A SYSTEM FOR APPLYING FOR A VISA FOR TEMPORARY ENTRY INTO A COUNTRY OR TERRITORY ON A COMPUTER DEVICE

Field

The present disclosure relates to a digital wallet system for electronically applying for a visa for temporary entry into a country or territory. The present disclosure also relates to a method for electronically applying for a visa for temporary entry into a country or territory.

Background

International travel has become increasingly accessible to the general public in recent years. One reason for this could be the increasing affordability of airfares which may be due to the advent of budget airlines. Additionally, an increased interest in travelling internationally may also be due to an increased amount of time spent watching television and the rising popularity of travel documentaries or movies depicting foreign landscapes.

An aspect of international travel that is usually dreaded by travellers is the immigration procedures necessary to gain legal entry into a foreign country, usually through obtaining a valid visa. The visa application process for each country is different and typically has varying procedures depending on the applicant's nationality. Therefore, travellers who want to visit a country for the first time may feel daunted if the process is complicated and may abandon their travel plan altogether. For a traveller who is travelling to multiple countries, it may be difficult to keep track of the varying processes and requirements for each country which may place undue stress upon a traveller.

An alternative which a traveller may consider is to use a travel agent. A travel agent may alleviate some of the stresses associated with the administrative processes involved in planning a trip. However, engaging a travel agent will incur additional fees which may be expensive. Additionally, this may be time consuming involving multiple meetings or correspondences with the travel agent to finalise a trip.

There are many different types of visas and visa application processes. Some

countries with more advanced systems may have an online visa application process and may issue an electronic visa (e-visa) prior to travel. This is convenient and travellers would know prior to travel that they have secured a legitimate travel document allowing entry into the country of interest. However, some countries may only offer visa on arrival applications. These applications are typically only available at the destination country's immigration check point, i.e. at the airport if travelling by air or at the border if travelling by land. This means that the traveller may not be aware of the documents required, actual process involved or visa application fee prior to travelling. This uncertainty may cause anxiety in a traveller which will diminish their travel experience.

A traveller typically has to go through many steps involving various waiting times before he or she is legally allowed to enter the country. For example, a traveller travelling by airplane would be largely confined to his or her seat throughout the period of travel. Upon touchdown of the airplane, the traveller would have to wait for his or her turn to disembark from the plane into the airport terminal. Following this, the traveller has to wait for his or her luggage if they checked one in. Finally, the traveller would lug their luggage towards the immigration/customs checkpoint. At this point, the traveller may not be in the most patient or tolerant state of mind.

A traditional visa-on-arrival immigration process involves:

(a) a traveller obtaining a paper application form;
(b) rummaging through his or her bag to obtain the appropriate documents;
(c) finding a pen and a location to fill in the form;
(d) filling in the form referencing multiple documents;
(e) joining a queue to submit the application form and relevant documents;
(f) showing the form and documents to the immigration officer;
(g) waiting for the immigration officer to go through the relevant documents;
(h) if required, answering any additional questions or amending the form;
(i) if required, paying a fee to obtain the visa;
(j) waiting for the visa to be issued; and
(k) obtaining the visa and returned documents.

This process takes a long time and as such may result in a bottleneck of travellers at

this point of the process. Additionally, travellers may not be aware of the documents required for the application process. This is an undesirable situation to be in as the traveller may be unable to enter the country without fulfilling the necessary requirements or documents and in the worst case, may be deported.

An additional frustration with this process may be the payment of fees associated with the visa. This is usually in the country's local currency. Travellers may not be aware of the total cost and as such may not have obtained sufficient local currency prior to travelling. A traveller would have to hunt down an ATM or money changer within the airport. Sometimes, an option is available to transact in a foreign currency however, these options usually offer unfavourable exchange rates.

From the visa processing entity's point of view, cash transactions may be cumbersome. Sufficient cash for providing change in a variety of denominations need to be ensured throughout operational hours. Additionally, good security protocols need to be implemented to mitigate mishandling of cash, theft or robbery. Finally, cash transactions increase the processing time of visa on arrival applications.

With the advent of new electronic payment systems, travellers are more readily equipped to perform electronic payment transactions. Most travellers would have payment cards (magnetic stripe, EMV or NFC-enabled) in the form of a credit or debit card which may be capable of performing transactions in foreign currencies. Digital wallets are also becoming increasingly popular enabling users to use their mobile computer device to complete an electronic payment transaction.

Traditional visa applications in the form of paper hardcopy applications may result in a number of issues. Firstly, the vast number of applications would result in a large amount of documents that would need to be filed or stored appropriately. A filing system would need to be implemented with assigned personnel to manage this system. Additionally, a dedicated storage area for the documents would need to be maintained. To retrieve a document at a later date would require a substantial amount of time and effort. In addition, paper applications may be susceptible to erroneous entries. This may be due to the application form being hastily written by a tired, impatient traveller. Additionally, the information may not be legible due to bad handwriting.

Traditional visa on arrival checkpoints require immigration officers to be stationed there, in some cases 24 hours 7 days a week, which is costly and inefficient. Additionally, these applications need to be assessed in their entirety resulting in a long processing time and potential bottlenecks.

