(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
04 June 2020 (04.06.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/111929 A1

(51) International Patent Classification:
G06Q 10/00 (2006.01) *G06Q 10/06* (2012.01)

(21) International Application Number:
PCT/MY2019/050085

(22) International Filing Date:
11 November 2019 (11.11.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI 2018002262 30 November 2018 (30.11.2018) MY

(71) Applicant: **MIMOS BERHAD** [MY/MY]; Technology Park Malaysia, Kuala Lumpur, 57000 (MY).

(72) Inventors: **ILYAS, Zanawiyah**; c/o Mimos Berhad, Technology Park Malaysia, Kuala Lumpur, 57000 (MY). **ISMAIL, Tengku Fatimah Roslina**; c/o Mimos Berhad, Technology Park Malaysia, Kuala Lumpur, 57000 (MY). **CHE MAT, Rahayya**; c/o Mimos Berhad, Technology Park Malaysia, Kuala Lumpur, 57000 (MY).

(74) Agent: **MIRANDAH ASIA (MALAYSIA) SDN BHD**; Suite 3B-19-3, Plaza Sentral, Jalan Stesen Sentral 5, Kuala Lumpur, 50470 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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, SA, 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, ST, 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).

Declarations under Rule 4.17:
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
— *of inventorship (Rule 4.17(iv))*

(54) **Title:** SYSTEM AND METHOD FOR STEERING A HELPDESK SUPPORT FOR ACCESSING AN EXTERNAL SYSTEM IN HELPDESK SYSTEM

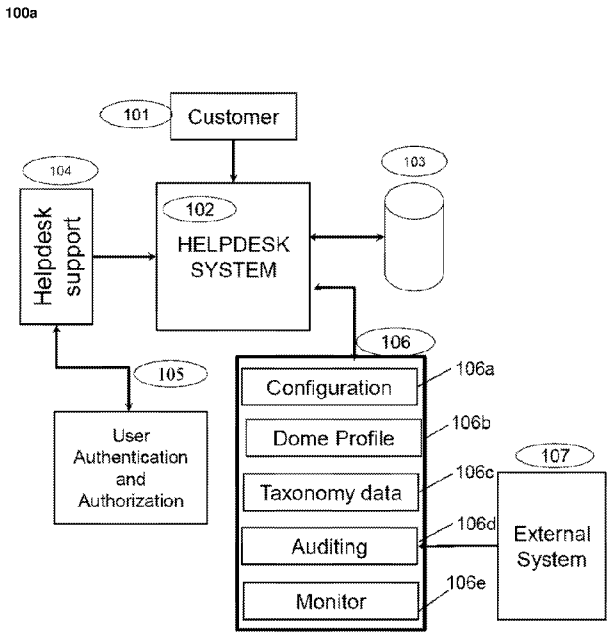

Figure 1.0a

(57) **Abstract:** The present invention relates to a system (100) and method (300) for steering a helpdesk support (104) for accessing an external system (107) in helpdesk system (102). The system (100) of the present invention provides that the helpdesk system (102) comprises at least one customer (101), at least one storage (103) and a user authentication and authorization (105) module linked to the helpdesk support (104). The present invention further provides that the helpdesk system (102) and the external system (107) is integrated through an embedded module (106). The embedded module comprises a Configuration module (106a), a Data Taxonomy module (106c), a Dome Profile module (106b), an Auditing module (106d) and a Monitoring module (106e). The present invention provides that integration of the helpdesk system (102) and the external system (107) through embedded module (106) enables the helpdesk support to access sensitive information on a specific domain to resolve any possible issues in the helpdesk system (102).

WO 2020/111929 A1

[Continued on next page]

Published:

— *with international search report (Art. 21(3))*
— *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))*
— *in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE*

SYSTEM AND METHOD FOR STEERING A HELPDESK SUPPORT FOR ACCESSING AN EXTERNAL SYSTEM IN HELPDESK SYSTEM

FIELD OF INVENTION

The present invention relates to a system and method for steering a helpdesk support to enable a helpdesk system to access an external system. In particular, the system and method of the present invention provides for an integration of the helpdesk system and the external system through an embedded module.

BACKGROUND OF INVENTION

Helpdesk system provides technical information to users, troubleshooting and solves technical or known problems by providing support as well as best information regarding the products or services of company or organization. The current available system in helpdesk system is generally structured into different level or multi-tier support to solve the issues or problem reported by customer or users and an issue tracking system is utilized to track the reported customer issues. A ticket having a unique ID is provided whereby the ticket is assigned to helpdesk support and tracked in a central location.

United States Patent No. US 6859783 B2 (hereinafter referred to as US'783 B2 Patent) entitled "Integrated Interface for web based customer care and trouble management" having a filing date of 24 September 1998 (Patentee: WORLDCOM, INC.) discloses a system and method for opening and tracking trouble tickets over the public Internet. The US'783 B2 Patent discloses a customer service management system which provides information included within a customer profile record to a Web enabled infrastructure which is accessible by a remote customer workstation having a web browser and Internet access. The customer profile information of US'783 B2 Patent is used to prepopulate data fields in dialogs used to open a trouble ticket and input data are classified by Question Tree. Once the trouble ticket is opened, the customer workstation tracks the existing trouble tickets through a browser based graphical user interface. The US'783 B2 Patent further provides Service Inquiry which utilizes the Common Object security model enabling secured access to external data by a user.

United Patent Publication No. US 2009/0100371 A1 (hereinafter referred to as US'371 A1 Publication) having a filing date of 11 December 2008 (Applicant: MICHAEL HU) entitled "User Support System Integrating FAQ and Helpdesk Features and FAQ Maintenance Capabilities" relates to a user Support system interface with integrated FAQ and helpdesk features and a user Support system that integrates user Support request

handling and FAQ maintenance. The US'371 A1 Publication provides that a summary screen enable support team members to filter and sort support request by their attributes (ID, Title, Status, Update) thereafter the support team members would select a ticket to handle. The US'371 A1 Publication further discloses that the user support request handling interface allows the support team member to select from a database, a template answer to the user's request or the support staff may directly edit the template answer in the database, add new questions and answers to the database, or assign a question to a category.

As disclosed in the US'371 A1 Publication, a common helpdesk support structure involves three-tier technical support whereby tier-1 is an initial support level for resolving basic customer issues. Currently, the helpdesk support relies on information provided by customers, general information or answers to the queries commonly found in Frequently Asked Question (FAQ) or in a knowledge base. Should the issue is not resolved in tier-1, the issue can be forwarded to tier-2. Tier-2 is a more in-depth technical support which provides advance technical troubleshooting and analysis methods. The next level of a helpdesk support structure is tier-3 which is an expert level responsible for handling the most difficult or advanced problems.

International Publication No. WO 02067171 A1 (hereinafter referred to as WO'171 A1 Publication) entitled "Helpdesk System" having a filing date of 25 February 2002 (Applicant: COMPUDIGM INTERNATIONAL LIMITED) relates to a helpdesk system in which a plurality of customer workstations are connected to the server over a network or networks and a plurality of staff workstations are connected to the server over the network(s). The helpdesk system of WO'171 A1 Publication comprises a fault manager which assigns one of the predefined knowledge levels to each fault report record whereby each fault report records is identified by a unique identifier to enable each fault report record to be actioned by a staff member having the corresponding knowledge level. The helpdesk system of WO'171 A1 Publication further comprises a customer tracker which monitors traffics trough the website to track the steps taken by a customer to resolve a helpdesk request which thereafter guiding a support technician on how to assist the customer.

As outlined above, various systems and methods have been developed to improve the helpdesk system. However, it is desirable for a helpdesk system to be able to access an external system whereby the helpdesk support will have visibility of sensitive information on a specific domain to resolve any possible issues.

SUMMARY OF INVENTION

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 details may be made without departing from the scope of the invention or sacrificing any of the advantages of the present invention.

One aspect of the present invention provides a system (100) for steering a helpdesk support (104) to enable a helpdesk system (102) to access an external system (107). The helpdesk system (102) comprising at least one customer (101) linked to the helpdesk system (102) whereby the customer (101) logs in issues into the helpdesk system (102); at least one storage (103) linked to the helpdesk system (102) whereby the at least one storage (103) having knowledge base and frequently asked questions of specific domains; and a user authentication and authorization module (105) linked to the helpdesk support (104) for verifying authentication and authorization of the helpdesk support.

The present invention further provides that the external system (107) having a collection of specific domain related information; and the helpdesk system (102) and the external system (107) is integrated through an embedded module (106).

Further, the present invention provides that the embedded module (106) comprises a Data Taxonomy module (106c) which is further comprised of at least one Data Collector for classifying and marking tables and fields of the external information with data protection level based on data classification standard for generating data protection metric; a Dome Profile module (106b) comprises a collection of profiles and assigning profiles with data protection level to the helpdesk support for enabling the helpdesk support (104) to access the external system (107); an Auditing module (106d) for tracing access transaction of the external information by the helpdesk support (104); a Monitoring module (106e) for retrieving the external information access transaction by the helpdesk support (104) in the Auditing module (106d) and generating a report based on the external information access transaction; and a Configuration module (106a) for configuring a connection between the helpdesk system (102) and the external system (107), configuring Dome Profile module (106b) for assigning profiles with data protection level to the helpdesk support (104), configuring parameters for Data Taxonomy module (106c), configuring Auditing module (106d), and configuring Monitoring module (106e).

Another aspect of the helpdesk system (102) is linked to the helpdesk support (104) to enable the helpdesk support (104) to resolve issues logged in by the customer (101) to the helpdesk system (102).

