US011838483B2

(12) **United States Patent**
Nithianand et al.

(10) **Patent No.: US 11,838,483 B2**
(45) **Date of Patent: *Dec. 5, 2023**

(54) **UNIVERSAL SECURE WORKFLOW WITH UPGRADEABLE CAPABILITY SCHEMA WITH CUSTOM COMMANDS, THE UPGRADEABLE CAPABILITY SCHEMA BASED ON THE SUPPLIER MODEL, A GATEWAY IP ADDRESS, AND A DOMAIN NAME**

(71) Applicant: **THINXTREAM TECHNOLOGIES PTD. LTD.**, Singapore (SG)

(72) Inventors: **Ranganathan Nithianand**, Bangalore (IN); **Ranga Raj**, Bangalore (IN); **Teck Lee Low**, Singapore (SG)

(73) Assignee: **Thinxtream Technologies PTE LTD**, Singapore (SG)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **17/947,190**

(22) Filed: **Sep. 19, 2022**

(65) **Prior Publication Data**

US 2023/0216976 A1 Jul. 6, 2023

Related U.S. Application Data

(63) Continuation of application No. 14/801,446, filed on Jul. 16, 2015, now Pat. No. 11,457,123.

(51) **Int. Cl.**
G06F 3/12 (2006.01)
H04N 1/00 (2006.01)
(Continued)

(52) **U.S. Cl.**
CPC ***H04N 1/4426*** (2013.01); ***G06F 3/1204*** (2013.01); ***G06F 3/1222*** (2013.01);
(Continued)

(58) **Field of Classification Search**
CPC G06F 3/1247; G06F 3/1292; G06F 3/1206; G06F 3/1287; G06F 3/1289;
(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

2014/0282481 A1* 9/2014 Ohara G06F 8/654 717/172

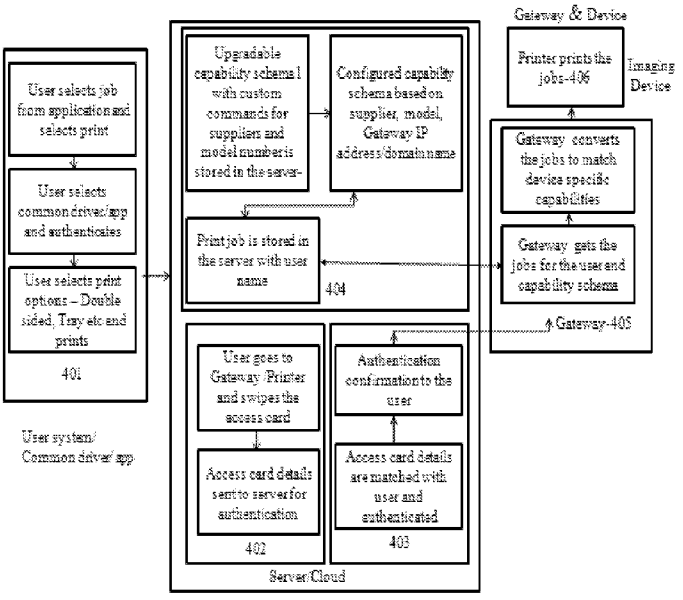
* cited by examiner

Primary Examiner — Chad Dickerson
(74) *Attorney, Agent, or Firm* — Michael D. Eisenberg

(57) **ABSTRACT**

Embodiments disclosed include systems and methods for computer automated print services control comprising authenticating a user credential input via a user device. The system and method includes generating, by a printer driver comprised in the user device, a user interface comprising features supported by a plurality of printing devices. Further, it includes receiving via the user device over the network, a print instruction comprising the features supported by the plurality of printing devices connected to the computer system over the network. And based on the print instruction, generating a print job in an embodiment. Further, based on the user authentication at one of the plurality of printing devices, converting via a gateway, the received print instruction into a format compatible with that printing device and releasing the generated print job for printing at that printing device, according to an embodiment.

12 Claims, 7 Drawing Sheets



(51) **Int. Cl.**

H04N 1/44	(2006.01)
G06F 21/60	(2013.01)
G06K 15/00	(2006.01)

(52) **U.S. Cl.**

CPC ***G06F 3/1236*** (2013.01); ***G06F 3/1238*** (2013.01); ***G06F 3/1244*** (2013.01); ***G06F 3/1267*** (2013.01); ***G06F 3/1276*** (2013.01); ***G06F 3/1285*** (2013.01); ***G06F 3/1288*** (2013.01); ***G06F 3/1292*** (2013.01); ***G06F 3/1298*** (2013.01); ***G06F 21/608*** (2013.01); ***G06K 15/4095*** (2013.01); ***H04N 1/0023*** (2013.01); ***H04N 1/00501*** (2013.01); ***H04N 1/00854*** (2013.01); ***H04N 1/4406*** (2013.01); *G06F 3/1247* (2013.01); *H04N 2201/006* (2013.01); *H04N 2201/0094* (2013.01)

(58) **Field of Classification Search**

CPC G06F 3/1204; G06F 3/1222; G06F 3/1236; G06F 3/1238; G06F 3/1244; G06F 3/1267; G06F 3/1276; G06F 3/1285; G06F 3/1288; G06F 3/1298; H04N 1/0023; H04N 1/00501; H04N 1/00854; H04N 1/4406; H04N 1/4426; H04N 2201/006; H04N 2201/0094; G06K 15/4095; G06K 7/10297

USPC 358/1.11–1.18, 1.9, 2.1, 1.5, 1.2; 709/203, 208, 223, 229; 455/556.2, 557

See application file for complete search history.

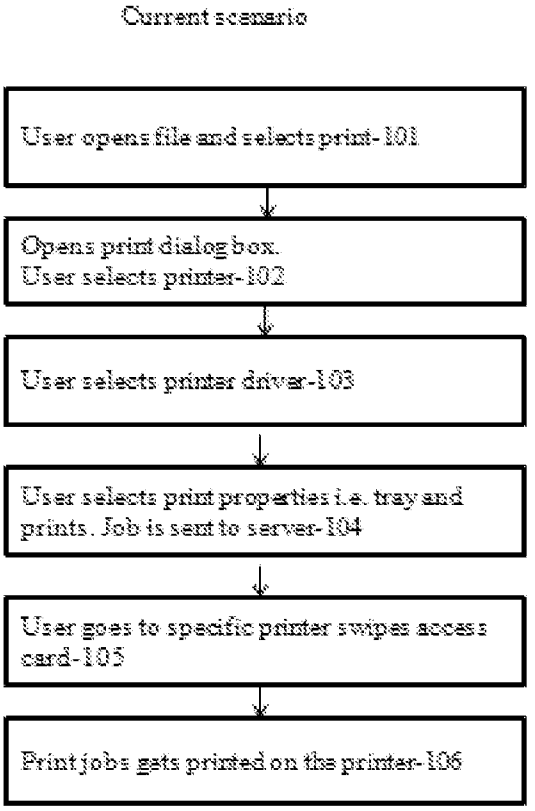

Current scenario
User opens file and selects print-101
Opens print dialog box.
User selects printer-102
User selects printer driver-103
User selects print properties i.e. tray and prints. Job is sent to server-104
User goes to specific printer swipes access card-105
Print jobs gets printed on the printer-106

