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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 April 2010 (29.04.2010)

PCT

(10) International Publication Number
WO 2010/047871 A1

(54) Title: SECURE CONSULTATION SYSTEM
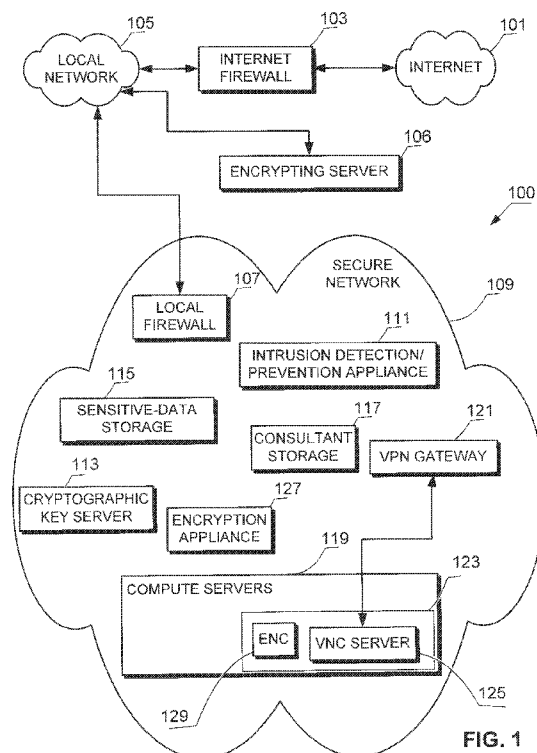
(57) Abstract: A secure consultation system is disclosed that enables an owner entity to securely store its most secure and private data such that designated entities of the owner entity and a consultant entity can execute application programs on that data and thus, to consult on the operation and correctness of the application programs and the data.

FIG. 1

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

SECURE CONSULTATION SYSTEM

Inventor: Van Q. Nguyen

BACKGROUND

Technical Field

[0002]   The disclosed technology relates to the field of secure consultation systems.

Related Art

[0003]   Designing integrated circuits is complex and difficult. Electronic Design Automation software provides design automation tools to assist designers of integrated circuits. These tools assist the designer in the creation of design data (for circuit design modules) that can eventually be embodied in an integrated circuit. EDA software attempts to model and validate the circuit design prior to the actual fabrication of the first integrated circuit to that design. The design data generated by the use of EDA software contains the intellectual property of the designer. This intellectual property is extremely valuable, and is zealously protected and is considered by the designer to be their most secure and private data and is thus sensitive data. If the intellectual property becomes known, a competitor can more quickly compete in the marketplace.

[0004]   EDA software is complex, and even designers who are experienced in its use sometimes need to consult with the developers of the EDA software or with those who have libraries of design data used by the designer. However, obtaining assistance from a consultant entity about an owner's problem with the EDA software (and/or other application program) related to a given design often requires the owner entity of the design to expose their sensitive data used or generated by the EDA software to the consultant entity's technical team.

[0005]   Such a disclosure increases the risk that the design could be misappropriated. Misappropriation can occur by interception of the sensitive data if it is mailed, couriered, or transmitted over a network, as well as by unauthorized access to the data by rogue persons associated with the consultant entity or the owner entity. In some situations this disclosure could be considered to be a public disclosure and thus vitiate trade secret assertions as to the design. Thus, there is a need for some mechanism to enable the consultant entity to be able to

assist the owner entity regarding the owner's problem while keeping the owner entity's sensitive data secure, thus minimizing risk to the owner entity.

[0006]   In general, however, the consultant entity services multiple owner entities. Thus, the consultant entity must insure that the sensitive data of each owner entity is completely and verifiably kept secret from other owner entities. Each owner entity's sensitive data must be protected against threats that originate within the consultant entity, as well as threats that originate outside the consultant entity. For example, the owner entity's sensitive data must be protected even against trusted site administrators, system administrators, or other privileged users of the consultant entity.

[0007]   While contractual agreements between the owner entity and the consultant entity can specify damages for the owner entity if the sensitive data is compromised by the consultant entity, proving how, who, and when is difficult, and any damages that may be obtained are often long delayed.

[0008]   The facility and technology disclosed herein has been used by Synopsys since 2004 and has been made available to selected Synopsys customers since that time under a non-disclosure agreement. This technology has been a factor in closing business deals and has contributed significant revenue to Synopsys. It satisfies a long-standing need in the field of secure consultation systems and is well respected by the companies to which Synopsys has provided the facility.

BRIEF DESCRIPTION OF THE FIGURES

[0009]   Fig. 1   illustrates a secure consultation system site;

[0010]   Fig. 2   illustrates an import data process; and

[0011]   Fig. 3   illustrates a verify agent process.

DETAILED DESCRIPTION

[0012] The technology disclosed herein is a secure consultation system that enables an owner entity to securely store its most secure and private data such that designated personnel of the owner entity and a consultant entity can execute application programs on that data and to consult on the operation and correctness of the application programs when applied to the sensitive data. The secure consultation system includes a secure network and a local firewall that is in communication with a local network and the secure network. The local firewall is configured to pass virtual private network communications between the local network and the secure network. The secure consultation system also includes an intrusion detection appliance in communication with the secure network, and is configured to detect an unauthorized network operation in the secure network. Also, a cryptographic key server is in communication with the secure network, and is configured to provide cryptographic services for use within the secure network. The secure consultation system also includes a sensitive data storage that is in communication with the secure network and is configured to store sensitive data within an owner mount point on the sensitive data storage. The sensitive data is encrypted when stored in the sensitive data storage. In addition, an application program storage is in communication with the secure network, and is configured to store an application program. The secure consultation system also includes a compute server that is in communication with the secure network and is configured to retrieve and execute the application program from the application program storage. The application program is configured to process the sensitive data. The compute server is further configured with a virtual network computing server. The application program is configured to process the sensitive data when invoked by an authenticated and authorized user. In addition, a virtual private network gateway is in communication with the secure network, and is configured to extend the secure network through the local firewall to enable a virtual network computing client external to the secure network to communicate with the virtual network computing server.