A further aspect of the present invention provides that the data protection metric generated by the Data Taxonomy module (106c) is utilized by the Dome Profile module (106b) to enable the helpdesk support (104) to access the tables and fields of the external information.

Yet another aspect of the present invention provides a method (300) for steering a helpdesk support (104) to enable a helpdesk system (102) to access an external system (107) whereby the method comprising steps of linking (302) the helpdesk system (102) to at least one customer (101) whereby the customer logs in issues into the helpdesk system (102); linking (304) the helpdesk system (102) to at least one storage whereby the storage having knowledge base and frequently asked questions of specific domains; linking (306) the helpdesk system (102) to the helpdesk support (104) to enable the helpdesk support (104) to resolve issues logged in by the customer (101) to the helpdesk system (102); and linking (308) the helpdesk support to a user authentication and authorization module (105) for verifying authentication and authorization of the helpdesk support (104); and integrating (310) the helpdesk system (102) with an external system (107) by an embedded module for enabling secured access to the external system (107) by the helpdesk support (104).

The present invention provides that integrating the helpdesk system (102) with the external system (107) by the embedded module (310) comprising steps of configuring (310a) a Configuration module; classifying and marking (310b) external information of the external system (107) with data protection level by a Data Taxonomy module; assigning (310c) profile with data protection level to the helpdesk support (104) by a Dome Profile module (106b) for enabling the helpdesk support (104) to access the external system (107); tracing (310d) the external information access transaction by the helpdesk support (104) through an Auditing module; and monitoring (310e) the external information access transaction in the Auditing module (106d) and generating a report based on the said external information access transaction through a Monitoring module (106e).

Still another aspect of the present invention provides that configuring (310a) the Configuration module (106a) further comprising steps of configuring (401) a connection between the helpdesk system (102) and the external system (107); configuring (403) data

protection level; configuring (409) an Auditing module (106d); and configuring (411) a Monitoring module (106e).

The present invention provides that configuring (401) a connection between the helpdesk system (102) and the external system (107) further comprising steps of determining if connection between helpdesk system (102) and external system (107) is successfully established (402); completing connection between helpdesk system (102) and external system (107) if the connection between helpdesk system (102) and the external system (107) is successfully established; displaying an error and resolving the error log (420) by reconfiguring the connection (402) if the connection between helpdesk system (102) and external system (107) is not successfully established (402a); and establishing connection between helpdesk system (102) and external system (107).

The present invention provides that configuring data protection level (403) further comprising steps of proceeding to use default data protection level (405) if the data protection level is generated automatically (404a); and completing the data protection level configuration; creating (406) a new data protection level, if data protection level is not generated automatically (404); creating (407) data protection instructions and description; saving (408) the created data protection level and the created data protection instructions and the description in the storage (103); and completing the data protection level configuration.

The present invention provides that configuring (409) an Auditing module (106d) further comprising steps of setting (410) auditing parameters; and saving (408) the auditing parameter in the storage.

The present invention provides that configuring (411) a Monitoring module (106e) further comprising steps of setting (412) monitoring parameter; and saving (408) the monitoring parameter in the storage (103).

Another aspect of the present invention provides that classifying and marking (310b) the external data of the external system (107) with data protection level by Data Taxonomy module further comprising steps of confirming (501) establishment of connection to the external system (107) during configuration of connection between the helpdesk system (102) and the external system (107); reading (502) tables and fields in external storage system (107); and determining if the tables and fields are marked automatically. If automatic marking option is chosen (503); generating (505) a data protection metric report utilizing auto marking data protection instructions; and verifying (506) the data protection metric report; if the helpdesk support (104) does not correlate (506a) with the

data protection metric report, reiterating step (503); else proceeding to save (507) the data protection metric report in the storage (103). If automatic marking option is not chosen (503a); marking (504) the tables and fields with data protection instructions; generating (505) data protection metric report utilizing data protection instructions; and verifying (506) the data protection metric report. If the helpdesk support (104) does not correlate (506a) with the data protection metric report, reiterating step (503); else proceeding to save (507) the data protection metric report in the storage.

A further aspect of the present invention provides that assigning (310c) profile with data protection level to the helpdesk support (104) by Dome Profile module (106b) for enabling the helpdesk support (104) to access the external system (107) further comprising steps of determining (601) if profile is generated automatically. If automatic profile creation is chosen (601); creating default profile (620) utilizing default data protection level; and assigning (604) profile to the helpdesk support (104). However, if automatic profile creation is not chosen (601a); creating a new profile (602); assigning (603) profile to data protection level generated during data protection level configuration (403); and assigning (604) profile to the helpdesk support (104).

Another aspect of the present invention provides that tracing (310d) the external information access transaction by the helpdesk support (104) through Auditing module further comprising steps of tracing (702) access transaction of the external information system by a helpdesk support (104), if the Auditing module is enabled (701); saving (703) the transaction log in the storage (103); and producing (704) an auditing report and displaying audit trail by the helpdesk system (102).

A further aspect of the present invention provides that monitoring (310e) the external information access transaction in the Auditing module (106d) and generating a report based on the said external information access transaction through Monitoring module (106e) further comprising steps of retrieving (802) information of access transaction by the helpdesk support (104) in the Auditing module (106d), if Monitoring module is enabled (801); obtaining (803) profile information in the Dome Profile module (106b); and generating a monitoring (804) report based on the information of the access transaction by the helpdesk support (104) in the Auditing module and profile information in the Dome profile module (106b).

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 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.

FIG. 1.0a illustrates a schematic diagram of integration of helpdesk system and external system through an embedded module.

FIG. 1.0b illustrates a schematic diagram of the architecture of the helpdesk system of the present invention which enable the helpdesk support to access the external system and the storage through integration of the embedded module.

FIG. 2.0 illustrates a schematic diagram of an exemplary of data protection level configuration, Data Taxonomy module classifying the external data based on data protection level and Dome Profile module assigning profiles with data protection level.

FIG. 3.0 is a flowchart illustrating an overview of the general methodology of the present invention which involves integrating the helpdesk system with the external system by the embedded module.

FIG. 4.0 is a flowchart illustrating the steps involved in Configuration module to establish connection between helpdesk system and external system and configuration of data protection level, Auditing module and Monitoring module.

FIG. 5.0 is a flowchart illustrating the steps involved in Data Taxonomy module to classify and mark external information with data protection level.

FIG. 6.0 is a flowchart illustrating the steps involved in Dome Profile module for assigning profile with data protection level to helpdesk support.

FIG. 7.0 is a flowchart illustrating the steps involved in Auditing module.

FIG. 8.0 is a flowchart illustrating the steps involved in Monitoring module.

DETAILED DESCRIPTION OF THE PREFFERED EMBODIMENTS

The present invention relates to a system and method for steering a helpdesk support to enable a helpdesk system to access an external system. In particular, the system and method of the present invention comprises integration of the helpdesk system and the external system through embedded module by classifying external information based on data protection level and assigning profile with data protection level to the helpdesk support to enable the helpdesk support to access the external system. 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.

A currently available helpdesk system is configured by linking the helpdesk system to at least one customer which logs in issues into the helpdesk system. The helpdesk system is further linked to at least one storage which includes a knowledge base and a helpdesk support which is linked to a user authentication and authorization module to verify authentication and authorization of the helpdesk support. The currently available helpdesk system provides that, the helpdesk support can only rely upon information provided by the customer or the storage to resolve the issues logged in by the customer in the helpdesk system. Since the helpdesk system is not linked to an external system, the helpdesk support is unable to access the external system to retrieve required information which including sensitive or confidential information to resolve the issues logged in by the customer. Such a problem will cause a delay in resolution time due to lack of information accessible by the helpdesk support.

The present invention provides a solution to the above-mentioned problem by enabling the helpdesk support to resolve the issues or problems within a short resolution time by integrating the helpdesk system with the external system through an embedded module. The present invention provides a secure external information access protection based on data protection level to prevent sensitive information from being abused or harmed by helpdesk support, administrator and other authorized personnel.

Figure 1.0a illustrates a schematic diagram of integration of helpdesk system and an external system through an embedded module of the present invention (100a). As illustrated in figure 1.0a, the helpdesk system of the present invention comprises at least one customer (101), at least one storage (103) and a user authentication and authorization module (105). The present invention provides that the at least one customer (101) is linked to the helpdesk system (102) whereby the at least one customer (101) logs

in issues into the helpdesk system (102). The helpdesk system (102) is linked to a helpdesk support (104) to enable the helpdesk support (104) to resolve issues logged in by the customer (101) to the helpdesk system (102). The helpdesk system (102) is further linked to the at least one storage (103) having knowledge base and frequently asked questions of specific domains for enabling the helpdesk support (104) to provide technical assistance to resolve issues logged in by the customer (101) to the helpdesk system (102). The helpdesk support (104) is further linked to a user authentication and authorization module (105) for verifying authentication and authorization of the helpdesk support.

The present invention provides that the external system (107) comprises a collection of specific domain related information which includes sensitive information which cannot be published or shared with others and is only accessible by an authorized person in an organization. The present invention provides that the helpdesk system (102) and the external system (107) is integrated through an embedded module (106) enabling the helpdesk support (104) to access the external system (107).

The embedded module (106) comprises a Configuration module (106a), a Dome Profile module (106b), a Data Taxonomy module (106c), an Auditing module (106d) and a Monitoring module (106e). A detailed explanation of each module is described in the following sections.

