platform (704) as described and illustrated in FIG. 2.0. Thereafter, user selects modal of authentication to access application site (705) and presents user credential information required for selected modal of authentication (706) and user is authenticated based on user credentials (707). Access is granted to a user to access to the application site upon successful authentication (708).

The system and method of the present invention for authentication provides multimodal authentication platform as a front channel for user to access a particular application site with security intact. The present invention is user configurable in which user can dynamically select any multiple authentication method set to user preference. Alternatively, the present invention is system configurable in which system can preset user selection of multiple authentication method. The present invention allows and reinforce security in selection of authentication mechanism by allowing system preference of multi modal authentication to precede the user preference.

The present invention may be embodied in other specific forms without departing from its essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore

indicated by the appended claims rather than by the foregoing description. All changes, which come within the meaning and range of equivalency of the claims, are to be embraced within their scope.

CLAIMS

1. A system (100, 300) for authentication by providing multimodal authentication platform as a front channel to access a particular application site (106) with at least one user (101); at least one authentication gateway(105) and at least one authentication server (102);

wherein the said authentication server (102) comprising:

at least one user registration module (302);

at least one user profile module (303);

at least one manage authentication module (301); and

at least one authentication database interface (304)

characterized in that

the said manage authentication module (301) further comprises of

at least one interface having means for selecting default authentication based on user preference for user registration and authentication wherein said interface is system configurable in which system can presets user selection of multiple authentication method.

2. A system (100) according to Claim 1, wherein the at least one authentication gateway (105) having means a support multiple level and factors of authentication based on multimodal authentication to add user registration module, profiling module and user account module.

3. A system (100) according to Claim 1, wherein the at least one authentication server (102) further comprises of at least one interface; said interface having means for displaying multiple iconic interfaces set in accordance to either user or system preference.

4. A system (100) according to Claim 3, wherein the at least one interface is user configurable in which user can dynamically select any multiple authentication method set to user preference.

5. A system (300) according to Claim 1, wherein the at least one user registration module (302) comprises of at least one interface for selection default authentication based on user preference further comprises:

submission the user identification;
entering any unique identification based on chosen authentication
method;
re-entering unique identification for verification;
confirming registration for validation; and
storing user registration information.

6. A system (300) according to Claim 1, wherein the at least one user profile module (303) comprises of at least one interface for selection default authentication based on user preference further comprises:

selecting only or multiple authentication method (s) based on user
preference for authentication;
selecting order of authentication method based on user preference for
authentication;
submitting Media Access Control (MAC) address of machines used to
trigger another level of authentication;
submitting any unique user information used to trigger another level of
authentication; and
storing user profile information.

7. A method (700) for authentication by providing multimodal authentication platform as a front channel to access a particular application site; the method comprising steps of:

accessing application site by providing URL link (701);
setting authentication module (s) for user access based on authentication
module (s) preference list (702);
redirecting user to authentication site (703);
providing interface with multimodal authentication platform (704);
selecting modal of authentication to access application site (705);
presenting user credential information required for selected modal of
authentication (706);

authenticating user based on user credentials (707); and
granting user access to application site upon successful authentication
(708)

characterized in that

5 setting authentication module (s) for user access based on authentication
module (s) preference list (702) further comprises steps of:

checking availability of any authentication module (s) set by
authentication server (808);

10 removing authentication module (s) in L1, S1 against any risk
factor when no authentication module is set by authentication
server (810);

adding unlisted authentication module (s) in L1, S1 for any known
risk factor (812);

setting current authentication module (s) as L2, S2 (814);

15 checking availability of any flag to adopt user profiles for the adaptive or
next level of authentication (816);

adding elements of user profiles in L2, S2 when there are flags to
adopt user profiles for the adaptive or next level of

authentication (818);

20 setting current authentication module (s) as L3, S3 (820);

checking availability of authentication module (s) set by user (822);

grouping and ranking extracted authentication module (s) set by
user based on security intensity (824);

25 ranking extracted authentication module (s) against L3, S3 by
group (826);

ranking extracted authentication module (s) against L3, S3 by sub
group (828);

setting current authentication module (s) as L4, S4 (830); and

30 presenting selected authentication module (s) as a front channel
in accessing a protected application site (832).

