

DATA SECURITY SYSTEM AND METHOD
ADJUNCT TO A BROWSER, TELECOM OR ENCRYPTION PROGRAM

[0001] This is a continuation of patent application no. 10/155,525 filed on May 23, 2002, now pending, which is a continuation-in-part of patent application no. 10/008,209 and 10/008,218, both filed on December 6, 2001, which are a continuations-in-part of patent application no. 09/916,397 filed July 27, 2001 which is a regular patent application is based upon provisional patent application no. 60/287,813, filed on May, 2, 2001; application no. 60/267,944, filed February 12, 2001; application no. 60/260,398, filed January 9, 2001; application no. 60/247,242, filed November 13, 2000 and application no. 60/247,232, filed November 13, 2000, all of which are incorporated herein by reference thereto.

[0002] The present invention relates to a data security system and method and, more specifically, to a process, program and system which is adjunct or additive to a browser program or a telecommunications program or an encryption process. The invention filters, extracts, disperses, via a controlled release of data segments to storage locations and permits reconstruction utilizing security protocols to provide a security system, for data. Scrubbing credit card data or financial data from text, a data object or data stream is also discussed herein.

Background of the Invention

[0003] The extensive use of computers and the continued expansion of telecommunications networks, particularly the Internet, enable businesses, governments and individuals to create documents (whether text, images, data streams or a combination thereof, sometimes identified as “data objects”) and distribute those documents widely to others. Although the production, distribution and publication of documents is generally beneficial to society, there is a need to limit the distribution and publication of security sensitive words, characters or icons. Concerns regarding the privacy of certain data (for example, an individual’s social security number, credit history,

medical history, business trade secrets and financial data) is an important issue in society. In another words, individuals and businesses have a greater concern regarding maintaining the secrecy of certain information in view of the increasing ease of distribution of documents through computer networks and the Internet.

[0004] U.S. Patent No. 6,055,544 to DeRose et al. discloses the generation of chunks of a long document for an electronic book system. DeRose '544 discloses solutions available to book publishers to publish books in electronic format on the worldwide web. One of the problems is that the books are published as small document fragments rather than publishing an entire book which, due to the formatting, protocol and command structure on the Internet, downloads an entire book to the user. The problem involved with publishing small documents is that there is no relationship to other portions of the book. See col. 3, lines 51-55 and col. 4, lines 3-5. One methodology to solve the problem involves inserting hypertext links in the book. This places a large burden on the book publisher. Col. 4, lines 19-21. Accordingly, it is an object of DeRose '544 to provide a mechanism for accessing only a portion of a large, electronically published document and automatically determining what portion of the document to download to the user based upon user selections that is, previous portions and subsequent portions of the document are downloaded with the selected portion, without maintaining separate data files for each portion of the document. Col. 4, lines 34-39. In other words, if a person wanted to access chapter 4 of a text, the system in DeRose '544 would display chapter 4, chapter 3 (the preceding chapter) and chapter 5 (the subsequent chapter). This publishing of portions of the document utilizes a subset of marked up elements established as being significant and a second subset of elements being less significant. For example, "Title elements" define a table of contents. A first representation of the document structure defined by all of the marked up elements may be used in combination with a second representation of the

document structure defined only by the significant elements to control selection of portions of the documents such that previous and subsequent portions may be selected and rendered in a consistent and intuitive manner.” Col. 4, lines 38-55. A computer system stores a first representation of the hierarchy of all elements in the electronic document. As example, this may be each chapter in its entirety. The computer also stores a second representation of the hierarchy of only significant elements in the electronic document. As an example, this may be a listing of each chapter without the text associated with the chapter. In response to request for a portion of the document, the computer system selects the portion defined by the significant element in the second representation. For example, if the user requested chapter 4, the entirety of chapter 4 would be downloaded from the web server to the client computer. In addition to rendering or publishing the selected chapter, the computer system looks to the relationship of the elements in the first representation of the hierarchy (the list of all chapters) and downloads from the web server the adjacent chapters. In this example, this would involve downloading chapters 3 and chapter 5. In a further embodiment, the computer system selects only a leaf element of the second representation as a significant element during the download. See the Summary of the Invention, col. 4, line 40 through col. 6, line 14.

[0005] U.S. Patent No. 5,832,212 to Cragun et al. discloses a censoring browser method for viewing downloaded and downloading Internet documents. The abstract describes the system as including a user profile including user selected censoring parameters. Data packet contents are received from the Internet and the packets are compared with the user selected censoring parameters. Responsive to the comparison, the received data packet contents are processed and selectively displayed. The user selected censoring parameters include censored words and word fragments, and user selected categories. Compared word and word fragments can be removed and selectively replaced with predefined characters or acceptable substitute words. Tallies of weights for user

selected categories are accumulated and compared with used selected threshold values. A predefined message can be displayed responsive to an accumulated tally exceeding a user selected threshold value without displaying the received data packet contents.

[0006] U.S. Patent No. 6,094,483 to Fridrich discloses an encryption methodology hiding data and messages in images. In one application of the system in Fridrich '483, a method is disclosed of embedding a secret digital square image with 256 gray levels within an image carrier. The secret image is first encrypted using a chaotic Baker map. The resulting image is a random collection of pixels with randomly distributed gray levels without any spatial correlations. The carrier image is twice the size (height and width or $2n \times 2m$) the secret image with 256 gray levels. The carrier image is modified according to a mathematical formula.

[0007] U.S. Patent No. 5,485,474 to Rabin discloses a scheme for information dispersal and reconstruction. Information to be transmitted or stored is represented as N elements of a field or a computational structure. These N characters of information are grouped into a set of n pieces, each containing m characters. col. 1, lines 37-46. The system is used for fault tolerance storage in a partitioned or distributed memory system. Information is disbursed into n pieces so that any m pieces suffice for reconstruction. The pieces are stored in different parts of the memory storage medium. A fairly complex mathematical algorithm is utilized to provide reconstruction of the information utilizing no fewer than m pieces.

[0008] U.S. Patent No. 6,192,472 B1 to Garay et al. discloses a method and apparatus for the secure distributed storage and retrieval of information. Garay '472 identifies the problem as how to store information in view of random hardware or telecommunications failures. Col. 1, lines 17-20. The initial solution is to replicate the stored data in multiple locations. Col. 1, lines 28-31.

Another solution is to disburse the information utilizing in Information Disbursal Algorithm (IDA). The basic approach taking in IDA is to distribute the information F being stored among n active processors in such a way that the retrieval of F is possible even in the presence of up to t failed (inactive) processors. Col. 1, lines 40-44. Another issue is the utilization of cryptographic tools. With the use of tools called distributed fingerprints (hashes), the stored data is distributed using the fingerprints and coding functions to determine errors. In this way, the correct processors are able to reconstruct the fingerprint using the code's decoding function, check whether the pieces of the file F were correctly returned, and finally reconstruct F from the correct pieces using the IDA algorithm. Col. 2, lines 50-59. Garay '472 also discloses the use of Secure Storage and Retrieval of Information (SSRI) with the added requirement of confidentiality of information. Col. 3, line 56. With this added requirement, any collision of up to t processors (except ones including the rightful owner of the information) should not be able to learn anything about the information. Confidentiality of information is easily achieved by encryption. Col. 3, lines 56-61. The issue involves encryption key management, that is, the safe deposit of cryptographic keys. Garay '472 discloses confidentiality protocol utilizing distributed key management features. This mechanism allows the user to keep his or her decryption key shared among several n servers in such a way that when the user wants to decrypt a given encrypted text, the user would have to interact with a single server (the gateway) to obtain the matching plaintext while none of the servers (including the gateway) gets any information about the plaintext. Col. 4, lines 5-14.

[0009] U.S. Patent No. 5,996,011 to Humes discloses a system and a method for filtering data received over the Internet by a client computer. The system restricts access to objectionable or target data received by a client computer over an Internet by a web server by filtering objectionable data from the data received. The Humes '011 system filters the data "on the fly."

Further, the Humes '011 system can be applied to process any type of target data from the data received and displayed to the user. Col. 2, lines 32-44. If the web page requested by the user contains only a minimum amount of objectionable or target data, the user receives only a portion of the filtered web page for viewing. Hume '011 also provides that if the web page contains a large amount of objectionable material, the system blocks the entire display of the web page on the user's computer monitor. Col. 2, lines 56-62. Hume '011 provides three levels of filtering. At the first level, if the domain name contains objectionable words or material, the initial download from the domain is blocked. At the second level, the text in the download is filtered and objectionable words are replaced with a predetermined icon, for example, "----". Col. 3, lines 32-35. The filter uses a dictionary. Col. 3, lines 45-48. The filtered out words are counted. If the final score of "filtered out" material exceeds a predetermined threshold, the entire page is blocked from the user's view. Col. 4, lines 2-4.

[0010] U.S. Patent No. 5,905,980 to Masuichi, et al., discloses a document processing apparatus for processing various types of documents, a word extracting apparatus for extracting a word from a text item including plural words, a word extracting method used in the document processing apparatus, and a storage medium for storing a word extracting program. Extracted words are associated with other words via an algorithm. The extracted words and associated words are used as a search index for the document.

[0011] U.S. Patent No. 5,996,011 to Humes discloses a computer based system and method for filtering data received by a computer system, and in particular, for filtering text data from World Wide Web pages received by a computer connected to the Internet, for purposes of restricting access to objectionable web sites.

[0012] U.S. Patent No. 6,148,342 to Ho discloses a system for managing sensitive data. The system prevents a system administrator from accessing sensitive data by storing data and identifier information on different computer systems. Each query from a user's terminal is encrypted using two codes, the first code readable only by an identifier database and a second code readable only by a data access database. The data is routed from the user's source terminal to the identifier database at the first computer. The first computer/identifier database first verifies the user's ID and the security clearance for the requested information and substitutes a second internal ID to the data packet/query. The modified query is then presented to the data access database (the second computer) and, subject to a second security clearance, the response to the data query is sent back to the user's source terminal.

[0013] A publication entitled "Element-Wise XML Encryption" by H. Maruyama T. Imamura, published by IBM Research, Tokyo Research Laboratory, April 20, 2000 discloses a protocol or process wherein certain parts of an XML document are encrypted and the balance of the plaintext is not encrypted. The protocol is useful in three party transactions, for example, when a buyer sends an order in an XML document to a merchant which contains the buyer's credit card information. The credit card information is sent to a credit company and the merchant does not need to know the credit number as long as he obtains clearance or authorization from the credit card company. Another instance is an access control policy which requires a certain part of an XML document to be readable only by a privileged user (for example, a manager could access the salary field in an employee records but others could only access name, phone and office fields). The Imamura article discusses encryption protocol, the delivery of keys and the utilization of compression. The article does not discuss separate storage of the critical data apart from the plaintext of the XML document.

[0014] The Ingrain i100 Content Security Appliance product brochure, available in June, 2001, discloses a system coupled to multiple web servers (computers) to accelerate secured transactions between multiple client computers (over the Internet) and prevents Secure Sockets Layer SSL performance bottlenecks by performing high-performance SSL handshakes and encrypting all data sent to back end servers using long-lived SSL session.

[0015] An article entitled “Survivable Information Storage Systems” by J. Wylie M. Bigrigg, J. Strunk, G. Ganger, H. Kiliccote, and P. Khosla, published August, 2000 in COMPUTER, pp. 61-67, discloses a PASIS architecture which combines decentralized storage system technologies, data redundancy and encoding and dynamic self-maintenance to create survivable information storage. The Bigrigg article states that to achieve survivability, storage systems must be decentralized and must spread information among independent storage nodes. The decentralized storage systems partition information among nodes using data distribution and redundancy schemes commonly associated with disc array system such as RAID (redundancy array of independent discs) insuring scalable performance for tolerance. P. 61. Thresholding schemes - also known as secret sharing schemes or information disbursement protocols - offer an alternative to these approaches which provide both information confidentiality and availability. These schemes and codes, replicate, and divide information to multiple pieces or shares that can be stored at different storage nodes. The system can only reconstruct the information when enough shares are available. P. 62. The PASIS architecture combines decentralized storage systems, data redundancy and encoding and dynamic self-maintenance to achieve survivable information storage. The PASIS system uses threshold schemes to spread information across a decentralized collection of storage nodes. Client-side agents communicate with the collection of storage node to read and write information, hiding decentralization from the client system. P. 62. The device maintains unscrutable audit logs --that

is, they cannot be erased by client-side intruders -- security personnel can use the logs to partially identify the propagation of intruder-tainted information around the system. P. 63. The article states that, as with any distributed storage system, PASIS requires a mechanism that translates object names -- for example file names -- to storage locations. A directory service maps the names of information objects stored in a PASIS system to the names of the shares that comprised the information object. A share's name has two parts: the name of the storage node on which the share is located and the local name of the share on the storage node. A PASIS file system can embed the information needed for this translation in directory entries. P.63. To service a read request, the PASIS client (a) looks up in the directory service the names of the n shares that comprise the object; (b) sends read requests to at least m of the n storage nodes; (c) collects the responses and continues to collect the responses until the client has collected m distinct shares; and (d) performs the appropriate threshold operation on the received shares to reconstruct the original information. P. 63. The p - m - n general threshold scheme breaks information into n shares so that (a) every shareholder has one of the n shares; (b) any m of the shareholders can reconstruct the information; and (c) a group of fewer than p shareholders gains no information. P. 64. Secret-sharing schemes are m - m - n threshold schemes that trade off information confidentiality and information availability: the higher the confidentiality guaranty, the more shares are required to reconstruct the original information object. Secret sharing schemes can be thought of as a combination of splitting and replication techniques. P. 64. The article discusses the technique of decimation which divides information objects into n pieces and stores each piece separately. Decimation decreases information availability because all shares must be available. It offers no information theoretic confidentiality because each share expresses $1/n$ of the original information. P. 64. Short secret sharing encrypts the original information with a random key, stores the encryption key using secret

sharing, and stores the encrypted information using information dispersal. P. 64. An extension to the threshold schemes is cheater detection. In a threshold scheme that provides cheater detection, shares are constructed in such a fashion that a client reconstructing the original information object can tell, with high probability, whether any shares have been modified. This technique allows strong information integrity guarantees. Cheater detection can also be implemented using cryptographic techniques such as adding digest to information before storing it. P. 65. For the highest architecture to be effective as possible, it must make the full flexibility of threshold schemes available to clients. The article believes this option requires automated selection of appropriate threshold schemes on a per object basis. This selection would combine object characteristics and observations about the current system environment. For example, a client would use short secret sharing protocol to store an object larger than a particular size and conventional secret sharing protocol to store smaller objects. The size that determines which threshold scheme to use could be a function of object type, current system performance, or both. P. 67.

[0016] The MAIL sweeper and MIME sweeper programs by ReSoft International uses a keyword search engine to review e-mails for certain words or phrases. IF the e-mail does not clear the filter, the addressee data must clear a data base check to protect the privacy and/or confidentiality of the e-mail data. See re-soft.com/product/mimesweep. The Aladdin eSafe Appliance restricts outgoing e-mails from sending classifier or prohibited content. See aks.com/news/2001/esafe.

Objects of the Invention

[0017] It is an object of the present invention to provide a data security system, an information processing system and a method for securely storing data and rebuilding that data in the presence of an adequate security clearance.

[0018] It is another object of the present invention to provide a method for securing data on a single personal computer (PC), on a plurality of computers linked together through a local area network (LAN) or a wide area network (WAN) or the Internet.

[0019] It is a further object of the present invention to provide a method for securing data utilizing a client-server computer system. The client-server computer system may be implemented over the Internet. The security system may be provided to the public, to government or to private entities as an Application Service Provider or ASP over the Internet.

[0020] It is a further object of the present invention to provide a method for securing data which is highly flexible and programmable by a user.

[0021] It is an additional object of the present invention to enable the user to establish (a) the scope of the security sensitive words, characters or icon, data objects, (b) the future use (or destruction or encryption) of a filter enabling extraction of security sensitive data, (c) the selection of storage locations (local, removable, in an LAN, a WAN or on the Internet) for extracted data and remainder or common data and (d) one or multiple levels of security limiting full reconstruction and enabling partial reconstruction of the extracted data and the remainder or common data.

[0022] It is another object of the present invention to establish and manage the separation of user-based communities of interest based upon crypto-graphically separated, need to know security levels.

[0023] It is another object to provide an adaptive system responsive to hacking attempts and hacking attacks.

[0024] These steps may be completely automated (after some parameters are set or programmed by a system administrator), may be fully programmable by the user, or may be a

combination of automated and manual controls implemented by the systems administrator and/or the user-client.

[0025] It is an object of the present invention to parse, disperse and reconstruct the data or data object thereby enabling secure storage of the data. For example, financial data maintained by an institute, can be parsed with an algorithm, the parsed segments dispersed off-site and away from the financial institute, and, upon appropriate security clearance, the dispersed data can be reconstructed to duplicate the data. Large distribution of parsed data is contemplated by this aspect of the invention. The original data remains stable, operable and immediately useful. The securing dispersed data is a back-up of the original data.

[0026] It is a further object of the present invention to secure e-mail data transmissions and web browser transmissions by extraction of security sensitive data, facilitating the remote storage of said data and sending remainder data to the e-mail addressee or the recipient.

[0027] It is another object of the present invention to use fine-grained selection of security critical data, extraction and encryption and separate storage of the secured data. The parsing or filtering of plaintext, data object, file or data stream thereby bridges the gap between full encryption of the plaintext etc. and no encryption. The present system is therefore a more efficient use of processing speeds, times, and storage resources.

[0028] It is a further object to create a credit card number or financial data scrubber. The scrubber may be employed to remove any security critical data.

[0029] It is another object of the present invention to permit the user to decide on and select a level of risk he or she believes appropriate by selecting no, minimal, intermediate or maximum levels of data security.