[0013] **Fig. 1** illustrates a secure consultation system site **100** that can be used to allow owner entity personnel and consultant entity personnel to cooperate in efforts to resolve an owner's problem that the owner entity may have when applying EDA or related application programs to the owner entity's sensitive data. The secure consultation system site **100** can usually communicate with an internet **101** (such as the Internet). An internet firewall **103**

protects a local network **105** from the internet **101** as is well known in the art. The local

network **105** enables communication between a variety of computing equipment and other

networked appliances, again as is known in the art. These connections can include an

encrypting server **106** and a local firewall **107**. The local firewall **107** controls access from

5   the local network **105** to a secure network **109** and prohibits unauthorized intrusion attempts

into the secure network **109** from the local network **105**. The secure network **109** is a

separate, physically isolated network.

[0014]   As will be subsequently described, access from the local network **105** to the secure

network **109** through the local firewall **107** is extremely limited. In addition, the packets

10   flowing within the secure network **109** are monitored by an intrusion detection/prevention

appliance **111** to detect and (in some embodiments) prevent unauthorized network operations

originating from within the secure network **109**, thus helping detect whether an appliance

connected to the secure network **109** has been compromised (for example, by a virus, or by

an authenticated and authorized user performing prohibited operations). The secure network

15   **109** also includes a cryptographic key server **113** that provides cryptographic services needed

to protect (for example) the owner entity's sensitive data that resides in the sensitive data

storage **115** and that supports other cryptographic operations used within the secure network

109. These services can include the generation and provision of symmetric keys used within

the secure network **109**.

20   [0015]   A consultant storage **117** is used to store application programs and data

provided/used by the consultant entity. Personnel representing the consultant entity and the

owner entity can reproduce the owner's problem by applying these application programs to

the owner entity's sensitive data. Consultant entity personnel and owner entity personnel can

execute these application programs using a computer from a compute server bank **119**.

25   Access to the compute server bank **119** resources can be through a VPN gateway **121**. The

authenticated and authorized users of the owner entity and the consultant entity do not have

direct access to the sensitive data stored on the sensitive data storage **115**. Instead,

application programs that execute on the allocated compute server **123** provide a presentation

to the user of the user interface rendered by the application program as it operates on the

30   sensitive data. The sensitive data storage **115** is organized into shares (exports). The

appropriate share containing the owner entity's sensitive data is an owner mount point that

can be mounted by an authenticated and authorized user of the allocated compute server **123**.

The owner entity's sensitive data is prohibited from being moved, copied, or otherwise stored

outside the owner mount point assigned to the owner entity. Thus, this data cannot be transferred to a tangible storage media. Further, the intrusion detection/prevention appliance **111** and/or the local firewall **107** prohibit this data from being transferred outside the secure network **109**.

[0016]   The secure network **109** is preferably completely arrayed within a secure physical location to which only authenticated and authorized people are allowed access. Such access can be allowed and logged by using access procedures (for example, using keycard and biometric authentication techniques), as is known by one skilled in the art. Electronic access for authenticated and authorized users can be through a virtual private network (VPN) to a virtual network computing server **125** (a VNC server) on the allocated compute server **123**.

[0017]   The consultant entity's personnel and the owner entity's personnel debug and test the application programs against the owner entity's sensitive data to resolve the owner's problem. Generally the allocated compute server **123** can only mount a single owner mount point, and only authenticated and authorized users for that owner mount point can log in to the allocated compute server **123**.

[0018]   The secure network **109** protects against internal and external threats to the owner entity's sensitive data, because this data is physically located in a known and secure physical location, is encrypted in the sensitive data storage **115**, cannot be copied out of the secure network **109**, cannot be copied outside the owner mount point, and cannot be copied into tangible media (that could be removed from the secure physical location). Thus, external threats from rogue personnel of either the owner entity or the consultant entity are foiled. In addition, site administrators, system administrators, or other privileged users of the secure network **109** and the secure physical location are prohibited from viewing the sensitive data so that internal threats by rogue, but trusted, personnel are also foiled. Furthermore, all access to the sensitive data is audited.

[0019]   The design data can be conveniently and securely delivered to the secure consultation system by using a secure network protocol such as secure FTP (SFTP) to transmit encrypted design data over the Internet. In one embodiment, the SFTP transfer protocol requires a two-factor authentication.

[0020]   The encrypting server **106** can be used to provide a secure means for the owner entity to deliver their design data to the sensitive data storage **115**. Once the constraints from

the non-disclosure agreement have been incorporated into the encryption appliance **127** (in particular, once the owner entity's permissions, privileges, and cryptographic keys are defined), the owner entity can deliver their sensitive data to the secure network **109**. One of the more secure ways to deliver this data is by using Secure FTP to send the data over the Internet in an encrypted form, such that the sensitive data is encrypted while in transit. In one embodiment, the encrypting server **106** executes VanDyke Software's SecureFX® application to provide a secure data transfer capability. The sensitive data can be encrypted when stored on the encrypting server **106** using any appropriate encryption package. In one embodiment, the encryption package uses Vormetric, Inc.'s CoreGuard™ Information Protection System.