It is generally desirable to overcome or ameliorate one or more of the above mentioned difficulties, or at least provide a useful alternative.

Summary of Invention

In accordance with embodiments of the present disclosure, there is provided a digital wallet system for electronically applying for a visa for temporary entry into a country or territory, comprising one or more processors in communication with non transitory data storage having instructions stored thereon which, when executed by the processor or processors, cause the system to perform the steps of:

(a) receiving, from a request server, a request for a user's data including the user's digital wallet account login data;

(b) using the digital wallet account login data to access the user's digital wallet account data stored in said data storage and verifying that the login data matches the user's digital wallet account data;

(c) retrieving user communication data associated with the user’s digital wallet account data, the communication data including details of the user's preferred mode of communication;

(d) sending a request to the user in accordance with the user's preferred mode of communication for user permission to send the user's data for a visa application;

(e) receiving user permission data to send the user's data for the visa application;

(f) retrieving the user's data for the visa application from data storage; and

(g) sending, to the request server, the user's data for the visa application so as to electronically apply for a visa for the user.

In accordance with some embodiments, there is also provided a method for electronically applying for a visa for temporary entry into a country or territory, comprising:

(a) receiving, from a request server, a request for a user's data including

the user's digital wallet account login data;

(b) using the digital wallet account login data to access the user's digital wallet account data stored in said data storage and verifying that the login data matches the user's digital wallet account data;

(c) retrieving user communication data associated with the user’s digital wallet account data, the communication data including details of the user's preferred mode of communication;

(d) sending a request to the user in accordance with the user's preferred mode of communication for user permission to send the user's data for a visa application;

(e) receiving user permission data to send the user's data for the visa application;

(f) retrieving the user's data for the visa application from data storage; and

(g) sending, to the request server, the user's data for the visa application so as to electronically apply for a visa for the user.

In accordance with some embodiments, there is also provided a non-transitory computer readable storage medium embodying thereon a program of computer readable instructions which, when executed by one or more processors of a digital wallet system in communication with a plurality of devices, cause the system to electronically apply for a visa for temporary entry into a country or territory, the method embodying the steps of:

(a) receiving, from a request server, a request for a user's data including the user's digital wallet account login data;

(b) using the digital wallet account login data to access the user's digital wallet account data stored in said data storage and verifying that the login data matches the user's digital wallet account data;

(c) retrieving user communication data associated with the user’s digital wallet account data, the communication data including details of the user's preferred mode of communication;

(d) sending a request to the user in accordance with the user's preferred mode of communication for user permission to send the user's data for a visa application;

(e) receiving user permission data to send the user's data for the visa application;

(f) retrieving the user's data for the visa application from data storage; and

(g) sending, to the request server, the user's data for the visa application so as to electronically apply for a visa for the user.

Brief Description of the Drawings

Embodiments of disclosure are hereafter described, by way of non-limiting example only, with reference to the accompanying drawing in which:

Figure 1 is a schematic diagram of a system for allowing travellers to apply for a visa application using a mobile computer device;

Figure 2 is a block diagram of a mobile computer device of the system shown in Figure 1;

Figure 3 is a flow diagram showing steps performed by a digital wallet application being executed by the mobile computer device of the system shown in Figure 1;

Figure 4 is an image of an exemplary embodiment of the mobile computer device shown in Figure 1;

Figure 5 is a flow diagram showing the onboarding process of the digital wallet application process shown in Figure 3;

Figure 6 is a flow diagram showing the visa application process of the digital wallet application process shown in Figure 3;

Figure 7 is a flow diagram showing the payment transaction process of the digital wallet application process shown in Figure 3;

Figure 8 is a flow diagram showing interoperation of the components of the system to execute the visa application process; and

Figure 9 is a flow diagram showing interoperation of the components of the system to execute the visa approval process; and

Figure 10 is a is a schematic diagram showing components of an exemplary server of the system shown in Figure 1.

Detailed Description of Embodiments of the Invention

The system 10 shown in Figure 1 allows travellers who use digital wallets to electronically apply for a visa for temporary entry into a country or territory using a digital wallet application. The system 10 includes one or more of the following:

(a) a mobile computer device 12;

(b) a digital wallet system 14;
(c) a request server 16;
(d) a visa authority system 22;
(e) an onsite system 18; and
(f) a third party payment processor server 24.

The components of system 10 are in communication via the network 20. The communication network 20 may include the Internet, telecommunications networks and/or local area networks.

The system 10 makes visa application processes simpler, faster and more convenient. The system 10 removes the hassle of the traditional visa on arrival application process usually located at the onsite customs checkpoint. The system 10 allows for electronic payment transactions to pay for fees associated with the visa application.

Mobile Computer Device 12

Figure 2 is a block diagram showing an exemplary device 12 in which embodiments of the invention may be practiced. The device 12 is preferably a mobile computer device such as a smart phone, a personal data assistant (***PDA***), a palm-top computer, and multimedia Internet enabled cellular telephones. In another preferred embodiment, the mobile computer device 12 is a computer system, for example, a laptop or desktop computer.

For ease of description, the device 12 is below described, by way of non-limiting example, with reference to a mobile device in the form of an iPhone, such as the one shown in Figure 4, or one manufactured by LG™, HTC™ or Samsung, for example.