[0030] It is another object of the present invention to permit the user to access data security risks, access data processing resources (processing time, storage facilities, data access time, etc.) and select a security level which balances risks and resources.

Summary of the Invention

[0031] Data security for a telecommunications or browser-input data operates on security sensitive content which are extracted, then either encrypted or stored in remote extract stores, and processed separate from remainder data. Extracted data, in one system, is remotely stored. Other methods attach an encrypted version of the extract to the document. The browser system operates with an extract store. Remainder data is sent to the addressee or designated web server. The addressee is permitted to retrieve the extracted data from said extract store only in the presence of a security clearance and hence, reconstruct the source input data with the extract data. In other systems, the addressee reconstructs the input by decryption and integration. The browser method extracts data, facilitates the storage in an extract store, forwards the remainder data to a target. The financial data or credit card scrubber may use a pop-up window to alert the user to enable the system.

[0032] Another method for securing data in a computer system in one embodiment includes establishing a group of security sensitive content (** words, characters, icons, data streams or data objects, filtering the data input from a data input device and extracting the security sensitive data. The extracted data is separated from the remainder data and is separately stored. In one embodiment on a personal computer (PC) system, the extracted data and the remainder or common data is stored in different, distributed memory segments. In a network implementation, the extracted data may be stored in one computer and the remainder or common data may be stored in another computer. In

a client-server implementation, the server may direct storage of the extracted data to a different location than the remainder data, either on the server or on a further memory system (computer) interconnected to the server or on the client computer and in distributed memory segments. A map may be generated by a software module or sub-system indicating the location of the extracted data and the remainder data in the network. The filter may be destroyed (via a deletion routine) or may be retained for future use by the user. If retained, encryption is preferred. The map may be stored on the client computer or the user's PC or may be stored on the server. Copies of the map may be removed (deleted) from the user's PC or the client computer. The map may be encrypted. The extracted data and/or the remainder data may be removed (deleted or scrubbed) from the originating computer. Encryption can be utilized to further enhance the security levels of the system. All transfers of the filter between the client to the server may be encrypted, and all data (whether extracted data or remainder data) may be encrypted prior to storage in the distributed memory. Any transfer of extracted data or remainder data or maps or filters may include an encryption feature. Reconstruction of the data is permitted only in the presence of a predetermined security clearance. A plurality of security clearances might be required which would enable a corresponding plurality of reconstructing users to view all or portions of the data. Persons with low level security clearance would only be permitted to have access to low level extracted data (low level security sensitive data) and the common data. Persons with high level security clearances would be permitted access to the entire document reconstituted from the extracted data and the remainder data. A computer readable medium containing programming instructions carrying out the methodology for securing data is also described herein. An information processing system for securing data is also described.

[0033] In another embodiment, the method for securing data in a computer network and transparently establishing and managing the separation of user-based communities of interest based

upon crypto-graphically separated, need to know, security levels, by necessity, utilizes communities of interest representing a plurality of users having corresponding similar security levels, each with a respective security clearance. In other words, all members of Community A have the same security level and security clearance, which is different than the users of Community B which have a different security level and security clearance. The method and the computer media containing programming instructions includes filtering data from the data input computer, extracting security sensitive words, phrases, characters, icons, or data objects and forming subsets of extracted data and remainder data. The subsets of extracted data are stored in one or more computer memories in the network identified as extracted stores. The remainder data is also stored in the network if necessary. Reconstruction of some or all of the data via one or more of the subsets of extracted data and the remainder data is permitted only in the presence of a predetermined security clearance from the plurality of security levels. The cryptographically separated, need to know, security levels correspond to respective ones of the plurality of security levels and the method includes, in one embodiment, encrypting subsets of extracted data with corresponding degrees of encryption associated with the plurality of security levels. During reconstruction, all or a portion of the plaintext data is decrypted only in the presence of the respective security level. The information processing system which secures data per the community of interest security level in the includes a data filter for the data input from the data input computer which extracts the security sensitive words, phrases, icons or data objects. A system and a methodology for storing the subsets of extracted data and remainder data is provided and a compiler permits reconstruction of some or all of the plain text data in the presence of an appropriate security clearance level. Multiple level encryption in one document is also available.

[0034] An adaptive method of securing data responsive to a plurality of hacking events utilizes a hacking monitor which generates a corresponding plurality of hack warnings dependent upon the severity of the hacking attack. Based upon respective ones of the hacking or hack warnings, data is filtered to extract security sensitive words, phrases etc. and the extracted data and the remainder data (if necessary) is stored based on the degree of hack warning. Reconstruction is permitted of some or all the data utilizing the extracted data and the remainder data only in the presence of the predetermined security clearance level. Automatic reconstruction is permitted after the hack attack terminates. The method sometimes includes encrypting extracted data dependent upon the degree or severity of the hack warning and decrypting that data during reconstruction. A computer readable medium containing programming instructions similar to the method is also provided. The information processing system includes a filter which is adjusted based upon the degree of hack warning to extract security sensitive words. A storage system stores extracted data and remainder data (if necessary) based upon the level of the hack warning and a compiler is used to reconstruct the data in the presence of the appropriate security clearance level.

[0035] The parsing and dispersion aspects of the present invention enable the user to parse, disperse and reconstruct the data or data object thereby enabling secure storage of the data. The original data may be maintained in its original state and stored as is customary, encrypted or destroyed. For example, financial data maintained by an institute in its original state, and a copy thereof can be parsed with an algorithm, the parsed segments dispersed off-site, (that is, separated and stored in extract and remainder stores or computer memories), away from the financial institute, and, upon appropriate security clearance, the dispersed data can be reconstructed to duplicate the data. Large distribution of parsed data is contemplated by this aspect of the invention. The original data remains stable, operable and immediately useful in its stored location. The secured and

dispersed data is a back-up of the original data. Destruction of the original source is also an alternative embodiment.

[0036] Another embodiment of the present invention operates in an e-mail or a web browser environment. In a specific embodiment, the invention operates as a credit card or financial data scrubber. The e-mail data has one or more security sensitive words, characters or icons and the method or computer program works in a distributed computer system with a remote memory designated as an extract store. The method extracts the security sensitive words, characters or icons from said e-mail data to obtain extracted data and remainder data therefrom. The extracted data is stored in the extract store. The methodology emails the remainder data to the addressee. the addresses is permitted to retrieve the extracted data from said extract store only in the presence of a predetermined security clearance and hence, reconstruct the e-mail data with said extracted data and remainder data. The program and method on the user's e-mail device extracts the security sensitive data, facilitates storage of the extracted data in said extract store and, emails the remainder data to the addressee. Rather than extracting security data, the method and program may parse the data. The method and program for safeguarding data entered via a browser involves extracting security sensitive data, facilitating the storage of such data in the remote store, and forwarding the remainder data to a targeted destination in the distributed computer system. The scrubber may utilize a pop-up window to enable user activation of the scrubber on an email or a web browser communication.

[0037] The present invention can be configured in various forms. The following descriptions discuss various aspects of the invention and further advantages thereof.

[0038] The present invention enables automatic classification and declassification of documents on the fly. The extraction process downgrades and declassifies documents on the fly (in real time) so that they are useless to unauthorized parties. Presentation by a user of a valid security clearance enables substantially instant and seamless reconstitution of the security sensitive content.

[0039] The present invention automatically secures unstructured documents and freeform documents for example, e-mail, instant messaging, or Word documents (input documents).

[0040] The present invention automatically secures structured documents and transactional documents for example, database records or XML documents (input documents).

[0041] The present invention introduces flexibility into security management, risk management of data, data storage, and data flows and enable automatic responsiveness to threats. The innovation enables automatic response to security challenges and threats. The innovation can maintain, upgrade and downgrade the levels of security through implementation of a leveled granular extraction process and a controlled-release mechanism. Attacks or other external events can trigger a response in the form of higher extraction levels, expanding the type of content extracted, and constricting the release of important and critical data control from storage. How much and what to extract depends on the level of threat or perceived risk. In same manner, the amount and type of content released from storage and reconstituted depends on the level of threat or risk perceived by the system. The system delivers a level of security protection specifically matched to meet security needs as dictated by the changing security threats, environment, policy and organizational needs.

[0042] The present invention introduces multiple levels and standards of security. It is common knowledge that the highest security is delivered through total separation. Whereas this concept has only been implemented physically or by isolating computer environments, the invention

achieves this concept of total separation within open and networked computer environments. The invention can implement a total physical and logical separation of important and critical data from its context and can preclude access to that information without a needed granular access permission. The invention is also effective for sounds and images (data objects or data streams with security words, characters, terms, icons or other data objects).

[0043] The present invention introduces a new method and apparatus to monitor security sensitive content through a process of analysis and categorization of each word or character, in a document. The invention enables processing of every character, word, number, as they are entered into a document and categorizes each into one of many pre- set categories. Categories can include surnames, locations, currency, defined terminology, and unknown words or phrases.

[0044] The present invention introduces a method and apparatus for plain text extraction and dispersion of security sensitive data. Maximum security with traditional methods encumbers free flow of information and business efficiency. Encryption burdens computer systems with high performance overhead, and its use is limited to the parties who have decryption capabilities. The invention offers a new solution. It enables leveled security in plain-text format, in addition to none, some, or all of pre-existing encryption, decryption, firewalls, and other security infrastructure. The level of security is determined by the extent of the security sensitive items, selection process; the extent of dispersal to various distributed storage locations; the rules for controlled-release from storage; and the access rules governing the reconstitution of extracts into the secured document.

[0045] The extractions are dispersed to distributed storage on a granular level. The rest of the document can be stored at its original location and/or other storage locations. Dispersal of extractions introduces new barriers not existing in current security. In certain situations, an attacker

has first to find the (encrypted) map to the locations, then locate and access the distributed storage, get the data released from the controlled-release storage, and finally reintegrate the extracts into the appropriate documents.

[0046] The present invention introduces a method and apparatus for targeted extraction and encryption of security sensitive items. The extraction capabilities of the system enable different workflow modes. The system enables extraction and encryption of important and critical content. In essence, only the critical content is extracted and/or encrypted, whereas the rest of the document remains as plaintext. This capability enables the following: advantages and flexibility; and the ability to share the document within the organization or transmit it to outsiders while still maintaining security over the most important and critical content of the document. This is an automatic process for controlling the content of outgoing e-mail. The document owner releases the important and critical content by enabling access to it to defined parties at defined times within defined threat modes.

[0047] The present invention introduces a method and apparatus for encrypting document or extractions with multiple encryption types. The invention can deliver the highest level of security by using multiple types of encryption (and/or multiple keys) for one line, paragraph or document or different keys one line, paragraph or document. Maximum security is delivered through automatic selection of security sensitive items, and encrypting these extractions with one or more types of encryption. The remainder data can also be encrypted. Multiple encryption types (or keys) within one document statistically precludes deciphering that document regardless of the available computer power. Common encryption methods are vulnerable through existing technologies, social engineering methods, carelessness, and workflow habits. Furthermore, simple encryption becomes more vulnerable (including triple DES) assuming future mathematical breakthroughs or quantum

computing. Existing methods to crack block ciphers are being improved to compromise the future AES Rijndael standard.

[0048] The present invention to introduce a method and apparatus for content dispersion. The innovation enables control over specific important and critical content items within the general contents of documents or digital files in a computer or within a network. The immediate controlled-release of those important content items according to specific identification and access criteria proactively safeguards the security and the value of documents or digital files. The content control enables broad dissemination of the digital files in closed networks, as well as open networks including the Internet, without compromising the security of the important and critical information in the digital file. The dispersal channels can include any of all of the following: networks, Internet, Virtual Private Channel. Telephone lines, Optical lines, Wireless, Fax, Documents, Verbal communication.

[0049] The present invention introduces a method and apparatus for enhancing the survivability capabilities of an organization and its networks. If networks get damaged, the decryption capability, such as PKI, is likely to be compromised, or at a minimum, suspended. In such instances, the invention enables continuation of work on channels, which need not be secure. In addition, the dispersion of information guarantees maximum partial reconstitution to documents and transactions, or total reconstitution to documents and transactions benefiting from backup at distributed storage facilities.

[0050] The present invention introduces a method and apparatus for delivering security for inter-connecting networks. It enables security for closed networks connecting to the Internet and other open networks. The Internet infrastructure and open networks are not secure. Even secured

closed networks, such as VPNs, are not secured enough. The critical content of documents is the critical asset of the organization and must be highly secured, with maximum reliability, full transparency and instant accessibility. To remain competitive, organizations must maximize utility of the critical data within their documents, files, databases and servers. The securing of such documents must not be at the expense of compromising the access or processing speed of such documents. The invention enables work in plain text, as well as with encryption. Working in plain text reduces the computing performance overload.

[0051] The present invention introduces a method and apparatus for delivering information flow control in decentralized environments. Protection of privacy and confidentiality of information represents a long-standing challenge, The challenge has become much bigger with the expansion of the Internet, which has created decentralized networks. Parties, who do not know or trust each other, have to exchange information. The invention enables free flow and sharing of information between parties by removing burdening security restrictions and creating top security with a controlled-release of the security sensitive content in the documents. The technology enables top security through introduction of user and organization's ownership and control of the critical granular data in documents.

[0052] The system introduces an additional layer of access controls at the granular level of the user document. In order to view the reconstructed critical information the user would need to be verified by additional access controls at the data storage level. The user access code or a physical key enables release of data from the storage. Today's access controls do not stop the user from distributing documents to other parties. The inventions fined grained controlled-release mechanism releases the critical information, only under a required set of circumstances and access validation. The invention enables the user ownership of his security sensitive critical data and conditions for

its release and dissemination. The user has the option to hide the critical data through declassification process and release through a reclassification process in which the critical data would be reconstituted in the document.

[0053] The present invention introduces a method and apparatus for delivering Compartmentalization of security sensitive content by leveled access to users. The invention creates leveled sharing of information, for example such that persons with level 3 access will have keys for encryption type RSA persons with level access 2 will have access to Blowfish encryption within one document.

[0054] The present invention introduces a method and apparatus for enabling more use of distributed and dispersed storage including ASPs (application service providers). There is a major human tendency to refrain from sending important documents to web storage locations because of potential security breaches. This cultural issue is both driven by psychological issues and well-founded security concerns. The retention of those documents as is in physical proximity or locked security, provides actual security but precludes gaining any utility from those documents in a functional business setting. Instead the invention enables functional distribution of those documents without the security sensitive data, and a controlled-release of some or all of the extractions in a granular way in order to support business activities while retaining security.

[0055] The present invention introduces a method and apparatus for enabling lower storage costs. The extraction process declassifies and downgrades mission critical documents. The downgrading and transformation of a critical document into a non-critical document, enables storage in less secured and lower cost storage. Taking advantage of this security-initiated, extraction process can yield substantial storage cost savings. The invention enables a high return on investment ROI

for system storage cost arbitrage. Splitting the data into critical and non-critical enables 20 to 90% savings on storage cost.

[0056] The present invention delivers an automated security risk management system that creates added in-depth security defenses at the semantic-level as well as creation of controlled-release mechanisms at the storage-level with significantly reduced performance overhead requirements.

[0057] The present invention presents a technology which answers the security demands as required by Committee on Information Systems Trustworthiness of the National Research Council. The Committee's report, Trust in Cyberspace (1999), defines the security paradigms needed for a safe future. The report states: The substantial commercial off-the-shelf (COTS) makeup of a network information systems, the use of extensible components, the expectation of growth by accretion, and the likely absence of centralized control, trust, or authority demand a new approach to security: risk mitigation rather than risk avoidance; technologies to hinder attacks, rather than prevent them outright; add-on technologies and defense in depth; relocation of vulnerabilities rather than their elimination; none of the existing or security technologies addresses these needs in whole. The invention breakthroughs this barrier by providing a single system which implements each one of those four elements in a unified way. The invention controls information flow in centralized and decentralized environments, through controlled-release of information within distributed systems.

[0058] The present invention implements security measures while accommodating the performance needs of a network. The invention provides a method and apparatus to ease overhead performance on congested computer networks. It can adjust the security defenses based on the performance needs of the network. Many security systems overburden the already burdened

computing environment in terms of computational overhead, labor, and training requirements. The invention enables to ease the overhead performance of a network by transforming from high overhead performance, encryption methods, and other security methods, to the method presented by this invention.

[0059] The present invention minimizes the time of exposure of the important content within a document. The invention enables to separate the important content from the rest of the document for substantial periods of time, thereby minimizing substantially the exposure to risk. It is possible for example to extract the important content from the document and release it for reconstitution only when the user will open the document. In such situations the important content could for example be time and unexposed for over 99% of the time and exposed for less than 1% of the time, which lowers the risk substantially.

[0060] The present invention provides a security risk management method and system to minimize security risks. The invention enables minimization of security risks by: Automatic separation and extraction of granular critical data from the core document. Dispersal of the extracted critical data groups to different secured storage locations. Reconstitution of the critical data in document for limited time, to minimize exposure to risk. Partial reconstitution, of the critical data, in core document, through a controlled release of granular critical data. Granular controlled release of data to specific authorized people only.

[0061] The present invention provides a controlled release security mechanism to enable the release of content and granular content from storage locations in a centralized and decentralized environment. The controlled release mechanism enables release of the appropriate content to the authorized party at the right time under the right circumstances.

[0062] The present invention provides a security solution against damage by insiders. Studies show that insiders cause 70%-85% of the damage. These nine innovations are described in detail as follows: The invention enables insiders and employees to work with documents while managers and owners control the release of the critical prioritized information. The control is granular, thereby enabling continued work with the rest of the content in the document. The objective is to empower the user with the highest security while enabling him maximum sharing and delivery flexibility. This enables free flow of information between closed networks and public networks, such as the Internet, without compromising the security through extraction of important and critical content. The user can transport documents through various networks and e-mail services knowing that the critical information, which is still under control, and is not compromised.