8. A method according to Claim 7 wherein checking availability of any
authentication module (s) set by authentication server (808) further comprises

directly setting current authentication module (s) as L2, S2 when no authentication module (s) are set by authentication server (814).

- 5 9. A method according to Claim 7, wherein checking availability of any flag to adopt user profiles for the adaptive or next level of authentication (816) further comprises directly setting current authentication module (s) as L3, S3 when there is no flag to adopt user profiles for the adaptive or next level of authentication (820).
- 10 10. A method according to Claim 7, wherein checking availability of authentication module (s) set by user (822) further comprises directly setting current authentication module (s) as L4, S4 when no authentication module (s) are set by user (830).

1/6

100

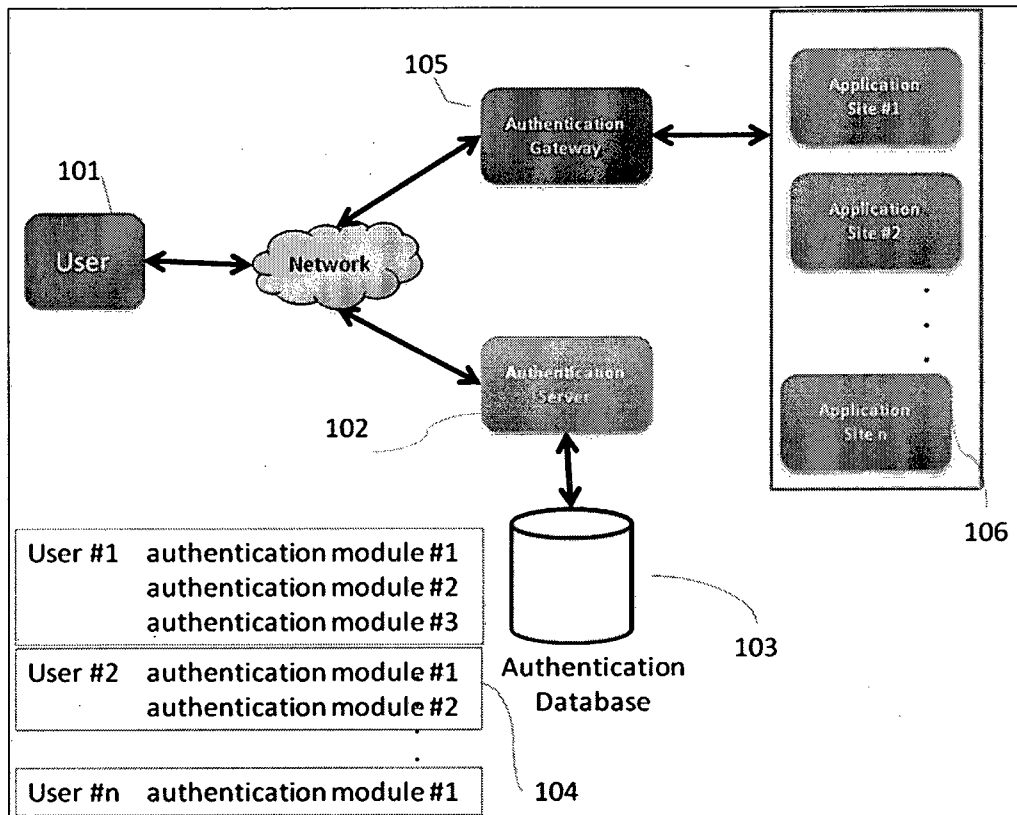


FIG. 1

200

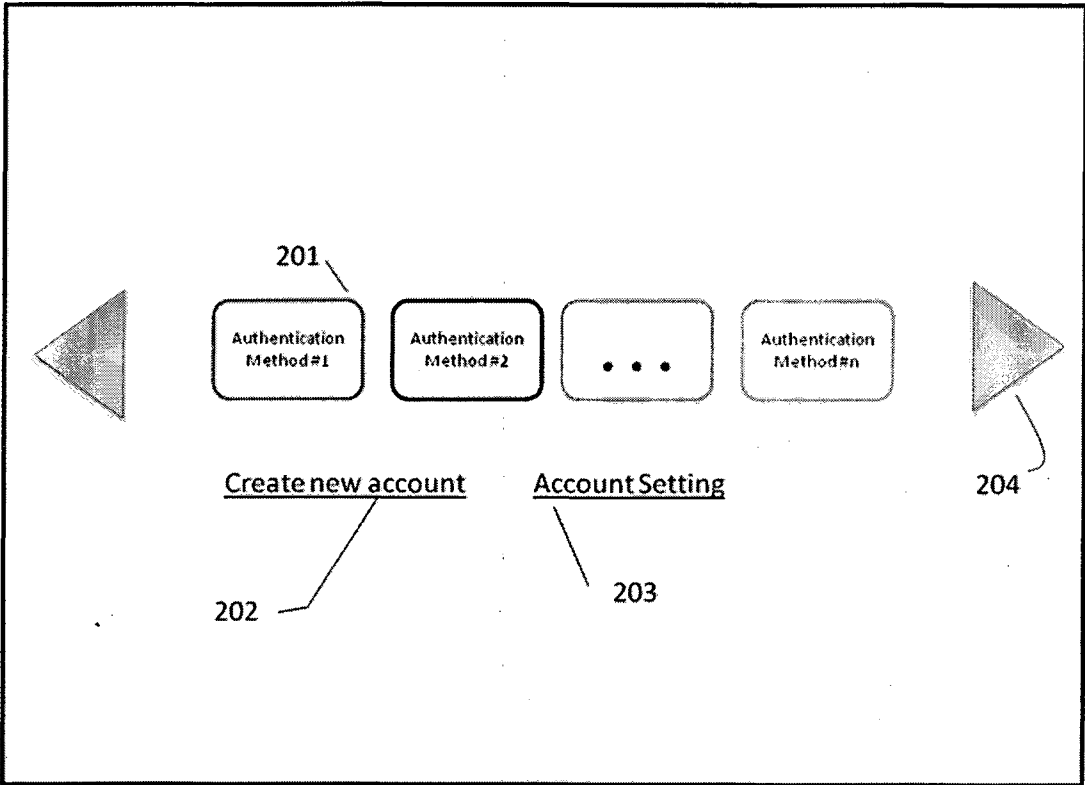


FIG. 2

3/6

300

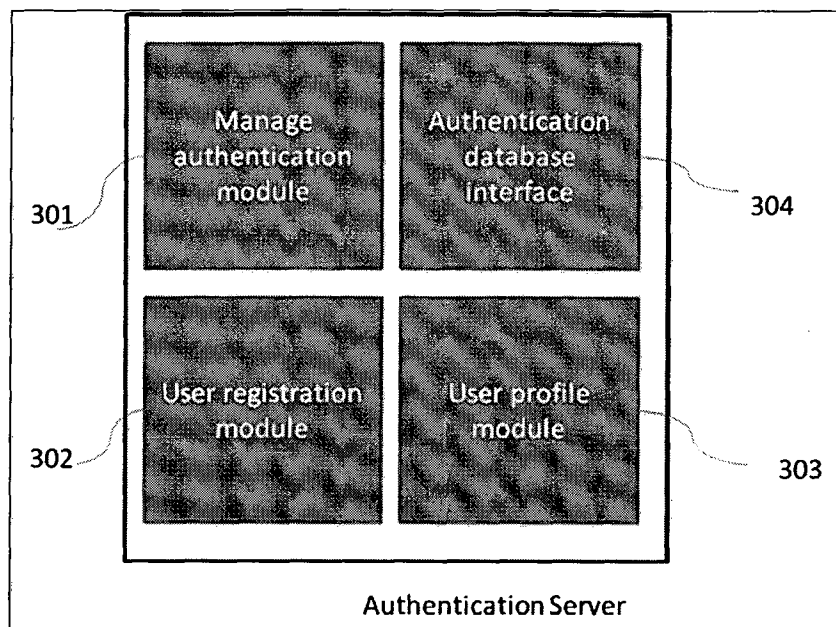


FIG. 3

400

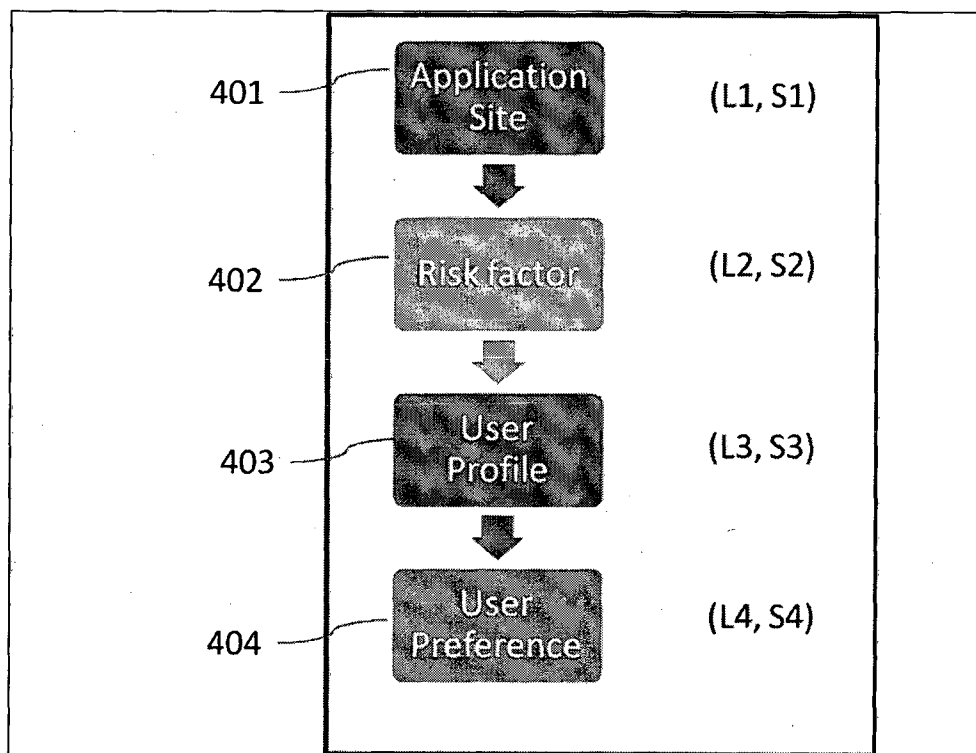


FIG. 4