As shown, the device 12 includes the following components in electronic communication via a bus 106:

(a) a display 102;
(b) non-volatile (non-transitory) memory 104;
(c) random access memory ("RAM") 108;
(d) N processing components 110;
(e) a transceiver component 112 that includes N transceivers; and

(f) user controls 114.

Although the components depicted in Figure 2 represent physical components, Figure 2 is not intended to be a hardware diagram. Thus, many of the components depicted in Figure 2 may be realized by common constructs or distributed among additional physical components. Moreover, it is certainly contemplated that other existing and yet-to-be developed physical components and architectures may be utilized to implement the functional components described with reference to Figure 2.

The display 102 generally operates to provide a presentation of content to a user, and may be realized by any of a variety of displays (e.g., CRT, LCD, HDMI, micro-projector and OLED displays).

In general, the non-volatile data storage 104 (also referred to as non-volatile memory) functions to store (e.g., persistently store) data and executable code including code that is associated with the functional components of a Digital Wallet (DW) Application (App) 118 that executes the processes 300 set out in Figure 3.

In some embodiments for example, the non-volatile memory 104 includes bootloader code, modem software, operating system code, file system code, and code to facilitate the implementation of one or more portions of the DW App 118 as well as other components, well known to those of ordinary skill in the art, which are not depicted nor described for simplicity.

In many implementations, the non-volatile memory 104 is realized by flash memory (e.g., NAND or ONENAND memory), but it is certainly contemplated that other memory types may be utilized as well. Although it may be possible to execute the code from the non-volatile memory 104, the executable code in the non-volatile memory 104 is typically loaded into RAM 108 and executed by one or more of the N processing components 110.

The N processing components 110 in connection with RAM 108 generally operate to execute the instructions stored in non-volatile memory 104. As one of ordinarily skill in the art will appreciate, the N processing components 110 may include a video processor, modem processor, DSP, graphics processing unit (GPU), and other processing components.

The transceiver component 112 includes N transceiver chains, which may be used for communicating with external devices via wireless networks. Each of the N transceiver chains may represent a transceiver associated with a particular communication scheme. For example, each transceiver may correspond to protocols that are specific to local area networks, cellular networks (e.g., a CDMA network, a GPRS network, a UMTS networks), and other types of communication networks.

The transceiver components 112 are also adapted to effect contactless payments. For example, the transceiver components are able to effect contactless payment using Near-Field Communications (***NFC***) by way of Apple Pay™, or MasterPass™, for example.

The camera component 120 includes a standard camera module communicating in a standard way with other components e.g. the user control 114, app 118, display 102, RAM 108, non-volatile memory 104 and any other components necessary to effect process of capturing a digital image (or multiple digital images continuously for a video).

It should be recognized that Figure 2 is merely exemplary and in one or more exemplary embodiments, the functions described herein may be implemented in hardware, software, firmware, or any combination thereof. If implemented in software, the functions may be stored on or transmitted over as one or more instructions or code encoded on a non-transitory computer-readable medium 104. Non-transitory computer-readable media 104 includes both computer storage media and communication media including any medium that facilitates transfer of a computer program from one place to another. A storage media may be any available media that can be accessed by a computer.

The operational steps for a preferred embodiment of the invention are described in further detail below.

Digital Wallet System 14

As shown in Figure 10, the digital wallet provider system 14 may comprise a server 14. In some embodiments, the digital wallet system 14 may comprise multiple

servers in communication with each other, for example over a local area network or a wide-area network such as the Internet. As described in the preceding section, the digital wallet provider system 14 is able to communicate with other components of the system 10 over the wireless communications network 20 using standard communication protocols.

The components of the digital wallet provider system 14 can be configured in a variety of ways. The components can be implemented entirely by software to be executed on standard computer server hardware, which may comprise one hardware unit or different computer hardware units distributed over various locations, some of which may require the communications network 20 for communication. A number of the components or parts thereof may also be implemented by application specific integrated circuits (ASICs) or field programmable gate arrays.

In the example shown in Figure 3, the digital wallet provider system 14 is a commercially available server computer system based on a 32 bit or a 64 bit Intel architecture, and the processes and/or methods executed or performed by the digital wallet provider system 14 are implemented in the form of programming instructions of one or more software components or modules 1022 stored on non-volatile (e.g., hard disk) computer-readable storage 1024 associated with the digital wallet provider system 14. At least parts of the software modules 1022 could alternatively be implemented as one or more dedicated hardware components, such as application-specific integrated circuits (ASICs) and/or field programmable gate arrays (FPGAs).

The digital wallet provider system 14 includes at least one or more of the following standard, commercially available, computer components, all interconnected by a bus 1035:

(a) random access memory (RAM) 1026;

(b) at least one computer processor 1028, and

(c) external computer interfaces 1030:

(i) universal serial bus (USB) interfaces 1030a (at least one of which is connected to one or more user-interface devices, such as a keyboard, a pointing device (e.g., a mouse 1032 or touchpad),

(ii) a network interface connector (NIC) 1030b which connects the

computer system 1000 to a data communications network, such as the wireless communications network 20; and

(iii) a display adapter 1030c, which is connected to a display device 1034 such as a liquid-crystal display (LCD) panel device.