[0063] The present invention provides an automatic security system in order to overcome human flaws that create security vulnerabilities. Human engineering flaws are the cause of 90% of security vulnerabilities. For example, passwords are exposed through human fault enabling reading of plain text before it is encrypted. The invention enables an automatic process of appropriate response to security threats in an objective way and on an on going basis.

[0064] The present invention provides an automatic security system in order to reduce human labor, and training costs.

[0065] The present invention provides protection for important granular content within a document. A feature left out in computer development is the protection and automatic protection of granular important content in a document. In every facet of life critical assets are immediately protected. For example, credit cards and cash are protected in a wallet, important items at home are

placed in closets, wall units, cabinets and safes. The present system extracts the digital equivalent of these items, e.g., extracts all credit card data, and stores the extracted data in secure location(s).

[0066] The present invention provides an alternative method to encryption. Mathematical security and encryption could be broken. Discovery of a mathematical equation for a shortcut of the factoring of prime numbers would make mathematical security and encryption extremely vulnerable.

[0067] In 1999 a 512-bit RSA key was broken- at that time 95% of keys in e-commerce were 512 bits long. U.S. government 56-bit Data Encryption Standard was cracked in just 22 hours by the Freedom Foundation. 100, 000 PCs were connected with a supercomputer which enabled the testing of 245 billion keys per second.

[0068] The invention provides an automated security risk management system. The system automatically responds to attacks by matching the defenses level to the level of threats. The system responds to security threats through the following mechanisms: (1) controlled extraction of sensitive security data: in normal circumstances, extractions will take place according to pre-set rules; in threat situations, additional extractions will take place to deliver higher security; in an attack, additional substantial amounts of critical data will be extracted to deliver the highest security; (2) controlled dispersal to storage locations; in normal circumstances, dispersal to different storage locations according to pre-set rules will take place; in threat and attack situations, more dispersal to more storage locations, via additional communication channels will take place; and (3) controlled release of extracts for reconstitution; controlling amount of extracts released for reconstitution; controlling time of exposure of extracts in reconstitution; limiting access to specific people; and limiting access to specific times.

[0069] The present invention defends against devices like keyboard sniffers and mouse sniffers that can read information keyed into the computer and transmit it to an adversary. The invention enables to input security sensitive items through data input devices other than the keyboard. For example credit card numbers can be inputted through a hand held wireless devise. The inputted data would be transferred to storage for possible reconstitution.

[0070] The present invention defends against as devices that intercept electromagnetic signals from computers, monitors, printers, and keyboards. For example the Van Eck receptors which can read information off the screen the display screen. The invention enables separation contents of document into two or more displays thereby limiting the potential damage of electromagnetic eavesdropping.

[0071] The present invention enables the controlled release of data objects, full or partial release of plaintext source documents to persons or organizations with the appropriate security clearances.

[0072] Another object of the present invention is to enable the control of information flow over a PC, a network, a LAN, a WAN and over the Internet.

[0073] A further object of the present invention is to enable the interoperability of several secured networks based upon the relative security clearances of each network.

[0074] It is another object of the present invention to provide a process for synthesizing a document.

Brief Description of the Drawings

[0075] Further objects and advantages of the present invention can be found in the detailed description of the preferred embodiments when taken in conjunction with the accompanying drawings in which:

[0076] FIG. 1A diagrammatically illustrates a basic system diagram showing filtering and storing extracted data and remainder or common data and, in an enhanced embodiment, generating and storing a map.

[0077] FIG. 1B diagrammatically illustrates a system diagram showing reconstruction of the data, various security clearances and both electronic reconstruction and visual reconstruction.

[0078] FIG. 2 diagrammatically illustrates a system showing major components of a single personal computer (PC) system, a networked system with several PCs (a LAN or WAN) and the network coupled to a telecommunications system and the Internet and shows the interconnection with a server and multiple, Internet-connected memory units.

[0079] FIG. 3 diagrammatically illustrates a basic flowchart showing reconstruction for various security levels.

[0080] FIG. 3A diagrammatically illustrates interleaving distinct data into different memory locations in a video memory.

[0081] FIG. 4 diagrammatically illustrates a flowchart showing one embodiment of the principal portions of the data security program.

[0082] FIG. 5 diagrammatically illustrates a flowchart showing the basic elements of the reconstruction process for the data security program.

[0083] FIG. 6 is a computer network diagram showing various user communities.

[0084] FIG. 7 diagrammatically illustrates a flowchart showing the key component steps for the multiple layer security program for the community of users.

[0085] FIG. 8 diagrammatically illustrates a flowchart showing the key components of an adaptive security program adaptable to various levels of electronic attacks, hacker or hack attacks.

[0086] FIG. 9 diagrammatically illustrates a flowchart showing the key components of a multiple encryption program using multiple types of encryption in one document or data object.

[0087] FIG. 10 diagrammatically illustrates a chart showing the key components of the parsing, dispersion, multiple storage and reconstruction (under security clearance) of data.

[0088] FIGS. 11A and 11B diagrammatically illustrate a flowchart showing the key components of one embodiment of the e-mail security system (jump points 11-A and 11-B link the flow charts).

[0089] FIGS. 12A and 12B diagrammatically illustrate a flowchart showing the key components of one embodiment of the invention implements the security system on a web browser (jump point 12-A links the flow charts).

[0090] FIG. 13 diagrammatically shows several revenue systems which may be employed with the data security systems described herein.

Detailed Description of the Preferred Embodiments

[0091] The present invention relates to a data security system, a methodology of securing data on a personal computer (PC) system, on a computer network (LAN or WAN) and over the Internet and computer programs and computer modules and an information processing system to accomplish this security system.

[0092] It is important to know that the embodiments illustrated herein and described herein below are only examples of the many advantageous uses of the innovative teachings set forth herein. In general, statements made in the specification of the present application do not necessarily limit any of the various claimed inventions. Moreover, some statements may apply to some inventive features but not to others. In general, unless otherwise indicated, singular elements may be in the plural and vice versa with no loss of generality. In the drawings, like numerals refer to like parts or features throughout the several views.

[0093] The present invention could be produced in hardware or software, or in a combination of hardware and software, and these implementations would be known to one of ordinary skill in the art. The system, or method, according to the inventive principles as disclosed in connection with the preferred embodiment, may be produced in a single computer system having separate elements or means for performing the individual functions or steps described or claimed or one or more elements or means combining the performance of any of the functions or steps disclosed or claimed, or may be arranged in a distributed computer system, interconnected by any suitable means as would be known by one of ordinary skill in the art.

[0094] According to the inventive principles as disclosed in connection with the preferred embodiment, the invention and the inventive principles are not limited to any particular kind of computer system but may be used with any general purpose computer, as would be known to one of ordinary skill in the art, arranged to perform the functions described and the method steps described. The operations of such a computer, as described above, may be according to a computer program contained on a medium for use in the operation or control of the computer as would be known to one of ordinary skill in the art. The computer medium which may be used to hold or

contain the computer program product, may be a fixture of the computer such as an embedded memory or may be on a transportable medium such as a disk, as would be known to one of ordinary skill in the art.

[0095] The invention is not limited to any particular computer program or logic or language, or instruction but may be practiced with any such suitable program, logic or language, or instructions as would be known to one of ordinary skill in the art. Without limiting the principles of the disclosed invention any such computing system can include, inter alia, at least a computer readable medium allowing a computer to read data, instructions, messages or message packets, and other computer readable information from the computer readable medium. The computer readable medium may include non-volatile memory, such as ROM, flash memory, floppy disk, disk drive memory, CD-ROM, and other permanent storage. Additionally, a computer readable medium may include, for example, volatile storage such as RAM, buffers, cache memory, and network circuits.

[0096] Furthermore, the computer readable medium may include computer readable information in a transitory state medium such as a network link and/or a network interface, including a wired network or a wireless network, that allow a computer to read such computer readable information.

[0097] In the drawings, and sometimes in the specification, reference is made to certain abbreviations. The following Abbreviations Table provides a correspondence between the abbreviations and the item or feature.

Abbreviations Table

A-com	computer or memory store for common or remainder data
ASP	application service provider - server on a network

B-ext	computer or memory store for extracted data
bd	board
CD-RW	compact disk drive with read/write feature for CD disk
comm.	communications, typically telecommunications
CPU	central processing unit
doc	document
dr	drive, e.g., computer hard drive
DS	data storage
e	encryption
ext-data	extracted data
I/O	input/output
I-com	Internet storage for common or remainder data
I-ext	Internet storage for extracted data
loc	location
mem	memory
obj	object, for example, a data object
pgm	program
re	regarding or relating to
recon	reconstruct
rel	release
req	request
rev	review
sec	security

sys	system
t	time
tele-com	telecommunications system or network
URL	Uniform Resource Locator, x pointer, or other network locator

[0098] FIG. 1A diagrammatically illustrates the basic processes for establishing a secure storage of information, generally identified herein as “data.” “Data,” as used herein, includes any data object, e.g., text, images, icons, moving images, multiple images, data representing sound, video etc. Sound bites and video images may also be extracted data. A source document 100, sometimes referred to as a “plaintext,” is passed through a filter 102. Although it is convenient to discuss and understand the invention herein in connection with a plaintext document, the document 100 is a data object. It is not limited to an electronic document representing words. The document 100 represents a data object that may be e.g., text, images, icons, moving images, multiple images, data representing sound, video etc. The term “data object” as used in the claims is broadly defined as any items that can be represented in an electronic format such that the electronic format can be manipulated by a computer as described herein. The data object, or as discussed herein, the “plaintext” is sent to a filter. Filter 102, in a most basic sense, separates out common text or remainder data 104 from uncommon text, words, characters, icons or data objects. The security sensitive content, represented by one or more security sensitive words, characters, images, data elements or data objects, are separated from remainder or common text 104 as extracted text 106. It should be noted that although the word “text” is utilized with respect to remainder text 104 and extracted text 106, the text is a data object and includes words, phrases, paragraphs, single characters, portions of words, characters, whole or partial images, icons or data objects. In a basic implementation, filter 102 may utilize a dictionary such that words present in the dictionary

(common words) are separated from the source plaintext document 100 and placed into remainder document or common data file 104. The uncommon words (extracted-security sensitive words), not found in the dictionary, would be placed in an extracted text or extracted data file 106. For example, a business may wish to impose a security system on a contract document such that the names of the contracting parties (not found in the dictionary) and the street names (not found in the dictionary) would be stored in extracted data text file 106. The common text or remainder data would be stored in remainder data file 104. In the illustrated embodiment, remainder data file 104 also includes place holders which enables the extracted data to be easily inserted or set back into the remainder data file.

[0099] The security sensitive words, characters, icons or data objects may be any word, phrase, letter, character, icon, data object (full or partial), image or whatever, as pre-defined or as established by the user. The user may specifically design the filter, begin with a dictionary to define common terms, identify any additional security sensitive words, letters, images, icon, data objects, partial versions of the foregoing or any other granular aspect of the plaintext. After defining the filter and accepting the data input, the system filters the plaintext and separates extracted data (security sensitive items) from the remainder data. The filter may also include elements of artificial intelligence (AI). For example, the user may select one word as a security word and the AI filter may automatically select all synonymous words. The AI filter may enable the user to define a filter is real time at the entry of data via a keyboard. For example, the user may select to secure (i.e., extract and store) some proper names and may instruct the filter to secure names such as Block, Smythe and Cherry. During input of the plaintext, the system may detect Smith and ask the user if he or she wants to secure (a) all proper names in a common name dictionary collection and/or (b) all names with spellings similar to the filter input data, Block, Smythe and Cherry. As is known

in the art, AI typically uses inference engines to define one pathway or to outline a course of action. The filter or extraction engine discussed herein can be configured with AI, inference engines, neural network systems or other automatic systems to carry out the functionality described herein for the dynamic operation of the security system.

[0100] The system and methodology described herein also encompasses parsing the plain text document by bit count, word, word count, page count, line count, paragraph count and parsing based upon any identifiable document characteristic, capital letters, italics, underline, etc. Algorithms may be implemented to parse the plain text document. The target of the parsing algorithm (a bit count, word, letter, etc.) is equivalent to the “security word, character or icon, data object” discussed herein. The parsing occurs with the filtering of the plain text source document 100 and the subsequent storage of extracted data apart from remainder data.

[0101] In a basic configuration, the common text or the remainder data is stored in common storage memory 108. This common or remainder data store is identified as A-com generally referring to a segmented memory in a PC or a computer A in a network (LAN or WAN). Remainder data storage 108 may include a confirm storage signal function 111 to send back a confirm storage signal to the data input device generating source plaintext document 100. The extracted data file 106 is stored in a different memory computer storage 110 (B-ext). In a preferred embodiment, memory segment 108 (A-com) is at a different location than computer storage memory segment 110 (B-ext). In a PC embodiment, memory A-com is a different memory segment than memory B-ext. In a networked embodiment, computer storage 108 may be on a different computer as compared with computer storage 110. In an Internet embodiment, common text or cleansed text storage is at one web site (which may be one computer) and the extracted, high security data is stored at another web site, buried web page or other Internet-accessible memory store location. In any event, the

remainder text is stored in a memory A-com and the extracted data or high security words, characters , icons or data objects are stored in memory B-ext. After storage of the extracted data in memory 110, a confirmation indicator 113 may be generated to the client computer or the computer handling source plaintext input document 100 (the originating computer system).

[0102] As a simple example, the program configured in accordance with the present invention, could automatically detect entry of all credit card numbers types into a user's computer. The filter is set to detect the unique credit card sequence and data string. Assuming that the user's computer is operating a browser and the user is communicating with a server on the Internet, the user's computer would filter out the credit card number and send the number to a secure storage site. The secure storage site is owned, operated or leased by a trusted party. The extracted data, i.e., the credit card data, is stored at the trusted site. The URL or other identifying data is sent to the vendor from which the user wants to purchase goods and services over the Internet. When the vendor seeks to complete the transaction, the vendor sends a request code to the secure site, the trusted party at the secure extracted data storage site debits the user's credit card account (or otherwise debits the user's bank account) and sends an approval code to the vendor. In this manner, the vendor is never given the user's credit card – the card number is sent to a trusted party automatically by the filter in the security program described herein. The security program may be incorporated in a browser to automatically protect credit card data, personal data (as a method to become anonymous on the Internet), etc. from being deliberately broadcast to others on the Internet or to block others from snooping into the user's personal data while the user communicates over the Internet.

[0103] In a further enhancement of the present invention, the computer or data input device handling source plaintext document 100 may also record the location of A-com 108 and B-ext 110. The location data is called herein a “map.” A memory mapping function is utilized. The map may

be stored in a third memory location 112. Memory location map 112 may be a segment of the memory of the data input computer originating plaintext 100. The map may be encrypted for security reasons.

[0104] As a further enhancement of the present invention, the user, prior to initiating the security system, may be given a choice of filtering out all the uncommon words or words not found in the dictionary and adding certain security sensitive words, characters, icons or data objects to filter 102. The added words or terms are filtered out with the uncommon words. Of course, the user may be required to manually input all security words or download the security word filter from the Internet or another system on the LAN. For security systems having multiple security levels, a plurality of filters would be created, each filter associated with a different security level. Further, multiple security levels would require, in addition to remainder text document or data 104, a plurality of extracted data documents 106. The common or remainder text document or data 104 would still be stored in remainder computer storage A-com 108. However, each extracted data document 106 would be stored in a respective, separate computer memory segment or computer B-ext 110. Separate storage of a plurality of extracted data at multiple, separate locations in B-ext is one of the many important features of the present invention.

[0105] In view of increasing levels of security relating to (a) the storage location A-com; (b) the transfer of remainder text document 104 to memory computer storage A-com 108; (c) the storage of map 112 (possibly encrypted); (d) the creation, storage or transfer of filter 102 (possibly encrypted); (e) the storage of extracted data at memory storage B-ext (whether singular or plural storage sites); and (f) the transfer of extracted data thereto, the system may include an encryption feature. The encryption function 115, 117 and 118 is diagrammatically illustrated in FIG. 1A.

[0106] The program of the present invention can be set to extract critical data (a) when the plaintext or the source document (data object) is created; (b) when the source document or data object is saved; (c) on a periodic basis; (d) automatically; (e) per user command; (f) per ascertainable or programmable event; and (g) a combination of the foregoing. Timing for storage of the extracted data is based on these aspects. Reconstruction of the data object or plaintext may be (a) automatic and substantially transparent to the user; (b) based upon manual entry of security clearance data; (c) periodic; or (d) a combination of the foregoing dependent upon outside events and who is the author of the data object or other definable aspects of the data object, its environment of origination, current and anticipated security threats and its environment of proposed reconstruction. The timing for the extraction, storage and reconstruction is oftentimes dependent upon the level of security required by the user and/or his or her organization.

[0107] FIG. 1B generally diagrammatically illustrates the major features of a reconstruction routine or system. The user, typically at a computer terminal, inputs a reconstruction request 120. The system first executes a security clearance protocol routine 122 in order to determine whether the user has the proper security clearance. The security clearance may be thought of as a security clearance control. If multiple users are permitted access to the documents and those multiple users have different security clearances, the security clearance protocol determines the level of security clearance and, hence, the full or partial reconstruction of the plaintext. The security code input by the user is checked against a security code database or list 124. Clearance is provided in step 126. The location of the map and, hence, the location of the remainder data A-com 108 and extraction is provided to the user's computer in step 128. This may include obtaining a copy of the map 130 showing the location of memory segments in (a) the local computer; (b) the LAN or WAN; or (c) the Internet storage sites. The storage segments are A-com 108 and B-ext 110. The common or

remainder data is downloaded or transferred or made available to the user's computer as shown at the output of map location and data step 128. Typically, the extracted or security sensitive data from B-ext is downloaded. As described hereinafter, the data can be reconstructed as a complete electronic document in function 130 or may be reconstructed only as a visual reconstruction in step 132. Visual reconstruction is discussed later. Function 130 operates as a compiler to gather the extracted data and remainder data into a single plaintext document. If the data object represents sound or audio signals, reconstruction and play back may require a speaker output in function block 130. In a telecommunications implementation of the present invention, the input would include a microphone or audio detector (supplemental to the input device for document 100), an analog to digital converter (possibly with a voice to digital converter), the filter, extractor, storage facilities at least for the extracted data, and at the output of the system, a converter to audio and an audio announcer. The recipient of the secured data stream or message would be required to clear a security clearance and possibly obtain a decoding key prior to listening to the entire, decoded message. The key and the security data is separately downloaded to the recipient's device.