[0021]   Once the sensitive data is stored on the encrypting server **106**, a program can transfer the sensitive data to the owner mount point on the sensitive data storage **115** within the secure network **109**. In one embodiment, the encrypted sensitive data is decrypted, a file digest (for example, a MD5 checksum) of the sensitive data is computed, and the sensitive data and the file digest are transmitted using a secure protocol (such as SFTP, SSH, or other encrypting protocol) from the encrypting server **106** to the sensitive data storage **115** where the file digest is used to verify that the copy was successful. Once the sensitive data has been verifiably copied to the sensitive data storage **115**, the encrypted file containing the sensitive data is deleted from the encrypting server **106**. As the sensitive data is received from the encrypting server **106**, it is encrypted by the encryption appliance **127** and stored (for example, as a relocated file) in the sensitive data storage **115** within an owner mount point. Fig. 2 and Fig. 3 and the accompanying descriptions further describe one embodiment of a data import process that can be used to relocate the sensitive data from the encrypting server **106** to the sensitive data storage **115**.

[0022]   In some embodiments, deletion of a file or owner mount point also includes the execution of a shred and/or scrub application to remove all traces of the sensitive data from the sensitive data storage **115**.

[0023]   The previously discussed technology first decrypted the sensitive data in the encrypting server **106**, and copied the sensitive data to the secure network **109** through a secure connection to the sensitive data storage **115**, where the data is encrypted by the encryption appliance **127**. This approach is useful when the encrypting server **106** and the encryption appliance **127** do not have compatible encryption management capability. For

embodiments that do have compatible encryption management capability, the encrypted sensitive data can be copied from the encrypting server **106** to the sensitive data storage **115** without decryption. In this situation, the file digest can be created from the encrypted sensitive data.

[0024]   In some embodiments, the sensitive data can be delivered to an administrator of the secure network **109** on tangible media that can be read by a computer. For example, this delivery could be accomplished by using a trusted courier to physically deliver the design data to the consultant entity; however, such a courier could be intercepted, robbed, bribed, etc. One skilled in the art will understand that delivery of tangible media containing the sensitive data carries more risk than the previously described network approach.

[0025]   Within the secure network **109**, the owner entity's sensitive data can be encrypted and decrypted by an encryption appliance **127** (for example, NetApp, Inc.'s DataFort™ security storage security appliance) as well as an encryption service **129** residing on the allocated compute server **123**.

[0026]   The local firewall **107** can be a level-4 firewall that can be configured to allow only specific accesses from the local network **105** to the secure network **109**. In one embodiment, the local firewall **107** can be configured to disable the transfer of any data or application from the sensitive data storage **115** or the consultant storage **117** to outside of the secure network **109**. In one embodiment, the data transferred from within the secure network **109** can be via a virtual network computing protocol over a virtual private network. The local firewall **107** and the intrusion detection/prevention appliance **111** can be configured to prohibit other data transfers within the secure network **109**. In one embodiment, the local firewall **107** is configured to deny all file transfers into the secure network **109** except those from the encrypting server **106** to the sensitive data storage **115**.

[0027]   The sensitive data storage **115** can be configured as a redundant storage (as is known to one skilled in the art) to obviate the need for backup media (and its associated risk). The sensitive data can be deleted from the sensitive data storage **115** when it is no longer needed by deleting the file or owner mount point to securely remove any trace of the sensitive data from the sensitive data storage **115**.

[0028]   The local firewall **107** can be configured to allow VPN communications to access the VPN gateway **121** and so allow an authenticated and authorized user access to the virtual

network computing server **125** executing in the allocated compute server **123**. The VNC

protocol is encapsulated by the VPN gateway **121**. The local firewall **107** can be configured

to detect and log activities of interest such as logon attempts, application execution, file

accesses, and file decryption and encryption events, etc., and provide alerts and reports to the

specified auditors. By using VPN and VNC, authenticated and authorized users (including

personnel of the owner entity as well as personnel of the consultant entity) have access to the

application programs stored on the consultant storage **117**, and these application programs

can access the owner entity's sensitive data stored on the sensitive data storage **115**. Thus,

the owner entity's personnel and the consultant entity's personnel can identically replicate the

owner's problem with the application program and/or sensitive data, and can work together to

resolve the owner's problem. The VNC server has its clipboard function disabled, such that

the sensitive data cannot be transferred from within the secure network **109** using copy-and-

paste GUI functions.

[0029] One skilled in the art will understand that the intrusion detection/prevention

appliance **111** also can be configured to detect and log activities of interest such as logon

attempts, application execution, file accesses, and file decryption and encryption events, etc.,

and provide alerts and reports to the specified auditors. The intrusion detection/prevention

appliance **111** can also monitor and record unusual network traffic flowing over the secure

network **109**, and can notify the specified auditors when particular events occur. These

notifications can be via e-mail, SNMP, or by execution of user-defined programs. In some

embodiments the intrusion detection/prevention appliance **111** can block a detected attack

(for example, by blocking access to the targeted appliance, blocking access to the targeted

appliance from the attacker, dropping the connection, etc.). In addition, the intrusion

detection/prevention appliance **111** can identify reconnaissance activity that can be a prequel

to an attack. In some embodiments, the intrusion detection/prevention appliance **111** can be

configured to perform network behavior analysis to identify attacks that generate unusual

network traffic and policy violations. Further, the intrusion detection/prevention appliance

111 can prevent installation of unauthorized patches or updates to application programs

stored in the consultant storage **117** or to application/system programs on the compute server

bank **119**. The local firewall **107** and the intrusion detection/prevention appliance **111** prevent

installation of unauthorized patches or updates to the compute server bank **119** and to the

consultant storage **117**. In one embodiment, the intrusion detection/prevention appliance **111**

is provided by 3Com Corporation's TIPPINGPOINT® IPS device.

[0030]   The sensitive data storage **115** contains the sensitive data for each owner entity. The sensitive data is always stored in an encrypted form. The local firewall **107** and the intrusion detection/prevention appliance **111** are configured so that the sensitive data cannot be transferred outside of the secure network **109**. Furthermore, direct access to the owner entity's sensitive data is only provided to application programs executing on the allocated compute server **123** under control of the virtual network computing server **125**.