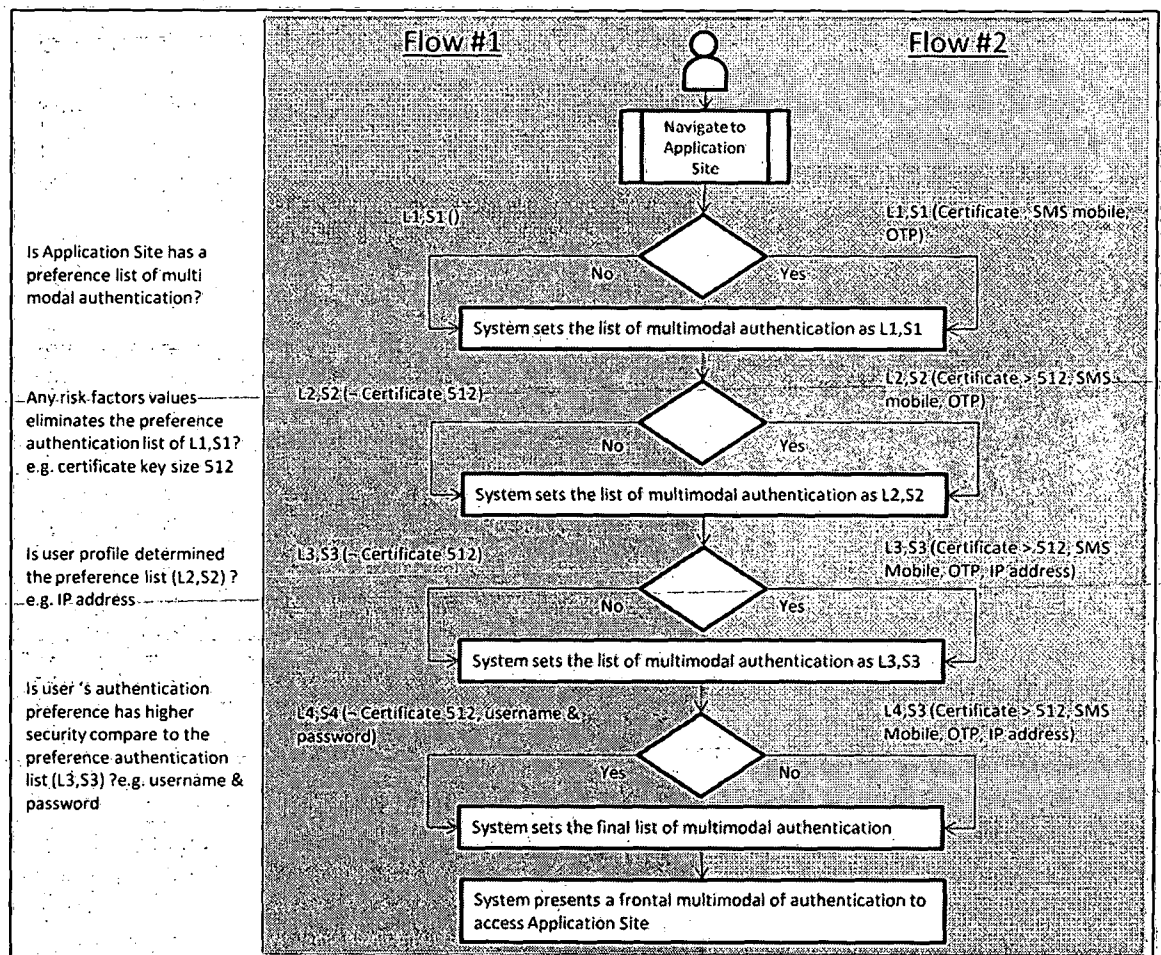
4/6

500

	Authentication Group	Authentication Module(s)	
501 Ranking via group	Highest	Multi factor authentication, biometric	502 Ranking via subgroup
	Intermediate	Hardware Token - Smart card, Mobile, One time password	
	Low	Software Token - Software certificate, Username and password	
	Zero	No authentication method implemented	