Reference is now made to figure 1.0b which illustrates a schematic diagram of the architecture of the helpdesk system of the present invention (100b) which enables the helpdesk support (104) to access the external system (107) and the storage (103) through integration of the embedded module to resolve issues logged in by the customer onto the helpdesk system. As illustrated in figure 1.0b, the connection between the helpdesk system and the external system based data protection level are configured in the Configuration module (106a). The data protection level can be generated automatically or through manual configuration.

Upon establishing the connection between the helpdesk system and the external system (107) and upon configuring the data protection level with assumption that the user identification has full read access or authorization to the external system, Data Collector which resides within the Data Taxonomy module (106c) will mark and classify tables and fields of information of the external information in the external system based on the data protection level.

Examples of default data protection levels includes P, Public; I, Internal use; C, Confidential; and T, Top secret whereby public refers to information that if breached owing to accidental or malicious activity would have an insignificant impact on the Company's activities and objectives; Internal use refers to information that if breached owing to accidental or malicious activity would have a low impact on the Company's activities and objectives; Confidential refers to information that if breached owing to accidental or malicious activity would have a medium impact on the Company's activities and objectives; and Top Secret refers information that if breached owing to accidental or malicious activity would have a high impact on the Company's activities and objectives. However, information protection levels are not limited to these levels.

The present invention provides that the default data protection level is marked as data protection instructions P depending on the data classification standard of the information in the external system.

Dome profile module (106b) comprises a collection of profiles created by the helpdesk support (104). Each helpdesk support (104) will be assigned a profile with data protection level by the Dome profile module (106b). The Dome profile module (106b) allows the helpdesk support to access different information from the external system (107) based on the data protection level assigned to the profiles.

The transaction of external information accessed by the helpdesk support (104) can be traced by enabling an Auditing module (106d). The helpdesk support may enable or disable the Auditing module (106d) based on their requirement. Further, the present invention provides that the helpdesk support may enable or disable a Monitoring module (106e) based on its requirement. Once the Monitoring module (106e) is enabled, the helpdesk system will monitor the external information access transaction in the Auditing module (106d) and generates a report based on the external information access transaction.

Reference is now made to figure 2.0 which illustrates a schematic diagram of an exemplary (200) data protection level configuration, Data Taxonomy module classifying the external information based on data protection level and Dome Profile module assigning profiles with its data protection level. As illustrated in figure 2.0, data protection level is configured automatically or through manual configuration in the Configuration module (201) whereby default data protection level is configured automatically. Generally, default date protection level is set as data protection level 1 with data protection instruction P, Public. The data protection level is configured based on data classification

standard and not limited to Public, P; Internal use, I; Confidential, C; or Top Secret, T. It is provided herein that other data classification standard may be utilized.

In order for the helpdesk system to read the information in the external system, connection between the helpdesk system and the external system must be established in the Configuration module (201).

Once the connection between the helpdesk system and the external system is established, Data Taxonomy module (202) which comprises a Data Collector will mark the tables and fields of the external information with data protection level of either Public , P; Internal use, I; Confidential, C; or Top Secret, T. In a default system, the tables and fields are marked with data protection level instructions “P”. The tables and fields which are not going to be accessed by the helpdesk support can be unmarked.

As illustrated in the Data taxonomy module (202), Table1 comprises Field1 to Field7 and Table2 comprises Field1 to Field6. The Data Collector will mark the tables and fields with data protection level instructions through a marking process. For example, in table 1, field 1 is marked with data protection level instructions P, whereas table1, field3 is marked with data protection level instructions I.

Upon marking of the tables and fields, the helpdesk system will generate a marking table metric for the helpdesk support for confirmation or verification. The verification process is only required to be executed for the first time for initial configuration of the system. The subsequent request will be configured automatically based on the marking table metric.

Thereafter, the Dome Profile module (203) will assign a profile to the helpdesk support with data protection level. It is provided herein that some profiles might include multiple data protection level. For example, Helpdesk 1 was assigned with profile1 and is allowed to access the Tables and Fields which are marked as “P” (i.e. Data Protection Level1) only whereas Helpdesk 4 which was assigned with profile7 is allowed to access Tables and Fields which are marked as “I”, “C” and “T” which represents Data Protection level 2, Data Protection level 3, Data Protection level 4 respectively.

The present invention further provides a method for steering a helpdesk support to enable a helpdesk system to access an external system. Reference is now made to figure 3.0 which illustrates an overview of the general methodology of the present invention which involves integrating the helpdesk system with the external system by the embedded module. The method (300) comprising steps of linking the helpdesk system to at least one customer (302) whereby the customer logs in issues into the helpdesk

system. The helpdesk system is further linked to at least one storage (304) whereby the storage having knowledge base and frequently asked questions of specific domains. The present invention further provides that, the helpdesk support (306) which provides technical assistance to resolve the issues logged in by the customer to the helpdesk system. Further, the helpdesk support is linked to a user authentication and authorization module (308) for verifying authentication and authorization of the helpdesk support. The present invention further provides that, the helpdesk system is integrated with an external system by an embedded module (310) for enabling secured access to the external system by the helpdesk support.

As illustrated in figure 3.0, integrating helpdesk system with external system by an embedded module further comprises steps of configuring a Configuration module (310a). A Detailed explanation of the steps involved in configuring a Configuration module is illustrated in figure 4.0. Subsequently, the Data Taxonomy module (310b) will classify and mark tables and fields of external information of the external system with a specific data protection level. Thereafter, the Dome Profile module (310c) which comprises a collection of profiles will assign profiles with data protection level to the helpdesk support for enabling the helpdesk support to access the external system. The Auditing module (310d) will continue to trace the external information access transaction by the helpdesk support. Upon tracing the external information access transaction by the Auditing module, the Monitoring module (310e) will monitor the external information access transaction in the Auditing module and proceeded to generate a report based on the audited external information access transaction.

Reference is now made to figure 4.0 which illustrates the steps involved in configuring a Configuration module (400) to establish a connection between the helpdesk system and the external system (401). As illustrated in figure 4.0, configuration of connection between the helpdesk system and the external system (401) further comprising steps of configuring data protection level (403), Auditing module (409) and Monitoring module (411). In configuring a connection between the helpdesk system and the external system (401) it is first determined if the connection between the helpdesk system and the external system is established (402) providing that the letter of agreement is already signoff between the external system and the helpdesk system. If a connection is successfully established (402) the configuration of connection between helpdesk system and external system is completed. However, if a connection between the helpdesk system and the external system is not established (402a), an error message will be displayed in the helpdesk system and error log will be resolved (620) by reconfiguring the connection between the helpdesk system and the external system and the step 401 is

reiterated. Upon establishing the connection between the helpdesk support and the external system, the configuration of connection between helpdesk system and external system is completed.

In configuring the configuration of data protection level (403) it is first determined if the data protection level is generated automatically. If the data protection level is generated automatically (404a), the configuration module (400) proceeds to use default data protection level (405); and the data protection level configuration is considered as completed.

However, if the data protection level is not generated automatically (404), a new data protection level is created (406) by the helpdesk support by creating data protection instructions and description (407). Thereafter, the created data protection level, the data protection instructions and its descriptions are stored in the storage (408).

In configuring an Auditing module (409), auditing parameters (410) are set based on the helpdesk support requirements. Upon setting the auditing parameters, said auditing parameters are stored (408) in the storage.

In configuring a Monitoring module (411), monitoring parameters (412) are first set based on the helpdesk support requirements. The monitoring parameters include an email notification for alerting the helpdesk support. Upon setting the monitoring parameters, the monitoring parameters are stored (408) in the storage.

Reference is now made to figure 5.0 which illustrates the steps involved in classifying and marking external information of the external system with data protection level by Data Taxonomy module (500). As illustrated in figure 5.0, in classifying and marking the external information of the external system with data protection level, the establishment of connection to the external system is confirmed (501) in the configuration module (401). Subsequently, all tables and fields in the external storage system are read (502). Upon reading the tables and fields in the external system, the helpdesk support determines if the tables and fields of the external storage system are marked automatically (503). If automatic marking is selected, the helpdesk system will generate a data protection metric report utilizing auto marking data protection instructions. It is provided herein that auto marking data protection instructions is set as Public, P. Thereafter, the data protection metric report is verified by the helpdesk support. Step 503 is reiterated if non-correlation of the helpdesk support with the data protection metric report is observed (506a). Else proceed to save the data protection metric report in the storage (507).

If automatic marking option is not selected (503a), the helpdesk support is required to mark the tables and fields with data protection instructions (504) of either Public, P; Internal use, I; Confidential, C; or Top Secret, T; then a data protection metric report is generated utilizing data protection instructions (505). Subsequently, the data protection metric report is verified by the helpdesk support. If the helpdesk support does not agree (506a) with the data protection metric report, step 503 is reiterated. Else proceed to save the data protection metric report in the storage (507). The data protection metric report will be used by Dome Profile module to allow the helpdesk support to access the tables and fields of the external information.

Reference is now made to figure 6.0 which illustrates the steps involved in Dome Profile module (600) for assigning profile with data protection level to helpdesk support. As illustrated in figure 6.0, it is first determined if the profile is generated automatically (601). If the profile is generated automatically (601a), a default profile is created (620) by utilizing default data protection level. Thereafter, the default profile is assigned (604) to the helpdesk support. It is provided herein that the default profile is assigned with data protection level 1 which enables the helpdesk support to access fields and tables of external information which marked with data protection level instructions “P”. However, if automatic profile creation is not selected (601), a new profile is created (602). For example Profile1, Profile2, and etc. Subsequently, data protection level (603) is assigned to the created profile. It is provided herein that the data protection level has been generated in the configuration module in step 403. Thereafter, the profile will be assigned to the helpdesk suport (604) which allows the helpdesk support to access the external data system with data protection level according to the data protection level assigned to its profile. For example, Helpdesk Support1 with profile1 is only allowed to access the public information in the external system whereas Helpdesk Support2 with profile2 is allowed to access the Internal use information.