[0031]   The compute server bank **119** provides a number of compute servers for use by any of the owner entities. In one embodiment, at login, a single one of the compute servers in the compute server bank **119** is assigned to a particular owner entity (such as an allocated compute server **123**) to minimize the possibility of some other owner entity being able to access the particular owner entity's sensitive data. Consultant entity and owner entity personnel can operate on the owner entity's sensitive data using application programs from the consultant storage **117**. In some embodiments multiple personnel from the owner entity and/or multiple personnel from the consultant entity can simultaneously share the sensitive data storage **115** in the owner mount point if the authentication and authorization of the users allow mounting of the same owner mount point. In some embodiments, the allocated compute server **123** can be shared by users who have access to the same owner mount point.

[0032]   Encryption can be accomplished by the encryption appliance **127** that encrypts the sensitive data when it is stored on the sensitive data storage **115** (for example, when the sensitive data is relocated from the encrypting server **106**). The sensitive data can be decrypted when accessed by the allocated compute server **123** by flowing the encrypted sensitive data through the encryption appliance **127** (once decrypted, the sensitive data flows to the allocated compute server **123** in the clear — but within the secure network **109**).

[0033]   Encryption/decryption of the sensitive data can also be accomplished by the encryption service **129** executing on the allocated compute server **123** and configured to decrypt and encrypt data read from and written to the sensitive data storage **115**. This technique keeps the data encrypted even when flowing through the secure network **109**.

[0034]   The owner entity can specify whether their sensitive data can be modified or copied while in the secure network **109**. If modifications and/or copies are allowed, such modifications and copies are audited. In one embodiment, such modifications and/or copies are only allowed within the owner entity's owner mount point.

[0035]   The previous discussion has described the configuration of the secure consultation system site **100**. Before the owner entity can transfer its sensitive data to the secure consultation system site **100**, the site administrators, system administrators, or other privileged users of the secure consultation system site **100** must initialize the required authorization, authentication, and cryptography characteristics for the owner entity as well as create a corresponding owner mount point on the sensitive data storage **115**.

[0036]   Once an owner entity has recognized an owner's problem that needs consultation with the consultant entity, the owner entity and the consultant entity select personnel from each entity that will have the ability to execute application programs on the sensitive data, as well as specified auditors who will receive reports and event information about accesses to the sensitive data. This understanding is memorialized, for example, by an executed non-disclosure agreement (NDA). From the information in the NDA, the site administrators, system administrators, or other privileged users condition the cryptographic key server **113** to set up the authenticated and authorized users for appropriate access to the sensitive data and identify the specified auditors for event and report notifications. Access to the sensitive data is fine-grained at the logon, application execution, file access, and file decryption/encryption levels. Site administrators, system administrators, or other privileged users are blocked from prohibited access to the owner entity's sensitive data by software agents that provide kernel–mode controls to restrict access by such privileged users. Thus, the site administrators, system administrators, or other privileged users only provide oversight, control, setup, and protection of the secure network **109** in the securely controlled access area.

[0037]   Once the encryption appliance **127** is conditioned, the authentication and authorization parameters defined, and the owner mount point allocated, the owner entity can send its sensitive data to the secure consultation system site **100** as previously described. Once the owner entity's data resides on the sensitive data storage **115** (for example, in a relocated file), the designated personnel (who are authenticated and authorized users) can VPN into the secure network **109** to obtain VNC access to the allocated compute server **123**, and so execute applications that are stored on the consultant storage **117** on the owner entity's sensitive data that is stored on the sensitive data storage **115** within the owner mount point. These resident applications can (if the relocated file's permissions allow) modify or copy the owner entity's sensitive data so long as the copy/modification remains in the owner mount point. In this manner, the consultant entity's personnel and the owner entity's personnel can debug and consult within a secure environment. Note that because the authenticated and

authorized user can only access the allocated compute server **123** within the secure network **109**, the sensitive data cannot be directly accessed or transferred outside of the securely controlled access area.

[0038]   Events can be logged by the local firewall **107**, the intrusion detection/prevention appliance **111**, the cryptographic key server **113**, the VPN gateway **121**, etc. The specified auditors designated in the NDA receive an audit trail of all users and executables that access the sensitive data as well as account logon/logoff attempts, file accesses, and file decryption attempts, file modifications, file copies, etc. Once the owner's problem is resolved, the sensitive data is no longer needed and is deleted (as well as any other copies or modified copies), and deletion notifications are sent to the specified auditors. In some embodiments, when the owner's problem is resolved, the owner entity's owner mount point is shredded/scrubbed when it is deleted.

[0039]   Fig. 2 illustrates an import data process **200** that can be used to relocate the owner entity's sensitive data from the encrypting server **106** to a relocated file in the sensitive data storage **115**. The import data process **200** executes on the encrypting server **106** and initiates at a start terminal **201** responsive to initialization of the encrypting server **106**, in response to an operator command, in response to a cron event, etc. Once initiated, the import data process **200** continues to a 'scan directory' procedure **203** that scans the directories on the encrypting server **106** that are eligible for receiving owner entities' sensitive data. A 'new file' decision procedure **205** determines whether a new file was found in the scanned directories. If no new file was found, the import data process **200** returns to the 'scan directory' procedure **203**.

[0040]   However, if a new file was found (in other words, the encrypting server **106** has completely received sensitive data from the owner entity), the import data process **200** continues to a 'generate file digest' procedure **207** that calculates a file digest (for example, a MD5 checksum) for the newly found file. A 'copy file to secure network' procedure **209** then securely transfers the file to the sensitive data storage **115** through the local firewall **107** (which is configured to allow files to be transferred into the secure network **109** by the encrypting server **106**). Also a 'send file digest to verify agent' procedure **211** sends the file digest to a verify agent application within the secure network **109** for processing as subsequently described with respect to Fig. 3. In one embodiment, the encrypting server **106** decodes the sensitive data and generates the file digest as the data is being copied to the

sensitive data storage **115** (for example, by using a combination of pipes and filter applications).

