

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
28 May 2009 (28.05.2009)

PCT

(10) International Publication Number
WO 2009/066978 A2

(51) International Patent Classification:
H04L 9/32 (2006.01) *G06F 15/16* (2006.01)

Azhar Bin [MY/MY]; Technology Park Malaysia, 57000 Kuala Lumpur (MY).

(21) International Application Number:
PCT/MY2008/000115

(74) Agent: **SU, Siew Ling**; Tai & Partners, 6th Floor, Plaza See Hoy Chan, Jalan Raja Chulan, 50200 Kuala Lumpur (MY).

(22) International Filing Date:
26 September 2008 (26.09.2008)

(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI20071724 5 October 2007 (05.10.2007) MY

(71) Applicant (*for all designated States except US*): **MIMOS BERHAD** [MY/MY]; Technology Park Malaysia, 57000 Kuala Lumpur (MY).

(72) Inventors; and

(75) Inventors/Applicants (*for US only*): **WONG, Hau Keong** [MY/MY]; Technology Park Malaysia, 57000 Kuala Lumpur (MY). **HARON, Galoh Rashidah** [MY/MY]; Technology Park Malaysia, 57000 Kuala Lumpur (MY). **TAN, Fui Bee** [MY/MY]; Technology Park Malaysia, 57000 Kuala Lumpur (MY). **SEA, Chong Seak** [MY/MY]; Technology Park Malaysia, 57000 Kuala Lumpur (MY). **NG, Kang Siong** [MY/MY]; Technology Park Malaysia, 57000 Kuala Lumpur (MY). **ABU TALIB,**

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with declaration under Article 17(2)(a); without abstract; title not checked by the International Searching Authority*



WO 2009/066978 A2

(54) Title: METHOD AND SYSTEM FOR GENERATING A PROXY DIGITAL CERTIFICATE TO A GRID PORTAL IN DISTRIBUTED COMPUTING INFRASTRUCTURE BY DATA TRANSFER ACROSS A PUBLIC NETWORK

(57) Abstract:

METHOD AND SYSTEM FOR GENERATING A PROXY DIGITAL CERTIFICATE TO A
GRID PORTAL IN DISTRIBUTED COMPUTING INFRASTRUCTURE BY DATA TRANSFER
ACROSS A PUBLIC NETWORK

5

FIELD OF THE INVENTION

This invention concerns a method and a system for the issuance of a proxy digital certificate to a grid portal in distributed computing infrastructure through data transfer across a public network. More specifically, the invention concerns a method and a system for proxy digital
10 certificate issuance from an end entity certificate to a grid portal of a distributed or grid computing infrastructure via a web browser, where the proxy digital certificate resides in a web server and the issuance of the proxy digital certificate may be applied on any web based application through a public network such as the Internet.

15 **BACKGROUND OF THE INVENTION**

In the quest of building computers with more computation power, distributed computing or grid computing has gained in popularity over recent years. A primary advantage of grid computing is that each node within the grid computing infrastructure can be purchased as a commodity hardware unit. When the commodity hardware units are combined in this manner, grid
20 computing can achieve similar computing performance comparable to a many-central processing unit (CPU) supercomputer, and at a lower financial cost.

In an article, Ian Foster et al., "The Anatomy of the Grid: Enabling Scalable Virtual Organizations", *International Journal of High Performance Computing Applications*, vol. 15, no. 3, pp. 200-222, August 2001, a 'grid problem' is identified as the challenge to enable
25 coordinated resource sharing among dynamic collections of individuals, institutions and resources. In an effort to address this 'grid problem', Ian Foster et al. initiated the open sourced globus toolkit (GTK) middleware for building grid computing based on commodity computer infrastructure. Even though other software toolsets exist for the construction of
30 computing grids, GTK is widely used and continuously maintained and upgraded middleware toolkit for the construction of computing grids.

In view of the fact that computing nodes typically share resources over open public networks, such as the Internet, a set of libraries and toolkits called grid security infrastructure (GSI) is
35 included in the standard GTK to provide the necessary security measures to support the computing grids. GSI relies on public key infrastructure (PKI) technologies to provide mutual strong authentication and message protection through TLS/SSL protocol. For example, X.509 digital certificate is used extensively to identify users, services and hosts. A proxy digital

certificate that conforms to IETF RFC 3820 can be used by GSI for job delegation and single sign-on to multiple computing nodes.

5 By providing a web interface to GTK, grid portal allows an end user to interact with computing grids using a common and mature user interface technology. Due to the fact that grid portal acts as the man-in-the-middle between GTK and the end user using a web browser, the proxy certificate issuance capability provided by GTK is not usable in the situation that involves web browser.

10 Attempts have been made and a few implementations have been proposed for issuance of proxy certificates when the grid portal is between GTK and the end user using a web browser. One attempt, as disclosed by Novotny et al., "An Online Credential Repository for the Grid: MyProxy", *10th IEEE International Symposium on High Performance Distributed Computing*, 104, 2001, is shown in FIG. 1. FIG. 1 shows one conventional system 200 that allows the
15 user to create proxy credential in the form of private key and proxy certificate using a dedicated client program. The user can access the user's credential with standard web browser using a userID and passphrase. The user can also instruct the client 202 through grid portal 48 to generate proxy-proxy certificate based on the proxy certificate residing in the server 204.

20

The operations of the proxy certificate issuance of a conventional method is shown in steps in FIG. 1. In step 1, the user 12 interacts with server 204 through client 202 software. UserID and passphrase are required for the user 12 to gain access to server 204, and the user can instruct the client 202 running on the user's computer to initiate a proxy₁ certificate creation
25 using the user's certificate which resides in the same user's computer 12. The proxy₁ certificate acts on behalf of the user so that the user certificate is not required all of the time.

In step 2, the user can access grid portal 48 using a standard web browser 42. At this stage, the user can request client to issue proxy₂ certificate based on the proxy₁ certificate created in server in step 1. The preconditions for this operation to be successful are that the proxy₁
30 certificate created in step 1 is not expired; and to access the server, userID and passphrase are provided by the user.