Reference is now made to figure 7.0 which illustrates the steps involved in Auditing module (700) for tracing the external information access transaction by the helpdesk support. The present invention provides that the Auditing module can be enabled or disabled based on the helpdesk support requirements. As illustrated in figure 7.0, it is first determined if the Auditing module is enabled. If the Auditing module is enabled (701), access transaction of the external system by the helpdesk support is traced (702) and the transaction log is stored (703) in the storage. Thereafter, an auditing report is produced and an audit trail will be displayed by the helpdesk system (704). However, the process will end if the Auditing module is disabled (701a).

Reference is now made to figure 8.0 which illustrates the steps involved in Monitoring module (800) for monitoring the external information access transaction in the Auditing module and generating a report based on the audited external information access transaction. The present invention provides that the Monitoring module can be enabled or disabled based on the helpdesk support requirements. As illustrated in figure 8.0, it is first determined if the Monitoring module is enabled (801). If the Monitoring module is enabled (801), information of access transaction by the helpdesk support in the Auditing module (802) is retrieved. Thereafter, the profile information in the Dome Profile module is obtained (803) and a monitoring report is generated based on the information access transaction by the helpdesk support in the Auditing module and profile information in the Dome Profile module (804). However, the process will end if the Monitoring module is disabled (801a).

In conclusion, the distinctiveness of the present invention lies in the an integration of the helpdesk system and the external system through an embedded module enabling the helpdesk support to access sensitive information on a specific domain to resolve any possible issues in the helpdesk system.

Unless the context requires otherwise or specifically stated to the contrary, integers, steps or elements of the invention recited herein as singular integers, steps or elements clearly encompass both singular and plural forms of the recited integers, steps or elements.

Throughout this specification, unless the context requires otherwise, the word “comprise”, or variations such as “comprises” or “comprising”, will be understood to imply the inclusion of a stated step or element or integer or group of steps or elements or integers, but not the exclusion of any other step or element or integer or group of steps, elements or integers. Thus, in the context of this specification, the term “comprising” is used in an inclusive sense and thus should be understood as meaning “including principally, but not necessarily solely”.

CLAIMS

1. A system (100) for steering a helpdesk support (104) to enable a helpdesk system (102) to access an external system (107), wherein

the helpdesk system (102) comprising:

at least one customer (101) linked to the helpdesk system (102) whereby the customer (101) logs in issues into the helpdesk system (102);

at least one storage (103) linked to the helpdesk system (102) whereby the at least one storage (103) having knowledge base and frequently asked questions of specific domains; and

a user authentication and authorization module (105) linked to the helpdesk support (104) for verifying authentication and authorization of the helpdesk support (104);

the external system (107) having a collection of specific domain related information; and

the helpdesk system (102) and the external system (107) is integrated through an embedded module (106),

characterized in that

the embedded module (106) further comprises:

a Data Taxonomy module (106c) comprises at least one Data Collector for classifying and marking tables and fields of the external information with data protection level based on data classification standard for generating data protection metric;

a Dome Profile module (106b) comprises a collection of profiles and assigning profiles with data protection level to the helpdesk support (104) for enabling the helpdesk support (104) to access the external system (107);

an Auditing module (106d) for tracing access transaction of the external information by the helpdesk support (104);

a Monitoring module (106e) for retrieving the external information access transaction by the helpdesk support (104) in the Auditing module (106d) and generating a report based on the external information access transaction; and

a Configuration module (106a) for configuring a connection between the helpdesk system (102) and the external system (107), configuring Dome Profile module (106b) for assigning profiles with

data protection level to the helpdesk support (104), configuring parameters for Data Taxonomy module (106c), configuring Auditing module (106d) and configuring Monitoring module (106e).

2. The system according to claim 1, wherein the helpdesk system (102) is linked to the helpdesk support (104) to enable the helpdesk support (104) to resolve issues logged in by the customer (101) to the helpdesk system (102).

3. The system (100) according to claim 1, wherein the data protection metric generated by the Data Taxonomy module (106c) is utilized by the Dome Profile module (106b) to enable the helpdesk support (104) to access the tables and fields of the external information.

4. A method (300) for steering a helpdesk support (104) to enable a helpdesk system (102) to access an external system (107) wherein, the method comprising steps of:

linking (302) the helpdesk system (102) to at least one customer (101) whereby the customer (101) logs in issues into the helpdesk system (102);

linking (304) the helpdesk system (102) to at least one storage (103) whereby the storage (103) having knowledge base and frequently asked questions of specific domains;

linking (306) the helpdesk system (102) to the helpdesk support (104) to enable the helpdesk support (104) to resolve issues logged in by the customer (101) to the helpdesk system (102);

linking (308) the helpdesk support (104) to a user authentication and authorization module (105) for verifying authentication and authorization of the helpdesk support (104); and

integrating (310) the helpdesk system (102) with an external system (107) by an embedded module (106) for enabling secured access to the external system (107) by the helpdesk support(104),

characterized in that

integrating (310) the helpdesk system (102) with the external system (107) by the embedded module (106) further comprising steps of:

configuring (310a) a Configuration module (106a);

classifying and marking (310b) external information of the external system (107) with data protection level by a Data Taxonomy module (106c);

assigning (310c) profile with data protection level to the helpdesk support (104) by a Dome Profile module (106b) for enabling the helpdesk support (104) to access the external system (107);

tracing (310d) the external information access transaction by the helpdesk support (104) through an Auditing module(106d); and

monitoring (310e) the external information access transaction in the Auditing module (106d) and generating a report based on the said external information access transaction through a Monitoring module (106e).

5. The method (300) according to claim 4, wherein configuring (310a) the Configuration module (106a) further comprising steps of:

configuring (401) a connection between the helpdesk system (102) and the external system (107);

configuring (403) data protection level;

configuring (409) an Auditing module (106d); and

configuring (411) a Monitoring module (106e);

wherein,

configuring (401) a connection between the helpdesk system (102) and the external system (107) further comprising steps of:

completing (402) connection between helpdesk system (102) and external system, if the connection between helpdesk system (102) and external system (107) is successfully established;

displaying an error and resolving the error log (420) by reconfiguring the connection, if the connection between helpdesk system (102) and external system (107) is not successfully established (602a); and

establishing (107) connection between helpdesk system (102) and external system (107);

configuring data protection level (403) further comprising steps of:

proceeding (405) to use default data protection level, if the data protection level is generated automatically (404a);

completing the data protection level configuration;

creating (406) a new data protection level, if data protection level is not generated automatically (404);

creating (407) data protection instructions and description;

saving (408) the created data protection level, the created data protection instructions and the description in the storage (103); and

completing the data protection level configuration;

configuring (409) an Auditing module (106d) further comprising steps of:

setting (410) auditing parameters; and

saving (408) the auditing parameter in the storage (103); and

configuring (411) a Monitoring module (106e) further comprising steps of:

setting (412) monitoring parameter; and

saving (408) the monitoring parameter in the storage (103).

6. The method according to claim 4, wherein classifying and marking (310b) the external data of the external system (107) with data protection level by Data Taxonomy module (106c) further comprising steps of:

confirming (501) establishment of connection to the external system (107) during configuration of connection between the helpdesk system (102) and the external system (107);

reading (502) tables and fields in external storage system; and

determining if the tables and fields are marked automatically;

if automatic marking option is chosen (503);

generating (505) a data protection metric report utilizing auto marking data protection instructions;

verifying (506) the data protection metric report;

if the helpdesk support (104) does not correlate (506a) with the data protection metric report, reiterating step (503); else proceeding (507) to save the data protection metric report in the storage (103); and

if automatic marking option is not chosen (503a);

marking (504) the tables and fields with data protection instructions;

generating (505) data protection metric report utilizing data protection instructions;

verifying (506) the data protection metric report;

if the helpdesk support (104) does not correlate (506a) with the data protection metric report, reiterating step (503); else proceeding to save (507) the data protection metric report in the storage (103).

7. The method according to claim 4, wherein assigning (310c) profile with data protection level to the helpdesk support (104) by Dome Profile module (106b) for enabling the helpdesk support (104) to access the external system (107) further comprising steps of:

determining (601) if profile is generated automatically;

if (601) automatic profile creation is chosen;

creating default profile (620) utilizing default data protection level; and

assigning (604) profile to the helpdesk support (104); and

if automatic profile creation is not chosen (601a);

creating (602) a new profile;

assigning (603) profile to data protection level generated during data protection level configuration (403); and

assigning (604) profile to the helpdesk support (104).

8. The method according to claim 4, wherein tracing (310d) the external information access transaction by the helpdesk support (104) through Auditing module (106d) further comprising steps of:

tracing (702) access transaction of the external information system by a helpdesk support (104), if the Auditing module (106d) is enabled (701);

saving (703) the transaction log in the storage (103); and

producing (704) an auditing report and displaying audit trail by the helpdesk system (102).