[0041]   After the file digest has been sent to the verify agent application, the import data process **200** eventually receives a result status such as a success or error status message from the verify agent application. If a 'transfer verified' decision procedure **213** determines that the file was successfully transferred to the sensitive data storage **115**, then the secure consultation system site **100** continues to a 'delete file' procedure **215** that deletes the sensitive data from the encrypting server **106**.

[0042]   However, if the 'transfer verified' decision procedure **213** received an error status message from the verify agent application, the import data process **200** returns to the 'copy file to secure network' procedure **209** to retry the transfer.

[0043]   **Fig. 3** illustrates a verify agent process **300** that can execute on any computer in the secure network **109**. The verify agent process **300** can also execute as a service on the cryptographic key server **113** or on the sensitive data storage **115**. The verify agent process **300** initiates at a start terminal **301** responsive to initialization of the computer hosting the verify agent application, in response to an operator command, in response to a cron event, etc. Once initiated, the verify agent process **300** continues to a 'scan directory' procedure **303** that scans the directories on the sensitive data storage **115** that are eligible for receiving owner entities' sensitive data from the encrypting server **106**. A 'new file detected' decision procedure **305** determines whether a new relocated file was found in the scanned directories. If no new relocated file was found, the verify agent process **300** returns to the 'scan directory' procedure **303**.

[0044]   However, if a new relocated file was found (in other words, that the sensitive data storage **115** has completely received a file from the encrypting server **106**), the verify agent process **300** continues to a 'receive file digest' procedure **307** that receives the file digest sent by the 'send file digest to verify agent' procedure **211** executing on the encrypting server **106**. A 'generate local file digest' procedure **309** calculates a file digest for the newly found relocated file. The file digest received by the 'receive file digest' procedure **307** and the newly generated file digest are compared by a 'file digests match' decision procedure **311**. If the file digests are the same, the verify agent process **300** continues to a 'send success status' procedure **313** that sends a result status indicating success back to the encrypting server **106** where it is received by the 'transfer verified' decision procedure **213**.

[0045]   If the file digests do not match, the verify agent process **300** continues to a 'delete file' procedure **315** that deletes the relocated file from the sensitive data storage **115** and a 'send error status' procedure **317** that sends a result status indicating failure back to the encrypting server **106**, where it is received by the 'transfer verified' decision procedure **213** such that the file transfer can be retried.

[0046]   One skilled in the art will understand that the 'scan directory' procedure **303** can incorporate a delay, such as by implementing a timer, by causing the import data process **200** to exit and be restarted by a cron event, etc. Such a one will also understand that there are many ways to implement the import data process **200** and the verify agent process **300**, and that the sequence of operations implied by Fig. 2 and Fig. 3 is not required to provide equivalent functionality. Such a one will also understand that such functionality can be implemented using scripts or an application that utilizes a threaded design. Such a one will also understand that for clarity error recovery details have not been included. For example, such a one would include logic needed to distinguish files that are partially transferred from files that are completely transferred.

[0047]   One skilled in the art will understand that the prior description has been of an embodiment where the consultant entity is servicing multiple owner entities. Such a one will understand that the secure consultation system site **100** can be implemented by an owner entity and that the consultant entity's personnel would have equivalent capability for assisting the owner entity's personnel in resolving the owner's problem.

[0048]   As used herein, a procedure is a self-consistent sequence of steps that can be performed by logic implemented by a programmed computer, specialized electronics or other circuitry, or a combination thereof that leads to a desired result. These steps can be defined by one or more computer instructions. These steps can be performed by a computer executing the instructions that define the steps. Further, these steps can be performed by circuitry designed to perform the steps. Thus, the term "procedure" can refer (for example, but without limitation) to a sequence of instructions, a sequence of instructions organized within a programmed-procedure or programmed-function, a sequence of instructions organized within programmed-processes executing in one or more computers, or a sequence of steps performed by electronic or other circuitry, or any logic or combination of the foregoing. In particular, the methods and processes described herein can be implemented with logics.

[0049]   One skilled in the art will understand that the system described herein provides an extremely secure consulting platform that enables an owner entity to securely store its most secure and private data such that designated personnel of the owner entity and a consultant entity can execute application programs on that data, and thus, enables consultation about the operation and correctness of the application programs and the data.

[0050]   From the foregoing, it will be appreciated that the technology has (without limitation) the following advantages:

    1)   A secure and automatic delivery mechanism for transfer of the owner entity's sensitive data from the owner entity to the secure network **109**.

    2)   Continued security of the owner entity's sensitive data (because it is encrypted in storage residing on a secure network **109**, it is protected from viewing by privileged accounts, and it cannot be copied out of the secure network **109**).

    3)   Prohibits direct access to the sensitive data because an authenticated and authorized user can only access the sensitive data through application programs residing on the consultant storage **117**, and these programs can only be invoked using the virtual network computing client using the VPN gateway **121**.

    4)   Securely generates and stores encryption keys by the cryptographic key server **113** within the secure network **109**.

    5)   Uses "fine-grained" control of authenticated and authorized user access to the sensitive data and the compute server bank **119**.

    6)   Ensures that site administrators, system administrators, or other privileged users are authenticated and operate as intended.

    7)   Provides a full audit trail of access to the owner entity's sensitive data, and changes of protection related to the sensitive data, as well as automatic notification of changes to secure policies and verification when the owner entity's sensitive data has been deleted.

    8)   Controls and audits attempts to access sensitive configuration files, logs, etc. and provides "real-time" evidentiary audit of system & data integrity.

    9)   Provides a secure environment for the owner entity and the consultant entity to investigate the owner's problem.

10)   Logically and physically protects the owner entity's design data against both internal and external threats.