In step 3, the server responds to the request from Grid Portal to create proxy₂ certificate (level 2 proxy certificate acting on behalf of level 1 proxy certificate) on the grid portal to be used by the portal as proxy credential for the user to access computing resources using GTK
35 middleware.

In step 4, the proxy₂ certificate is used by the grid portal via GTK to establish digital certificate based mutual authentication to GTK computing grids.

40 With the configuration of the conventional system shown in FIG. 1, a limitation is that the secondary path is required for the user to create proxy certificate on the server, such that the

user needs to use the dedicated client to establish connection to the server. This secondary path exposes the system to a potential breach of the system and opens up for potential unauthorized exploitation. Additionally, authentication is limited to userID and passphrase. Even though communication between computing nodes within GTK computing grids are based on digital certificate based mutual authentication, introducing grid portal with the server does not extend the mutual authentication to the end user who uses the web browser. The problem is compounded further because the grid portal is generally exposed to the public network such as Internet. Therefore, the weakest link in the entire system coincides with the part of the system that is opened to public and invites attacks from potentially large number of internet users. Anyone who manages to get hold of the right combination of UserID and passphrase can impersonate the legitimate user to access the computing grids.

There is thus a need to further improve and ensure the security of data transmitted on a public network environment such the Internet in a method and a system for the issuance of a proxy digital certificate to a grid portal in distributed computing infrastructure.

SUMMARY

In accordance with an aspect of the invention a method of generating a proxy digital certificate to a distributed computing infrastructure by secure data transfer across a public network using a client-server communication protocol, the method comprises a web browser obtaining a user key independently of a web server; the web browser sending a request to the web server across the public network using the protocol; the web server generating a key pair that includes a public key and a private key in response to the request; the web server storing the key pair at a key storage location remote to the web browser; the web server sending the public key to the web browser across the public network using the protocol; the web browser generating the proxy digital certificate by signing the public key received from the web server using the user key; the web browser sending the proxy digital certificate to the web server across the public network using the protocol; and the web server storing the proxy digital certificate received by the web browser at a certificate storage location remote to the web browser.

In an embodiment the public network is the Internet. The protocol is hyper text transfer protocol. The web browser obtains the user key from a smart card. The web server generates the key pair using an RSA asymmetric algorithm. The web server generates the key pair using an ECC asymmetric algorithm. The web server sends the public key and additional information to the web browser across the public network using the protocol. The web browser generates the proxy digital certificate by signing the public key and the additional information received from the web server using the user key. The web browser calculates a hash value using the user key and signs the public key received from the web server using the hash value. The proxy digital certificate is in X.509 format. The proxy digital certificate

includes a name and an e-mail address of a user that uses the web browser. The proxy digital certificate includes a validity period for the proxy digital certificate.

In accordance with an aspect of the invention a system of generating a proxy digital certificate to a distributed computing infrastructure by secure data transfer across a public network using a client-server communication protocol, the system comprises a web browser obtaining a user key independently of a web server; the web browser sending a request to the web server across the public network using the protocol; the web server generating a key pair that includes a public key and a private key in response to the request; the web server storing the key pair at a key storage location remote to the web browser; the web server sending the public key to the web browser across the public network using the protocol; the web browser generating the proxy digital certificate by signing the public key received from the web server using the user key; the web browser sending the proxy digital certificate to the web server across the public network using the protocol; and the web server storing the proxy digital certificate received by the web browser at a certificate storage location remote to the web browser.

In accordance with an aspect of the invention a computer program comprises program instructions for causing a computer to generate a proxy digital certificate to a distributed computing infrastructure by secure data transfer across a public network using a client-server communication protocol, comprising a web browser obtaining a user key independently of a web server; the web browser sending a request to the web server across the public network using the protocol; the web server generating a key pair that includes a public key and a private key in response to the request; the web server storing the key pair at a key storage location remote to the web browser; the web server sending the public key to the web browser across the public network using the protocol; the web browser generating the proxy digital certificate by signing the public key received from the web server using the user key; the web browser sending the proxy digital certificate to the web server across the public network using the protocol; and the web server storing the proxy digital certificate received by the web browser at a certificate storage location remote to the web browser.

BRIEF DESCRIPTION OF THE DRAWINGS

In order that the present invention may be fully understood and readily put into practical effect, there shall now be described by way of non-limitative example only preferred embodiments of the present invention, the description being with reference to the accompanying illustrative drawings.

FIG. 1 illustrates a conventional method for proxy certificate issuance;

FIG. 2 shows a block diagram of a system architecture in accordance with an embodiment of the invention;

FIG. 3 shows a simplified block diagram of FIG. 2 of the system architecture in accordance with an embodiment of the invention;

FIG. 4 illustrates a chain of trust from a certification authority (CA) within the system architecture in accordance with an embodiment of the invention; and

5 FIG. 5 shows a sequence diagram of a process in accordance with an embodiment of the invention.

DETAILED DESCRIPTION

A method and system for of generating a proxy digital certificate to a distributed computing
10 infrastructure by secure data transfer across a public network using a client-server communication protocol. An embodiment of the invention is shown in FIG. 1 of a system architecture diagram of a system 10. FIGS. 1-5 and the following discussion are intended to provide a brief, general description of a suitable computing environment in which the present invention may be implemented. Although not required, the invention will be described in the
15 general context of computer-executable instructions, such as program modules, being executed by a personal computer. Generally, program modules include routines, programs, characters, components, data structures, to perform particular tasks or implement particular abstract data types. As those skilled in the art will appreciate, the invention may be practiced with other computer system configurations, including hand-held devices, multiprocessor
20 systems, microprocessor-based or programmable user electronics, network PCs, minicomputers, mainframe computers, and the like. The invention may be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