9. The method according to claim 4, wherein monitoring (310e) the external information access transaction in the Auditing module (106d) and generating a report based on the said external information access transaction through Monitoring module (106e) further comprising steps of:

retrieving (802) information of access transaction by the helpdesk support (104) in the Auditing module (106d), if the Monitoring module (106e) is enabled (801);

obtaining (803) profile information in the Dome Profile module (106b); and

generating (804) a monitoring report based on the information of the access transaction by the helpdesk support (104) in the Auditing module (106d) and profile information in the Dome profile module (106b).

100a

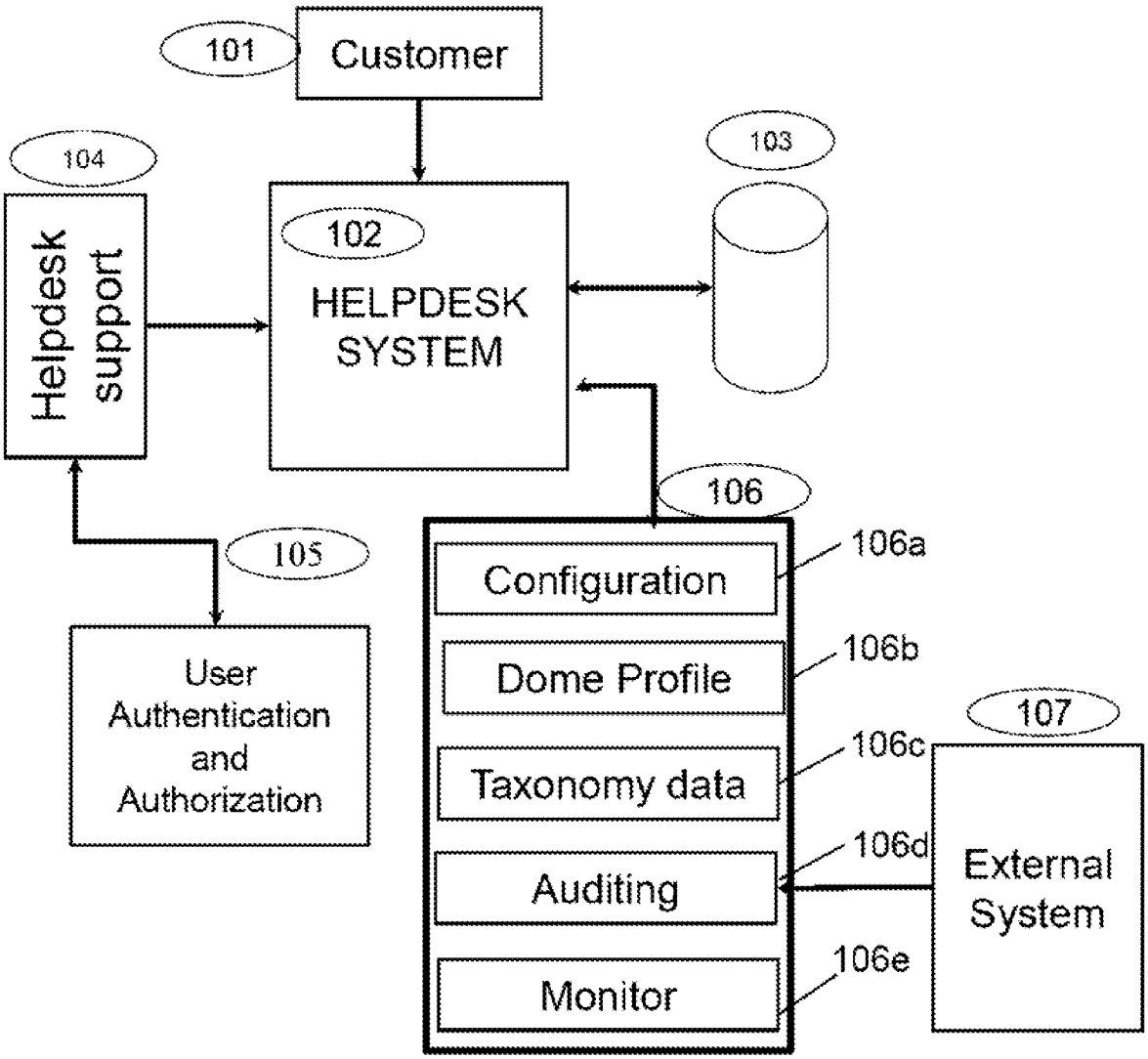

Figure 1.0a

100b

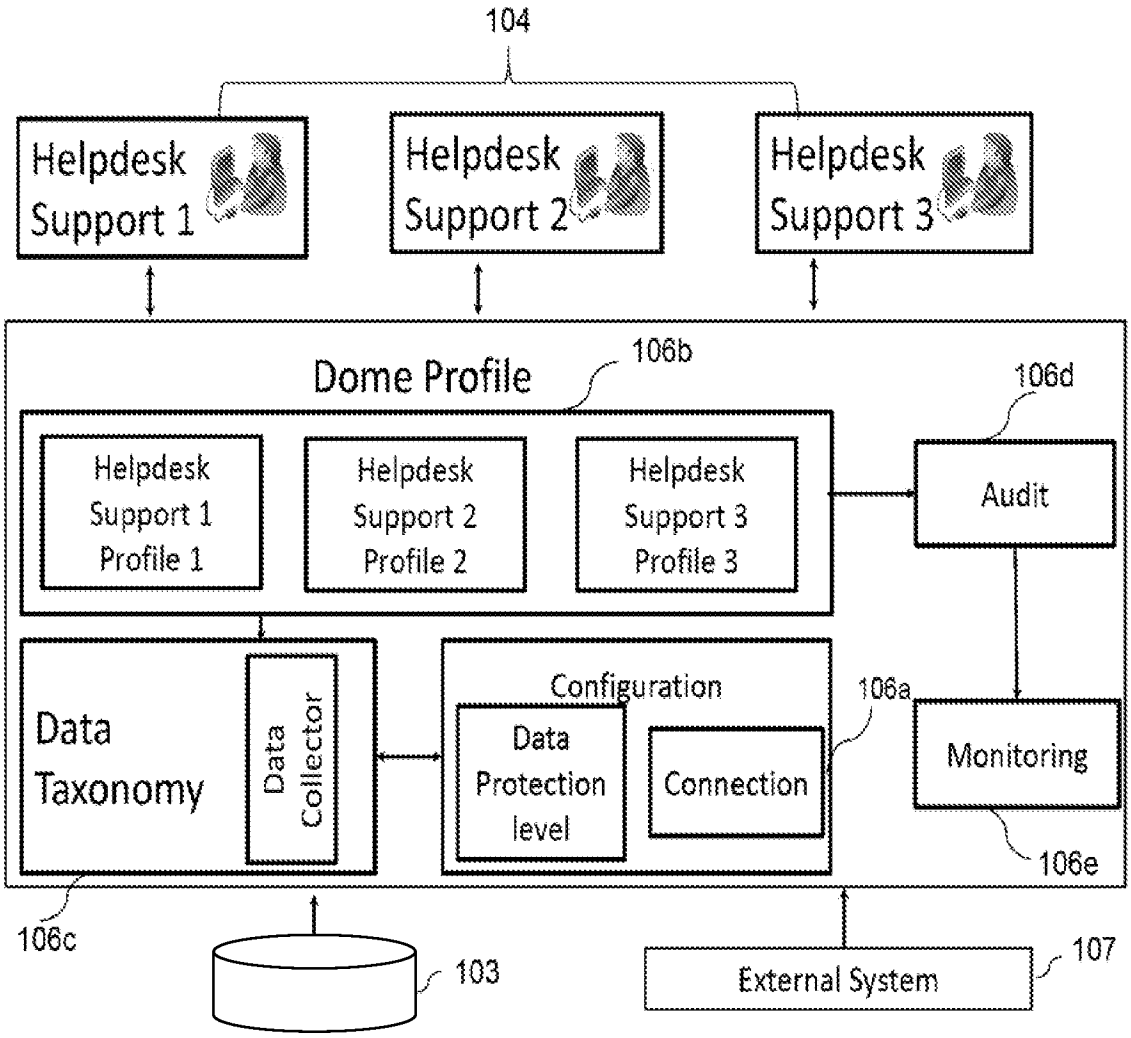

Figure 1.0b

200

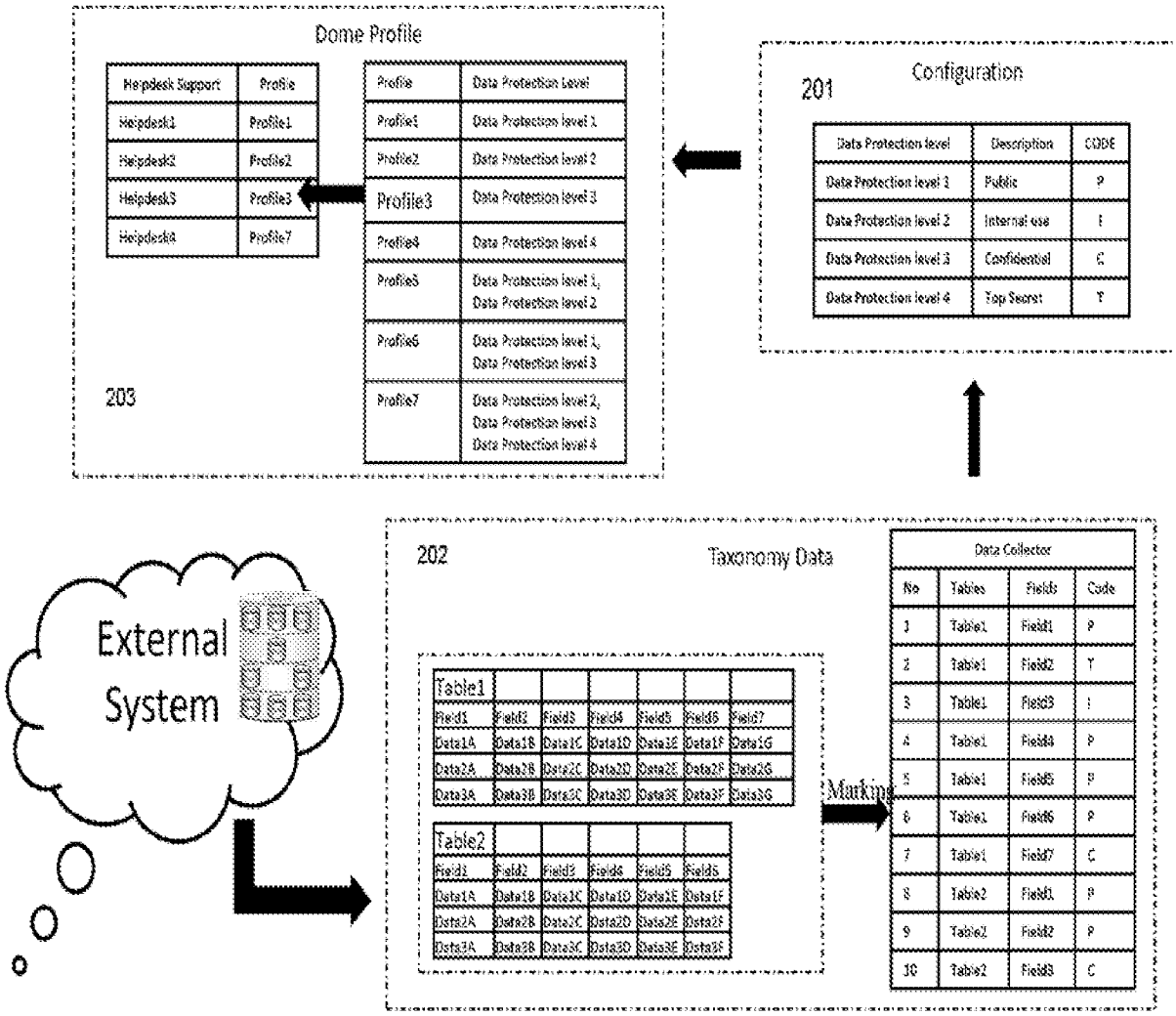