FIG. 5

600



5/6

700

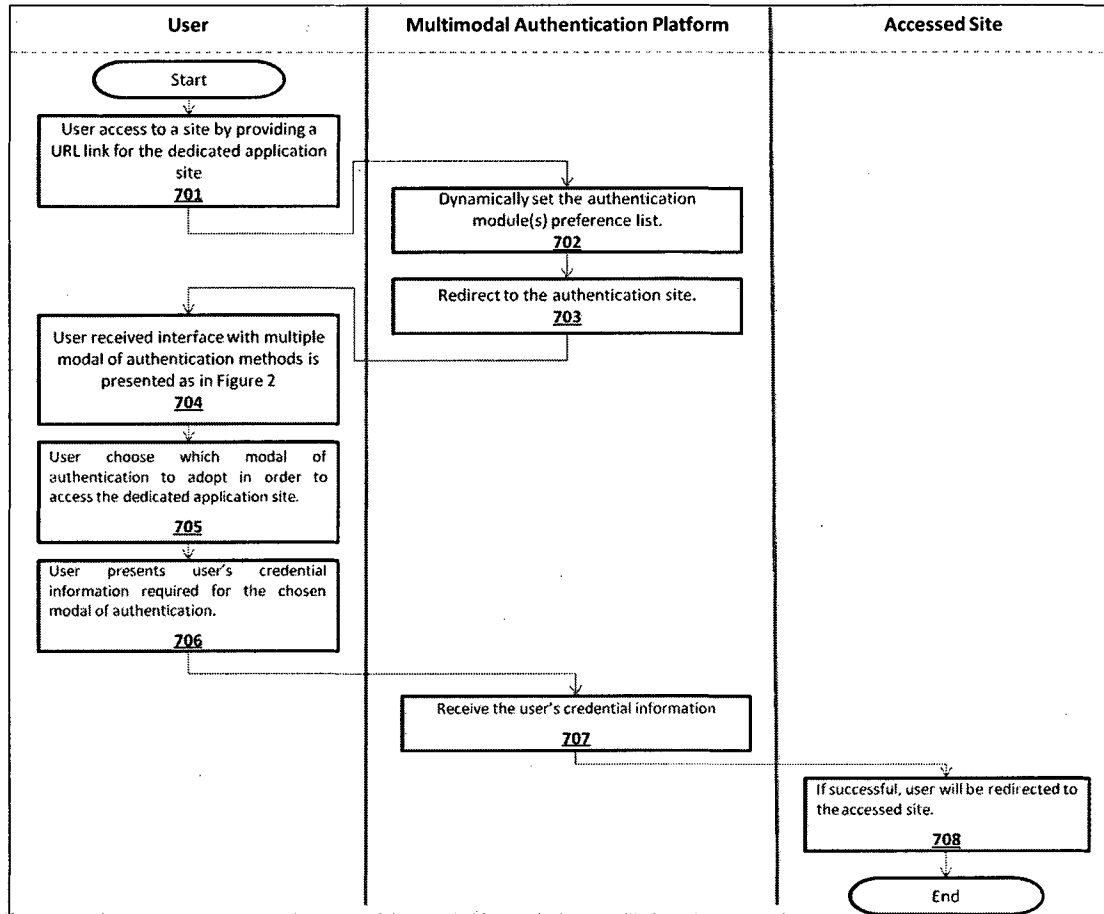


FIG. 7

6/6

800

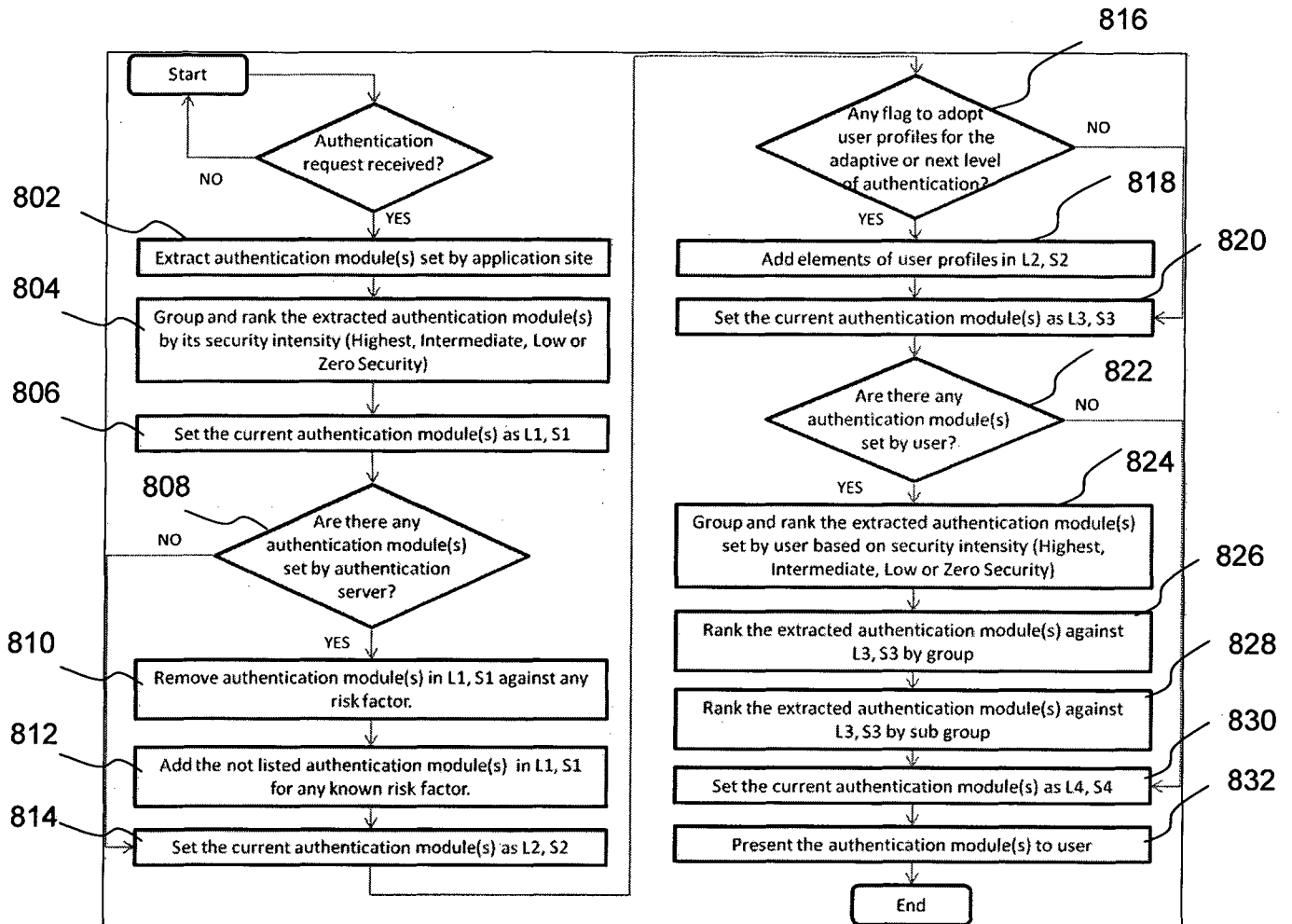


FIG. 8

INTERNATIONAL SEARCH REPORT

International application No
PCT/MY2013/000124

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EP0-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2011/047608 A1 (LEVENBERG RICHARD [US]) 24 February 2011 (2011-02-24) paragraph [0014] - paragraph [0057] figures 1,5	1-10
X	US 2002/087894 A1 (FOLEY JAMES M [US] ET AL FOLEY JAMES [US] ET AL) 4 July 2002 (2002-07-04) paragraph [0010] paragraph [0025] - paragraph [0041] paragraph [0050] figure 5	1-10



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

2 December 2013

Date of mailing of the international search report

10/12/2013

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Olaechea, Javier

INTERNATIONAL SEARCH REPORT

International application No
PCT/MY2013/000124

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Luís Miranda ET AL: "Context-aware multi-factor authentication", Repositorio Institucional da FCT-UNL, 24 September 2010 (2010-09-24), XP055091109, PT Retrieved from the Internet: URL:http://hdl.handle.net/10362/4111 [retrieved on 2013-12-02] Sections 4 and 5	1-10
A	----- US 2008/155662 A1 (VYKUNTA VENKATESWARA R [US]) 26 June 2008 (2008-06-26) paragraph [0021] - paragraph [0036] -----	1-10

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/MY2013/000124

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011047608 A1	24-02-2011	NONE	

US 2002087894 A1	04-07-2002	US 2002087894 A1	04-07-2002
		US 2011197074 A1	11-08-2011
		US 2011197265 A1	11-08-2011
		US 2011202978 A1	18-08-2011
		US 2013019287 A1	17-01-2013

US 2008155662 A1	26-06-2008	NONE	