[0108] If remainder data in A-com memory 108 and extracted data in B-ext computer memory 110 is encrypted, the reconstruction process includes a decryption step. Encryptors and decryptors are relatively well known by persons of ordinary skill in the art. Further, the filter 102 (FIG. 1A) may include some encryption routine operating on the data object (plaintext) during the filtering. A simple encryption may include substituting "dummy" text or images for the security words and keeping a pointer to an encryption key document mapping the security words with the dummy words. The filter may be stored or may be destroyed at the option of the user. Storage of the filter impacts the degree of security of the entire data system but storage of the same filter enables the user to reuse the filter at a later time. Encryption of the stored filter increases the

security of the data. Creation and storage of map in memory 112 also impacts the degree of security of the system. However, if the filter 102 is destroyed and all copies of the map are destroyed on the user's computer originating plaintext document data 100, and the map is stored offsite in a third computer memory location 112, this offsite map storage may enhance the degree of security of the data. The originating computer processing plaintext 100 may be scrubbed to remove all reference and copies of the plaintext, remainder text, extracted data map storage data, etc., i.e., a deletion routine may be employed on the data input computer.

[0109] FIG. 2 diagrammatically illustrates a personal computer or PC computer system 140, a second PC or computer 142, and a third PC -3. PCs 140, 142 and PC-3 are connected together via a network 145(LAN or WAN) and are also connected to an input/output device 146 that may be generally described as a router or a server to an outside communications system. The input/output device 146 is connected to a telecommunications system 148 which leads to Internet 150. The Internet is a global computer network. Internet 150 is coupled to a plurality of servers, one of which is server 152. Server 152 may be designated as an application service processor ASP. Internet 150 also includes various computer memory storage devices such as computer storage I-com 154, computer storage I-ext 156 and computer storage map 158. Computer storage enabling the store of extracted data includes a security level clearance module 157. Similarly, map computer storage 158 includes security level clearance module 159.

[0110] As stated earlier, the present data security system can be implemented on a single personal computer 140. In this case, different memory segments or hard drive 168 may be used for A-com and B-ext. Typically, PCs include a keyboard or data input device 161, a display 163, a central processing unit CPU 165, a video board 167 having video board memory 169, a fixed disc hard drive 168, a RAM 166, and input/output device 164, a removable memory media floppy drive

162 and a removable compact disk (CD) read-write (CD-RW) device or drive 160. The system may include other removable disk drives, tape drives, or flash memory units. Internal units CPU 165, video board 167, hard drive 168, RAM 166 input/output device 164, floppy drive 162 and CD-ROM device 160 are all coupled together via an internal bus 171. Bus 171 represents a plurality of buses as is known to persons of ordinary skill in the art.

[0111] One methodology of implementing the present invention utilizes distinct memory segments which may be designated in one or more of the following: hard drive 168, memory in a removable disk in floppy drive 162, memory in a removable CD disc in CD-RW device 160, and, to a very limited extent, RAM 166. In this manner, the user may select, generally at the outset of the process, that the extracted data memory storage B-ext 110 be stored on a floppy (removable memory) via floppy drive 162 or a CD via CD-RW drive 160. The user can then simply remove the floppy or the CD and carry it with him or her. To reconstruct the data, the operative program, generally discussed above would have access to the floppy or the CD and particularly the memory location of the data on the floppy and the CD in order to reconstruct the entire plaintext document 100 (see FIG. 1A). Alternatively, different portions of hard drive 168 may store A-com and B-ext. Of course, the computer system may utilize tape drives and memories or flash card, programmable memory.

[0112] In a local area network or wide area network implementation, PC 142 includes memory similar to memory units described in PC 140 and a memory segment may be set aside in PC 142 separate from the common data or remainder data storage typically placed on hard drive 168 in PC 140. As a further expansion of the present invention, the extracted data (that is, the high security data), may be stored on computer storage I-ext memory unit 156 via Internet 150, telecommunications system 148 and router/server 146. In this manner, the common data or

remainder data is stored on hard drive 168 and the highly sensitive data is stored off site in a secured location. Access to that secured location may be limited via security layer 157. If the user implements an encryption system (see encryption e 118 in FIG. 1A), the extracted data is further secured by the encryption during the transfer from computer 140 through network 145, router/server 146, telecommunication system 148, Internet 150 and ultimately to computer storage I-ext 156.

[0113] The present invention may also be embodied utilizing an Application Service Provider on server 152 and in a client-server network.

[0114] An implementation of the present invention over Internet 150 most likely includes the use of a uniform research locator or URL for map memory computer 158, computer storage I-ext 156, computer storage I-com 158 and ASP server 152. In a client-server environment, server 152 acts as a server generally commanding the operation of client computer 140. Of course, persons of ordinary skill in the art recognize that the server may be located on the local area network 145 rather than being interconnected with Internet 150 as shown in FIG. 2. The claims appended hereto are meant to cover the alternative embodiments.

[0115] As an example of a client-server or web-based implementation of the present invention, the user at computer 140 may define the filter 102 as described above, and input data (plaintext) via keyboard 161 or load plaintext data from floppy drive 162 or CD-ROM drive 160 into RAM 166. In any event, whether the plaintext data is input via keyboard 161 or copied or accessed from floppy drive 162 or CD-RW drive 160, the plaintext data is filtered as discussed above in connection with FIG. 1A. Prior to filtering, it would be appropriate for the user at computer 140 to identify where the remainder data or common data will be stored and where the extracted or high security data would be stored. A simple program may automatically select the

secure store location. The system is sufficiently flexible to enable the user to select local storage on different memory segments of PC 140 (hard drive 168, floppy drive 162, CD-RW drive 160) or be flexible enough to enable user at computer 140 to designate off site storage of the high security data (extracted data) and/or the common or remainder data. An automatic store routine may only require the user to accept or reject to preferred first security level, second security level and higher security level stores. The off site data storage process may include activating server 152 and enabling the server to take over the process directly from user 140. In other words, the user at computer 140 could call up the URL of the server 152, the server could request certain user information (user name, password), and would request data from the client computer to establish the filter pursuant to input selected by the user. The client computer may (a) filter the plaintext thereat or (b) send the data to the server for filtering. The server could store data either locally on computer 140 or remotely at computer memories 154, 156. After storage of the data at any of these locations, the server 152 may establish a map and store the map in memory location 158. Of course, remainder data (cleansed, plaint-text data) and the map may be stored at ASP 152 or client computer 140. The map, if stored at map storage 158, may be downloaded to the user at computer 140. The filter may be stored at computer 140 or may be stored at a secured location on server 152. Alternatively, the map could be destroyed on user computer 140. The filter could also be destroyed on user computer 140. Of course, the filter could be stored in a fourth remote location (not shown), different from I-com 154, I-ext 156 and map computer memory 158. Storage of the map and decryption keys is a critical, high security task. Appropriate security measures should be utilized to protect those items. Local removable memory storage on disc in floppy drive 162 or disc in CD-RW 160 may be reasonable. All traces of the map, the filter, the encryption key, the extracted data, and possibly the remainder data may be scrubbed or deleted from all computer memories (by write-over or disc

reformat routines) other than the “com” and “ext” storage sites. Deletion of all URLs, links, x-pointers, etc. is also recommended for high security applications. Deletion systems are known to persons of ordinary skill in the art. For multiple security levels, multiple web site for storage of cleansed plaintext, first, second, third and higher security level extract text is preferable. Where the community of interest has access to the targeted and protected data via the Internet, multiple secured storage locations, multiple stores for filters, for encryption keys and for maps locating the secured stores is provided by multiple storage locations distributed throughout the Internet.

[0116] To reconstruct the document, the user at computer 140 would be required to call up the URL of server 152 and input the appropriate security code. The server 152 would then call up and download data from various memory locations whether they be memory locations on computer 140 or memory locations I-com 154, I-ext 156 and map memory 158. The system compiles the entirety of the plaintext document by gathering the dispersed components thereof or compiles partial reconstructions for different levels of security. By implementing different security levels, the system is dynamic enough such that server 152 can easily locate the various extracted data levels based upon various security codes representing different security levels, as those codes are input by the user at computer 140. Multiple security codes, at the inception and during the process, may be utilized. The user may be required to input security codes at multiple times during the reconstruction or compilation process.

[0117] It should be noted that computer storage 154, 156 and 158 may be located on the same computer or may be located on different computers spread throughout the Internet. If the storage units are different computers spread throughout the Internet, computer storage 154, 156 and 158 would each have their own URL or Uniform Resource Locator. In any event, during reconstruction, the server 152 gathers the information and downloads the information into RAM 166

of computer 140. This download may include a first download of the common or remainder data from I-com 154. At a separate time, which may or may not include a decryption routine, the extracted from I-ext 156 is downloaded. Preferably, other than inputting initial security codes and any required or desired intermediate security codes, the system operates automatically without further input from the operator at client computer 140. The download of both data sets may be simultaneous in that the download is not humanly perceivable. This is especially true if storage in different memory locations in PC 140 is utilized.

[0118] The role of server 152 may be expanded or reduced dependent upon the desires of the user and the degree of security necessary. For example, server 152 may only enable separate storage of extracted data in I-ext 156. In this limited role, server 152 would require the input of a proper security code and clearance prior to identifying and enabling the download of extracted data from I-ext 156.

[0119] In an expanded mode, server 152 may be involved in filtering the data, extracting the security sensitive words, characters, icons or data objects to obtain extracted data and remainder data thereat, separately storing the extracted data from the remainder data (extracted data being placed in computer memory I-ext 156 and remainder data being stored in common remainder data memory I-com 154) and then permitting reconstruction via separate or combined downloads of the remainder data and the extracted data into computer 140.

[0120] FIG. 3 diagrammatically illustrates a system diagram for various reconstruction routines. A complete reconstruction is shown as security level path A. This involves an electronic integration of plaintext in step 202 resulting from the complete electronic reconstruction of document 100. For example, a merge may occur between the extracted data and the remainder data

or common text data. The document is completely compiled in this process. Placeholders in the remainder document are utilized to locate and insert the extracted data. Most likely, there will be no process controls imposed on the integrated document as shown in step 204. In other words, if the user at computer 140 has the proper security clearance, he or she could download or recreate the entire original source, plaintext document and the user would be entitled to edit the document or change it in any way or copy it and reproduce it.

[0121] The second level of security, path B, results in storage of the common or remainder data in a different memory location on the hard drive 168 as compared with the extracted data. This is noted in step 206. Another words, in a simple example, hard drive 168 or RAM 166 would hold a copy of a remainder data document and another copy of the extracted data document, that is, two separate documents. Since two documents are available in RAM 166 or hard drive 168, these documents are stored in different locations in the memory. In step 208, a map showing the memory location of the common or remainder document and the extracted data document is provided to computer 140. Step 210 commands the processor CPU 165 in computer 140 to interleave the extracted data with the common or remainder data in the video board memory. In this process, the extracted data would typically have placeholders for the missing remainder data. Otherwise, control codes to locate the extracted data into the remainder data would be executed by CPU 165 to properly place the extracted data into the “visual space” of the placeholders in the remainder data document. The extracted data document may have placeholder for the remainder data. Some type of register between the two image documents may be necessary. The compiler, in this embodiment, gathers the document elements and visually compiles and presents the plaintext to the user.

[0122] FIG. 3A diagrammatically shows that video board memory 169 is loaded with remainder or common data 1 and a different location of the video memory is loaded with extracted

data 1. The next video memory location is loaded with common data 2 and then a different video memory location is loaded with extraction data 2. Since the refresh rate of computer monitor 163 is fast, the display 163 will show the common or the remainder data and then show the extracted data such that the user could not humanly perceive a difference in the document. However, the user could not copy the document from display screen 163 (a “screen shot”) since the document is never electronically integrated into a single document. There is only a visual presentation of the combined document by interleaving the extracted data with the common or remainder in the video memory 169. Step 212 notes that the user may be limited in his or her ability to process, edit and store the reconstructed and presented plaintext document.

[0123] Security level path C recognizes in step 214 that the data is stored in different memory or computer locations. In this situation, two video boards, video board A and video board B are shown as board 216 and 218. Video board 216 drives display monitor 220. Video board 218 drives display monitor 222. Display screens 220, 222 are overlaid atop each other. Video board 216 is fed with common or remainder data from the remainder data store (see I-com store 154 in FIG. 2) and video board 218 is fed with the extracted data from the extracted data store, for example, I-ext store 156. In this manner, as noted in step 224, the user is presented only with a visual presentation or compilation of the plaintext. Since there was physical separation between video monitor 222 and video monitor 220, there is no electronic integration at all of the plaintext document. Hence, the ability for the user to do any significant editing on the plaintext document is blocked or prohibited because the user only has access to either the data on video board 216 or the video board 218.

[0124] Security level path D shows that the extracted data may be parsed or further separated based on a plurality of security clearances in step 226. Step 228 recognizes that the system can

repeat process and security process paths A, B and C only with portions of the extracted data presented to the user based upon the user's security clearance.

[0125] FIG. 4 diagrammatically illustrates the major components of a flowchart for the data security program. It should be noted that this flowchart may be truncated to limit user selection of certain items. The system would be pre-set to contain these features. Step 230 initializes the system. Step 232 enables the user to designate various levels of security for the activity which he or she will soon engage. The system, in step 234, enables the user to define the levels of security parameters. The following Security Table gives some examples of the type of security that may be available to the user.

Security Table

to whom

to where

when (time of day, day of week, month, floating but predetermined time frame)

why (purpose, match purpose to other security parameters or to certain predetermined criteria)

how (through what medium (LAN, WAN, Internet, direct dial link), download to what site or destination)

how long (duration) the reconstruction process will be permitted per each security clearance level

how much (different security levels enable reconstitution of documents and data with different amounts of secure data therein)

timing systems may require synchronization for a standard clock (i.e., atomic clock)

[0126] As an example of a truncated or pre-set program, a client-server system over the Internet may have URLs designating storage sites and an ASP 152 (FIG. 2) controlling storage. In this pre-set system, the user does not select the sites. The sites may be randomly selected by ASP 152. The ASP may use artificial intelligence AI to locate secure extract data storage sites. AI or inference machines can ascertain (a) traffic on communications channels, (b) storage limit issues, (c) transmission failures in the communications links, and (d) the degree of security necessitated by exterior events, i.e., terrorism alerts, virus alerts, war, data security warnings posted by trusted sources, MicroSoft, Norton, NASA, DoD, CDC, FBI, etc. Higher security alerts trigger the AI configured storage locator and facilitator to locate memory stores in higher secured places. These higher security facilities may be more costly, may be located in more stable countries or on more stable servers and may have greater degrees of encryption capabilities.

[0127] The user, in step 326 can designate the location of the filter, the common storage area for the remainder data, the extraction data storage and potentially multiple data storage areas or segments. The user may enable an AI filter design. Step 238 permits the user to engage or disengage encryption and, if engaged, establish the degree of encryption for the system. Step 240 enables the user to define the parameters of the filter. The user can retrieve a preexisting filter or may define a new filter for each data security session. These filters may consist of dictionaries or any type of compilation of words, characters, icon, data objects or pixel formation or any indication that can be perceived by the computer system. Granular extraction of data elements in a data object may be permitted. Step 242 recognizes that the user either inputs a preexisting plaintext document or types data into the system. In any event, the plaintext document is fed through the filter. Step

246 extracts the security data from the input document. Step 248 stores the extracted data. The extracted data may be encrypted prior to storage. Step 250 conducts an error check on the extracted data. This error check is helpful in discerning problems in the storage of the data prior to closing down the data security system. Step 252 stores the common data or the remainder data. Step 254 conducts an error check on the common or remainder data. The decision step 256 determines whether the user has selected a “destroy filter” command. If not, the filter is stored with or without encryption in step 257. If YES, the filter is destroyed with a deletion routine. Typically, deletion is complete erasure of all traces of the file including, in high security systems multiple write-overs or disc reformatting. Step 258 stores a map. The map may be stored locally or remotely as described earlier. The system ends in step 260. All traces of these data elements or objects may be swiped clean or removed from whatever computer system generated the data objects or processed them, other than the memory storage locations. Deletion of data also includes the concept of deletion of data transmission paths, URLs, storage site locations and all temporary memory stores. Deletion of file location in the root directory of hard drive 168 of computer 140 is preferable in high security systems.

[0128] FIG. 5 diagrammatically illustrates basic flowchart features for the reconstruction process. Step 302 accepts a request to reconstruct the secured data. Step 304 queries a local map and the security system or protocol. In a preferred embodiment the user would have to input several passwords, one of them being a local password on computer 140. A local map which may be accessed only through the password, may simply identify the URL of server 152. Decision step 306 determines whether the local password is acceptable. If not, an error step is indicated in step 307, the attempt to log on to the security system is noted in step 309 (an audit trail), and the system either branches to repeat step 311 or bars the user from further activity in step 313.