The digital wallet provider system 14 includes a plurality of standard software modules, including:

(a) an operating system (OS) 1036 (e.g., Linux or Microsoft Windows);

(b) web server software 1038 (e.g., Apache, available at http://www.apache.org);

(c) scripting language modules 1040 (e.g., personal home page or PHP, available at http://www.php.net, or Microsoft ASP); and

(d) structured query language (SQL) modules 1042 (e.g., MySQL, available from http://www.mysql.com), which allow data to be stored in and retrieved/accessed from an SQL database 1016.

Advantageously, the database 1016 forms part of the computer readable data storage 1024. Alternatively, the database 1016 is located remote from the server 14 shown in Figure 3.

The boundaries between the modules and components in the software modules 1022 are exemplary, and alternative embodiments may merge modules or impose an alternative decomposition of functionality of modules. For example, the modules discussed herein may be decomposed into submodules to be executed as multiple computer processes, and, optionally, on multiple computers. Moreover, alternative embodiments may combine multiple instances of a particular module or submodule. Furthermore, the operations may be combined or the functionality of the operations may be distributed in additional operations in accordance with the invention. Alternatively, such actions may be embodied in the structure of circuitry that implements such functionality, such as the micro-code of a complex instruction set computer (CISC), firmware programmed into programmable or erasable/programmable devices, the configuration of a field-programmable gate array (FPGA), the design of a gate array or full-custom application-specific integrated circuit (ASIC), or the like.

Each of the blocks of the flow diagrams of the processes of the digital wallet provider system 14 may be executed by a module (of software modules 1022) or a portion of a module. The processes may be embodied in a non-transient machine-readable and/or computer-readable medium for configuring a computer system to execute the method. The software modules may be stored within and/or transmitted to a computer system memory to configure the computer system to perform the functions of the module.

The digital wallet provider system 14 normally processes information according to a program (a list of internally stored instructions such as a particular application program and/or an operating system) and produces resultant output information via input/output (I/O) devices 1030. A computer process typically includes an executing (running) program or portion of a program, current program values and state information, and the resources used by the operating system to manage the execution of the process. A parent process may spawn other, child processes to help perform the overall functionality of the parent process. Because the parent process specifically spawns the child processes to perform a portion of the overall functionality of the parent process, the functions performed by child processes (and grandchild processes, etc.) may sometimes be described as being performed by the parent process.

Authorization Server 24

The authorization server 24 is able to communicate with the digital wallet system 14 through standard communication protocols provided for by communications network 20, in order to receive requests for payment authorization, process such requests, and convey responses back to the digital wallet provider system 14.

For example, the authorization server 24 may comprise an acquirer system (which may in turn comprise a core banking system in communication with an acquirer processor system), a payment network (such as Mastercard, Visa or China Unionpay) and an issuer system (which may comprise a core banking system and an issuer processor system).

The authorization server 24 may receive the payment authorization request via the acquirer system, which routes the request via the payment network to the issuer system in a manner known in the art. The request may be formatted according to the ISO 8583 standard, for example, and may include a primary account number (PAN) of

the payment instrument being used for the transaction, a merchant identifier (MID), and an amount of the transaction, as well as other transaction-related information as will be known by those skilled in the art. The issuer system receives the request, applies authorization logic to approve or decline the request, and sends an authorization response (approve or decline, optionally with a code indicating the reason for the decline) back to the acquirer system via the payment network in known fashion. The acquirer system then communicates the authorization response to the digital wallet system 14.

Alternatively, in some embodiments, the authorization server 24 may receive the payment authorization request via the issuer system, which approves or declines the request (which again may be in ISO 8583 format, and comprise a PAN, MID, transaction amount etc.) and sends a response directly back to the digital wallet system 14.

In addition to processing requests for payment in which funds are actually transferred from the cardholder's account (maintained in the issuer's core banking system) to the merchant's account (maintained in the acquirer's core banking system), the authorization server 24 may process a pre-authorization (or "pre-auth") request, in which funds are not transferred on approval of the request, but are instead placed on hold. The pre-auth can later be completed, for example by the the digital wallet system 14, in order to release the funds. Alternatively, the pre-auth can be cancelled, thus effectively cancelling the transaction.

Digital Wallet Application 118

The interoperations of the components of system 10 are hereafter described by way of non-limiting example, with reference to a DW App 118 being executed on a user's mobile computer device 12. The DW App 118 could be a mobile application, web page application, or computer application and may be accessed by a computer device such as a laptop or desktop computer. The DW App 118 can be used with payment cards including credit cards, debit cards, store cards, etc. For ease of description, the DW App 118 is below described by way of reference to credit cards only. However, the DW App 118 and the system 10 can be used with any suitable payment card.

On execution of the DW App icon, the DW App 118 performs the process 300 shown in

Figure 3 including, generating at step 302, the "Home" graphical user interface (GUI) 400 shown in Figure 4 on the display 102 of mobile computer device 12. The "Home" GUI includes the following function buttons:

(a) Onboard Document or Information 404;
(b) Visa Application 406; and
(c) Electronic Payment Transaction 408.