Figure 2.0

300

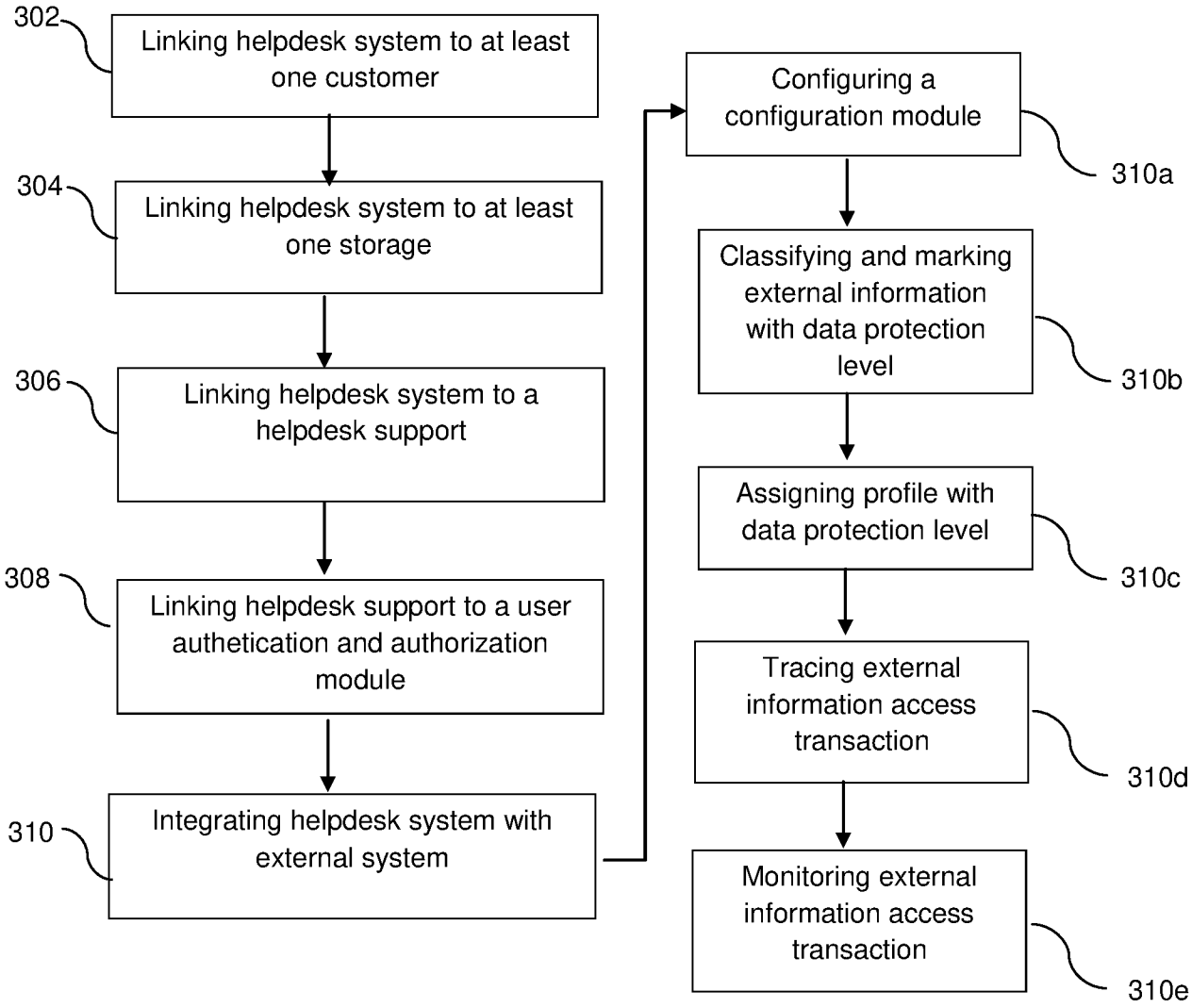

Figure 3.0

400

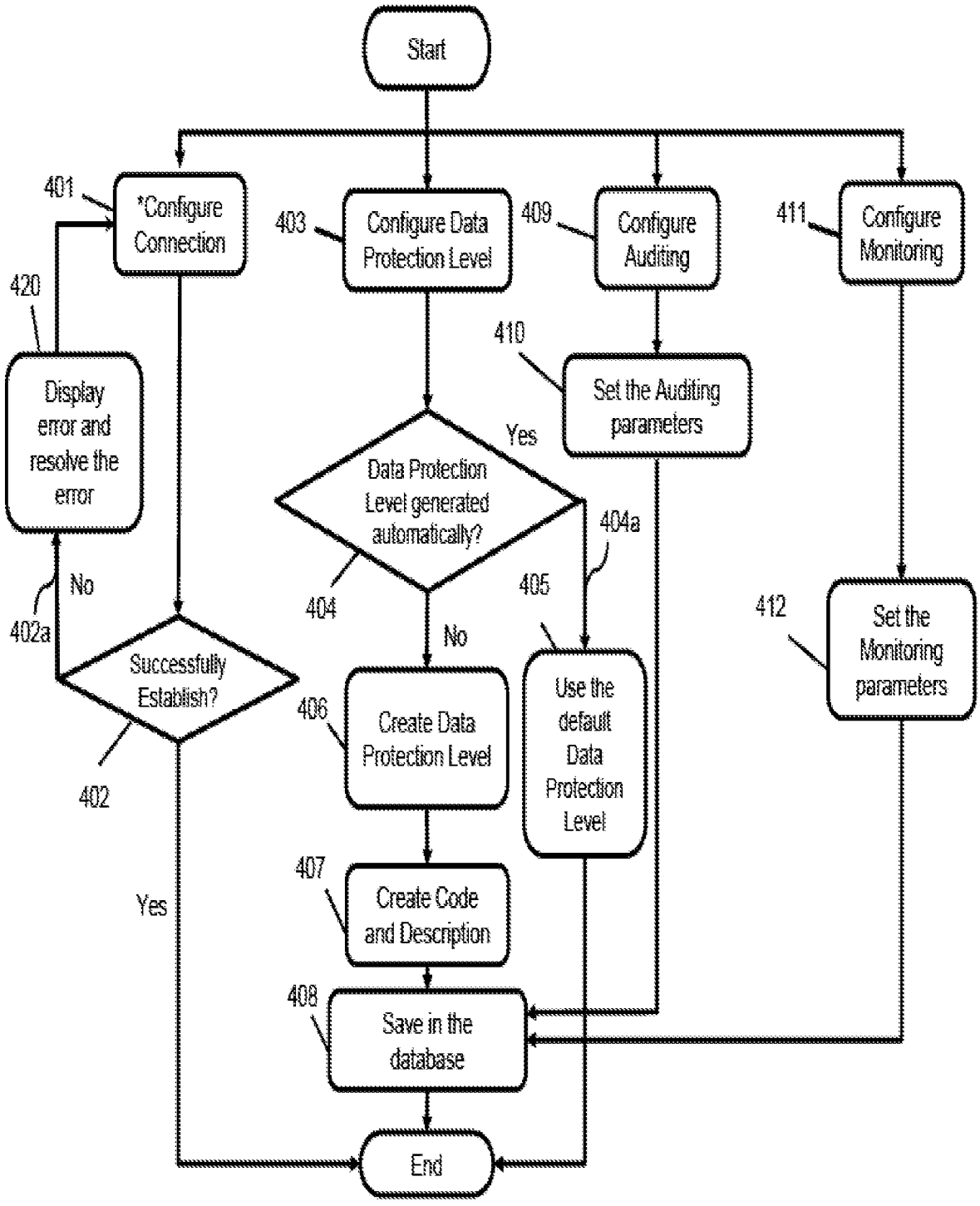

Figure 4.0

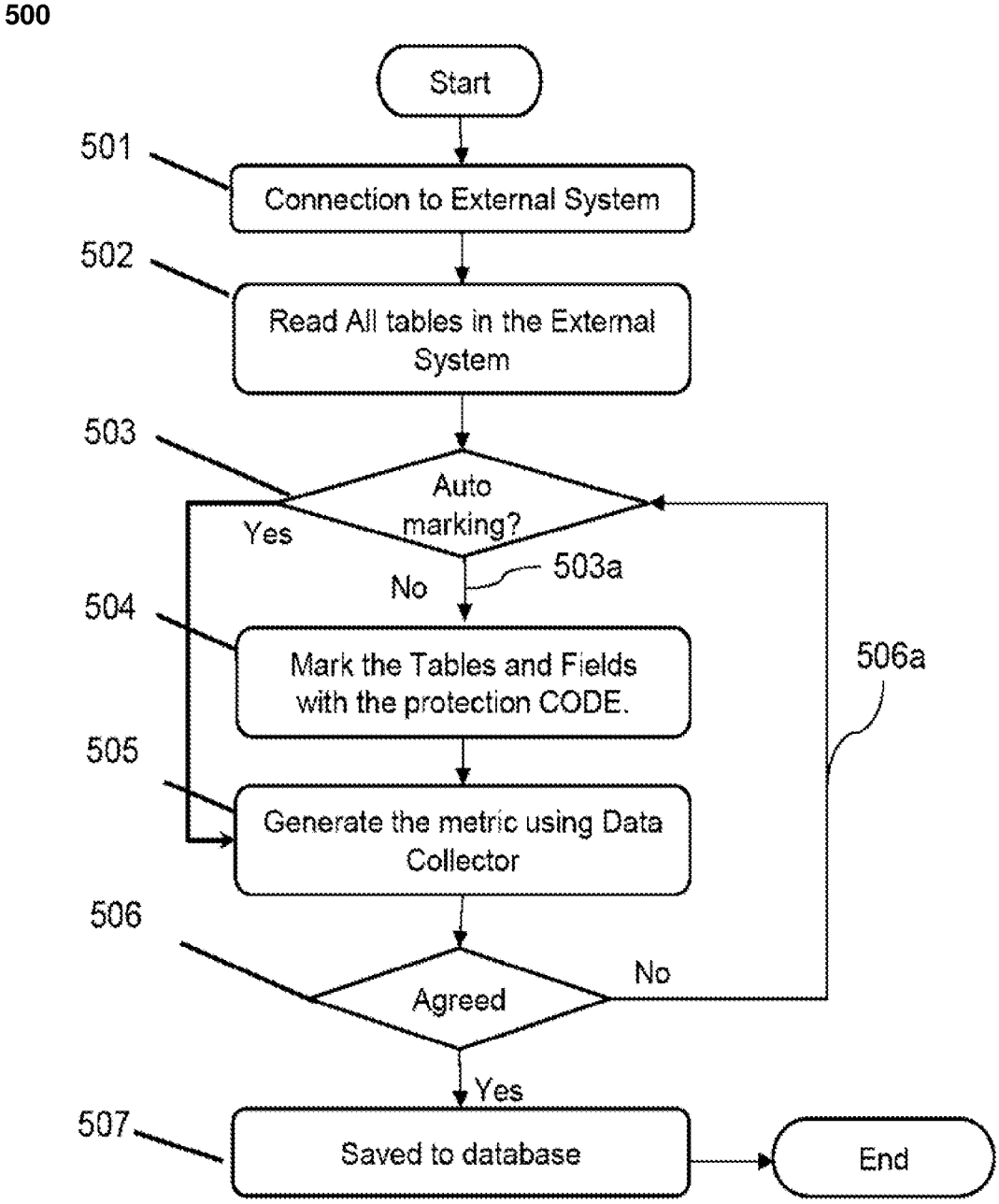
500
Start
501
Connection to External System
502
Read All tables in the External System
503
Auto marking?
Yes
No
503a
504
Mark the Tables and Fields with the protection CODE.
505
Generate the metric using Data Collector
506
Agreed
No
506a
Yes
507
Saved to database
End