11)   Prevents installation of unauthorized patches or updates, and prevents unauthorized and altered applications and libraries from launching, e.g., trojans, worms, etc.

[0051]   The claims, as originally presented and as they may be amended, encompass variations, alternatives, modifications, improvements, equivalents, and substantial equivalents of the embodiments and teachings disclosed herein, including those that are presently unforeseen or unappreciated, and that, for example, may arise from applicants/patentees and others.

[0052]   It will be appreciated that various of the above-disclosed and other features and functions, or alternatives thereof, may be desirably combined into many other different systems or applications. It will also be appreciated that various presently unforeseen or unanticipated alternatives, modifications, variations or improvements therein may be subsequently made by those skilled in the art, which are also intended to be encompassed by the following claims. Unless specifically recited in a claim, steps or components of claims should not be implied or imported from the specification or any other claims as to any particular order, number, position, size, shape, angle, color, or material.

[0053]   What is claimed follows:

CLAIMS

1.   A secure consultation system comprising:

        a secure network;

        a local firewall in communication with a local network and said secure network, said local firewall configured to pass virtual private network communications between said local network and said secure network;

        an intrusion detection appliance in communication with said secure network and configured to detect an unauthorized network operation in said secure network;

        a cryptographic key server in communication with said secure network and configured to provide one or more cryptographic services within said secure network;

        a sensitive data storage in communication with said secure network and configured to store sensitive data within an owner mount point on said sensitive data storage, said sensitive data encrypted when stored in said sensitive data storage;

        an application program storage in communication with said secure network and configured to store an application program;

        a compute server in communication with said secure network and configured to retrieve and execute said application program from said application program storage, said application program configured to process said sensitive data, said compute server further configured with a virtual network computing server, said application program configured to process said sensitive data when invoked by an authenticated and authorized user; and

        a virtual private network gateway in communication with said secure network and configured to extend said secure network through said local firewall to enable a virtual network computing client external to said secure network to communicate with said virtual network computing server.

2.   The secure consultation system of claim 1, further comprising an encryption appliance configured to encrypt said sensitive data as said sensitive data is sent to said sensitive data storage.

3.   The secure consultation system of claim 1, wherein said compute server is further configured to encrypt said sensitive data when writing to said sensitive data storage.

4.   The secure consultation system of claim 1, further comprising a secure delivery system.

5.   The secure consultation system of claim 4, wherein said secure delivery system comprises:

     an encrypting server in communication with said local network and configured to receive said sensitive data using a secure communication protocol, said encrypting server further configured to encrypt said sensitive data when stored outside said secure network; and

     said encrypting server configured to verifiably copy said sensitive data to said sensitive data storage, said sensitive data stored on said sensitive data storage encrypted by said encryption appliance.

6.   The secure consultation system of claim 1, wherein said compute server is one of a plurality of compute servers.

7.   The secure consultation system of claim 1, wherein said intrusion detection appliance is configured to prohibit transfer of said sensitive data out of said secure network.

8.   The secure consultation system of claim 1, wherein said intrusion detection appliance, said cryptographic key server, said sensitive data storage, said application program storage, and said compute server are located within a securely controlled access area.

9.   The secure consultation system of claim 1, wherein said owner mount point is one of a plurality of owner mount points.

10.   A computer controlled method for relocating sensitive data from an encrypting server to a sensitive data storage on a secure network, said sensitive data residing in at least one file, said method comprising:

determining, outside said secure network, that said sensitive data exists on said encrypting server;

generating, outside said secure network, a first file digest responsive to said at least one file;

sending said at least one file to said secure network for storage on said sensitive data storage as a relocated file;

sending said file digest to said secure network;

generating, within said secure network, a second file digest responsive to said relocated file;

determining, within said secure network, whether said first file digest and said second file digest are equal; and