25 The system as shown in FIG. 2 in accordance with an embodiment comprises a person or user at a user workstation 12 holding a private key and a corresponding digital certificate that are connected to a web browser 42 with a browser plug-in module or browser extension program 54 to issue a proxy digital certificate to a web server 22 via hyper text transfer
30 protocol (HTTP). A smartcard 52 and smart card reader 60 is connected via user workstation 12 as shown in FIG. 2; however, it will be appreciated that other configurations may be envisaged. In the smart card, the hash value of the proxy certificate is signed by the private key stored in the key store 58 of the smart card 52. This operation is performed in the processor 56 of the smart card 52. The private key is retrieved from the key storage 58 in the
35 smart card, and under this configuration, the private key in the smart card remains within the smart card and is not transmitted from the smart card 52. The user work station 12 may comprise a memory 14, processor 16 and an interface 18 for interfacing with a public network
20 such as the Internet. The proxy certificate can be implemented and created, for example, at the single-sign-on server or protocol server such that the server can login to multiple
40 subsequent servers using the proxy certificate. In this configuration, the user only needs to

login to the single-sign-on server. An input device 34 and display 32 is provided for a user to interface with the user workstation for inputting and displaying data. A web server 22 may comprise a web server memory 24, processor 26 and interface 28 for interfacing and communicating and transfer of data with the public network 20. The web server 22 may also
5 comprise a key module 36 for generating keys and a key store 38 for storing the key information. The web server is arranged to allow digital certificate in web browser to issue proxy digital certificate. Also database 44 may also be in a location remote to the web server 22 for storage of key data 46. A grid portal 48 for access to GTK computing grids 50 of a distributed computing or grid computing environment is accessible via the public network 20.

10 FIG 3. shows a simplified block diagram of the system of FIG. 2 in accordance with an embodiment of the invention that allows a proxy digital certificate to be issued by a user certificate via a standard web browser to a grid portal. The steps involved include in step 1, the user 12 logs in to grid portal 48 hosting on a standard web or HTTP server 22 using a
15 standard web browser 42, such as Firefox, via a strong digital certificate, such as for example transport layer security (TLS)/ secure socket layer (SSL) (TLS/SSL) digital certificate based mutual authentication. Proxy₁ certificate is issued 60 by the user certificate through a web extension program 54 and the web extension program's corresponding CGI program 50 running on the grid portal 48. In step 2, the grid portal 48 can utilize the newly generated
20 proxy₁ certificate to engage globus toolkit (GTK) based computing grids using digital certificate based mutual authentication with GTK client 50 running on the grid portal 48.

In issuing the proxy certificate reference to FIG. 4 is made. Globus security infrastructure (GSI) is the portion of the GTK that provides the fundamental security services needed to
25 support grid computing. The primary motivations behind GSI are that the need for secure communication (authenticated and perhaps confidential) between elements of a computing grid; the need to support security across organizational boundaries, thus prohibiting a centrally-managed security system; and the need to support "single sign-on" for users of the Grid, including delegation of credentials for computations that involve multiple resources
30 and/or sites.

Public Key Infrastructure (PKI) is used as the primary security measure to fulfill the above mentioned motivation for GSI. In PKI, all entities are identified using digital certificates and their corresponding private keys. Digital certificate contains a globally unique name known as
35 Distinguish Name (DN). Authentication within the GSI is a matter of proving that the user is the entity identified by the DN coded in the digital certificate. Digital certificates are signed by a trusted Certification Authority's (CA) private key. The integrity and origin of the digital certificate can be verified using the Certification Authority's (CA) public key extracted from CA's digital certificate, called root certificate.

Transport Layer Security (TLS) and its predecessor standard Secure Socket Layer (SSL) are used by GSI to provide strong digital certificate based mutual authentication between computing nodes that use GTK middleware to form computing grids. All messages transferred between the two computing nodes using TLS/SSL are encrypted based on the agreed encryption algorithm and key length provisioned under the TLS/SSL handshake protocol to ensure data secrecy during transmission across open network or Internet.

Delegation capability is supported by globus security infrastructure (GSI) to ease the burden of the user to keep using the user's private key for mutual authentication between globus toolkit (GTK) nodes and the user computer. A proxy consists of a new CA root certificate (proxy certificate with a public key) and a corresponding private key. The key pair that is used for the proxy is regenerated for each proxy created. The new certificate contains the user's identity with additional information to indicate that it is a proxy. The new certificate is signed by the user's private key, rather than a certification authority (CA) as depicted in FIG. 4. The proxy certificate contains a validity period specified by the user for a limited time to act as proxy. The proxy's private key must be kept secure, but because the proxy isn't valid for very long, it does not have to be kept quite as secure as the owner's private key. Once a proxy is created and stored, the user or the system can use the proxy certificate and private key for digital certificate based mutual authentication. When proxies are used, the mutual authentication process differs slightly. The remote party receives not only the proxy's certificate (signed by the user's private key), but also the user's certificate. During mutual authentication, the user's public key (obtained from her certificate) is used to validate the signature on the proxy certificate. The CA's public key is then used to validate the signature on the owner's certificate. This establishes a chain of trust from the CA to the proxy through the user. Multiple level of proxy certificate can be created, i.e. a proxy certificate can issue a proxy-proxy certificate by using proxy certificate's private key to sign the proxy-proxy certificate public key.