Figure 5.0

600

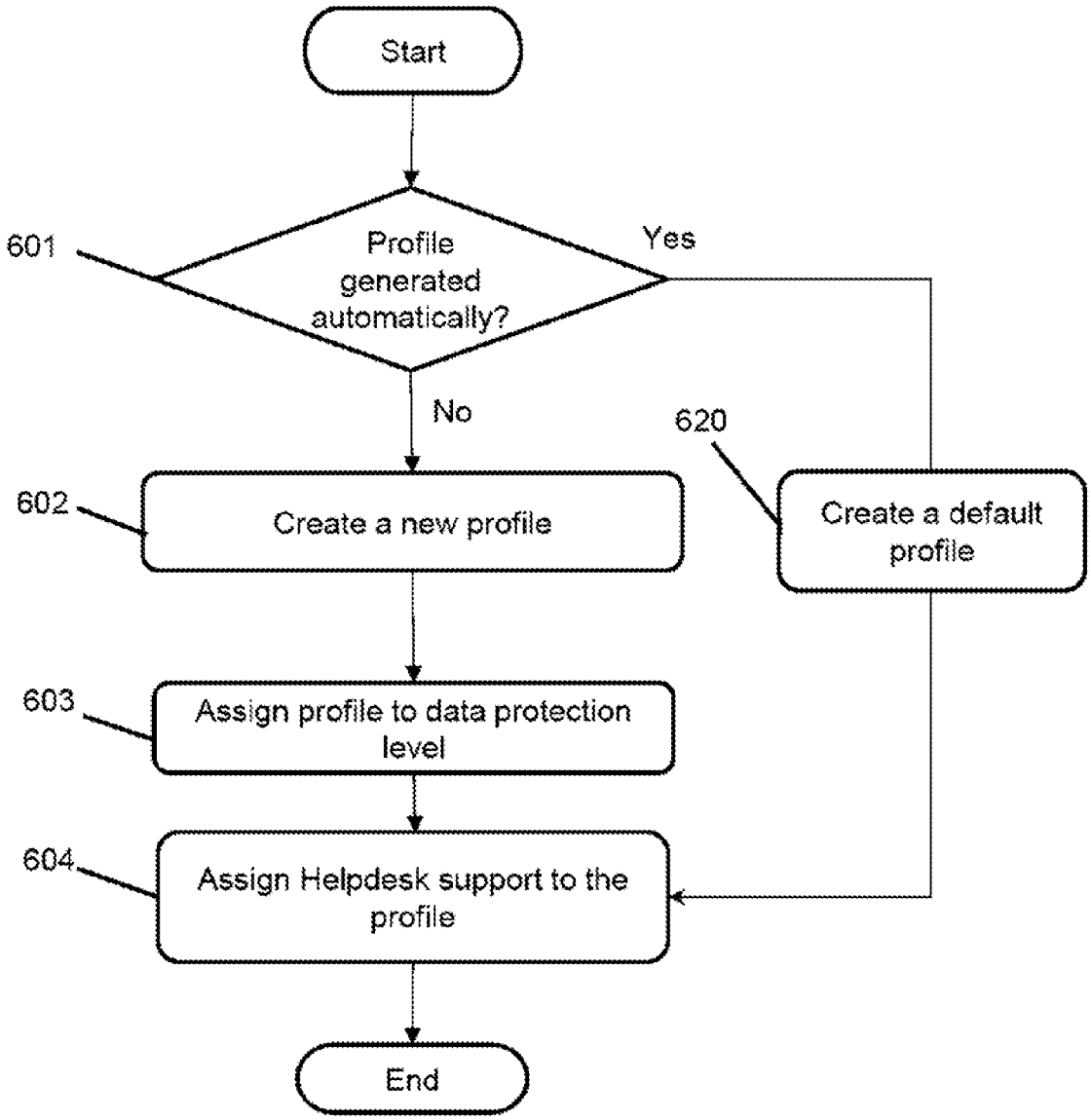

Figure 6.0

700

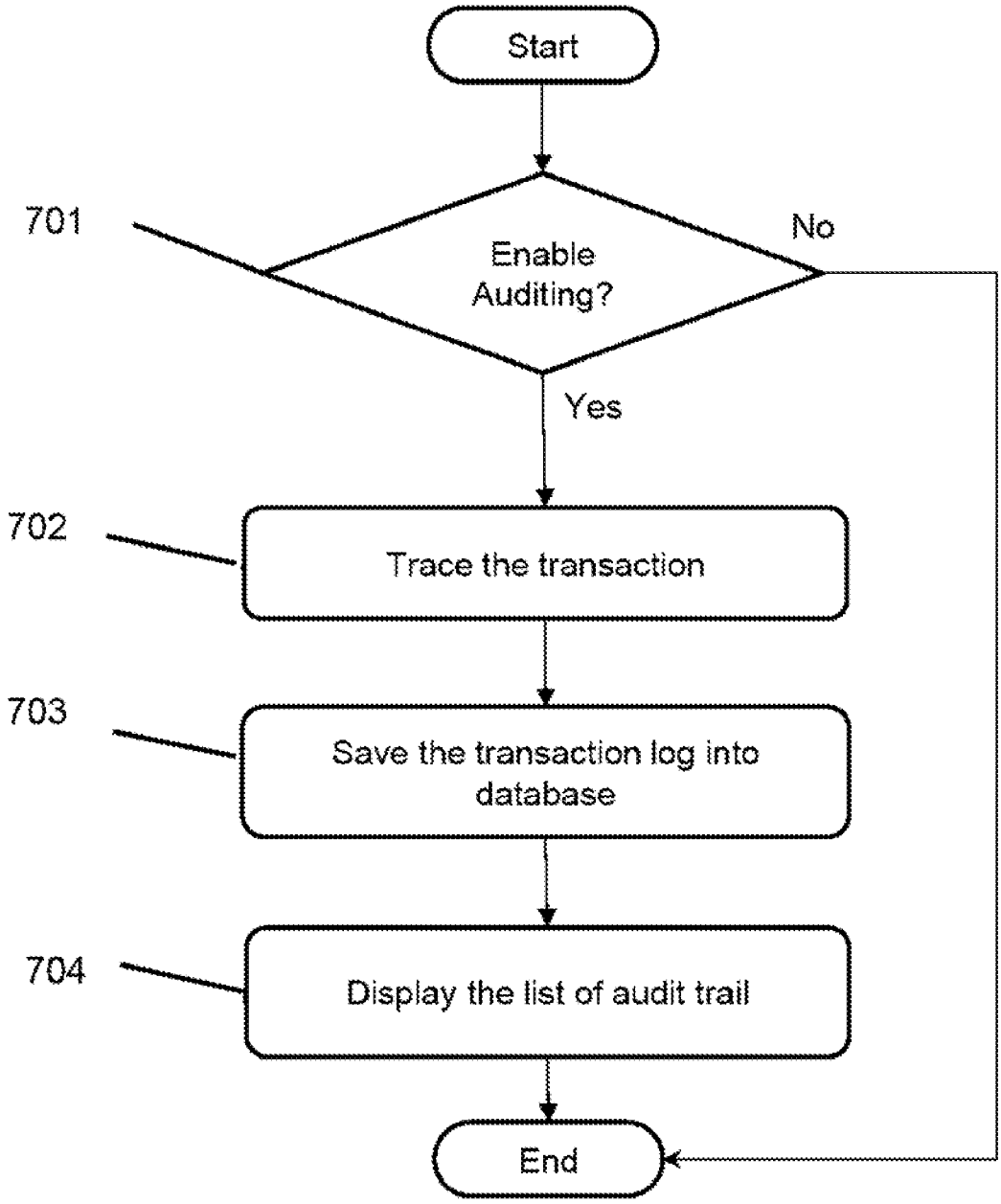

Figure 7.0

800

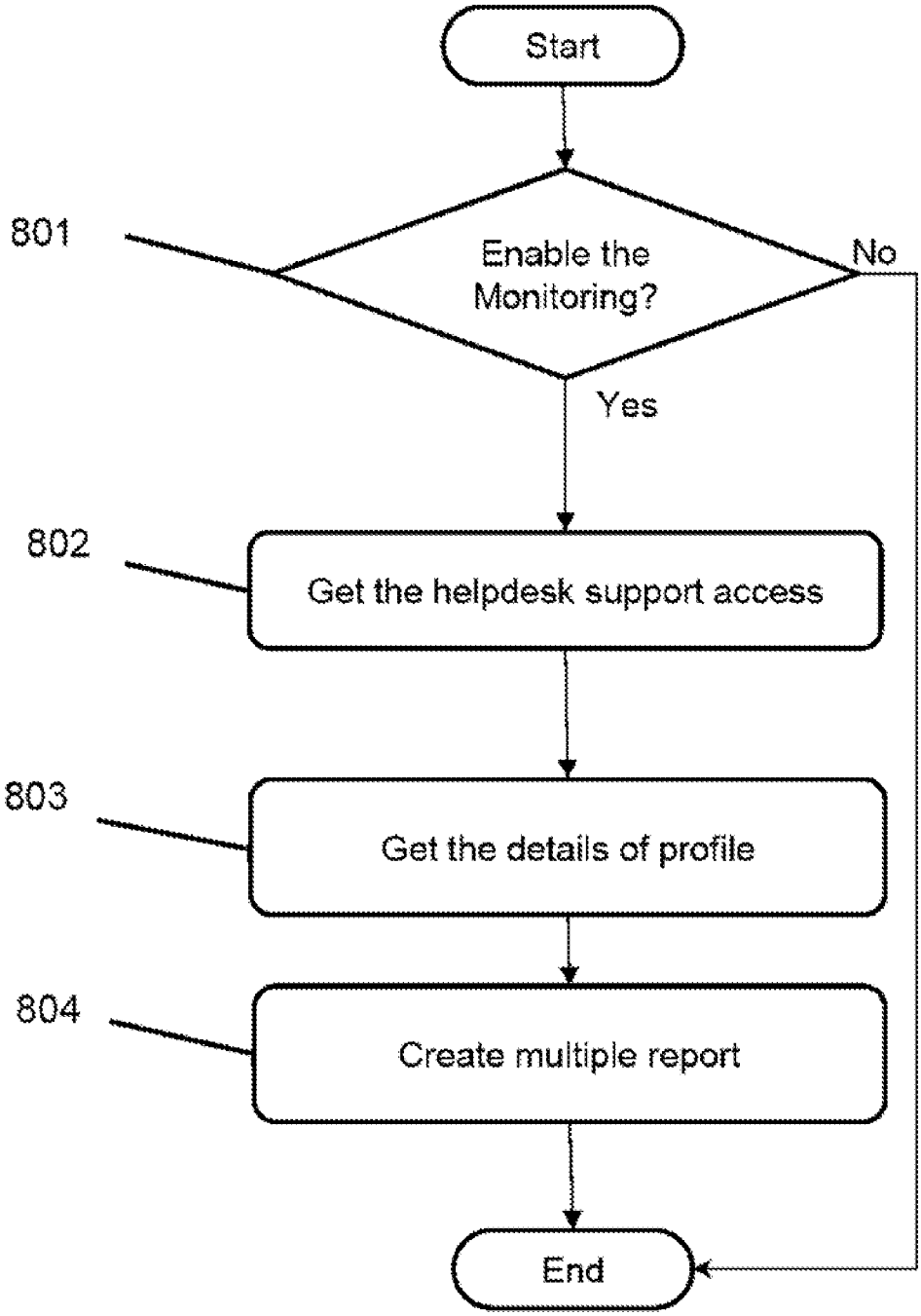

Figure 8.0

INTERNATIONAL SEARCH REPORT

International application No.
PCT/MY2019/050085

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 10/00(2006.01)i, G06Q 10/06(2012.01)i

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)
G06Q 10/00; G06F 007/00; G06F 1730; G06F 3/048; G06Q 30/00; H04L 12/58; H04W 12/06; H04W 4/00; G06Q 10/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: helpdesk, support, classify, protection level, access

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6377944 B1 (ANDREW T. BUSEY et al.) 23 April 2002 See column 10, line 38, column 11, line 27, column 13, lines 24-36 and claim 52.	1-9
Y	US 2012-0309351 A1 (SIDDHARTHA DUTTA) 06 December 2012 See paragraphs [0008],[0059],[0062] and claims 1-8.	1-9
A	US 2009-0100371 A1 (MICHAEL HU) 16 April 2009 See claims 1-8 and figures 1-3.	1-9
A	US 2018-0343223 A1 (LITHIUM TECHNOLOGIES, LLC) 29 November 2018 See paragraphs [0057]-[0060] and claim 1.	1-9
A	US 2004-0073535 A1 (JUN IWASAKI) 15 April 2004 See paragraphs [0020],[0087]-[0089] and claims 1,7.	1-9

☐ 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
"D" document cited by the applicant in the international application
"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	Date of mailing of the international search report
16 April 2020 (16.04.2020)	**16 April 2020 (16.04.2020)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer
JANG, Gijeong
Telephone No. +82-42-481-8364

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/MY2019/050085

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6377944 B1	23/04/2002	None	
US 2012-0309351 A1	06/12/2012	US 2016-0042360 A1	11/02/2016
		US 9171294 B2	27/10/2015
		WO 2012-166694 A1	06/12/2012
US 2009-0100371 A1	16/04/2009	US 2007-0150812 A1	28/06/2007
		US 8560948 B2	15/10/2013
US 2018-0343223 A1	29/11/2018	US 10204344 B2	12/02/2019
		US 10204383 B2	12/02/2019
		US 10489866 B2	26/11/2019
		US 10497069 B2	03/12/2019
		US 2013-0282417 A1	24/10/2013
		US 2013-0282594 A1	24/10/2013
		US 2013-0282603 A1	24/10/2013
		US 2014-0278785 A1	18/09/2014
		US 2018-0341951 A1	29/11/2018
		US 2018-0349916 A1	06/12/2018
		US 2018-0349917 A1	06/12/2018
		US 9141997 B2	22/09/2015
		US 9483802 B2	01/11/2016
		WO 2013-158839 A1	24/10/2013
US 2004-0073535 A1	15/04/2004	JP 04002150 B2	31/10/2007
		JP 2004-064530 A	26/02/2004
		US 7814319 B2	12/10/2010