FIG.1

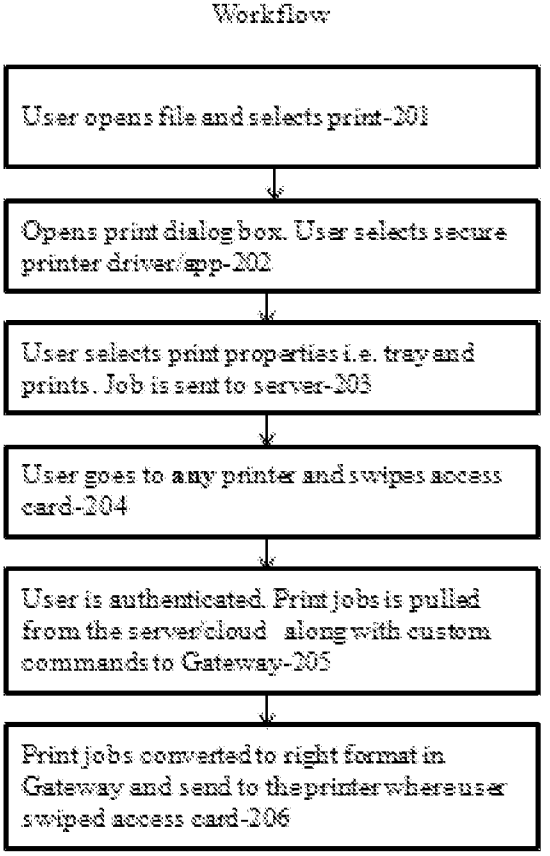

Workflow
User opens file and selects print-201
Opens print dialog box. User selects secure printer driver/app-202
User selects print properties i.e. tray and prints. Job is sent to server-203
User goes to any printer and swipes access card-204
User is authenticated. Print jobs is pulled from the server/cloud along with custom commands to Gateway-205
Print jobs converted to right format in Gateway and send to the printer where user swiped access card-206

FIG.2

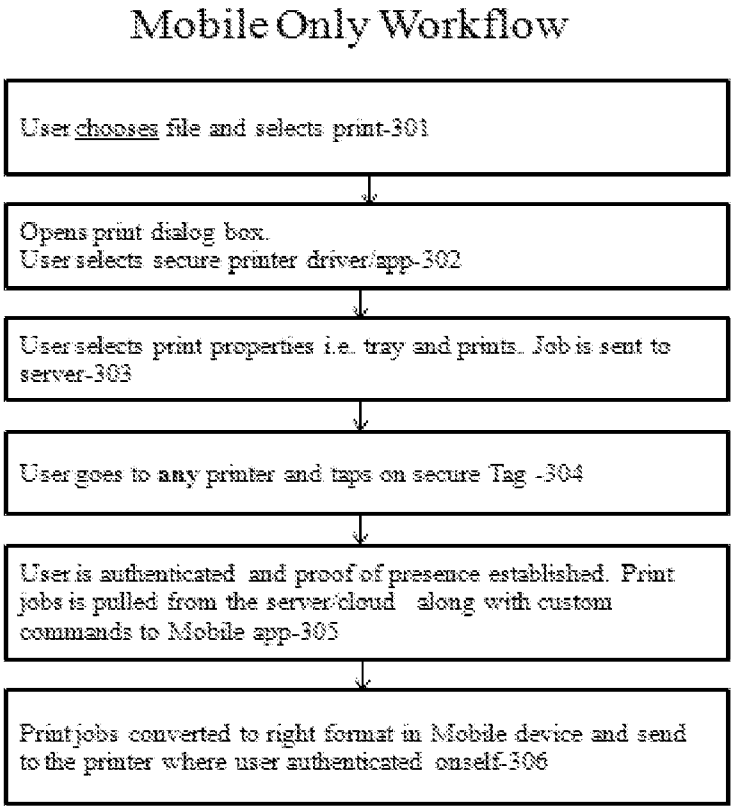

Mobile Only Workflow
User chooses file and selects print-301
Opens print dialog box.
User selects secure printer driver/app-302
User selects print properties i.e. tray and prints. Job is sent to server-303
User goes to any printer and taps on secure Tag -304
User is authenticated and proof of presence established. Print jobs is pulled from the server/cloud along with custom commands to Mobile app-305
Print jobs converted to right format in Mobile device and send to the printer where user authenticated onself-306