Referring to the sequence diagram 100 of FIG. 5, a user initiates a web browser in the user workstation to send a request issuance to a grid portal that may be hosted on a web server via the public network via, for example hyper text transfer protocol (HTTP). Of course, it will be appreciated that other client-server-based communication protocols may be used. For example, under client-server environment, with reference to FIG. 5, one configuration is that browser plug-in or browser extension program and web browser may be collapsed into a single client, while web server CGI program of grid portal may be collapsed into the server component in the client-server environment. The CGI program may run on the grid portal. The CGI program may be activated via common gateway interface (CGI) by the web server running on the machine. The CGI program's main functions are to generate private-public key pair of the proxy certificate and to construct HTML file that contains embedded tag to activate the browser extension program that runs at the

user computer 12. The grid portal is a portal for computing grids running on a web server that acts as a hyper text transfer protocol (HTTP) server. The grid portal provides a web interface for user to interact with computing grids. Of course it will be appreciated that other protocols may be implemented. The web browser 42 may be an HTTP browser that runs on the user
5 computer 12 and interacts with a web server 22. Such web browsers that may be implemented are browsers such as Microsoft Internet Explorer, Mozilla Firefox, and a number of other browsers available commercially or freely obtained open sourced. The browser extension program 54 may be initiated by the web browser to carry out proxy certificate creation based on the parameters in the embedded tag and interfaces to PKCS#11 or CSP
10 library that links with private key storage devices. CSP provides interface for Microsoft Internet Explorer while PKCS#11 integrates with Mozilla Firefox. PKCS#11 (RSA Laboratorise, "PKCS#11: Cryptographic Token Interface Standard", June 2004), is a cryptographic token interface library that can be loaded into Mozilla Firefox while CSP serves the same purpose for Microsoft Internet Explorer. These cryptographic token interface libraries
15 allow the browsers and browser extension programs to interact with cryptographic tokens to perform RSA private key related operations that involved the use of smart card or virtual memory storage. The smart card 52 may be a cryptographic smart card that is capable of performing RSA private key operations using the stored private key. Malaysian national identity card, MyKad, is capable of performing such operation and therefore can also be used
20 for the purpose stated in this paper. The smart card can also be replaced by virtual memory storage of private key with the necessary cryptographic functions to perform the similar private key operations.

Once the user 12 initiates the web browser to send a request issuance to a grid portal, the grid
25 portal on the web server initiates a software program to request (104) and generate (106) a key pair. The generation of a key pair comprises generation of a private and public key (108). The key pair may be an asymmetric algorithm key-pair, such as for example RSA, error correcting code (ECC), and the like algorithms. RSA and ECC asymmetric algorithms for key-pair specify the mathematical conditions where an arbitrary two numbers may be considered
30 as a pair of interrelated numbers called key-pair. In one embodiment, the computer carries out the following operations in key-pair generation process, for example, two random numbers are generated, and mathematical test or tests are run and conducted based on the selected asymmetric algorithm, such as for example RSA and ECC, on the two random numbers generated. If all conditions specified by the algorithm are met, these two numbers are
35 considered as a key-pair. One of the numbers is given the name as private key while the other number is named as public key. The key pair is generated by CGI program 50 and transmitted (108) to grid portal 48 for storage (110) the key pair in a proper location for future retrieval by other software 48,50 (112). In an embodiment, the task of program such as CGI program 50 is to generate a key pair, while the task of program grid portal 48 is to store the
40 key pair in computer memory storage 46,38, etc. In FIG. 5; when each task is successfully

completed, the next task is executed as indicated. The storage of the key pair for example may be in key data 46 of database 44 or key store 38 of web server. The programs A,B (such as grid portal 48, CGI program 50, or other such programs) transmit (108) the public key to the web server 22. The web server 22 sends or transmits (110) the public key of the generated key pair and all necessary information for proxy certificate generation back to the web browser 42 via the public network 20 via HTTP. The web browser 42 activates (112) a web browser plug-in module 54 or software to calculate (114) hash value to generate a proxy digital certificate by signing the received public key and information from web server using the private key that belongs to the user, for example, within a smart card 52. The calculated hash value is sent (114) from the browser plug-in 54 to the smart card 52 and the private key signs (116) hash value, and the signed hash value is sent (118,120) from the smart card 52 to the browser plug-in 52. The web browser plug-in software initiates the web browser to construct (122) partial proxy digital certificate in a format such as X.509 format. The proxy certificate is constructed (134) after the complete process (124,126,128,130,132) to send hash to be signed. The proxy is then constructed (134) at browser extension program 54 of web browser (42), and sends (136,138) the proxy digital certificate to grid portal 48 of web server 22 via the public network 20 in HTTP for example. The web server initiates (140) another software program such as CGI program 50 to store (142) proxy digital certificate in a proper location for future retrieval by another software such as CGI program 50, grid portal 48 and the like. Once successful (144,146) as indicated in FIG. 5, the procedure is complete. In an embodiment, the proxy digital certificate contains information about the user, for example name and e-mail address, the validity period of the proxy certificate, and other information about issuance of the proxy certificate. The proxy certificate may be coded, for example in X.509 format.

Thus, in an embodiment, the user initiates the web browser to submit HTTP GET request to grid portal running on web server to activate the relevant CGI program that later initiates public-private key pair generation. Upon successful key pair generation, the CGI program stores the key pair in proper storage and replies to the HTTP GET request by sending back the public key that is encoded into base64 format and embedded in HTML file. An example of the embedded tag included in the HTML file is as follows:

```
<EMBED Type="application/x-mgt"  
  mKEY="AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxa.. "  
</EMBED>
```

One parameter called mKEY is included in the embedded tag. The based64 format encoded data that tails the mKEY is the public key generated by the CGI program. For example, when the web browser receives the HTML file with embedded tag containing the public key, the appropriate browser extension program that has been configured to associate with x-mgt application is activated. The browser extension program is pre-installed on the computer running the web browser and has been configured to associate itself with x-mgt application. The first task executed by the browser extension program is to construct a partial X.509 proxy certificate that also complies with the requirement of IETF RFC 3820 Tuechke et al., "Internet

X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile", IETF, RFC 3820, June 2004 (<http://www.ietf.org/rfc/rfc3820.txt>), for proxy certificate format. The browser extension program reads the user certificate from the smart card via PKCS#11 or CSP and extracts the necessary information from the user certificate which will become the issuance certificate or end entity certificate (EEC). The public key is extracted from the variable field mKEY from the embedded tag. The partial X.509 proxy certificate is constructed based on the above mentioned information. Certificate-digest or hash value is calculated from the partial X.509 format proxy certificate. This hash value is sent to the smart card via PKCS#11 or CSP interface to be signed using the private key in the smart card. The signed hash value is returned to the browser extension program and is combined with the partial proxy certificate to form a complete proxy certificate.