The abovementioned processes are described below by way of non-limiting example.

Onboard Document or Information Process 314

On execution of the Onboard Document or Information function button 404 on the "Home" GUI 400, the DW App 118 executes step 304. At step 304, the DW App 118 generates for display 102 a list of documents or information for user selection to onboard (also known as register) to the DW. An example of documents that may be requested for a visa application are government issued personal identity documents such as a passport, driver's licence, national identity card or birth certificate.

Other examples of documents or information that may be requested for a visa application is information pertaining to their travel (e.g travel itinerary, flight information or hotel bookings), proof of income or financial proof to support their travel (e.g. bank statements or payslips), insurance information (e.g. medical or travel insurance) and proof of address or residency. The request may also include a photo of the applicant that fulfil to certain specifications (e.g. colour of the background, dimensions of image and file size).

After a user selection is made at step 304, the DW App 118 executes the onboard document or information process 314 shown in Figure 5 which calls up the services of the components of the system 10. At step 502, the DW app 118 generates on the display 102 of the mobile computer device 12 a user input associated with the document or information type selected at step 304. For example, a user input for a passport could be a fillable form requesting for the following information, traveller's full name, passport number, expiration date, passport issuing office, country of birth, nationality, place of birth and date of birth.

Preferably, an option to upload a copy of the document (e.g. scanned document or image) would be available as part of the user input. On selection of this option, the DW App 118 generates on display 102 a list for user selection of files available on the memory 104 of the mobile computer device 12 or from a web-based cloud data storage system such as DropBox™. If a file is selected or an image captured, the DW App 118 retrieves the file or image and stores it on the non-transitory memory 104 as part of the user input.

At the end of the user input, the DW app 118 generates for display 102 on the mobile computer device 12 a function button with the text "Save to database". When the function button is selected, the DW App 118 executes step 504 whereby it receives the user input. At step 506, the DW App 118 sends the user input to the database to be stored. The database is a computer readable data storage that may be one or more of the following:

(a) the memory 104 on the mobile computer device 12;
(b) a cloud server accessible by communication network 20; or
(c) other external server accessible by communication network 20.

At step 508, the DW app 118 generates for display 102 on the mobile computer device 12, two function buttons with the text:

(a) "Onboard another document or information"; and
(b) "Quit to main menu".

Selecting function button (a) above will prompt the DW App 118 to loop back to step 502. Selecting function button (b) above will end process 314 and bring up the "Home" GUI 400 on the display 102.

Visa Application Process 800

The interoperation of the visa application process 800 is performed by the components of the system 10 is shown in Figure 8. A user may initiate a visa application by launching the DW app 118 on a mobile computer device 12 which generates the "Home" GUI 400 on display 102. Upon user selection of the Visa Application function button 406, step 306 is executed which generates for display 102 a list of visa

applications available using the DW App 118 for user selection. Upon user selection of a visa application, the mobile computer device 12 executes Visa Application Process 316 shown in Figure 6. Alternatively, the user may initiate a visa application by loading a visa application webpage on an internet browser using a mobile computer device 12.

At step 604 of process 316, the mobile computer device 12 sends a request to display the visa application page to a request server 16. At step 606, the mobile computer device 12 receives message data from the request server and generates the visa application page on display 102. Preferably, the visa application page includes a function button displaying the option to apply for the visa using a DW such as MasterPass™. At step 608, the function button to apply for the visa using a DW is selected and the mobile computer device 12 generates on display user input fields to prompt the user to provide their DW account login data (e.g. username and password). If the user does not have an existing DW wallet account, the mobile computer device provides an option to sign up for an account by generating for display 102 a fillable form for user input.

At step 610, the mobile computer device 12 sends a request to initiate a visa application via the DW to the request server 16. A request server 16 may be:

(a) a third party visa processing server;
(b) a digital wallet system 14; or
(c) an authorization server 24.

At step 802 of the Visa Application Process 800, the request server 16 receives the request to apply for a visa using a DW, generates a request for user data and sends it to DW system 14 associated with the DW provider system selected by the user in step 608. At step 804, the DW system 14 receives the request for a user's data including the user's digital wallet account login data. The request may include one or more of the following information:

(a) visa application information including:
    (i) type of visa application;
    (ii) name of country or territory for the visa application;
(b) list of government issued personal identity documents required; and

(c) any additional information or documents required.

At step 806, the DW system 14 uses the digital wallet account login data to access the user's digital wallet account data stored in data storage and verifies that the login data matches the user's digital wallet account data.

At step 808, the DW system 14 retrieves user communication data associated with the user's digital wallet account, the communication data including details of the user's preferred mode of communication. At step 810, the DW system 14 sends a request to the user in accordance with the user's preferred mode of communication for user permission to send the user's data for a visa application.

The user's preferred mode of communication includes communicating with the user's mobile computer device 12 by one or more of the following:

(a) an application running on the user's mobile computer device;

(b) a phone call;

(c) a message wherein the message data is any one of the following:

(i) a short message service (SMS) message;

(ii) a multimedia messaging service (MMS) message; and

(iii) a message sent using an instant messaging service.