FIG.3

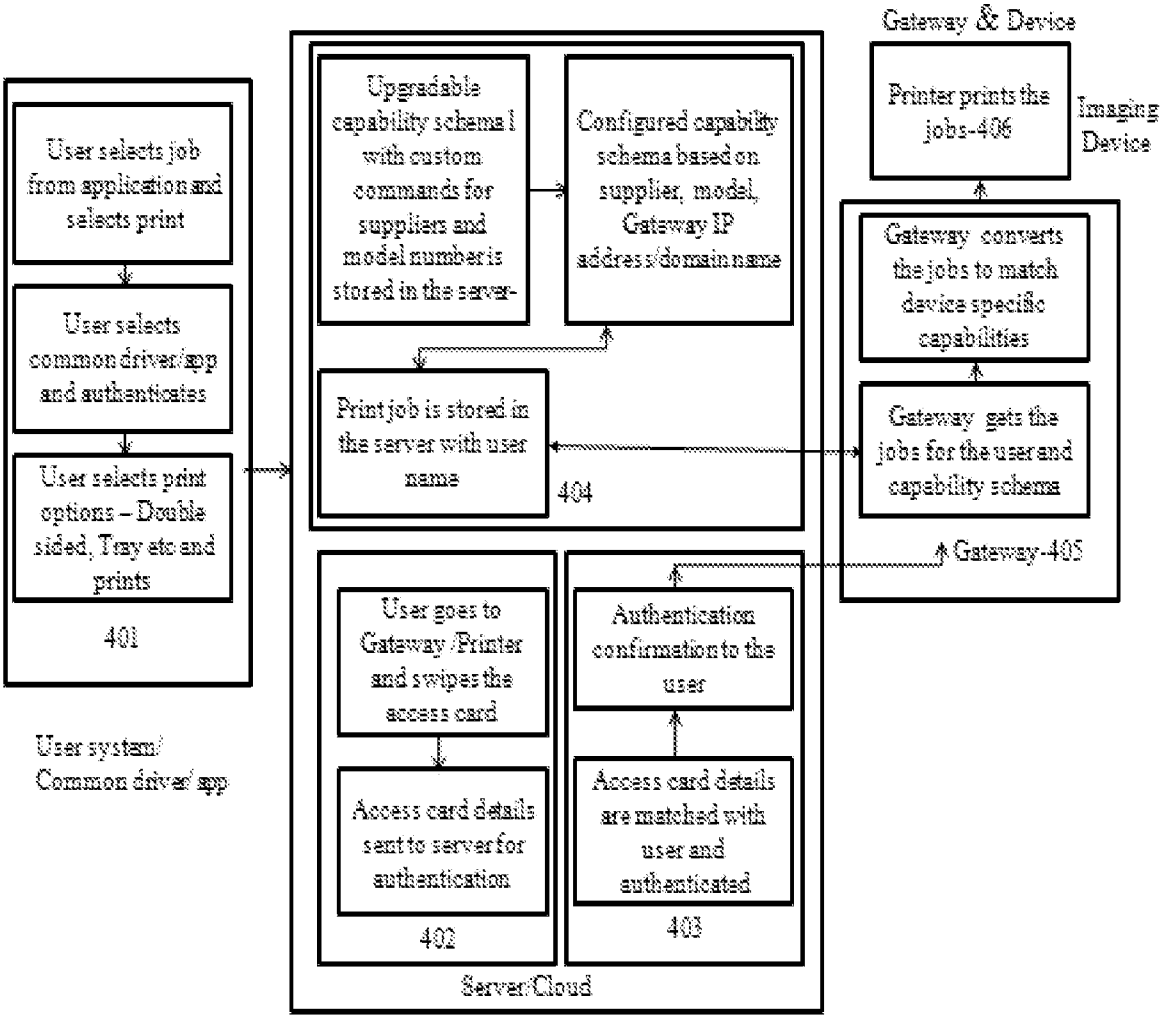

User selects job from application and selects print
User selects common driver/app and authenticates
User selects print options – Double sided, Tray etc and prints
401
User system/ Common driver/ app
Upgradable capability schema I with custom commands for suppliers and model number is stored in the server-
Configured capability schema based on supplier, model, Gateway IP address/domain name
Print job is stored in the server with user name
404
User goes to Gateway /Printer and swipes the access card
Access card details sent to server for authentication
402
Authentication confirmation to the user
Access card details are matched with user and authenticated
403
Server/Cloud
Gateway & Device
Printer prints the jobs-406
Imaging Device
Gateway converts the jobs to match device specific capabilities
Gateway gets the jobs for the user and capability schema
Gateway-405

FIG.4

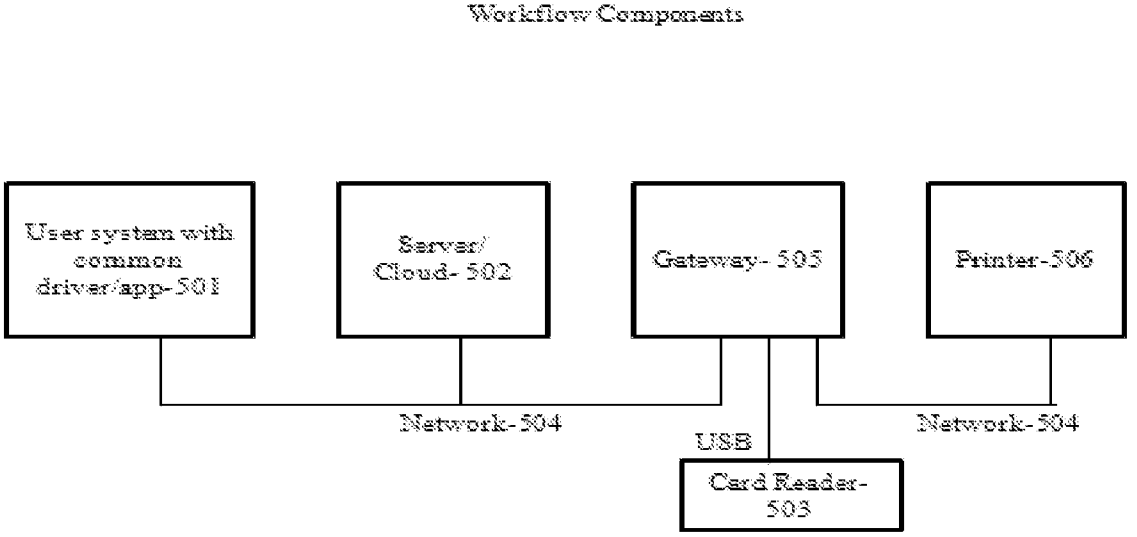

Workflow Components
User system with common driver/app-501
Server/ Cloud- 502
Gateway- 505
Printer-506
Network-504
USB
Network-504
Card Reader-503