sending a result status outside said secure network, said result status responsive to determining whether said first file digest and said second file digest are equal.
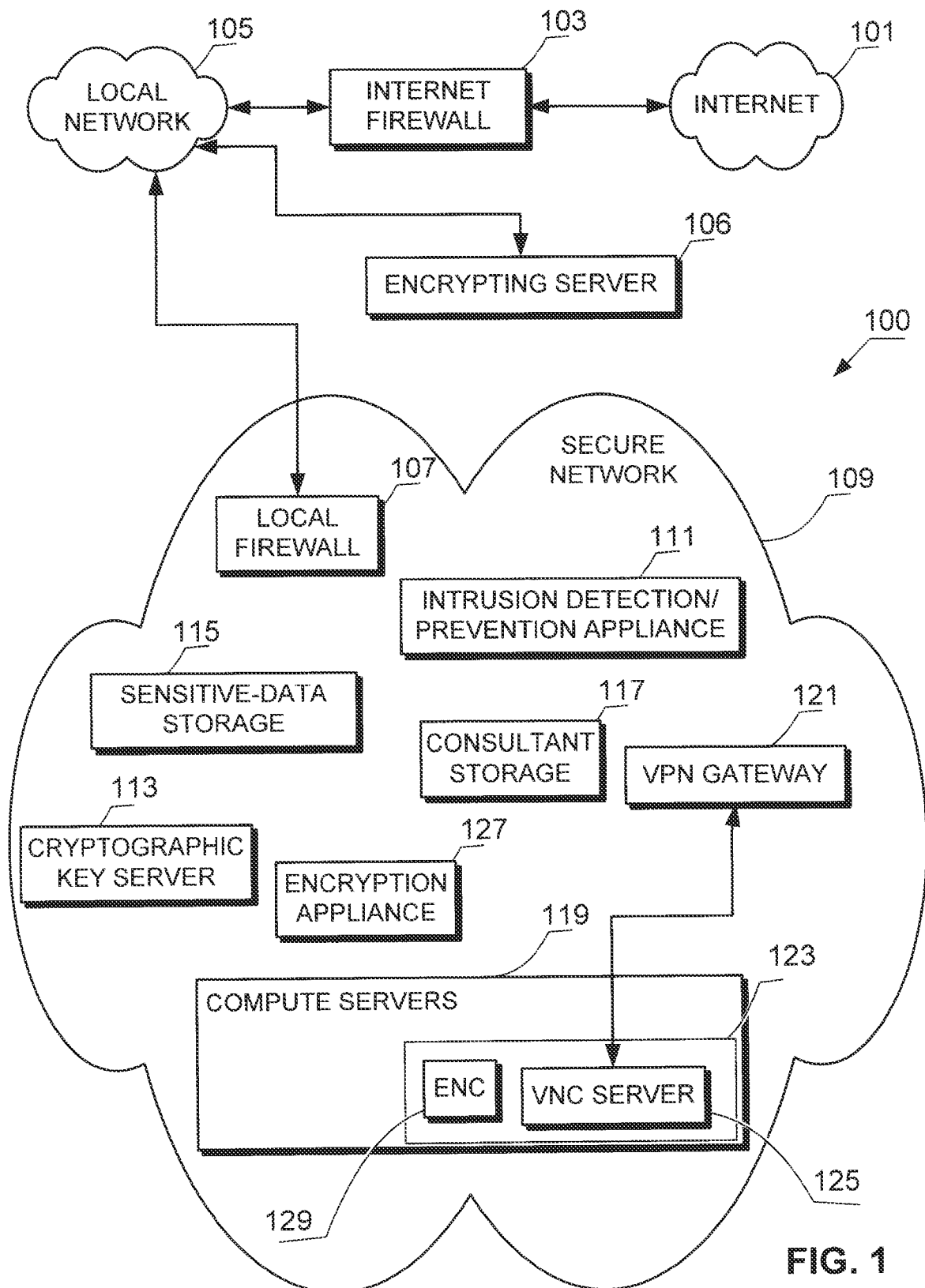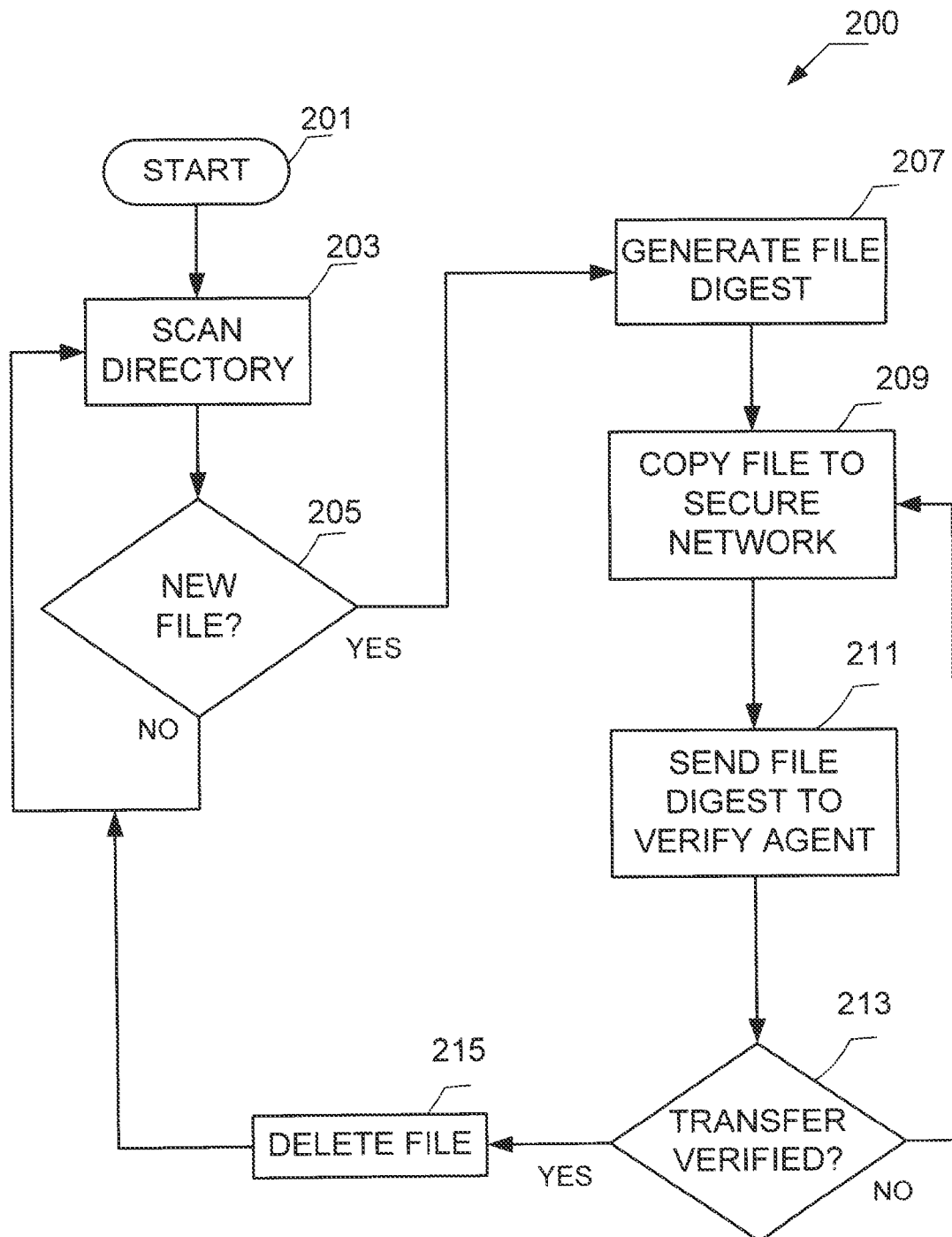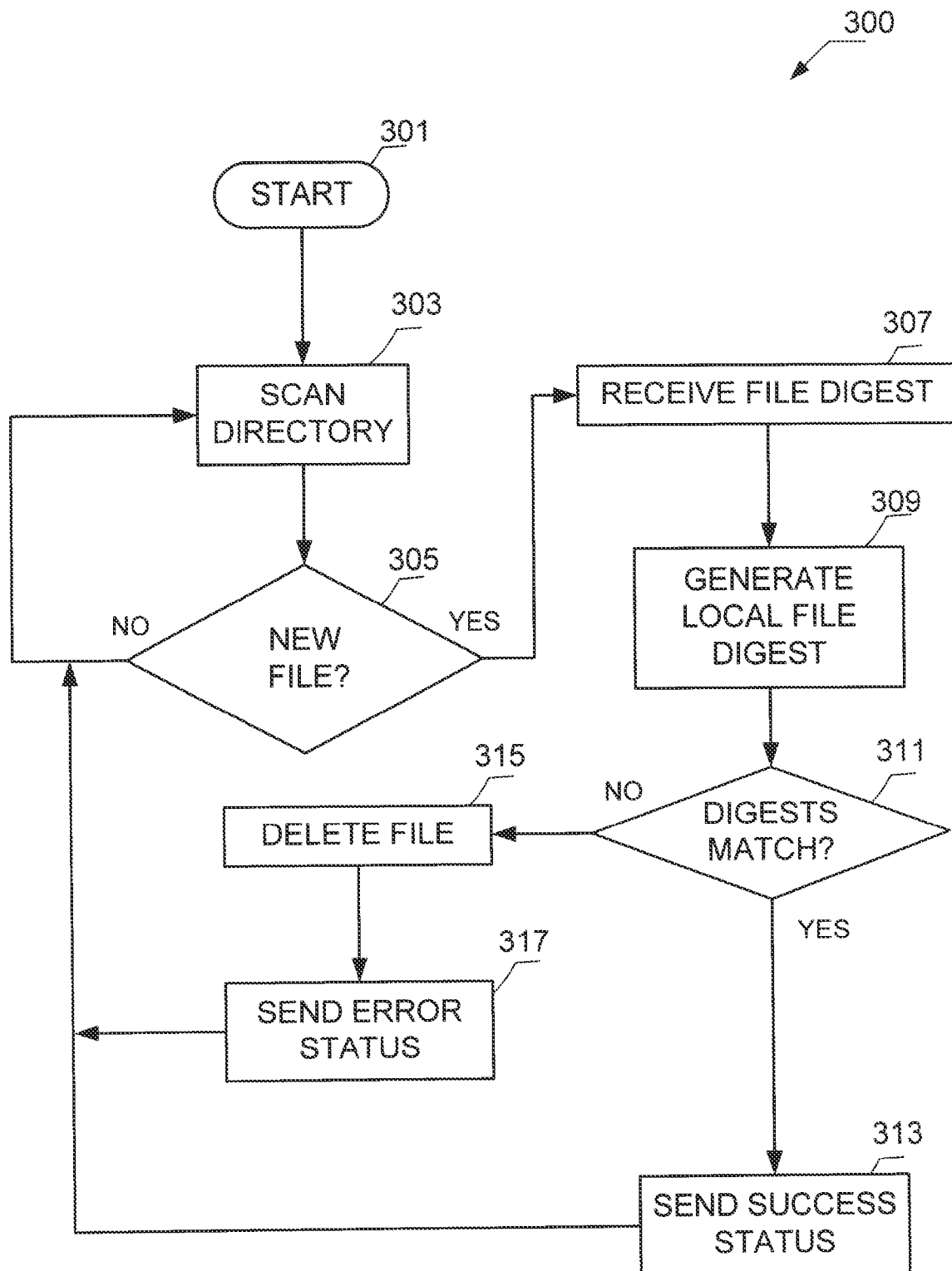
FIG. 1