[0129] Returning to decision step 306, if the password is locally acceptable, the YES branch is taken and the system executes step 308 which releases a reconstruction request to the common storage facility I-com 154 or A-com 108 (FIGS. 2 and 1A-B). The system in step 310 logs the user in, as well as time and date and the data regarding the request. In step 312, a download from the common data storage is provided to RAM 166 or hard drive 168.

[0130] In step 314, a query is made to obtain the remote map from the remote security system. The decision step 316 indicates that the user again successfully inputs his or her security code. If not, error routine 317 is activated, the password failure is noted in step 319 (an audit trail), and the user is given an opportunity to repeat in step 321 or is barred or prohibited from further activity in step 323. If the user has correctly input the security code, the system in step 318 releases the keys (to decrypt) and the map and releases the reconstruction request to the remote storage for the extracted data. This could be computer storage I-ext 156 or computer storage B-ext 110. In step 320, the user's access to the extracted data is logged in along with the time and day and type of data request. In step 322, the system downloads the extracted data into RAM 166 and/or hard drive 168 of computer 140. In step 324, an error routine is operated on the extracted data in order to insure that the extracted data properly matches the common or remainder previously stored. Decision step 326 determines whether the error routine properly generates the correct count or output. If not, the system in step 327 indicates an error, in step 329 the system deletes the common files and the extracted files and the system in step 331 logs in the failed attempt. If the error checking routine on the extracted data is acceptable, the YES branch is taken from decision step 326 and the system, in step 328, proceeds to display the plaintext document or to integrate the plaintext document pursuant to the security clearance initially input by the user. Step 330 ends this process. The end process may entail encrypting the data again and swiping clean all traces of data objects from the memory

stores and computer handling units. Of course, every use of encryption requires decryption of the data prior to reconstruction.

[0131] The system may incorporate various types of security systems or routines.

pass word

pass phrase

multiple choice questions and answers

initial, intermediate and subsequent security clearance routines

biometric security routines (voice, fingerprint, signature, eye or retina scan)

[0132] The reconstruction routines may be interrupted or the security system automatically activated or initiated upon the occurrence of externally generated triggers or upon certain predetermined conditions or conditional events. Limited extraction, security clearance, release of data and reconstruction limits may be imposed. Artificial intelligence (AI) engines, inference engines or neural networks may be implemented to vary the permitted level of reconstruction via the security clearances. In other words, the AI system, as applied to reconstruction, may, relatively independent of the filter and storage processes, increase the necessary security levels permitted to access and generate full or partial plaintext recreation.

[0133] The display systems 220, 222 in FIG. 3 include CRT monitors, LCD screens, projection screens and combinations of those systems.

[0134] The audit trail to monitor reconstruct and reconstruction attempts may include adding a time/data stamp to the remainder data and/or the extracted data prior to storage and a cross-check to the audit trail log during the reconstruction process.

[0135] Placeholders in the remainder document may be:

blank spaces

data symbols or elements “---“ or “xxx”

false data

clearly erroneous data “ABC Company” or “Baker”

chaff or hash marks

messages

bar code

serialization data

alerts

links to other data objects

null set indicators “[]”

URL or website addresses

[0136] It is believed that the present invention is faster, during reconstruction, than standard encryption techniques, on the order of 100 to 1,000 faster.

[0137] The system and method described herein may operate substantially automatically, that is, without operator intervention, other than the security clearance function. The clearance function does require some type of operator authentication prior to retrieval of the extracted and remainder data.

[0138] The system and the method may operate automatically in that the plaintext or originating data could be identified by a party desiring security. The system could obtain that data from any data input device (hard drive memory, floppy drive memory, flash card memory, personal

data assistant (PDA), or any other type of data input device), filter the data, separate the extracted text or the remainder text, encrypt (or not encrypt) the data, separately store the extract and remainder data (all automatically, that is, without operator intervention). Hence, it is not necessary that the system operate with significant operator or manual intervention. Of course, the system may also operate on a plaintext document or data object that is being created “in real time” by an operator and keyboard, mouse or other type of data input device.

[0139] The automatic operation of the system and the method can be caused by a triggering event. This triggering event may be a security attack (generating a trigger to start the gathering of plaintext, filtering, extraction and storing) or may be any other type of trigger such as a building burglar alarm, door alarm, fire alarm, or virus detection algorithm trigger. The event may be a time of day, week or month. It may be n seconds after the user stops typing on a keyboard. It may be a timed back-up feature.

[0140] Multiple filters may be utilized in the system and in connection with the method. These multiple filters may be useful in the operation of the system with a plurality of security levels. Each filter could filter out different levels of security sensitive items and each bundle or group of security sensitive items (from each distinct filter) could be stored at different computer storage locations. Multiple filters, multiple security levels and multiple storage areas may also include multiple encryption routines and decryption routines. Encryption and decryption routines can be related to the level of security of a particular group of data.

[0141] Multiple maps may also be provided for singular or multiple storage of extracted data and remainder data. These maps may or may not indicate the originating point of the data. Maps can be parsed such that an intruder, upon discovery of a single map or map portion, could not locate

the storage locations of all piece of the extracted data and remainder data. maps may also be encrypted. The map may also be stored at a distinct map store location.

[0142] The concept of partial reconstruction also includes the concept that a portion of the plaintext would be reconstructed and the unreconstructed portions of the plaintext could be encrypted or could show blanks or other symbolic indicators. See the placeholder table above.

[0143] Partial reconstruction of the plaintext also includes a concept that the security sensitive items or materials may be subject to different types or keys of encryption. Hence, a single plaintext document may have multiple levels of security and multiple levels of encryption wherein each encryption has a different level of security assigned to it.

[0144] The present invention can also be configured to provide a computer network which transparently establishes and manages the separation of user-based communities of interest. The separation is accomplished by extraction pursuant to security levels, dispersion of data into secure storage facilities (memory stores) and reconstruction based upon the assigned security level. A low level security clearance results in only partial reconstruction of the plain text or source document. These user-based communities of interest are a plurality of users each having respective security clearances. As described above, each successively higher level of security clearance permits the user to see greater degrees of reconstructed plain text obtained from the extracted data stored in extract stores and the remainder data from the remainder stores. By integrating encryption (and necessarily decryption), separation of user-based communities of interest are established such that the users in a particular community are permitted access to some or all of the plain text data based crypto-graphically separated communities and need to know security levels.

[0145] FIG. 6 is an exemplary computer network diagram showing various user communities. The telecommunications network 402 is connected to the server application server provider ASP 452 and to various networks and personal computers or PCs. the PCs may be computer work stations. Network A 404 is coupled to telecommunications network 402 via an input/output unit 406. Network A is coupled to various PCs identified in FIG. 6 as PC-4, PC-5 and PC-6. Of course, Network A could be coupled to other PCs not illustrated in FIG. 6. As described earlier, server 452 can facilitate remote or offsite storage of extract data and remainder data in store 1, store 2 and/or store 3. Further, the map showing the storage location may be encrypted and stored in any one or more of these stores. Also as described earlier, the memory in one of the PCs, for example PC-4, PC-5 could be utilized to store extract data and remainder data from PC-6 and PC-6 can be configured as the input data computer. Hence, the present system and methodology encompasses the concept of local storage and remote storage. On the local level, the storage begins by storing the extract data at different locations in the hard drive of the PC. The next level higher is storing the extract data in removable computer media such as floppy disk, removable tape drives, CDs etc. associated with the PC accepting data or associated with a server on Network A. The next higher level of extract store is storage of the extract data on a server or other computer in a particular network. If PC-6 is designated as the input computer, the extract data may be stored on PC-4. Of course, PC-4 could be designated as the server for Network A.

[0146] PC-7, PC-8 and PC-9 are coupled to telecommunications network 402. Network C 408 and Network B 410 is coupled to communications network 402. The lines, one of which is line 409 extending from Network C 408, represent a plurality of computers or workstations coupled to Network C. Line 411 represents a plurality of workstations or computers coupled to Network B 410. In an e-mail implementation of one embodiment of the present invention, PC-7, PC-8, etc. may represent computerized devices accepting e-mail (personal data assistant, pager, cell phone, etc.).

The sender and the e-mail addressee may utilize simple computerized systems to communicate via e-mail. Further, the network may be any telecommunications network including wire, cable, cellular, wireless, satellite, IR or RF systems.

[0147] FIG. 7 diagrammatically illustrates a flow chart showing the key component steps for the multiple layer security program for the community of users. The “community of interest” system described herein enables persons and organizations at the same security level to share data on a peer to peer level. Further the security system may operate automatically, with respect to extraction, storage and reconstruction, such that the peer to peer dissemination of data objects is quickly and readily available to all at the same or higher security levels. Step 420 initializes the program. Step 422 enables the user, administrator or system operator to designate multiple levels of security, that is, multiple words, characters, icon, data objects, or whatever, for each security level and further to define encryption for each security level. The designation step 422 also includes identifying the communities of interest and the particular security level and security clearance for each community of interest. One example of various security levels for communities is set forth below in the Community Security Level Table which is keyed to the computer network diagram of FIG. 6.

Community Security Level Table

Security level	Community Group
High	PC-7; PC-8
Medium high	all high group plus Network B
Medium	all above plus Network A
Low	all with nominal clearance
Special set medium	PC-7; PC-9; Network B

[0148] Further, designation step 422 will include identifying the words, phrases, icons or data objects subject to security concerns and the potential location of the extract data and, if necessary the remainder data and the degree of encryption. The following Selection Table provides some examples.

Selection Table

Level of encryption/storage	type or category of word or phrase; input specific word, phrase
High, web-based storage	dollar values, names of streets, countries, "Smith" and 5 words about "Smith," "avocado"
Medium high, remote storage	all addresses, all names
Medium network storage	all family names, all client names
Low, encrypt and separate store in local memory	all items not in dictionary

[0149] As an example of various encryption methodologies, the following Encryption Table is illustrative.

Encryption Table

DES, random pad A ("r. pad A")
Huffman, r. pad B
Crypto API, r. pad 7
Two fish, r. pad C-2
Blowfish
RC4
Skipjack

Ghost

[0150] In FIG. 7, step 424 executes or enables the security program with multiple filters, multiple encryption levels and multiple storage levels. Each one of these filters, encryption levels and storage levels correspond to the security level for the various communities of interest. Step 425 responds to an inquiry from a user to reconstruct the document. Step 426 accesses the user's security clearance and the particular inquiry. Decision 428 determines whether the inquiring party is entitled to full or partial access to the source document. If not, the NO branch is taken and the system, in step 429 adds placeholder substitutions. Step 429 may be optional. If YES, the system reconstruct pursuant to the clearance level in step 430. The following provides an example of multiple level encryption utilizing placeholder substitution.

Multiple Level Encryption

Applicants must be _____ zzxx xx _____ xxx _____ _____ citizens and have a high school diploma or equivalent. They must possess a valid subsubsub driver's license and qualify for top SUBWORD _____ clearance.

[0151] With this multiple level encryption, substitutions may be utilized "subword" to indicate to the user with a less than superior security level that a certain word, term or phrase has been extracted and stored by he or she is entitled to know that substitute word, term or phrase has been inserted into the plain text document. Of course, any type of substitution character may be used for the placeholder.

[0152] In step 432, the system displays the plain text in a normal format or utilizing a split or bifurcated video memory or utilizing overlay display screen. FIG. 3 and the description of that

figure set forth above describes the normal display in steps 202, 204, the split video memory display in steps 206, 208, 210 and 212 and the overlay display system in steps 214, 216, 218.

[0153] The system, in step 434, monitors and logs the location of the user making the inquiry, the type of inquiry, the time, day, date, clearance level and access level and logs all modifications to the plain text source document. One example of the log is set forth below in the Security Report Table.

Security Report Table

Privacy Scrubber Report

source file: path\filename

scrubbed file: path\filename-scrub

source file: date, time, size

process: date, time

user: name

system: name

Recovery File

(a) storage location, type of encryption, random key

(b) storage location B....

(c) store C

(d) store D

[0154] Step 436 enables the security program and parses and extracts the data per the security program, filters the data, extracts it and codes it disperses it and stores it as discussed above. The multiple layer security program ends in step 440.

[0155] The following Security Level Access Placeholder Table is another example of the type of placeholder substitutions that may be available. The example in the Security Table Access Placeholder Table may be used in conjunction with step 429.

Security Level Access Placeholder Table

[security level 2] intelligence located [security level 4] 20 miles from [security level 4]. He is using the name [security level 4], and dressed as a [security level 4] preacher. With him are his lieutenants, [security level 4] and [security level 4]. He is communicating with the international media through Mr. [security level 4], who resides at [security level 3], [security level 4], [security level 4]. Telephone is [security level 1] and Facsimile is [security level 1].

[0156] It should be noted that in order to reconstruct some or all of the plain text source data, some or all of the subsets of extracted data from the extract stores will be utilized dependent upon the respective security level of the inquiring party or user.

[0157] The present invention can also be configured as an adaptive security program which adapts and adjusts the security provisions based upon intrusion into a particular network or attempts to electronically attack or hack into that network or successful hack events. Programs are available to track electronic attacks or hacking attempts. One of these programs is manufactured by Cisco and identified as the Cisco Intrusion Detection System (IDS). The Cisco IDS system can work on a server or on PCs in a network. The Cisco IDS is an electronic intrusion detector, or an electronic attack detector or a hacking monitor. The hack or attack monitor is software loaded into a designated computer.

[0158] The output of the electronic attack or hacking monitor loaded into PC 142 (FIG. 2) for example, or loaded into PC-6 acting as a server for Network A 404 in FIG. 6, generates a

plurality of attack warnings. The attack warnings progressively and incrementally indicate the severity and degree of intrusion and hacking attacks directed to the computer system. The following Security Level Table illustrates an example of various responses to increasing levels of attacks. These increasing security responses include engaging the filter and extracting critical data and storing it locally; the next level involves storing the critical data on removable storage media; the next higher level involves offsite storage of all security data; the subsequent security alert results in multiple offsite storage for multiple levels of security or critical data and the highest level involves offsite storage of both common data (remainder data) and security data. Of course, other combinations responsive to the hack attack may be provided. The electronic attack monitor may use artificial intelligence AI to (a) assess the severity of the attack, (b) plan an appropriate “secure data” response, (c) select the degree of filter, extraction and/or encryption, and (d) locate secure extract data storage sites. AI or inference machines can ascertain (a) traffic on communications channels, both intra and inter network, (b) storage limit issues, (c) transmission failures in the communications links, and (d) the degree of security necessitated by exterior events, i.e., terrorism alerts, virus alerts, war, data security warnings posted by trusted sources, MicroSoft, Norton, NASA, DoD, CDC, FBI, etc. Higher security alerts trigger the AI security monitor to heighten the security level (or to decrease that security level in view of a reduction or withdrawal of an electronic attack). Aspects of AI systems, inference engines and neural networks are discussed above in conjunction with the AI configured filter. These AI aspects can be utilized with an AI configured security sensor.

Security Level Table

Attack (low threat level) Level One

engage filter

local storage - disk drive

encrypt map

Attack (moderate threat level) Level Two

same as Level One but use removable storage media (local)

Attack (nominal attack) Level Three

Engage higher level filter

Off site storage, single storage for all security data

Attack (moderate attack) Level Four

Multiple off site storage, multiple levels of security data

Attack (severe attack) Level Five

Off site storage both common data and security data

[0159] Hence, the filtering of data is based upon respective ones of the plurality of attack or hack warnings and the extraction of data and degree of extraction is dependent upon respective ones of the plurality of attack - hack warnings. Storage of the extracted data and the remainder data is also based upon the degree of attack which is reflected in the attack - hack warning issued by the monitor.

[0160] FIG. 8 diagrammatically illustrates a flow chart showing the key components of the adaptive security program adaptable to various levels of hacker of electronic attacks. Step 460 senses all intrusions and attempts, that is, electronic attacks, hack attacks or hacking actions on a computer or a computer network. This step is equivalent to the output of the attack - hack monitor. Step 462 assesses the current network performance, adjusts the storage location for the extract data

(the location of the extract store), the encryption level (the degree of encryption) and the storage of the map showing the extract data storage (if necessary) and storage of remainder data, if necessary given the severity of the attack. For example, during high utilization of the computer network (high utilization in a server computer in a server-client environment), local storage of extracted data may be preferable as compared with offsite storage of critical data. However, if the attack occurs during non-working hours, the performance of the network is very high, and the security system could utilize all the resources in the computer network to achieve the security goal of safe guarding the data during the attack. System resources include processing resources (for encryption/decryption), bandwidth resources to store extract data and any other resources that are critical for the utilization of the security system described herein. Decision step 464 determines whether a threat or attack as occurred. If not, the system takes the NO branch returns to step 460. If YES, the system in step 466 assigns an attack level or a hack warning level to the threat or attack. The system in decision step 468, monitors the network during the attack. If the network performance or the computer performance does not change, the YES branch is taken. If the computer performance or network performance changes based upon or during the attack, the NO branch is taken and the system returns to step 466 which reassigns an attack level or a warning level to the next higher or significantly higher warning levels.

[0161] After decision step 468, the system executes step 470 which assigns the security level and implements the security program based upon the attack. It should be noted that the administrator establishes the degree of security level, the encryption, the extract store and remainder store (if necessary) for various levels of attacks or hack warnings. The security level assigned to a particular attack warning is implemented in step 470. Decision step 472 determines whether the

security program's communication path is clear. For offsite storage of extract and/or remainder data, a communication path is important. If the path is blocked or compromised by the attack, the NO branch is taken and the system in step 473 reassigns the security level to a next higher level or a different, safer security level and returns to step 470. If the security and communications path is clear, the YES branch is taken from decision step 472 and, in step 474, the system maintains the security program. Decision step 476 determines whether sufficient time has passed from the attack. If not, the system loops to step 474. If YES, the system executes step 478 which either permits reconstruction of the user operating the plain text or source document or automatically reconstructs those documents that were filtered, parsed, extracted, and subject to outside storage. The system ends in step 480. To provide additional security, the attack monitor can be configured to monitor security warnings from trusted parties such as MicroSoft, Norton, NASA, DoD, CDC, FBI, etc. Emails or electronic communications from trusted parties can trigger higher levels of security. the attack monitor described above can be configured to accept messages from trusted parties. These messages are equivalent to detecting an electronic attack.