FIG.5

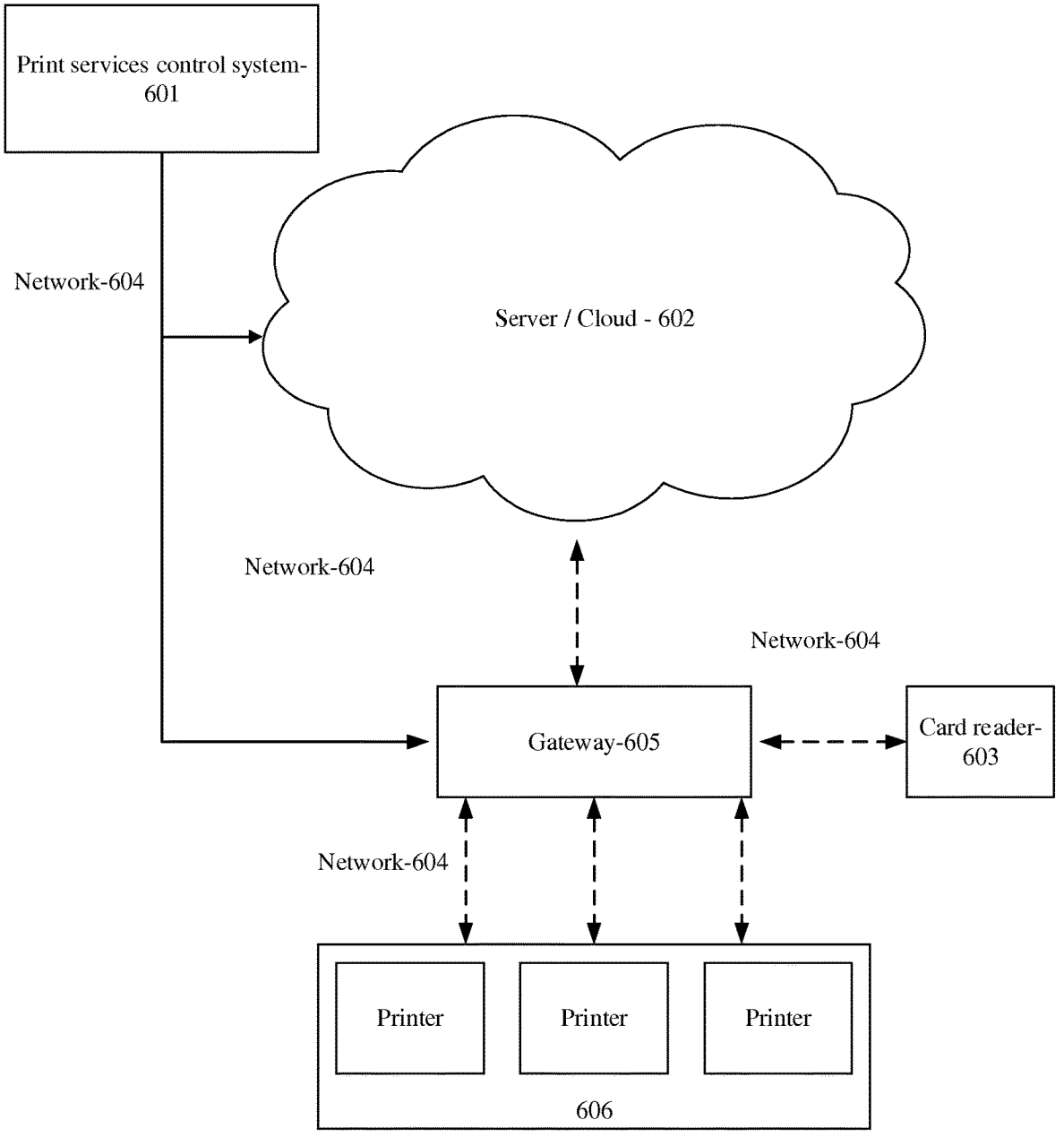

Print services control system-601
Network-604
Server / Cloud - 602
Network-604
Network-604
Gateway-605
Card reader-603
Network-604
Printer
Printer
Printer
606

FIG.6

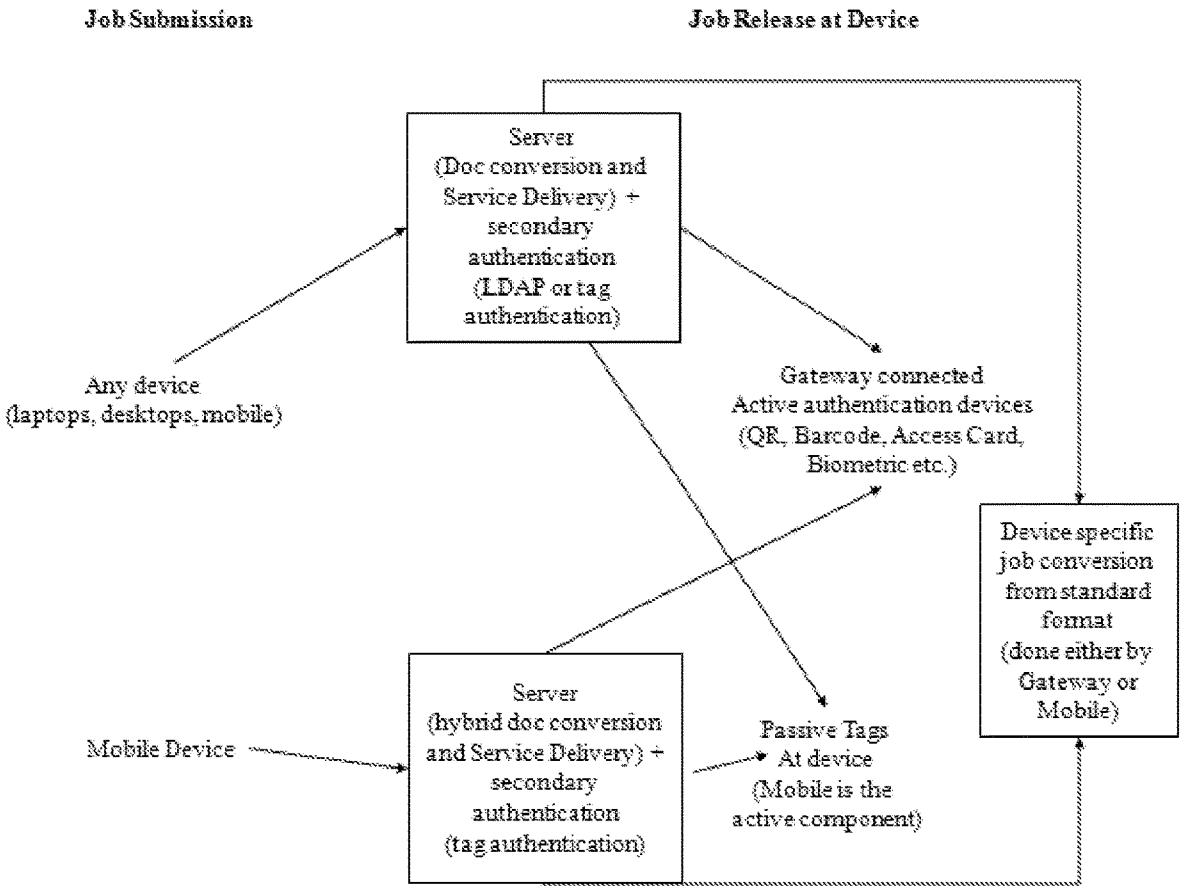

Job Submission
Job Release at Device
Server (Doc conversion and Service Delivery) + secondary authentication (LDAP or tag authentication)
Any device (laptops, desktops, mobile)
Gateway connected Active authentication devices (QR, Barcode, Access Card, Biometric etc.)
Device specific job conversion from standard format (done either by Gateway or Mobile)
Server (hybrid doc conversion and Service Delivery) + secondary authentication (tag authentication)
Mobile Device
Passive Tags At device (Mobile is the active component)

FIG.7

UNIVERSAL SECURE WORKFLOW WITH UPGRADEABLE CAPABILITY SCHEMA WITH CUSTOM COMMANDS, THE UPGRADEABLE CAPABILITY SCHEMA BASED ON THE SUPPLIER MODEL, A GATEWAY IP ADDRESS, AND A DOMAIN NAME

CROSS REFERENCE TO RELATED APPLICATIONS

This application is a continuation of application Ser. No. 14/801,446 entitled "UNIVERSAL SECURE IMAGING WORKFLOW" filed 16th Jul. which is incorporated herein by reference.