At step 612, the mobile computer device 12 receives a request for user permission from the DW system. At step 614, the mobile computer device 12 generates a request for user permission on display 102. An example of the request on display 102 include the following information:

(a) the visa application information;

(b) the list of government issued personal identity documents requested by the request server 16;

The mobile computer device 12 generates on display 102 the following options for user selection:

(a) "Yes, I agree to submit information for visa application"; and

(b) "No, do not submit. Modify application".

Further user identity verification representing user permission data may include one or more of the following:

(a) biometric authentication;
(b) token generated password;
(c) one time password (OTP);
(d) password;
(e) a personal identification number (PIN);
(f) an authentication token; and
(g) answer to a security question.

Biometric authentication may include one or more of the following:

(a) a fingerprint scan;
(b) a retina scan;
(c) voice recognition;
(d) facial recognition;
(e) hand geometry biometrics;
(f) finger geometry biometrics;
(g) an iris scan;
(h) signature recognition; and
(i) handwritten biometric recognition.

At 616, the mobile computer device 12 receives user permission data and sends the data to the digital wallet system 14. At step 812, the DW system 14 receives user permission data and verifies the data against user data associated with the user's DW account to verify the identity of the user.

At step 814, the DW system 14 compares the user data requested by the request server against user data registered to the user's digital wallet account. If the user data requested by the request server is not registered to the user's digital wallet account, the DW system 14 sends a request to the user to register user data. The DW system 14 communicates with the user's mobile computer device using the user's preferred mode of communication. At step 314, the mobile computer deice 12 receives the request to register user data and performs process 314 described in the preceding section. If the check affirms that all documents requested by the request server 16 have been registered and are available in the database, the process proceeds to the next step.

At step 816, the DW system 14 checks if the request from the request server 16

included an electronic payment request which may be a pre-authorisation request to be effected at a later date, or a payment capture request. If an electronic payment request is included, the DW system 14 performs the following:

(a) retrieving a primary account number (PAN) associated with a payment card from the user's digital wallet account;

(b) sending, to the authorization server, an electronic payment request including the PAN and transaction amount for authorisation or payment capture;

(c) receiving, from the authorization server, message data representing successful authorisation or capture for the electronic payment request; and

(d) sending message data representing electronic payment request approval to the request server.

In some embodiments, the authorisation server may be a third party payment processor server.

In some embodiments, the payment card associated with the user's digital wallet account may be a credit card or a debit card.

In certain embodiments, a further request for user authorisation of the electronic transaction may be required by the authorisation system 24. In this case, a request for user authorisation is sent to the user using the user's preferred mode of communication.

In another embodiment, the electronic payment process may be executed by the DW App 118 running on the mobile computer device 12. In this embodiment, the DW system 14 sends the electronic payment request to the mobile computer device which executes step executes process 318 as described in detail in the following section.

At step 820, the authorization system 24 authorises the electronic payment request and sends message data representing successful payment authorisation to the DW system 14.

At step 822, the DW system 14 retrieves user data from database 1016 corresponding to the list of user data requested by the request server 16 and sends the data to the

request server 16. At step 824, the request server 16 receives the requested user data. At step 826, the request server checks that all the user data has been received and if so, sends message data representing successful visa application status to the mobile computer device 12. At step 830, the mobile computer device 12 receives message data from the request server 16 and generates on display 102 a message indicating successful visa application status.

Electronic Payment Transaction Process 318

On execution of the Electronic Payment Transaction function button 408 on the "Home" GUI 400, the DW App 118 executes step 308 which generates for display 102 a list of payment transactions available for user selection. After a selection is made, the DW App 118 sends the request for payment transaction information to the request server 16 associated with the user selection. Alternatively, without user selection of function button 408, the DW App 118 may receive a payment request directly from the request server 16.

The DW App 118 executes the payment transaction process 318 as shown in Figure 7 which calls up the services of the components of system 10. At step 702, the DW App 118 receives from the request server 16 payment values associated with an electronic payment required for a visa application. Payment values may include the total cost of the transaction and the preferred currency of payment. In some visa applications, the payment is only effected at a later date, for example after the visa has been approved or at the time that the visa is issued. In this regard, preferably the DW App 118 provides an option to pre-authorise the payment of the visa to be effected at a later date.

At step 704, the DW App 118 generates on display 102:

(a) a list of payment cards registered to the DW;
(b) the prompt "Please select a card from the list"; and
(c) a function button with the text "Use another card".

DW App 118 will execute step 708 if above-mentioned function button in (c) is selected. In step 708, the DW App 118 generates on display 102, a user input to provide payment card details. This user input may be in the form of a fillable form

(e.g. name on card, primary account number (PAN), expiry date) or an option to take an image of the payment card using the camera 120 and extract the relevant information from the image. The payment card data is then stored in a database provided by a digital wallet system 14. A payment card may be a credit card or a debit card.

At step 710, the DW App 118 retrieves payment credentials associated with the selected payment card from a digital wallet system 14. Payment credentials include a primary account number (PAN) and may also include the expiry date of the card and the cardholder's name on the card.