[0162] Further, the attack - hack monitor can be configured to monitor and assess other environmental conditions such as fire, power failure, equipment failure, unauthorized physical entry into the building, plant, or computer room. These exterior threats or events are monitored by the attack monitor since they may quickly develop into an electronic attack on the secured data retained by the computer system. In response to these exterior events, the attack monitor generates corresponding attack warnings similar in nature to the hack attack warnings discussed above.

[0163] There are various methodologies that may be utilized in the adaptive system. The tables that follow set forth these various security methodologies.

Standard Automatic Defenses Matrix

Mode	Normal	Threat	Attack
Encryption	Targeted Encryption	Full Encryption	Multi Type Encryption
Extraction	Plain-text Extraction	Extraction of Encrypted Data	Extraction of Multi Type Encryption
Distributed Dispersion	Single Storage Location	Several Storage Locations	Many Storage Locations
Display	Single display	Color/Dither Protection	Multiple Displays

Optional Automatic Defenses Matrix

Mode	Normal	Threat	Attack
Substitution of Code Words	None	Partial	Many
Substitution of Misinformation	None	Partial	Many
Controlled Release-Storage	Full	Partial	Conditional
Storage Locations	2	4	10 or more
Time for release	Anytime	Working Hours	Conditional
Authorized Users	Many	Partial	Conditional
What to Release	All	Partial	Conditional
Secret Sharing	None	Two Users	As Configured

Security Meter Module Table

	Normal Mode	Threat Mode	Attack Mode
ENCRYPTION	Targeted encryption	Full encryption	Multi layer encryption
	(Secret sharing)	(Secret sharing)	(Secret sharing)
EXTRACTION	Plain-text extraction	Extraction of encrypted Data	Extraction of multi encryption
Distributed Storage	1 critical storage	few critical storage	many critical storage
Controlled Release-Storage	Storage # ID		
	Time for release		
	Authorized Users		
	What to release		
	Special conditions	2 users online	3 or more users
Display	single display	single display	multiple displays
Substitution of code words	No	No	No

Normal Work Mode

	Extraction				Storage				
	Level 1	Level 2	Level 3	Level 4	Web	Offline	Remote	Removable	Local
social security	X						X		
credit card	X						X		
included	X						X		
last name	X						X		
number	X						X		
telephone			X					X	
name			X					X	
URL			X					X	
e-mail			X					X	
uppercase			X					X	
initial capital			X					X	
currency				X					X
postal code				X					X
address				X					X
location				X					X
date				X					X

Threat Mode

	Extraction				Storage				
	Level 1	Level 2	Level 3	Level 4	Web	Offline	Remote	Removable	Local
social security	X							X	
credit card	X							X	
included	X							X	
last name	X							X	
number	X							X	
telephone		X						X	
name		X						X	
URL		X						X	
e-mail		X						X	
uppercase		X						X	
initial capital		X						X	
currency			X						X
postal code			X						X
address			X						X
location			X						X
date			X						X

Attack Mode

	Extraction				Storage			
	Level 1	Level 2	Level 3	Level 4	Web	Offline	Remote	Removable
social security	X					X		
credit card	X					X		
included	X					X		
last name	X					X		
number	X					X		
telephone	X						X	
name	X						X	
URL	X						X	
e-mail	X						X	
uppercase	X						X	
initial capital	X						X	
currency		X					X	
postal code		X					X	
address		X					X	
location		X					X	
date		X					X	

[0164] FIG. 9 diagrammatically illustrates a flowchart showing the key components of a multiple encryption program using multiple types or keys of encryption in one document or data object. Multiple levels, types, keys or modes of encryption are utilized in the same document or data object to enable securing data and transparently managing the separation of user-based communities of interest based upon crypto-graphically separated, need to know security levels. These security levels are associated with a plurality of encryption types or with different cipher keys using the same encryption. An example of a multiple level encrypted document is shown above in the Multiple

Level Encryption sample. Different levels or modes or types of encryption are listed in the Encryption Table above.

[0165] Step 510 in FIG. 9 initializes the system by organizing different security levels with different encryption types and cipher keys. Also, the program sets filters to create the multiple encryption or ML document or data object. Step 512 filters the document or data object. Step 514 encrypts the extracted data for each security level. These steps 510, 512 and 514 utilize many of the routines discussed above in connection with FIGS. 4 and 7, steps 232, 234, 236, 238, 240, 422 and 424. Step 516 recognizes that the secured document or data object may be stored for later use (with associated multiple decryption), published, distributed, or otherwise utilized to achieve the primary purpose of the document, i.e., to communicate information or to safely store security critical information. Step 518 permits the user, with the proper security clearance to retrieve the document or data object. Step 520 illustrates that the user must retrieve his or her cipher key to decode all or a portion of the ML encrypted document or data object. This step may be manual which engages the user to into certain codes or may be automatic such that the user's computer automatically, without operator input, decodes all or part of the document or data object. Step 522 decrypts the document pursuant to the user's security clearance. Step 524 recognizes that the user may review, re-publish, store, comment on, re-encrypt or otherwise deal and handle the full or partially decoded document or data object. The program ends or otherwise continues with other programs set forth herein. It should be noted that storage of the extracted data may be included in the flow path of the program in FIG. 9 is necessary.

[0166] FIG. 10 diagrammatically illustrates a chart showing the key components of the parsing, dispersion, multiple storage and reconstruction (under security clearance) of data. Document or data

object 100, in function element 550, is created or obtained by the input computer device. The document is stored in a normal manner in customary data store 552. A parsing algorithm function 554 is utilized in parsing step 556. The parsing algorithm, as stated earlier, targets the plaintext document or data object 100 and splits, cuts and segments (that is, parses) the document by bit count, word, word count, page, line count, paragraph count, any identifiable document or icon characteristic, or other identifiable feature such as capital letters, italics, underline, etc. Hence, the parsed document 100 constitutes at least remainder data and data which is extracted or parsed or segmented out. A plurality of data extracts may be obtained. The parsed data (which is both the extract data and remainder data) is then dispersed into storage facilities data store DS 1, 2, 3, 4, etc. Preferably, the parsed documents are encrypted as shown by “e” in FIG. 10. In order to facilitate the potential reconstitution of document 100, a map is stored in a map storage 558. Hence, the dispersement 560 largely spreads out or distributes the parsed document 100 to a plurality of memories in the distributed computer system. These memories may be removable memory devices (floppy disc, removable tape drive, CDs) or may be more fixed devices such as hard drives, Internet storage facilities, etc. Preferably, the map is also encrypted.

[0167] Reconstruction step 562 enables a person with the appropriate security to obtain the map from map storage 558, decode the map, gather the dispersed, parsed segments of document 100 and compile the document. This is noted in function 564.

[0168] Since the original document 100 is stored in a customary manner in data storage 552, the parsed document stored in multiple data storage units DS1-DS4 provides a unique backup for document 100. The algorithm can employ many different mathematical constructions but is, in the current embodiment, primarily based upon one or more of a bit count, a word, a word count, a page

count, a line count, a paragraph count, and identifiable document characteristic, and identifiable word characteristic, and identifiable icon characteristic and identifiable data object characteristic, capital letters, italics, and underline found in the plaintext document or data object. Further, the parsing algorithm can generate different security levels wherein parsed segments are stored at different storage facilities having various degrees of security clearance. This establishes a hierarchy of data storage units and corresponding degrees of security clearances. The parsing algorithm may identify unique words or strings of data, i.e., credit card numbers. The hierarchy of security clearances may involve first a password, second a biometric confirmation such as a voice match and a third highly unique biometric characteristic such as a fingerprint or retinal scan. The parsing system enables a large distribution of data in a secured environment. In this manner, if the original data object 100 at customary data storage 552 is destroyed, a person with an appropriate security clearance can reconstitute the original data document 100 due to the secured parsing and dispersal of document 100 through data storage units DS1-DS4 and map storage 558. The parsing may occur on a granular level. In particular, the parsing may occur on a financial document in electronic form.

Financial Document Table

Startcode; Abel, Robert, NMI; 100567; TRANSFER803; To8900586943;
FROM3897622891; \$700.00; endcode

[0169] In the Financial Document Table, the start code and end code is typically represented by a digital code unique to the communications channel, the name on the account has no middle initial (NMI) and the various words “transfer 803” and “to 8900586943” and the words “from” and “\$” are represented by predefined numeric or alpha numeric codes. The electronic financial document complies with an established protocol. In any event, financial documents are often times transmitted

through electronic communications and telecommunications channels. The present invention, in one embodiment, enables a higher level of security by parsing the financial document or data stream. Further, a higher level of security may be employed by extracting identified text or characters and storing the extracted text as discussed above in connection with FIGS. 1A, 1B and 2.

[0170] To some extent, the present system can also be utilized for key management and encryption systems.

[0171] In a broad sense, the parsing methodology disclosed herein is not based upon the separation of critical versus non-critical or classified versus non-classified security information. The primary focus of the parsing methodology is (1) automatic transparent parsing of data content into granular data groups which are thereafter dispersed to different storage locations in order to maintain a very high level of security with or without encryption; (2) dispersal of the segmented data to different storage locations each which, potentially, demand additional identification or security clearance prior to the release of the stored segmented data, including, possibly, the creation of a digital bureaucracy, in order to hinder or circumvent digital attacks on the plaintext document or data object; (3) proposing and implementing a system wherein the user has a very basic appliance since most of the user's data is stored both locally (customary data storage 552; FIG. 10) and parsed and stored in a distributed system (DS1-DS4) and wherein an important asset is the map stored in map location 558; (4) enabling an institutional system to parse highly confidential information and extract the same in granular form and disperse the same throughout the Internet or other storage locations with or without encryption without compromising the document's security privacy and integrity.

[0172] The process involves parsing the documents or content into granular data groups and optionally creating small groups of data wherein the data segments cannot be recognized even to the level of providing 2-4 data objects in each file; dispersing the granular data groups into different storage locations; creation of a map of dispersal to the different storage locations (wherein the map is secured and encrypted and stored); and reconstructing the documents or data content. The reconstruction utilizes the map of dispersed and distributed storage and requires the presentation of security clearances such as passwords, biometric information and/or physical identifiers for access at the storage level and potentially at all the other data storage sites. The data is compartmentalized through distributed storage and sometimes requires separate security clearance. This need for presenting additional security clearance at different storage locations (DS1-DS4) creates a digital bureaucratic process which enhances the security level of the entire system. The selection and extraction of data and dispersal of that data to select storage locations can be established under different criteria. For example, one level of criteria extracts last name, address and social security numbers. Another criteria extracts every other line, every third word, etc. The parsing algorithm can utilize random selection or systematic selection as long as the parsing algorithm is documented and utilized in reconstruct step 562. The parsing algorithm may be stored with map and map store 558 or may be stored separately. An additional feature, as discussed above, involves utilizing place holders or adding substitute content to the remainder data of the parsed document 100. The use of place holders and substitute content may be thought of as an algorithm for the parsing. By using place holders and substitute data, private or highly confidential data is masked insuring privacy, security, and confidentiality. The ability to parse the information and/or extract security information is important for financial transactions. The transactions which require account numbers (see

Financial Document Table above) are useless without the account numbers. The security of the account numbers, whether identified and extracted or severely parsed and segmented, stored and reconstituted under security clearances, is enhanced by the present system.

[0173] To achieve a very high level of security, the system can optionally incorporate a two-men key system. The system automatically separates the selected data stream into one or more data groups and extracts one or more of these data groups and disperses them into data storage DS1-DS4. To release the extracted data groups and/or critical content, the reconstruct step 562 may require two persons submitting identification credentials or security clearances. This two-man key method is a further protection against identity theft and insider attacks. The two-men key system can be implemented on a regular basis or on an emergency basis when there is need for a higher level of security.

[0174] Financial documents sometimes include substantial amounts of numerical data such as financial projections, balance sheets, electronic funds transfer messages, etc. It should be noted that the extraction may be based upon a particular item such a digit and a nine digit number representing money or may be parsed automatically based upon some parsing facility. Of course, the financial document may also be viewed as a data stream with delimiters “;” separating fields in the data stream. The parsing algorithm may work on the data in each field as well as different fields in the entire data stream.

[0175] Most storage facility systems require a map in order to reconstruct the original plaintext document 100. The map may be encrypted and may require a secret key sharing scheme for access thereto. Further, the map may be a physical map (a printout) or may be stored on a removable data storage medium, rather than be an electronic representation. In some instances, a map is not

necessary. For example, if the security data or the parsed or segmented data were automatically stored on a floppy disc, the originator of plaintext document 100 could move the floppy disc from the computer system thereby physically safeguarding the security data or the segmented, parsed data. Without the disc, another person or the originator of plaintext document 100 could not reconstitute the document. The originator may deliver the floppy disc to another in order to permit reconstitution. The same is true regarding removable tapes and CD-ROMs.

[0176] Advantages of the present parsing system, methodology and program, include the ability to connect to unsecured networks without adversely affecting the overall security of the plaintext document 100; less dependence on existing security system including fire walls; the reduction of the requirement to keep daily updates regarding vulnerabilities of the computer system originating plaintext document 100; the security of plaintext document 100 is not dependent upon the number of access points into the network or number of users located on the network originating plaintext document 100; there is no damage to the parsed and stored backup version of plaintext document 100 if new security systems are installed wrong or misconfigured and there is no damage if system administrators turn OFF the existing security systems or improperly install or operate the security systems.

[0177] The parsing system can operate as a main security operation or an emergency backup system or as a customary backup system. The plaintext source document or data object may be preserved with or without encryption, or destroyed as a further data security step. The parsing and disbursement of data protects plaintext document 100 and insures the survivability of plaintext document 100 if the system originating plaintext document 100 comes under significant electronic or physical attack. That is, if customary data storage 552 is destroyed electronically or physically,

the survivability of data in the plaintext document 100 is established by the present system. The storage of granular data groups most likely would defeat any attempt to view the entire content of plaintext document 100. Only verified user users with a confirmed security clearances or identifications verified at reconstruct step 562 and in data storage sites DS1-DS4 are permitted to reconstruct plaintext document 100. Further, the parsing of the system can be triggered based upon an electronic attack, an electronic hack or a physical environmental detection scheme. This system immediately protects of the critical data plaintext document 100 with a transparent, automatic parsing, dispersal and storage system.

[0178] It should be noted that various aspects of the methodology and program described above in connection with FIGS. 1A-9 can be incorporated into the parsing methodology and program in order to enhance or modify the system.

[0179] FIGS. 11A and 11B diagrammatically illustrate a flowchart showing the key components of one embodiment of the present invention, that is, an e-mail security system. FIG. 11A is linked to FIG. 11B via jump points 11-A and 11-B. The method of securing e-mail data operates on a distributed computer system which at least includes a remote memory designated as an extract store. Of course, the extract store may comprise a plurality of extract stores operative in conjunction with a plurality of security clearance levels. A singular security level is identified in FIG. 11A. Further, the e-mail may be subject to a parsing algorithm which, as discussed above, is generally independent of the identification of security sensitive data. However, with respect to the parsing aspect of the present invention, the original e-mail data is split into extracted data and remainder data and the extracted data is stored in an extract store. Hence, the parsing algorithm operates essentially independent of the content whereas the secured e-mail program operates based upon content

identification. Although FIGS. 11A and 11B primarily relate to identification of security data, the same is true regarding the use of securing e-mail data with a parsing algorithm.

[0180] The e-mail security system begins with step 602 wherein the system or program is turned ON or is activated. Step 603 recognizes that the user originating plaintext document 100 (not shown) has set a security filter identifying one or more security sensitive words, characters or icons. In step 604, the user composes the e-mail representative of plaintext document 100. In step 606, the user selects the “send” command in the typical e-mail program. As is customary, the system in step 608 conducts a spell checking routine prior to sending the e-mail. In step 610, the system conducts a security check on the plaintext document or composed e-mail generated in step 604. The filter is used in step 604. In step 612, security words are highlighted or distinguished in the e-mail prior to the actual sending of the e-mail to the addressee. This step 612 is optional. In step 614, the user selects the security words for data to be extracted out. The highlighting step facilitates this selection. In step 616, the system extracts the security data and, preferably, in step 618, the security data is encrypted. Step 618 is optional. In a parsing application to secure e-mail, the parsing algorithm operates automatically at step 610 thereby eliminating steps 612 and 614. The extracting step 616 simply represents that the segmented data obtained from the original plaintext e-mail generated at step 604 is separated from remainder data.

[0181] After encryption step 618, the e-mail security system generally operates in one of three manners. Other systems may be formulated based upon the systems and subsystems discussed herein. In one methodology, a second e-mail is created (see step 629), in a second methodology the secured data in encrypted form is attached or appended to the original e-mail containing remainder data (step 621) or, in a third methodology, the encrypted security data is simply added to or inserted

into the end of the remainder data of the e-mail (step 623). The methodology of generating a second e-mail is initially discussed. With respect to structured data files (such as a database) and unstructured document files (e.g., WORD documents), the secure content is added, inserted or appended into the resultant composite file.

[0182] A second e-mail having encrypted security data is created in step 620. Further, the system in step 622 adds a hyperlink to the remainder data in the original e-mail created in step 604. The hyperlink presents a pointer for the addressee to a secured application service provider or ASP. See the discussion of FIG. 2 above. The ASP represents a data storage facility for the secured e-mail data. In step 624, the remainder data from the original e-mail is sent to the addressee in a normal manner. This step also includes the concept that the second e-mail containing the encrypted security data is sent to the ASP. In step 626, the addressee receives the remainder e-mail which includes a hyperlink to the secured data ASP.