BACKGROUND

Field

Universal Secure Imaging Workflow

In general, the challenge is to be able to detect the presence of and authenticate a user by a print services control system to ensure secure printing and user confidentiality. In the context of secure printing, this translates into releasing print jobs queued by the user when he or she is near a secure printer. Print jobs are released by authenticating a registered user at the secure printer, and releasing a previously issued print job by the user, queued and held by a print server, and released over a network upon user authentication.

Related Art

Previously, the above challenge was addressed in the work environment by placing a badge reader (active element) in the context (say printer, in an embodiment), and the employee authenticating by showing his or her issued badge (passive element). Likewise, in the public space, an encoded token (say a boarding pass with a magnetic strip) would be issued to the user and scanned by a reader at the boarding gate in conjunction with other identity establishing mechanisms.

The issue with these mechanisms were: 1. The reader hardware had to be placed in the context (one per printer or one per boarding gate, for example), and the passive element would be with the user. This would add to the infrastructurecost. 2. The reader hardware had the intelligence to read the user tag, authenticate the user/tag, and release the service.

However, with the proliferation of mobile wireless devices, and especially smart mobile devices, there is an opportunity to swap the active and passive elements, thereby reducing infrastructure cost and consolidating processing and service release at the server.

SUMMARY

Embodiments disclosed include a computer automated print services control system comprising: a processor; a memory; a means for communicating over a wired or wireless network; instructions stored in the memory and executed by the processor, which instructions cause the computer system to: authenticate a user credential input via a user device; generate, by a printer driver comprised in the user device, a user interface comprising features supported by a plurality of printing devices; receive via the user device over the network, a print instruction comprising the features supported by the plurality of printing devices connected to the computer system over the network; based on the print instruction, generate a print job; based on the user authentication at one of the plurality of printing devices, convert via a gateway, the received print instruction into a format compatible with that printing device; and release the generated print job for printing at that printing device.

An embodiment further includes in a computer automated print services control system comprising a processor, memory, means for communicating over a wired or wireless network, and instructions stored in the memory and executed by the processor, a method comprising: generating, by a printer driver comprised in a user device, a user interface comprising features supported by a plurality of printing devices; receiving via the user device over the network, a print instruction comprising the features supported by the plurality of printing devices connected to the computer system over the network; based on the print instruction, generating a print job; based on the user authentication at one of the plurality of printing devices, converting via a gateway, the received print instruction into a format compatible with that printing device; and releasing the generated print job for printing at that printing device.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** shows a flow diagram according to aspects of the invention.

FIG. **2** shows a flow diagram according to aspects of the invention.

FIG. **3** shows a mobile only work-flow diagram according to an alternate embodiment.

FIG. **4** shows a details process of flow diagram according to aspects of the invention.

FIG. **5** shows a block diagram according to aspects of the invention.

FIG. **6** shows a block diagram according to aspects of the invention.

FIG. **7** illustrates an additional embodiment wherein conversion to a printer compatible format is performed by a mobile device or by an associated cloud-based converter supporting the mobile device conversion.

DETAILED DESCRIPTION

In the following description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the invention. It will be apparent, however, to one skilled in the art that the invention can be practiced without these specific details.

Reference in this specification to "one embodiment" or "an embodiment" means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the invention. The appearances of the phrase "in one embodiment" in various places in the specification are not necessarily all referring to the same embodiment, nor are separate or alternative embodiments mutually exclusive of other embodiments. Moreover, various features are described which may be exhibited by some embodiments and not by others. Similarly, various requirements are described which may be requirements for some embodiments, but not other embodiments.

All Devices especially printers and Multi-Function Printing (MFP) devices have capabilities that can be leveraged using custom commands specific to each manufacturer as

against standard commands. Many features like Tray selection etc can be supported using standard commands as well as custom commands. The practice has been to support features using custom commands. Very few capabilities are supported using standard commands. The usage of custom commands leads to using Original Equipment Manufacturer (OEM) specific printer drivers. This practice leads to installing device drivers, leading to multiple drivers in each desktop or computing device. The drivers have to be upgraded regularly to support any new features or/and Operating System (OS) upgrades in an environment where different OEM devices are in use.

Further, in today's workplace, Information Technology (IT) users access various devices, especially printers and Multi-Function Printing (MFP) devices to obtain a tangible output. The current IT users in enterprise, medium and small businesses use standard operating procedures and workflows to see their output. The workflow is optimized to deliver accurate and fast results. As per current practice, the user sends a print job to a device or devices associated with their desktop or computing device, using standardized trays for getting their output in the format they want.

Typically, the user prints to Tray **4** (say) if he needs the output on (say) a company letterhead, and that letterhead paper is contained in tray **4**. On the other hand, say the user wants a printout on bond paper, and the bond paper is contained in tray **2**. Accordingly a print instruction for a print job is executed using paper from tray **2**. Usually, the user has prior knowledge of the consumable type available in trays thereby enabling him or her to get the output using the right consumable to meet the need

The user environment typically has different types of printers and MFP devices from different suppliers. In the current scenario, the user needs to have drivers of different models from different suppliers to use the devices effectively

FIG. **1** illustrates via a flow diagram, current practice in prior art systems. In step **101** the user opens a file and selects the print option. In step **102**, the user opens a print dialog box and selects a printer from a single or plurality of connected printers. This step is followed by step **103** wherein the user selects the relevant printer driver according to the selected printer, and in step **104** user printer properties are selected and the created print job is sent to the server (step—**104**). The print job is held by the server till the user goes to the relevant selected printer and swipes an access card at the selected printer, subsequent to which, the print job is released by the server to the assigned printer. In step **106**, the released print job is executed by the selected printer.

FIG. **2** illustrates via a flow diagram the disclosed method according to an embodiment of the present invention. In the first step **201** the user opens a file and selects the print option. In the next step **202** user opens print dialog box and selects a secure printer driver application. In step **203** the user selects print properties i.e. tray and print job, which is then sent to the server. Step **204** involves swiping the user access card at any printer in the network. Upon authentication of the swiped access card, the print job is pulled from the server by the printer at which the access card is swiped along with custom commands to the gateway (step **205**). The pulled print job is held in the gateway, and the custom commands cause the held print job to be converted to a format compatible with the selected printer. Once converted, the print job is executed at the printer in step **206**.