At step 712, the DW App 118 sends a payment request (including the payment credentials e.g. PAN and payment parameters) to an authorization server 24 to authorise or capture the payment request. User authentication process may be one or more of the following:

(a) biometric authentication (e.g. fingerprint or retina scan);
(b) one time password (e.g. by SMS or OTP generator)
(c) personal identification number (PIN); or
(d) any other user authentication method.

At step 714, if the transaction is not authorised or not captured, the process loops back to 704 and prompts the user to choose a different payment card. If the transaction is authorised or captured, the DW App 118 generates on display 102 a message with the text "Transaction successful".

Visa Approval Process 900

The interoperation of the visa approval process 900 performed by the components of the system 10 is shown in Figure 9. After the request server 16 receives the completed visa application sent by the DW App 118 and successful payment transaction information (if any), the visa application is ready to be processed by the visa approval authority for example, the government's immigration department.

The request server 16 sends data representing completed visa application to the visa authority system 22. In this preferred embodiment, the visa authority system 22 is

located offsite typically in an office located in the country or territory of travel (i.e. not located at the checkpoint for example land border checkpoint, seaport, international airports or other ports of entry) and the visa approval occurs prior to the travel period.

In another embodiment of the invention, the visa authority system 22 is located onsite (i.e. located at the checkpoint for example land border checkpoint, seaport, international airports or other ports of entry). In this case, the visa authority system 22 is also the onsite system 18. The visa is approved and issued on arrival of the traveller at the checkpoint of the country or territory.

In this preferred embodiment, the visa authority system 22 receives data associated with a completed visa application. The visa authority system 22 waits until it receives user input indicating that the visa has been approved and sends data representing approval of visa to the request server 16. The request server 16 then sends data representing approval of visa to the mobile computer device 12 and the onsite system 18.

The mobile computer device 12 receives data representing an approval of visa sent as one or more of the following:

(a) an email to an email account accessible via the mobile computer device;
(b) a short message service (SMS) or multimedia messaging service (MMS) to a telephone number associated with the mobile computer device; and
(c) a digital file representing a visa for later access via a digital wallet associated with the mobile computer device.

The mobile computer device 12 generates on display 102 a message with the text "Visa application has been approved". The mobile computer device 12 stores the data representing approval of visa in memory 104.

When the traveller is onsite, the mobile computer device 12 is initiated to retrieve and display data representing an approval of visa on display 102. Alternatively, a traveller may display data representing an approval of visa by showing a printed document. The onsite system 18 also retrieves data representing an approval of visa. Typically, an immigration officer would check the data representing an approval of visa against the retrieved data from the onsite system 18. The immigration officer may also

request to verify retrieved information from the onsite system 18 against an original documentation to be provided by the traveller, for example passport, identity card, or driver license etc. If the visa approval or visa is authenticated by the immigration officer, the traveller is granted the legal temporary right to enter the country or territory.

In another embodiment of the invention, instead of an immigration officer, this process could be performed by an automated system (e.g. SmartGate system used by Australia and New Zealand). A traveller will scan his or her passport or any other identification documentation and if required, the data representing approval of visa generated on display 102 of the mobile computer device 12 using the automated system. The automated system will then verify the authenticity of the visa approval by matching the scanned user data against the user data on the request server 16. Upon authentication, the traveller then receives a message on the automated system indicating successful visa authentication and is then directed to exit the gated area. Depending on the visa authority, the traveller may still be required to produce physical documentation for verification by an immigration officer prior to final authentication.

Many modifications will be apparent to those skilled in the art without departing from the scope of the present invention

Throughout this specification, unless the context requires otherwise, the word "comprise", and variations such as "comprises" and "comprising", will be understood to imply the inclusion of a stated integer or step or group of integers or steps but not the exclusion of any other integer or step or group of integers or steps.

The reference to any prior art in this specification is not, and should not be taken as, an acknowledgment or any form of suggestion that the prior art forms part of the common general knowledge.

Claims Defining the Invention

1. A digital wallet system for electronically applying for a visa for temporary entry into a country or territory, comprising one or more processors in communication with non transitory data storage having instructions stored thereon which, when executed by the processor or processors, cause the system to perform the steps of:

(a) receiving, from a request server, a request for a user's data including the user's digital wallet account login data;

(b) using the digital wallet account login data to access the user's digital wallet account data stored in said data storage and verifying that the login data matches the user's digital wallet account data;

(c) retrieving user communication data associated with the user’s digital wallet account data, the communication data including details of the user's preferred mode of communication;

(d) sending a request to the user in accordance with the user's preferred mode of communication for user permission to send the user's data for a visa application;

(e) receiving user permission data to send the user's data for the visa application;

(f) retrieving the user's data for the visa application from data storage; and

(g) sending, to the request server, the user's data for the visa application so as to electronically apply for a visa for the user.

2. The digital wallet system claimed in claim 1, wherein the user’s preferred mode of communication includes communicating with the user’s mobile computer device by one or more of the following:

(a) an application running on the user’s mobile computer device;

(b) a phone call;

(c) a message wherein the message data is any one of the following:

(i) a short message service (SMS) message;

(ii) a multimedia messaging service (MMS) message; and

(iii) a message sent using an instant messaging service.