[0183] The system jumps at jump step 11-A from FIG. 11-A to FIG. 11-B.

[0184] In step 628, the addressee receives the remainder e-mail, visits the ASP via the hyperlink and clears the security levels at the secured ASP. In step 630, the secured data ASP obtains a map for each secured data e-mail (since the original e-mail may be broken up into a plurality of extracted, secured data e-mails) obtains all secured data e-mail and decrypts the same. In step 632, the secured ASP downloads the secured data as an e-mail to the addressee. In step 634, the addressee system compiles the original plaintext e-mail 100. A reconstruction program may be necessary to decode the secured data and insert the data into the document via the placeholders.

[0185] Optionally, the decryption could occur at the recipient's e-mail device somewhat prior to the reconstitution of the e-mail plaintext document 100 during step 634. This requires the addressee to

have the encryption routine and the correct key or decrypt code. The e-mail security system described above may include many of the features discussed earlier in connection with FIGS. 1-9. For example, both the security data and the remainder e-mail data can be encrypted prior to transmission to the addressee and the secured data ASP. The encryption may include multiple levels of encryption and decryption may require multiple levels of security clearance. The encryption may be mixed in the remainder e-mail. Partial as well as full reconstruction is enabled as discussed above in connection with FIG. 3.

[0186] From the senders or originator's viewpoint, the e-mail facility described herein facilitates the storage of the extracted data at one or more secured sites.

[0187] Another implementation of the secured e-mail system attaches the encrypted and secured data to the remainder e-mail data as indicated in step 621. E-mail attachments are well known. Alternatively, the encrypted secured data may be embedded or copied in encrypted form at the end of the remainder data in the original e-mail as indicated in step 623. In either case, in step 625, the e-mail is sent to the addressee. In step 627, the addressee opens the attachment. In step 629, the system of the recipient decrypts the secured data attachment or the embedded data attachment. In step 631, the recipient's system integrates the now decrypted secured data with the remainder data. Of course, this a compilation step. Place holders or other position indicators are customarily utilized. Appending the encrypted security data is generally equivalent to attaching a file to the original e-mail which constitutes, after extraction, the remainder data. Including the encrypted security data is adding the security data to the original e-mail at a predetermined location (either the top of the e-mail, the bottom of the e-mail or some predetermined line number). With respect to structured data files (such as a database) and unstructured document files (e.g., WORD documents),

the secure content is added, inserted or appended into the resultant composite file, that is, added or inserted in a particular location or appended to the original source.

[0188] It should be appreciated that the e-mail security system may work automatically or may be selected manually by the user. The highlighting or special distinguishing manner for the security words in step 612 is optional. By highlighting the security words, the user may select or deselect those words for extraction. At the addressee's side, the addressee's system may be configured to automatically seek out the secured data ASP, enter security clearance data, download the secure data and integrate the secure data in the remainder data e-mail. The present invention contemplates automatic as well as manual steps in steps 626, 628, 630, 632 and 634. The hyperlink with the original remainder e-mail essentially maps the remainder data to the secured data and the remote storage locations handling the secure data. Multiple security clearances may be required of the recipient or addressee. The e-mail system can be combined with other features of the security system discussed above such as multiple security data locations, secret key sharing schemes, multiple encryption of the data in a single document, multiple security clearance levels required for a plurality of storage facilities, the two man key system, automation of key management and a plurality of levels of access to the data such as partial reconstruction in step 634 and full reconstruction.

[0189] FIGS. 12A and 12B diagrammatically illustrate a flowchart showing the key components of one embodiment of the system and the invention which implements the security system on a web browser. Jump point 12-A links FIG. 12A to FIG. 12B. The system, at step 700 is ON. The filters establishing either the parsing or the identification of security data are established in the filter set step 701. In step 702, the user inputs data into open field of an HTML display page which the user

has previously downloaded from a web server. In step 704, the user may select “secure now” turning ON the system or the system may automatically be ON such that the filter is screening all the data input by the user in the open field. In step 706, the system scans all the open field data, locates security data and extracts security data. In step 708, place holders are added to replace the extracted security data in the remainder data and a hyperlink is added to the open field remainder data providing a link to the secure data ASP. In step 710, the user selects the “send button” or any other indicator on the HTML page triggering an operation which transmits the open field data (which is now remainder data) to the web server. In step 712, the web server and particularly the common gateway interface (CGI) receives the remainder data fields, identifies the place holders in the data and the hyperlink to the secure data ASP. In step 714, the web server receiving the data from user’s browser goes to the secure data ASP, inputs and clears any security level, and obtains the secured data. In step 716, the web server reconstructs the open field data which generally is represented by plaintext document 100. In step 718, the web server processes the data as necessary. Many of the features discussed above in connection with FIGS. 1A-11A may be implemented on the browser system.

[0190] The credit card scrubber or financial data scrubber operates in a similar manner to the email and browser data security system described above. The credit card or financial data scrubber (herein collectively “CC scrubber”) typically operates on a defined sequence of numbers. For example, if a credit card number is 17 digits, whenever the email or browser security system or program detects 17 sequential numerical digits (a pre-set filter), a pop-up window may appear enabling the user to select or turn ON the scrubber. If ON, the data security program strips or parses the credit card number and sends, for example, five of the 17 digits to a secure store. Placeholders

or substitute characters may be inserted into the remainder CC data. To reconstitute the entire CC data, the intended recipient would be required to pass security clearance levels at the secure store. Of course, the CC scrubber could be set to detect bank account numbers, personal or business account holder names, pre-set passwords, etc. In an OFF state, the CC scrubber would let pass the CC number, account number or pre-set data stream or string. The user may select (i) always ON; (ii) pop-up window, select ON or OFF per transaction; (iii) pop-up window to select OFF (default being ON); or (iv) always OFF but minor reminder (audible sound, icon appearance, etc.) of data security risk. The CC scrubber may encrypt the extracted data for security. Other visual cues may rather than a pop-up window may be used (for example, a drop down menu). The scrubber can also be deployed on wireless devices to scrub sensitive data such as credit card and other financial data.

[0191] FIG. 13 diagrammatically shows several revenue systems which may be employed with the data security systems described herein. Many types of revenue systems may be employed in conjunction with the present invention. FIG. 13 shows two basic systems, one at the data input stage and the second at the data output or reconstruction phase. Within each revenue subsystem are two types of revenue generators, an advertising revenue generator and a user charge generator. The user charge system contemplates charging or assessing a fee to the user's employer or organization. Therefore, the system operator may select up to four (4) revenue generation systems (ads at the input, charges at the input, ads at the output and charges at the output). It is well known that vendors selling goods and services over the Internet are willing to pay a certain percentage of their sales revenue to other entities referring customers to the vendor's web sites. The concept of display ads in FIG. 13 includes this revenue stream. The system operator may choose all, one, several or none of these revenue systems to be deployed in conjunction with the data security system described

earlier herein. Other revenue system may also be utilized. The steps in the revenue system described herein may be reorganized to attain higher consumer and user acceptance and/or to maximize the revenue to the system operator.

[0192] Decision step 730 determines whether the system is deployed at the data input phase or not. It is clear that the system operator may utilize the data reconstruction revenue system and hence the decision step 730 is not necessary. If the data input system is employed, step 732 displays the ad to the user. The user may be uploading a complete document to an application server on the Internet or may be using a application service provider on the Internet or an private LAN to secure his or her data. The display ad 732 step enables the user to click on the ad and visit the vendor, thereby potentially generating a referral fee. See referral fee branch 757. Step 734 requires password clearance. Step 736 processes the document or data object with the security system. The user may input the document real time or input it to the application server or may upload the complete document to the server. Alternatively, the ad could be buried in the email or application program run on the user's computer and the user would be shown an ad and given a link to the vendor's Internet site. Selecting the link points the user's browser to the vendor's site.

[0193] Step 738 shows display ad 2 to the user thereby potentially generating referral revenue for the system operator. Step 740 notes that the user exits the revenue system. Step 742 determines whether the system charges the user for the security service. If YES, the program processes the charge in step 745 (charge systems are known). If NO, the system ends or returns to other programs in step 747.

[0194] The NO branch from determination step 730 leads to the receipt of a reconstruction request by the user in step 750. Step 752 determines whether the user will be charged. If YES, the system

executes step 745. If NO, the system displays the ad 1 in step 754. Referral generation is noted by branch 757 from step 754. In step 756, the user's password is subject to clearance. In step 758, the user's request is processed, the document or data object is reconstructed (fully or partially as described earlier), and in step 759 the system displays ad 2. In step 762, the user's activity is logged in to the system. Step 764 determines whether the charge to the user is reduced (because he or she viewed the ads) and if not, the system ends in step 747, if YES, the system processes the charge in step 745. Alternatively, the user may be shown display ads and/or charged for services upon storage of extracted data. Step 750 includes this concept.

[0195] The claims appended hereto are meant to cover modifications and changes within the scope and spirit of the present invention.

What is claimed is:

Claims

1. A method of securing input data having security sensitive content, represented by one or more security sensitive words, characters, images, data elements or data objects therein, comprising:

extracting said security sensitive content from said input data to obtain a plurality of extract data grouped into different security levels;

encrypting said extracted data for each said security level and one of appending, adding or inserting said encrypted extracted data with remainder input data to form a composite;

responsive to a data request, reconstructing fully or partially said input data from said composite with decryption of said extracted data only in the presence of a respective predetermined security clearance, required for each said security level.

2. A method as claimed in claim 1 including displaying said security sensitive content in a distinguishing manner prior to extracting.

3. A method as claimed in claim 2 including permitting one of user selection and user confirmation of said security sensitive content.

4. A method as claimed in claim 1 including providing multiple levels of encryption and corresponding multiple levels of security clearance.

5. A method as claimed in claim 4 including providing multiple levels of encryption with different encryption keys corresponding to said multiple levels of security clearance.

6. A method as claimed in claim 4 wherein said remainder data is encrypted with said multiple levels of encryption.

7. A method as claimed in claim 6 wherein the step of reconstruction includes decrypting one or both of said extracted data and remainder data with respect to one of more of said multiple levels of encryption based upon one or more of said multiple levels of security clearance.

8. A method of securing input data having security sensitive content, represented by one or more security sensitive words, characters, images, data elements or data objects therein, the method of securing data deployed in a client-server computer system with at least one server computer operatively coupled to at least one client computer over a communications network, said client computer having a decryption routine, the method comprising:

extracting said security sensitive content from said input data to obtain a plurality of extract data grouped into different security levels;

encrypting said extracted data for each said security level and one of appending, adding or inserting said encrypted extracted data with remainder input data to form a composite; and

transmitting said composite to said at least one client computer.

9. A method as claimed in claim 8 wherein said one client computer is one of a plurality of client computers and the method includes, at one of said client computers, displaying said security sensitive content in a distinguishing manner prior to extracting.

10. A method as claimed in claim 9 including, at one of said client computers, permitting one of user selection and user confirmation of said security sensitive content prior to extracting.

11. A method as claimed in claim 8 including providing multiple levels of encryption and corresponding multiple levels of security clearance.

12. A method as claimed in claim 8 including providing multiple levels, types or keys for encryption for said different levels of security clearance.

13. A method as claimed in claim 11 wherein said remainder data is encrypted with said multiple levels of encryption.

14. A method as claimed in claim 8 wherein said extracting said security sensitive content and encrypting said extracted data and transmitting said composite to said at least one client computer occurs at said server computer.

15. A method as claimed in claim 8 wherein said one client computer is one of a plurality of client computers and the method includes said extracting said security sensitive content and encrypting said extracted data occurs at one of said client computers, and transmitting said composite to another client computer occurs via said server computer.

16. A computer readable medium containing programming instructions for a method of securing input data having security sensitive content, represented by one or more security sensitive words, characters, images, data elements or data objects therein, comprising:

extracting said security sensitive content from said input data to obtain a plurality of extract data grouped into different security levels;

encrypting said extracted data for each said security level and one of appending, adding or inserting said encrypted extracted data with remainder input data to form a composite;

responsive to a data request, reconstructing fully or partially said input data from said composite with decryption of said extracted data only in the presence of a respective predetermined security clearance, required for each said security level.

17. A computer readable medium containing programming instructions for the method as claimed in claim 16 including displaying said security sensitive content in a distinguishing manner prior to extracting.

18. A computer readable medium containing programming instructions for the method as claimed in claim 17 including permitting one of user selection and user confirmation of said security sensitive content.

19. A computer readable medium containing programming instructions for the method as claimed in claim 16 including providing multiple levels of encryption and corresponding multiple levels of security clearance.

20. A computer readable medium containing programming instructions for the method as claimed in claim 19 including providing multiple levels of encryption with different encryption keys corresponding to said multiple levels of security clearance.

21. A computer readable medium containing programming instructions for the method as claimed in claim 19 wherein said remainder data is encrypted with said multiple levels of encryption.

22. A computer readable medium containing programming instructions for the method as claimed in claim 21 wherein the step of reconstruction includes decrypting one or both of said extracted data and remainder data with respect to one or more of said multiple levels of encryption based upon one or more of said multiple levels of security clearance.

23. A computer readable medium containing programming instructions for a method of securing input data having security sensitive content, represented by one or more security sensitive words, characters, images, data elements or data objects therein, the method of securing data deployed in a client-server computer system with at least one server computer operatively coupled to at least one client computer over a communications network, said client computer having a decryption routine, the programming instructions comprising:

extracting said security sensitive content from said input data to obtain a plurality of extract data grouped into different security levels;

encrypting said extracted data for each said security level and one of appending, adding or inserting said encrypted extracted data with remainder input data to form a composite; and

transmitting said composite to said at least one client computer.

24. A computer readable medium containing programming instructions for a method as claimed in claim 23 operable wherein said one client computer is one of a plurality of client computers and the programming instructions include, at one of said client computers, displaying said security sensitive content in a distinguishing manner prior to extracting.

25. A computer readable medium containing programming instructions for a method as claimed in claim 24 operable wherein, at one of said client computers, permitting one of user selection and user confirmation of said security sensitive content prior to extracting.

26. A computer readable medium containing programming instructions for a method as claimed in claim 23 including providing multiple levels of encryption and corresponding multiple levels of security clearance.

27. A computer readable medium containing programming instructions for a method as claimed in claim 23 including providing multiple levels, types or keys for encryption for said different levels of security clearance.

28. A computer readable medium containing programming instructions for a method as claimed in claim 26 wherein said remainder data is encrypted with said multiple levels of encryption.

29. A computer readable medium containing programming instructions for a method as claimed in claim 23 wherein said extracting said security sensitive content and encrypting said extracted data and transmitting said composite to said at least one client computer occurs at said server computer.

30. A computer readable medium containing programming instructions for a method as claimed in claim 23 operable wherein said one client computer is one of a plurality of client computers and the programming instructions include extracting said security sensitive content and encrypting said extracted data at one of said client computers, and transmitting said composite to another client computer occurs via said server computer.

31. A method of securing input data passing through a browser, said input data having security sensitive content, represented by one or more security sensitive words, characters, images, data elements or data objects therein, the method deployed in a distributed computer system with a plurality of extract stores, each having a security level and a clearance therefor, comprising:

extracting said security sensitive content from said input data to obtain extracted data for respective security levels;

facilitating the storage of said extracted data in respective ones of said extract stores; and

forwarding any remainder input data to a target destination in said distributed computer system and requiring predetermined security clearances to access said extract stores.

32. A method as claimed in claim 31 including filtering said data while extracting.

33. A method as claimed in claim 32 including defining the filter with a group of security sensitive content and the method includes one of storing said filter or destroying said filter after storing said extracted data.

34. A method as claimed in claim 33 including encrypting one or both of said extracted data and said remainder data.

35. A method as claimed in claim 31 wherein the extracting step operates on credit data, financial data or account data.

36. A computer readable medium containing programming instructions for securing input data passing through a browser, said input data having security sensitive content, represented by one or more security sensitive words, characters, images, data elements or data objects therein, the programming instructions operably deployed in a distributed computer system with a plurality of extract stores, each having a security level and a clearance therefor, comprising:

extracting said security sensitive content from said input data to obtain extracted data for respective security levels;

facilitating the storage of said extracted data in respective ones of said extract stores; and

forwarding any remainder input data to a target destination in said distributed computer system and requiring predetermined security clearances to access said extract stores.

37. A computer readable medium containing programming instructions for securing input data as claimed in claim 36 including filtering said data while extracting.

38. A computer readable medium containing programming instructions for securing input data as claimed in claim 37 including defining the filter with a group of security sensitive content and the programming instructions include one of storing said filter or destroying said filter after storing said extracted data.

39. A computer readable medium containing programming instructions for securing input data as claimed in claim 38 including encrypting one or both of said extracted data and said remainder data.

40. A computer readable medium containing programming instructions for securing input data as claimed in claim 36 wherein the extracting step operates on credit data, financial data or account data.

41. A computer readable medium containing programming instructions for securing data passing through a browser, said data having one or more security sensitive words, characters or icons, used in conjunction with a distributed computer system with a plurality of remote memories respectively designated as corresponding extract stores, each having a respective security level and clearance, comprising:

extracting said security sensitive words, characters or icons from said data to obtain extracted data for respective security levels and remainder data therefrom;

facilitating the storage of said extracted data in respective ones of said extract stores; and

forwarding said remainder data to a targeted destination in said distributed computer system and requiring a respective predetermined security clearance for access to corresponding extract stores.