Embodiments disclosed include a computer automated print services control system comprising: a processor; a memory; a means for communicating over a wired or wireless network; instructions stored in the memory and executed by the processor, which instructions cause the computer system to: authenticate a user credential input via a user device; generate, by a printer driver comprised in the user device, a user interface comprising features supported by a plurality of printing devices; receive via the user device over the network, a print instruction comprising the features supported by the plurality of printing devices connected to the computer system over the network; based on the print instruction, generate a print job; based on the user authentication at one of the plurality of printing devices, convert via a gateway, the received print instruction into a format compatible with that printing device; and release the generated print job for printing at that printing device.

FIG. **3** illustrates via a flow diagram the disclosed method according to an alternate embodiment of the present invention. In the first step **301** the user chooses a file for printing. In the next step **302** user opens print dialog box and selects a secure printer driver application. In step **303** the user selects print properties i.e. tray and print job, which is then sent to the server. Step **304** involves identification of a user mobile device at any printer in the network. The mobile device may identify itself via an NFC tap capability, a Bluetooth or low power Bluetooth functionality, an RFID capability, a bar code or a quick response code, an infrared communication capability, or any other short range communications technology already invented or yet to be invented. Upon authentication of the user mobile device and thus proof or presence of the user, the print job is pulled from the server along with custom commands and sent to the authenticated mobile device (step **305**). Finally, in step **306**, the print job/s is/are converted to appropriate format in the authenticated mobile device and sent to the printer which authenticated the said device.

FIG. **4** illustrates a system level diagram according to an embodiment. The system comprises a common driver user application **401** having means to allow a user to select a print job and input a print command. Common driver application enables authentication of print selection. The common drive application further allows the user to select from a plurality of print options—for example, a double sided print job, a tray number, etc. The server, accessible via a network over the cloud comprises modules **402**, **403**, and **404**. Module **404** comprises means for storing the print job in the server along with user identification. Further, module **404** allows upgradable capability schema with custom commands for suppliers and printer or/and MFP device model numbers, stored in the server. Additionally and preferably, the configured capability schema is based on supplier model, Gateway IP address, and domain name. Module **402** comprises a means for accepting/recognizing user access card swipe at a gateway or printer, and authenticating access card details at the server. Module **403** comprises a means for matching received access card details with stored user information and for authenticating a legitimate user. Gateway **405** comprises means for receiving the print job stored in the server for a particular user, and for receiving that particular user's authentication confirmation. The gateway is configured to convert the print job to a format compatible with the selected printing device. Printer **406**, connected to the network via the gateway is where the user access card is swiped, and where the print job is finally executed.

FIG. **5** illustrates an embodiment section view of the system. The system comprises a user device **501** which includes a common driver application. The device is connected and configured to communicate over a network with server **502**, gateway **505**, and via gateway **505**, with printing device **506**. The communication is controlled by the server

and the card reader **503**, wherein an access card swiped by the user is used verify the user identity stored in the server, before releasing a print job associated with a user issued print command.

FIG. **6** illustrates an alternate embodiment of the system. Print services control system **601** is configured to communicate over the network with cloud server **602** and with gateway **605**. Further a print command for a print job to be executed is issued by the control system **601**, and stored in server **602**. The job is released via gateway **605** after being converted into a format compatible with a printer selected from a plurality of print devices **606**. The release of the print job is determined by an access card swipe at card reader **603**, and authentication of the said access card swipe at the server.

An embodiment includes in the system, converting the received print instruction via the gateway and further mapping of the received print instruction from the user device to invoke a manufacturer specific proprietary command based on the selected printing device, and wherein the mapping comprises translating the received instruction to the manufacturer specific proprietary command. According to an embodiment, the said translating of the received instruction comprises converting the received instruction to a printer specific page description language. [PS, PCL3 (HP), PCL 5/6 etc].

Prior art systems face a serious drawback, in that only certain models can be assigned to certain users, because assigning all models of printing devices from all OEMs will consume substantial space on the user device, and all models may not be easily accessible to all users i.e. not close to the user. This forces the users to remember the devices nearer to them and use them only.

Current security mechanisms using pin numbers, etc. are getting replaced by employee access cards, Biometrics and other forms such as Near Field Communication (NFC) which provide higher security i.e. tightly coupled to the user.

According to an embodiment the user authentication comprises, validating the input user credential at a printing device, wherein the validating is invoked via a short range communication means comprising at least one of an NFC tag, a blue tooth pairing functionality, an active or passive RFID tag, an infrared means, a bar code, and a quick response code, each of which is comprised in a printing device of the print services control system.

Preferred embodiments include validating the input user credential at a printing device, wherein the validating is invoked via an access card associated with the authenticated input user credential.

In an embodiment the system is further caused to recognize the user at the printing device based on the authenticated user credential input via the user device mapped to a user ID assigned to the user. The recognized user is authenticated at/by the printing device based on the assigned user ID. Upon authentication, the generated print job stored on the server, is queued at the selected/chosen printing device, and in turn released for delivery at the printing device. Preferred embodiments include configurations that allow the user to queue a secure print job to any of the printing devices connected to the computer system over the network. According to one embodiment the print job is invoked via an NFC tag attached to a printer and a mobile device comprising NFC functionality, such that the mobile device is caused to read the NFC tag and authenticate itself to the computer system based on the input user credential.

According to an additional embodiment the mobile device is configured to select content and generate a print instruction comprising the features supported by the plurality of printing devices connected to the computer system over the network. Based on the print instruction, a print job is generated. And based on the user authentication at one of the plurality of printing devices, the gateway converts the selected content into a format compatible with that selected printing device. However, according to an alternate embodiment, the mobile device further includes an assessment engine configured to determine the format of the selected content, and to determine if the format can be converted to another desired format compatible with the printers in the network. If it is determined that conversion is possible, a conversion engine comprised in the mobile device, and configured to convert the selected content to the other desired format is caused to convert the said selected content. And based on user authentication at one of the plurality of printing devices, the mobile device sends the converted content to the printing device for printing. Also included, according to another embodiment, is a network routing engine configured to route the content over the network, to a cloud-based converter, if the determined format cannot be converted to the desired format. The cloud-based converter converts the content to the desired format, and resends the converted format back to the mobile device. Finally, upon user authentication of the mobile device at a selected printing device, the print job is released by the mobile device, and printed by the printing device. FIG. **7** illustrates an additional embodiment wherein conversion to a printer compatible format is performed by a mobile device or by an associated cloud-based converter supporting the mobile device conversion.