The final task of the browser extension program is to initiate the web browser to send a POST command to deliver the proxy certificate to the Grid Portal via hyper text transfer protocol (HTTP). This POST command and its payload of proxy certificate are received by the CGI program running at the grid portal to store it to the appropriate location for proxy certificate storage. This concludes the entire proxy certificate issuance process. The proxy certificate and its corresponding private key will be used by GTK client to initiate digital certificate based mutual authentication with other GTK computing nodes.

It will be appreciated that the above mention method is one embodiment and other variations and different configurations are possible. For example, another variation is the construction of partial X.509 proxy certificate can be done at the CGI program instead of at the browser extension program. In order to ensure compliance that the subject name of the proxy certificate must be the same as the subject name of the issuer or user certificate as per the requirement of IETF RFC 3820, the CGI program must have the capability to access the user certificate for the purpose of extracting the subject name from the user certificate. The user certificate is at the smart card and can be accessed by the browser extension program running at the user computer via PKCS#11 or CSP as per the solution mentioned above. As the user certificate has been transmitted to the web browser via TLS/SSL digital certificate mutual authentication process, the user certificate can be accessed by the CGI program from the grid portal on web server SSL session variable. This situation makes it possible for the CGI program to generate the partial X.509 proxy certificate and subsequently the hash value. In this embodiment, the information exchange between the CGI program and the browser extension program is as described. The hash value can be sent to the browser extension program using the same mechanism of putting the parameter in the embedded tag. The signed hash value is returned to the CGI program using the similar mechanism as the above mentioned method. Hash value and signed hash value are being exchanged instead of public key and a complete proxy certificate. Upon receipt of the signed hash value, the CGI program constructs the complete proxy certificate at the machine running the grid portal. This solution variant achieves the same goal of direct proxy certificate issuance via web browser.

It will be appreciated that other configurations may be envisaged without departing from the scope of the invention, for example, components of the system may be collapsed into client-server environment as discussed. The devices and subsystems of the exemplary methods and systems described with respect to the figures may communicate, for example, over a communication network, and may include any suitable servers, workstations, personal computers (PCs), laptop computers, handheld devices, with visual displays and/or monitors, telephones, cellular telephones, wireless devices, PDAs, Internet appliances, set top boxes, modems, other devices, and the like, capable of performing the processes of the disclosed exemplary embodiments. The devices and subsystems, for example, may communicate with each other using any suitable protocol and may be implemented using a general-purpose computer system and the like. One or more interface mechanisms may be employed, for example, including Internet access, telecommunications in any suitable form, such as voice, modem, and the like, wireless communications media, and the like. Accordingly, network 30 may include, for example, wireless communications networks, cellular communications network, Public Switched Telephone Networks (PSTNs), Packet Data Networks (PDNs), the Internet, intranets, hybrid communications networks, combinations thereof, and the like.

It is to be understood that the embodiments, as described with respect to the figures, are for exemplary purposes, as many variations of the specific hardware used to implement the disclosed exemplary embodiments are possible. For example, the functionality of the devices and the subsystems of the embodiments may be implemented via one or more programmed computer system or devices. To implement such variations as well as other variations, a single computer system may be programmed to perform the functions of one or more of the devices and subsystems of the exemplary systems. On the other hand, two or more programmed computer systems or devices may be substituted for any one of the devices and subsystems of the exemplary systems. Accordingly, principles and advantages of distributed processing, such as redundancy, replication, and the like, also may be implemented, as desired, for example, to increase robustness and performance of the exemplary systems described with respect to the figures.

The exemplary systems described with respect to the figures may be used to store information relating to various processes described herein. This information may be stored in one or more memories, such as hard disk, optical disk, magneto-optical disk, RAM, and the like, of the devices and sub-systems of the embodiments. One or more databases of the devices and subsystems may store the information used to implement the exemplary embodiments. The databases may be organized using data structures, such as records, tables, arrays, fields, graphs, trees, lists, and the like, included in one or more memories, such as the memories listed above.

- All or a portion of the exemplary systems described with respect to figures may be conveniently implemented using one or more general-purpose computer systems, microprocessors, digital signal processors, micro-controllers, and the like, programmed according to the teachings of the disclosed exemplary embodiments. Appropriate software
- 5 may be readily prepared by programmers of ordinary skill based on the teachings of the disclosed exemplary embodiments. In addition, the exemplary systems may be implemented by the preparation of application-specific integrated circuits or by interconnecting an appropriate network of component circuits.
- 10 Whilst there has been described in the foregoing description preferred embodiments of the present invention, it will be understood by those skilled in the technology concerned that many variations or modifications in details of design or construction may be made without departing from the present invention.

CLAIMS:

1. A method of generating a proxy digital certificate to a distributed computing infrastructure by secure data transfer across a public network using a client-server communication protocol, comprising:
- 5 a web browser obtaining a user key independently of a web server;
the web browser sending a request to the web server across the public network using the protocol;
the web server generating a key pair that includes a public key and a private key in response to the request;
- 10 the web server storing the key pair at a key storage location remote to the web browser;
the web server sending the public key to the web browser across the public network using the protocol;
- 15 the web browser generating the proxy digital certificate by signing the public key received from the web server using the user key;
the web browser sending the proxy digital certificate to the web server across the public network using the protocol; and
the web server storing the proxy digital certificate received by the web browser at a certificate storage location remote to the web browser.
- 20
2. The method of claim 1, wherein the public network is the Internet.
3. The method of claim 1, wherein the protocol is hyper text transfer protocol.
- 25
4. The method of claim 1, wherein the web browser obtains the user key from a smart card.
5. The method of claim 1, wherein the web server generates the key pair using an RSA asymmetric algorithm.
- 30
6. The method of claim 1, wherein the web server generates the key pair using an ECC asymmetric algorithm.
- 35
7. The method of claim 1, wherein:
the web server sends the public key and additional information to the web browser across the public network using the protocol;
the web browser generates the proxy digital certificate by signing the public key and the additional information received from the web server using the user key.
- 40

8. The method of claim 1, wherein the web browser calculates a hash value using the user key and signs the public key received from the web server using the hash value.