3. The digital wallet system claimed in claim 1 or claim 2, wherein the user permission data includes one or more of the following:

(a) biometric authentication;

(b) token generated password;
(c) one time password (OTP);
(d) password;
(e) a personal identification number (PIN);
(f) an authentication token; and
(g) answer to a security question.

4. The digital wallet system claimed in claim 3, wherein biometric authentication includes one or more of the following:
(a) a fingerprint scan;
(b) a retina scan;
(c) voice recognition;
(d) facial recognition;
(e) hand geometry biometrics;
(f) finger geometry biometrics;
(g) an iris scan;
(h) signature recognition; and
(i) handwritten biometric recognition.

5. The digital wallet system claimed in any one of claims 1 to 4, wherein the system is configured to compare the user data requested by the request server against user data registered to the user's digital wallet account.

6. The digital wallet system claimed in claim 5, wherein the system is configured to send a request to the user to register user data responsive to a determination that the user data requested by the request server is not registered to the user's digital wallet account data.

7. The digital wallet system claimed in any one of claims 1 to 6, further including an authorisation server, wherein the request for user data further includes an electronic payment request wherein the system is configured to perform the steps of:
(a) retrieving a primary account number (PAN) associated with a payment card from the user's digital wallet account data;
(b) sending, to the authorization server, an electronic payment request including the PAN and transaction amount for authorisation or payment capture;

(c) receiving, from the authorization server, message data representing successful authorisation or capture for the electronic payment request; and

(d) sending message data representing electronic payment request approval to the request server.

8. The digital wallet system claimed in claim 7, wherein the system is configured to receive an electronic payment request including a pre-authorisation request to be effected at a later date, or a payment capture request.

9. The digital wallet system claimed in any one of claims 1 to 8, wherein the system is configured to, after the electronic payment request is received, send a request for user authorisation to the user using the user's preferred mode of communication.

10. The digital wallet system claimed in any one of claims 7 to 9, wherein the authorisation server is a third party payment processor server.

11. The digital wallet system claimed in any one of claims 1 to 10, wherein the system is configured to, after the request server receives the user data, perform the following steps:

(a) checking that all the user data has been received; and

(b) sending message data representing successful visa application status to the user.

12. The digital wallet system claimed in any one of claims 1 to 11, in communication with:

(a) a visa authority system; and

(b) an onsite system;

wherein after the request server is configured to, after receiving the user's data, perform the steps of:

(a) checking that all the user data has been received;

(b) sending message data representing successful visa application status to the user;

(c) sending message data representing the user's visa application to the visa authority system;

(d) receiving message data representing an approval of the visa application from the visa authority system; and

(e) sending message data representing approval status of the user's visa application to the user's mobile computer device and the onsite system.

13. The digital wallet system claimed in any one of claims 1 to 12, wherein the system is configured to send message data representing approval status of the user's visa application to the user as one or more of the following:

(a) an email to an email account accessible via the computer device;

(b) a short message service (SMS) or multimedia messaging service (MMS) to a telephone number associated with the computer device; and

(c) a digital file representing a visa for later access via a digital wallet associated with the computer device.

14. The digital wallet system claimed in any one of claims 1 to 13, wherein the user data includes data representing government issued personal identity documents including one or more of the following:

(a) passport;

(b) birth certificate;

(c) identity document; and

(d) a driver's licence.

15. The digital wallet system claimed in any one of claims 1 to 14, wherein the user data includes data representing one or more of the following:

(a) insurance card;

(b) travel information; and

(c) financial information.

16. The digital wallet system claimed in any one of claims 1 to 15, wherein the data associated with requested user data includes one or more of the following:

(a) user input in the form of text; and

(b) a digital file.

17. A method for electronically applying for a visa for temporary entry into a country or territory, comprising:

(a) receiving, from a request server, a request for a user's data including

the user's digital wallet account login data;

(b) using the digital wallet account login data to access the user's digital wallet account data stored in said data storage and verifying that the login data matches the user's digital wallet account data;

(c) retrieving user communication data associated with the user’s digital wallet account data, the communication data including details of the user's preferred mode of communication;

(d) sending a request to the user in accordance with the user's preferred mode of communication for user permission to send the user's data for a visa application;

(e) receiving user permission data to send the user's data for the visa application;

(f) retrieving the user's data for the visa application from data storage; and

(g) sending, to the request server, the user's data for the visa application so as to electronically apply for a visa for the user.

18. A non-transitory computer readable storage medium embodying thereon a program of computer readable instructions which, when executed by one or more processors of a digital wallet system in communication with a plurality of devices, cause the system to electronically apply for a visa for temporary entry into a country or territory, the method embodying the steps of:

(a) receiving, from a request server, a request for a user's data including the user's digital wallet account login data;

(b) using the digital wallet account login data to access the user's digital wallet account data stored in said data storage and verifying that the login data matches the user's digital wallet account data;

(c) retrieving user communication data associated with the user’s digital wallet account data, the communication data including details of the user's preferred mode of communication;

(d) sending a request to the user in accordance with the user's preferred mode of communication for user permission to send the user's data for a visa application;

(e) receiving user permission data to send the user's data for the visa application;

(f) retrieving the user's data for the visa application from data storage; and

(g) sending, to the request server, the user's data for the visa application

so as to electronically apply for a visa for the user.