An embodiment includes in a computer automated print services control system comprising a processor, a memory, means for communicating over a wired or wireless network, and instructions stored in the memory and executed by the processor, a method comprising generating, by a printer driver comprised in a user device, a user interface comprising features supported by a plurality of printing devices. The method includes receiving via the interface generated on the user device over the network, a print instruction comprising the features supported by the plurality of printing devices connected to the computer system over the network. Based on the print instruction, the method includes generating a print job, and based on the user authentication at one of the plurality of printing devices, converting via a gateway, the received print instruction into a format compatible with that printing device. And releasing the generated print job for printing at that printing device.

The user can collect the output from any device connected to the network instead of a specifically assigned device. The converting of the received print instruction via the gateway further comprises mapping of the received print instruction from the user device to invoke a manufacturer specific proprietary command based on the selected printing device, and wherein the mapping comprises translating the received instruction to the manufacturer specific proprietary command. The translating of the received instruction comprises converting the received instruction to a printer specific page description language. [PS, PCL3 (HP), PCL 5/6 etc]. The user authentication comprises, validating the input user credential at a printing device, wherein the validating is invoked via a short range communication means comprising at least one of an NFC tag, a blue tooth pairing functionality, an active or passive RFID tag, an infrared means, a bar code, and a quick response code, each of which is comprised in a printing device of the print services control system.

Embodiments of the disclosed method further comprise recognizing the user at the printing device based on the

authenticated user credential input via the user device mapped to a user ID assigned to the user. The method includes authenticating the recognized user at the printing device based on the assigned user ID, queuing the generated print job at the printing device, and releasing the queued context generated print job for delivery at the printing device. Preferably, the method further comprises allowing the user to queue a secure print job to any of the printing devices connected to the computer system over the network.

In an alternate embodiment, the method comprises invoking the print job via the NFC tag attached to a printer communicatively coupled to a mobile device comprising NFC functionality, such that the mobile device is caused to read the NFC tag and authenticate itself to the computer system based on the input user credential.

According to an additional embodiment, the method includes configuring the mobile device for selecting content and for generating a print instruction for the selected content. Of course, the print instruction is selected according to features supported by the plurality of printing devices connected to the computer system over the network. Based on the print instruction, a print job is generated. And based on the user authentication at one of the plurality of printing devices, the gateway converts the selected content into a format compatible with that selected printing device. However, according to an alternate embodiment, the method includes, determining via an assessment engine comprised in the mobile device, the format of the selected content, and further determining if the format can be converted to another desired format compatible with the printers in the network. If it is determined that conversion is possible, the method proceeds to convert via a conversion engine comprised in the mobile device, the said selected content to the said desired format. And based on user authentication at one of the plurality of printing devices, the method includes sending by the mobile device the converted content to the printing device for printing. Also included in the method, according to another embodiment, is a routing step via a network routing engine configured to route the content over the network, to a cloud-based converter, if the determined format cannot be converted to the desired format. This is followed by a converting step by the cloud-based converter, which is configured to convert the content to the desired format, and to resend the converted format back to the mobile device. Finally, upon user authentication of the mobile device at a selected printing device, the print job is released by the mobile device, and printed by the printing device.

Alternate embodiments include modifications and variations as would be apparent to a person having ordinary skill in the art. An example embodiment can be implemented for secure printing in a hospital, at a corporate organization, a bank, etc. For example, an issuer issues a job to a server and then switches to a requester mode at any imaging device to authenticate himself or herself, and collect the desired output. An alternate mode includes a delegating mode, wherein the issuer issuer issues the job and delegates to a requester(s) for the requester(s) to authenticate themselves to collect desired outputs. Applications can also be varied. For example, systems and methods disclosed can be used to book and receive tickets/passes to a movie or event, to create a travelers or cashier's check and redeem the created check at a terminal (such as an ATM machine), to create or apply for and redeem a coupon or voucher, to redeem a received doctor's prescription, etc.

The networked printing or imaging device could have special stationery in trays and depending on the request, the issuer can issue a job that upon authentication by the requester, the desired job gets released. For example, the trays could be assigned or/and designated to only execute specific jobs. Say some trays are healthcare jobs trays-they can have prescriptions, diagnosis results etc. in healthcare. Say other trays are entertainment trays-they can be configured to print tickets/passes for different events or movies. And so on. Again the networked printing devices need not be restricted to conventional 2D devices. There may be, in the network, a variety of imaging devices, medical, entertainment, banking devices, and 3D, 4D or/and other printing devices already invented or yet to be invented.

There now are available, several short range communication (SRC) protocols, which are supported by the major mobile operating systems. The mobile operating system, in general, monitors the communication channel, and then invokes the relevant app that can handle the communication. Near Field Communication (NFC) is one such widely supported short range communication technology. The NFC tag is generally passive, and contains the following: a tag ID that can be used to uniquely identify the tag; an authentication token that can be used to authenticate the tag itself; an application identifier in a format understood and used by the mobile operating system to invoke the relevant application; and additional context information that can be read by the app itself.

Once the mobile device is in proximity of the NFC tag, the mobile operating system (OS) invokes the relevant application and passes all the other parameters above to it for further processing. From a usability perspective, the OS even prompts the user to download and install the relevant application to the user device, if not already present. The application presents the graphical user interface which allows the user to provide his credentials. The application now has three raw pieces of information—the user credentials, the tag info, and the additional context info, in addition to having established presence of the user in the context due to the nature of the technology. The application sends all of the information to the server, which authenticates the user and the tag. Once authenticated, it can use the additional context information to deliver the service in the context.

Embodiments disclosed eliminate the need to have multiple print drivers from different OEMs. Users can use any device connected to the network with the secure print driver installed on the user device. All the current drivers use custom commands making it difficult to replace the driver with a single driver.

Embodiments disclosed allow for one common driver/application irrespective of which manufacturer or OEM equipment is used. This results in a single driver or application as against multiple drivers for different models and different OEMs. Preferred embodiments leverage the gateway to support different Page Description Languages and to support capabilities that use custom commands. Embodiments allow for the current workflow to be preserved, thereby enabling seamless integration into the existing environment. Preferred embodiments enable usage of the data model in the server to send custom commands based on supplier and model to the Gateway and append the commands to execute a print job at a selected print device, thus enabling virtualization of the output device. Traditional workflows have a one-one correlation between the job submission app/driver and the device manufacturer. With the proposed workflow in the disclosed embodiments, secure imaging workflows disassociate the app/driver from the vendor/OEMs equipment and location, thus allowing for the user to swipe and collect their output from any device in the

network instead of a specific device. Embodiments disclosed also eliminate the need for expensive hardware the printer terminals, as alternate embodiments utilize user mobile devices as the active component in short range communications initiation. Embodiments disclosed also enable conversion of the pulled print jobs at the user mobile devices into the appropriate format instead of at the gateway, before being sent to the print terminal for printing.