9. The method of claim 1, wherein the proxy digital certificate is in X.509 format.

5

10. The method of claim 1, wherein the proxy digital certificate includes a name and an e-mail address of a user that uses the web browser.

11. The method of claim 1, wherein the proxy digital certificate includes a validity period for the proxy digital certificate.

10

12. A system of generating a proxy digital certificate to a distributed computing infrastructure by secure data transfer across a public network using a client-server communication protocol, comprising:

15

a web browser obtaining a user key independently of a web server;

the web browser sending a request to the web server across the public network using the protocol;

the web server generating a key pair that includes a public key and a private key in response to the request;

20

the web server storing the key pair at a key storage location remote to the web browser;

the web server sending the public key to the web browser across the public network using the protocol;

25

the web browser generating the proxy digital certificate by signing the public key received from the web server using the user key;

the web browser sending the proxy digital certificate to the web server across the public network using the protocol; and

the web server storing the proxy digital certificate received by the web browser at a certificate storage location remote to the web browser.

30

13. A computer program comprising program instructions for causing a computer to generate a proxy digital certificate to a distributed computing infrastructure by secure data transfer across a public network using a client-server communication protocol, comprising:

35

a web browser obtaining a user key independently of a web server;

the web browser sending a request to the web server across the public network using the protocol;

the web server generating a key pair that includes a public key and a private key in response to the request;

40

the web server storing the key pair at a key storage location remote to the web browser;

the web server sending the public key to the web browser across the public network using the protocol;

the web browser generating the proxy digital certificate by signing the public key received from the web server using the user key;

5 the web browser sending the proxy digital certificate to the web server across the public network using the protocol; and

the web server storing the proxy digital certificate received by the web browser at a certificate storage location remote to the web browser.