WO 2010/047871   PCT/US2009/053677

2 / 3

FIG. 2

FIG. 3

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/00(2006.01)i, G06F 15/00(2006.01)i

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

B. FIELDS SEARCHED

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

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
 eKOMPASS(KIPO internal) "secure, network, firewall, eryptographic, VPN, virtual private, intrusion, detection"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	US 2003/0056063 A1 (HOCHMUTH et al.) 20 March 2003 See the abstract; figures 1 and 3; paragraphs [0014], [0021]-[0038].	1-3,6-9 4,5,10
A	US 2004/0221179 A1 (SESHADRI) 04 November 2004 See the abstract; figures 1, 2 and 4; paragraphs [0019]-[0025].	1-10
A	US 2005/0132221 A1 (MARCJAN) 16 June 2005 See the abstract; figure 1; paragraphs [0025]-[0026].	1-10
A	US 2004/0049702 A1 (SUBRAMANIAM et al.) 11 March 2004 See the abstract; figures 1, 3 and 4; paragraphs [0025]-[0034], [0071]-[0083].	1-10

☐ Further documents are listed in the continuation of Box C.   ☒ See patent family annex.

* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art "&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
05 MARCH 2010 (05.03.2010)	**11 MARCH 2010 (11.03.2010)**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office Government Complex-Daejeon, 139 Seonsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	KYUNG, Youn Jeong Telephone No. 82-42-481-8536

Form PCT/ISA/210 (second sheet) (July 2009)

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003-0056063 A1	20.03.2003	US 7500069 B2	03.03.2009
US 2004-0221179 A1	04.11.2004	EP 1473898 A1 US 2004-0230841 A1 US 7269848 B2 US 7269849 B2	03.11.2004 18.11.2004 11.09.2007 11.09.2007
US 2005-0132221 A1	16.06.2005	US 7346925 B2	18.03.2008
US 2004-0049702 A1	11.03.2004	US 6081900 A US 6640302 B1 US 6950936 B2	27.06.2000 28.10.2003 27.09.2005