Since various possible embodiments might be made of the above invention, and since various changes might be made in the embodiments above set forth, it is to be understood that all matter herein described or shown in the accompanying drawings is to be interpreted as illustrative and not to be considered in a limiting sense. Thus it will be understood by those skilled in the art that although the preferred and alternate embodiments have been shown and described in accordance with the Patent Statutes, the invention is not limited thereto or thereby.

The figures illustrate the architecture, functionality, and operation of possible implementations of systems and methods according to various embodiments of the present invention. It should also be noted that, in some alternative implementations, the functions noted/illustrated may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved.

The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting of the invention. As used herein, the singular forms "a", "an" and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms "comprises" and/or "comprising," when used in this specification, specify the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof.

In general, the steps executed to implement the embodiments of the invention, may be part of an automated or manual embodiment, and programmable to follow a sequence of desirable instructions.

The present invention and some of its advantages have been described in detail for some embodiments. It should be understood that although some example embodiments of the Universal Secure Imaging Workflow system and method are described with reference to secure printing across various devices, especially printers and Multi-Function Printing (MFP) devices, the system and method disclosed is reconfigurable, and embodiments include systems that may be dynamically adapted to be used in other contexts as well. It should also be understood that various changes, substitutions and alterations can be made herein without departing from the spirit and scope of the invention as defined by the appended claims. An embodiment of the invention may achieve multiple objectives, but not every embodiment falling within the scope of the attached claims will achieve every objective. Moreover, the scope of the present application is not intended to be limited to the particular embodiments of the process, machine, manufacture, and composition of matter, means, methods and steps described in the specification. A person having ordinary skill in the art will readily appreciate from the disclosure of the present invention that processes, machines, manufacture, compositions of matter, means, methods, or steps, presently existing or later to be developed are equivalent to, and fall within the scope of, what is claimed. Accordingly, the appended claims are intended to include within their scope such processes, machines, manufacture, compositions of matter, means, methods, or steps.

We claim:

1. A computer automated control system comprising:

a processor; a memory; a means for communicating over a wired or wireless network; instructions stored in the memory and executed by the processor, which instructions cause a computer system to:

via a common driver user application, authenticate an identified user wireless device;

receive an input a command selected from a plurality of commands through the authenticated and identified user wireless device;

store the selected input command in a server along with user identification;

wherein the command is stored in the server via a first module comprising upgradable capability schema with custom commands for a single or plurality of service delivery devices;

the upgradable capability schema is based on a supplier model, a gateway IP address, and a domain name;

via the common driver user application, authenticate the selected input command;

via a second module comprised in the server, authenticate the user wireless device at a gateway or a service delivery device from the single or plurality of service delivery devices by matching received user identification details at the gateway or the service delivery device with stored user identification in the server;

based on authentication of the user wireless device, release a deliverable to the selected service delivery device.

2. The computer automated control system of claim **1** wherein the computer automated control system comprises:

a print services control system;

the single or plurality of service delivery devices comprise a corresponding single or plurality of printers; and

releasing the deliverable to the selected delivery device comprises releasing a print job to the selected printing device.

3. The computer automated control system of claim **2** wherein the gateway is further configured to:

convert a generated print job based on the received input command into a compatible format; and

map the input command from the gateway to a manufacturer specific proprietary command based on the selected printing device.

4. The computer automated control system of claim **3** wherein:

said mapping of the received input command comprises converting the received input command to a printer specific page description language; and

wherein the printer specific page description language comprises at least one of PS, PCL3 (HP), PCL 5, and PCL 6.

5. The computer automated control system of claim **3** wherein the computer automated control system is further caused to:

authenticate the user wireless device, wherein the authentication is invoked via a short range communication means comprising at least one of an NFC tag, a blue tooth pairing functionality, an active or passive RFID tag, an infrared means, a bar code, and a quick response code, each of which is comprised in a service delivery device of the computer automated control system.

6. The computer automated control system of claim 5 wherein the computer automated control system is further caused to:

based on the authentication of the user wireless device, queue a generated deliverable at the selected service delivery device;

release the queued generated deliverable at the selected service delivery device; and

wherein the release of the deliverable is initiated via at least one of the user wireless device and the gateway.

7. The computer automated control system of claim 6 wherein the computer automated control system is configured to:

queue a secure print job via the user wireless device or gateway to at least one of the selected printing devices connected to the computer system over the network.

8. In a computer automated control system comprising a processor, memory, means for communicating over a wired or wireless network, and instructions stored in the memory and executed by the processor, a method comprising:

via a common driver user application, authenticating an identified user wireless device;

receiving an input command selected from a plurality of commands through the authenticated and identified user wireless device;

storing the selected input command in a server along with user identification;

wherein the selected input command is stored in the server via a first module comprising upgradable capability schema with custom commands for a single or plurality of service delivery devices;

the upgradable capability schema is based on a supplier model number, a gateway IP address, and a domain name;

via the common driver user application, authenticating the selected input command;

via a second module comprised in the server, authenticating the user wireless device at a gateway or a service delivery device from the single or plurality of service delivery devices by matching received user identification details at the gateway or the service delivery device with stored user identification in the server;

based on authentication of the user wireless device, releasing a deliverable to the selected service delivery device.

9. The method of claim 8 wherein:

the single or plurality of service delivery devices are comprised in a print services control system;

the single or plurality of service delivery devices comprise a corresponding single or plurality of printers; and

releasing the deliverable by to selected delivery device comprises releasing a print job to the selected printing device.

10. The method of claim 9 further comprising converting of a generated print job based on a received input command via the gateway, which further comprises mapping of the received input command from the gateway to a manufacturer specific proprietary command based on the selected printing device.

11. The method of claim 10 wherein said mapping of the received input command comprises converting the received input command to a printer specific page description language; and

wherein the printer specific page description language comprises at least one of PS, PCL 3 (HP), PCL 5, and PCL 6.

12. The method of claim 8 further comprising:

authenticating the user wireless device at the service delivery device based on the input user credential;

queuing a generated deliverable at the service delivery device; and

releasing the queued generated deliverable by the service delivery device; and

wherein the release of the deliverable is initiated via at least one of the user mobile device and the gateway.

* * * * *