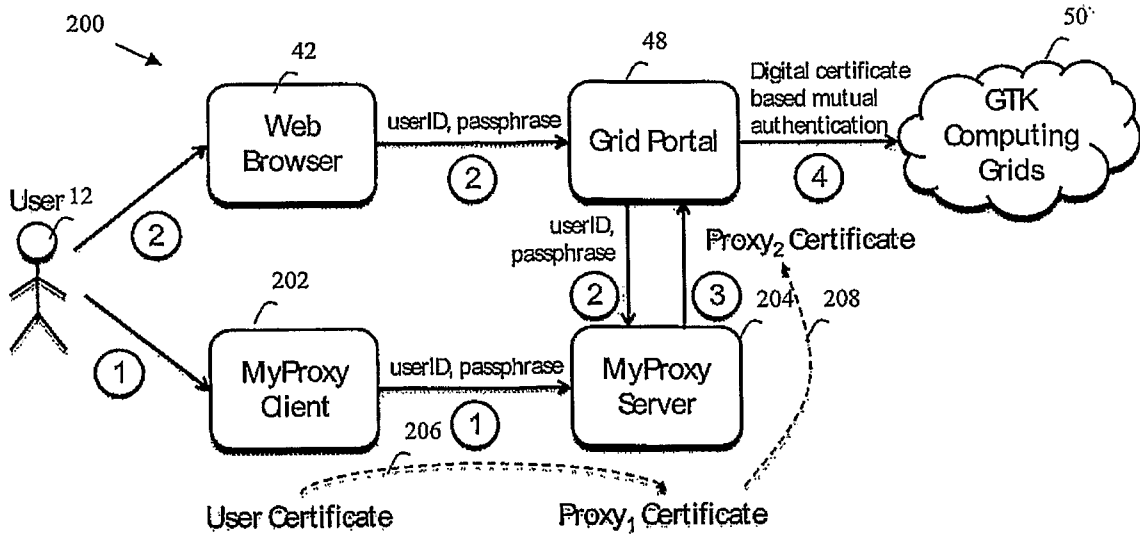


FIG. 1

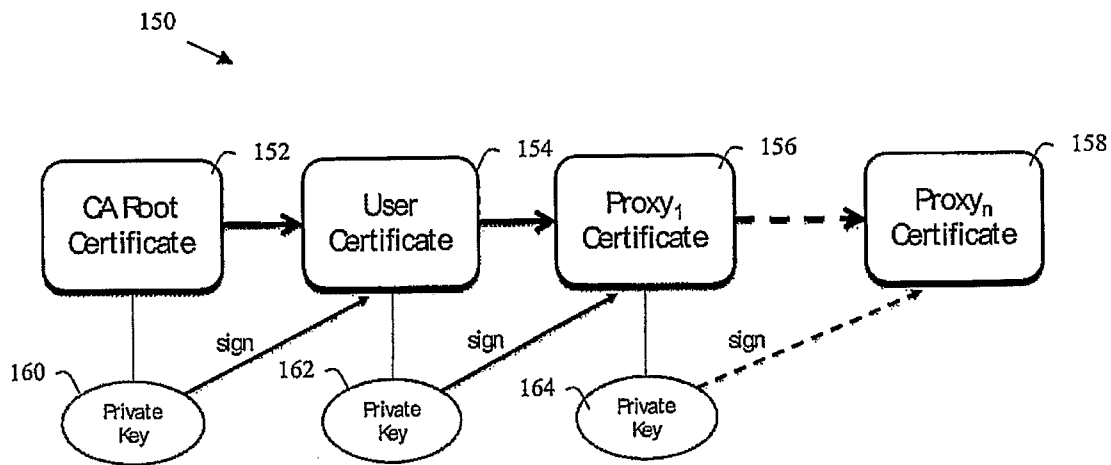


FIG. 4

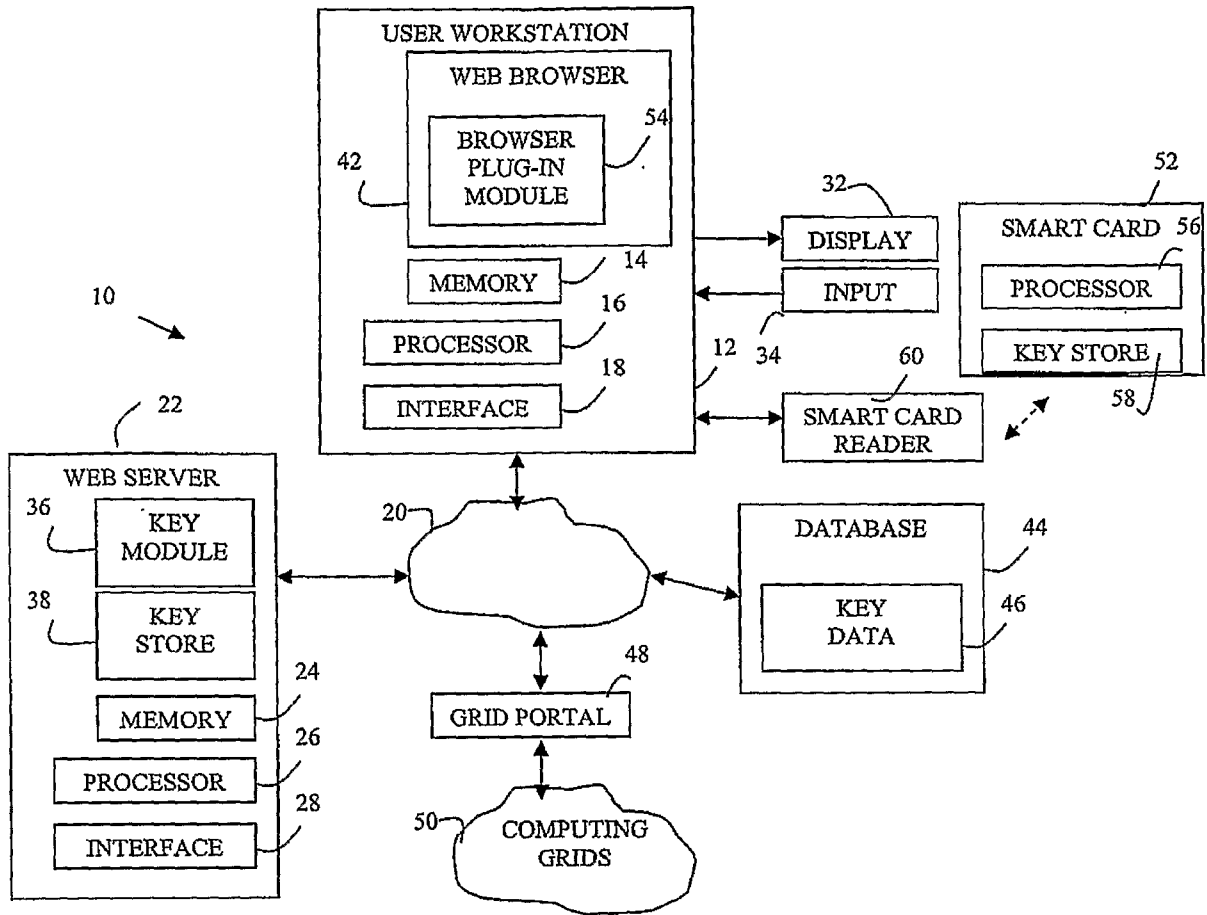


FIG. 2

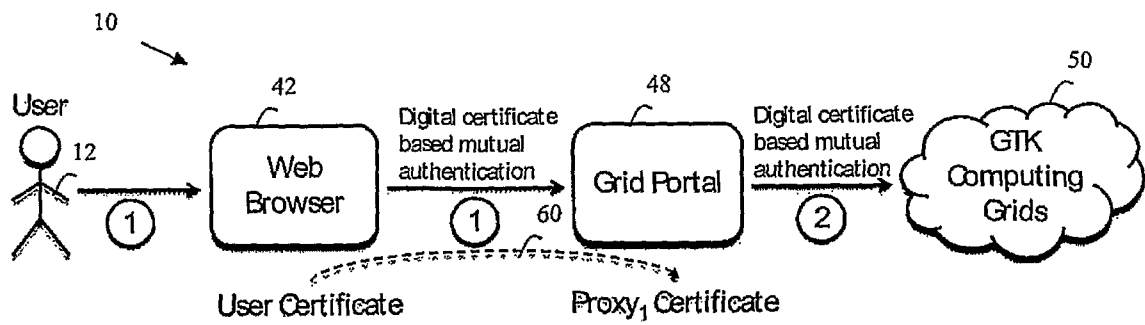


FIG. 3

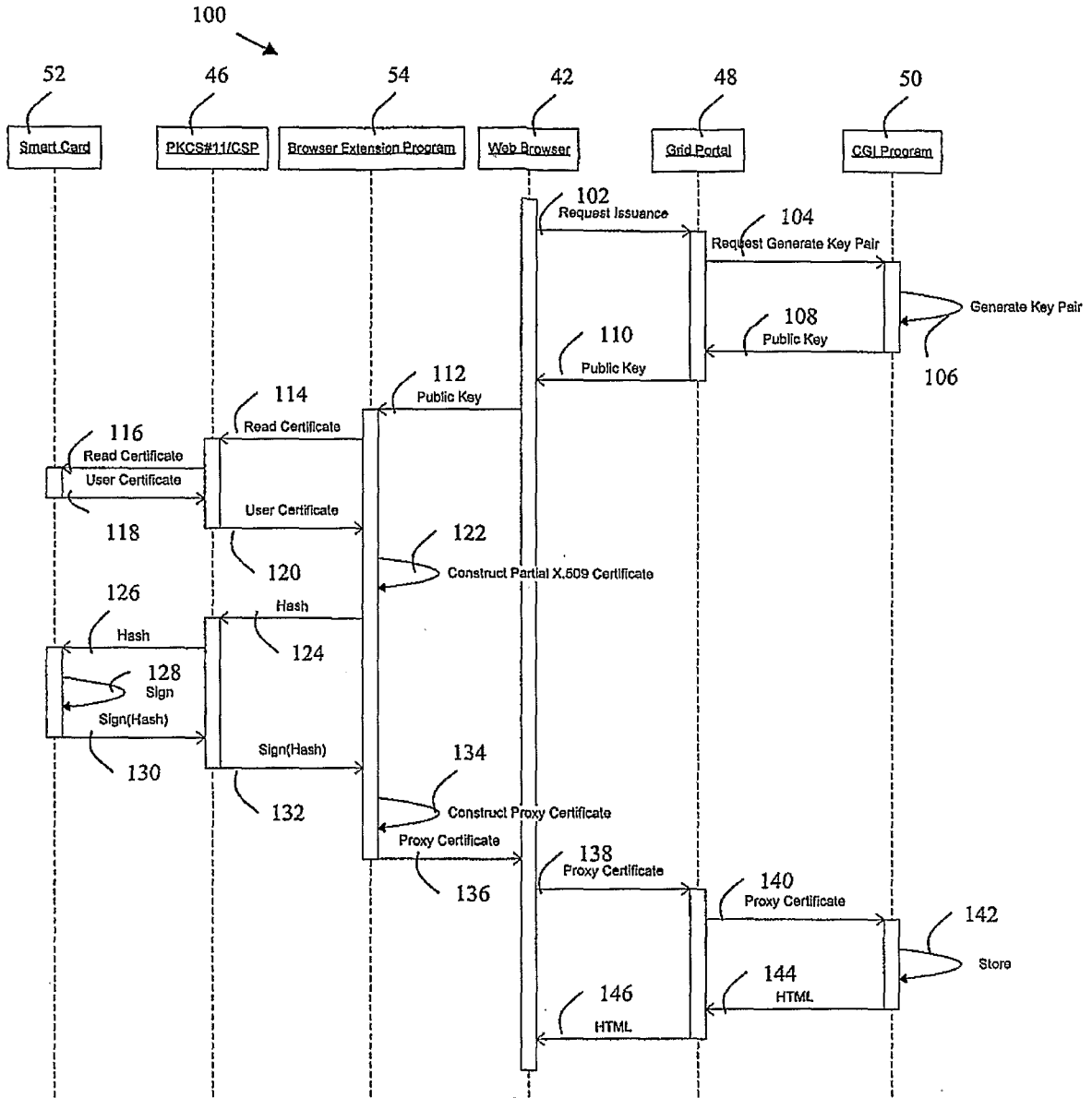


FIG. 5

PATENT COOPERATION TREATY

PCT



DECLARATION OF NON-ESTABLISHMENT OF INTERNATIONAL SEARCH REPORT
(PCT Article 17(2)(a), Rules 13ter.1(c) and (d) and 39)

Applicant's or agent's file reference 20806696/MIM	IMPORTANT DECLARATION	Date of mailing (<i>day/month/year</i>) 29 APRIL 2009 (29.04.2009)
International application No. PCT/MY2008/000115	International filing date (<i>day/month/year</i>) 26 SEPTEMBER 2008 (26.09.2008)	(Earliest) Priority date (<i>day/month/year</i>) 05 OCTOBER 2007 (05.10.2007)
International Patent Classification (IPC) or both national classification and IPC <i>H04L 9/32(2006.01)i, G06F 15/16(2006.01)i</i>		
Applicant MIMOS BERHAD et al		

This International Searching Authority hereby declares, according to Article 17(2)(a), that **no international search report will be established** on the international application for the reasons indicated below.

1. The subject matter of the international application relates to:
 - a. scientific theories.
 - b. mathematical theories.
 - c. plant varieties.
 - d. animal varieties.
 - e. essentially biological processes for the production of plants and animals, other than microbiological processes and the products of such processes.
 - f. schemes, rules or methods of doing business.
 - g. schemes, rules or methods of performing purely mental acts.
 - h. schemes, rules or methods of playing games.
 - i. methods for treatment of the human body by surgery or therapy.
 - j. methods for treatment of the animal body by surgery or therapy.
 - k. diagnostic methods practised on the human or animal body.
 - l. mere presentation of information.
 - m. computer programs for which this International Searching Authority is not equipped to search prior art.
2. The failure of the following parts of the international application to comply with prescribed requirements prevents a meaningful search from being carried out:

the description the claims the drawings
3. A meaningful search could not be carried out without the sequence listing; the applicant did not, within the prescribed time limit:
 - furnish a sequence listing on paper complying with the standard provided for in Annex C of the Administrative Instructions, and such listing was not available to the International Searching Authority in a form and manner acceptable to it.
 - furnish a sequence listing in electronic form complying with the standard provided for in Annex C of the Administrative Instructions, and such listing was not available to the International Searching Authority in a form and manner acceptable to it.
 - pay the required late furnishing fee for the furnishing of a sequence listing in response to an invitation under Rule 13ter.1(a) or (b)
4. A meaningful search could not be carried out without the tables related to the sequence listings; the applicant did not, within the prescribed time limit, furnish such tables in electronic form complying with the technical requirements provided for in Annex C-bis of the Administrative Instructions, and such tables were not available to the International Searching Authority in a form and manner acceptable to it.
5. Further comments:

Name and mailing address of ISA/KR  Korean Intellectual Property Office Government Complex-Daejeon, 139 Seonsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer MA, Jung Youn Telephone No. 82-42-481-5679 
---	--