42. A medium with programming instructions as claimed in claim 41 including filtering said data while extracting.

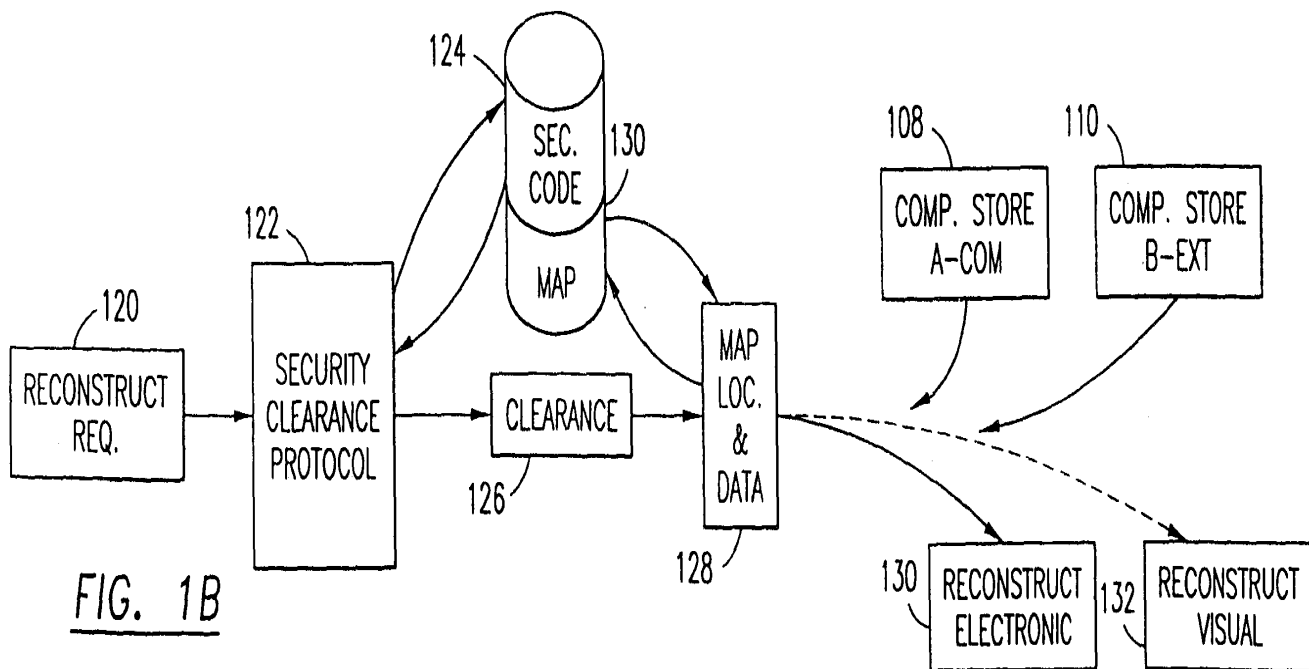
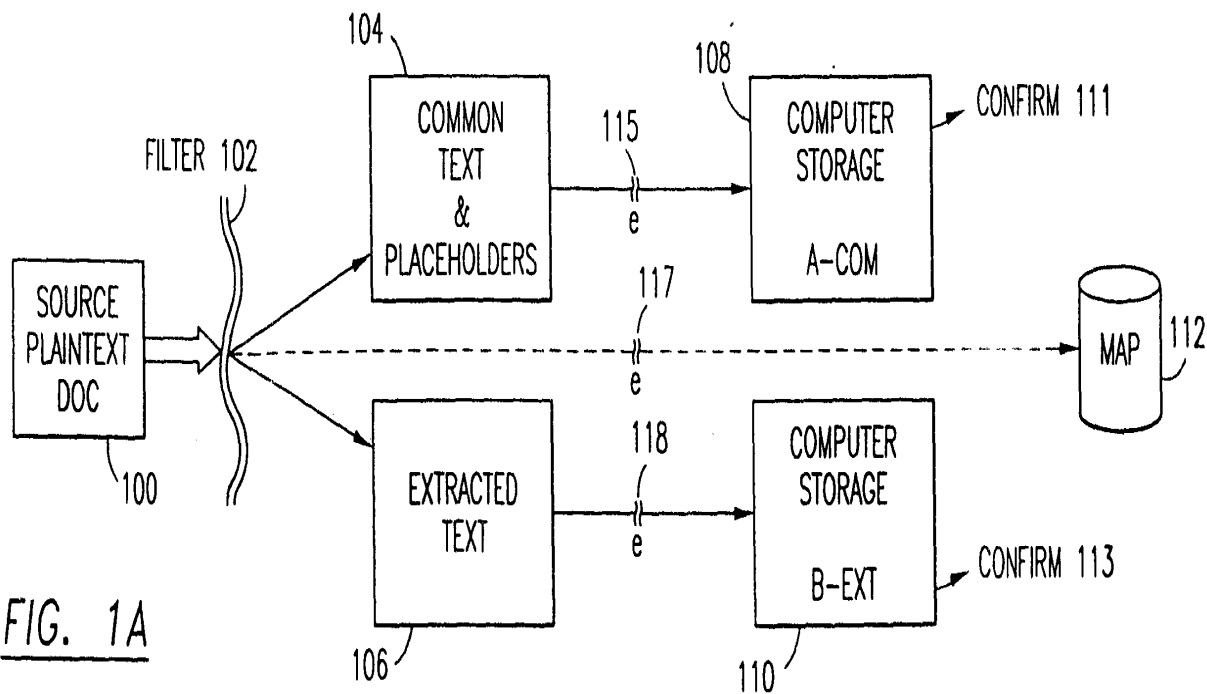
43. A medium with programming instructions as claimed in claim 42 including defining the filter with a group of security sensitive words, characters or icons and the method includes one of storing said filter or destroying said filter after storing said extracted data.

44. A medium with programming instructions as claimed in claim 43 including encrypting one or both of said extracted data and said remainder data.

ABSTRACT

Data security for processing data or securing browser-input data operates on security sensitive content which is extracted, then either encrypted or stored in remote extract stores, and processed separate from remainder data. Extracted data, in one system, is remotely stored. Other methods attach, append, add or insert an encrypted version of the extract content to the document. The browser system operates with an extract store. Remainder data is sent to the addressee or designated client by the web server. The addressee is permitted to retrieve the extracted data from said extract store only with a security clearance and hence, reconstruct the source input data with the extract data. In other systems, the addressee reconstructs the input by decryption and integration. The browser method extracts data, facilitates the storage, forwards the remainder data to a target. Financial data or credit card scrubber may use pop-up windows for enablement.

\\TIGER\Data Share\RCK\CLIENTS\Redlich\Patents\6851-02-cip-4con-pa.wpd



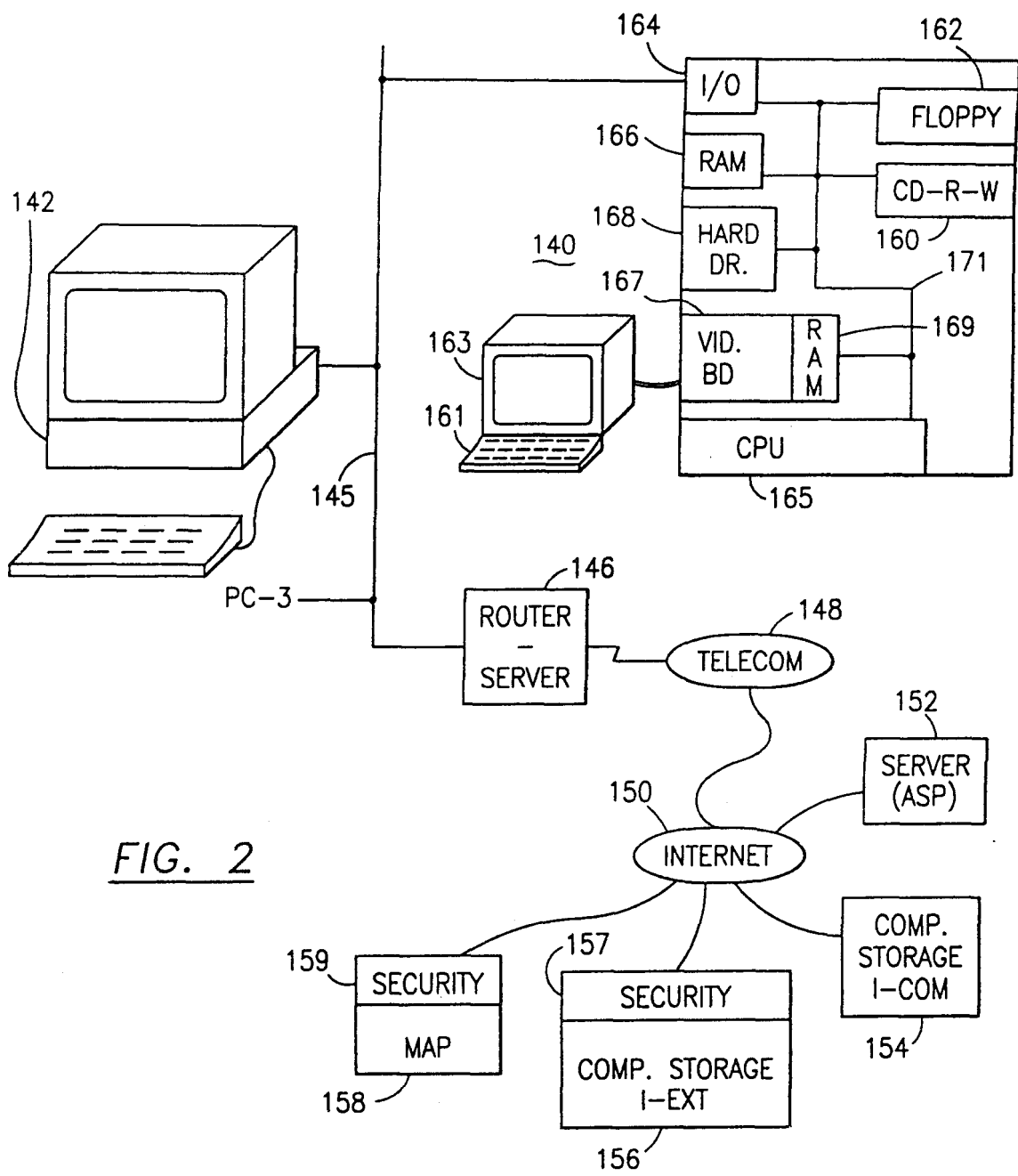


FIG. 2

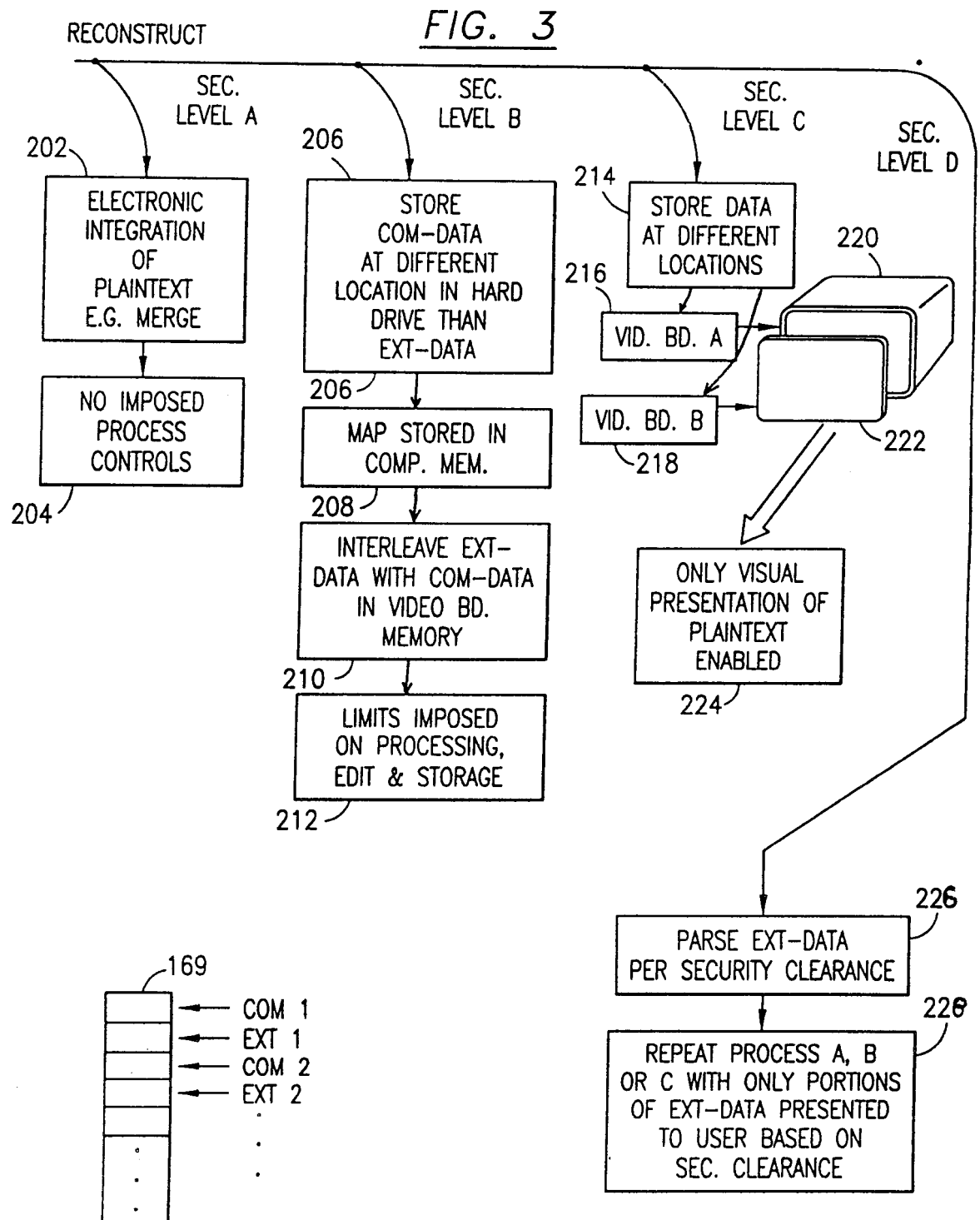
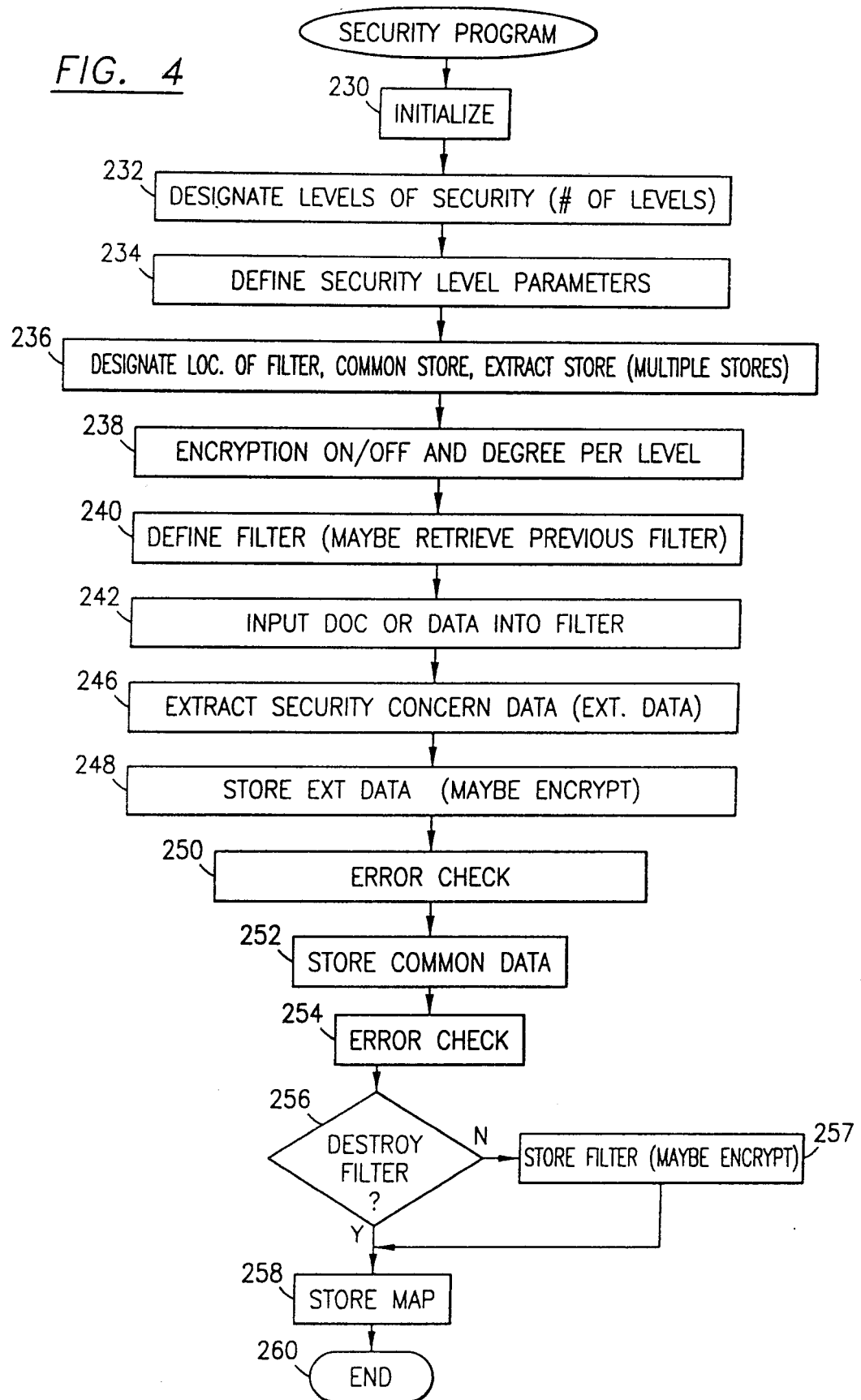
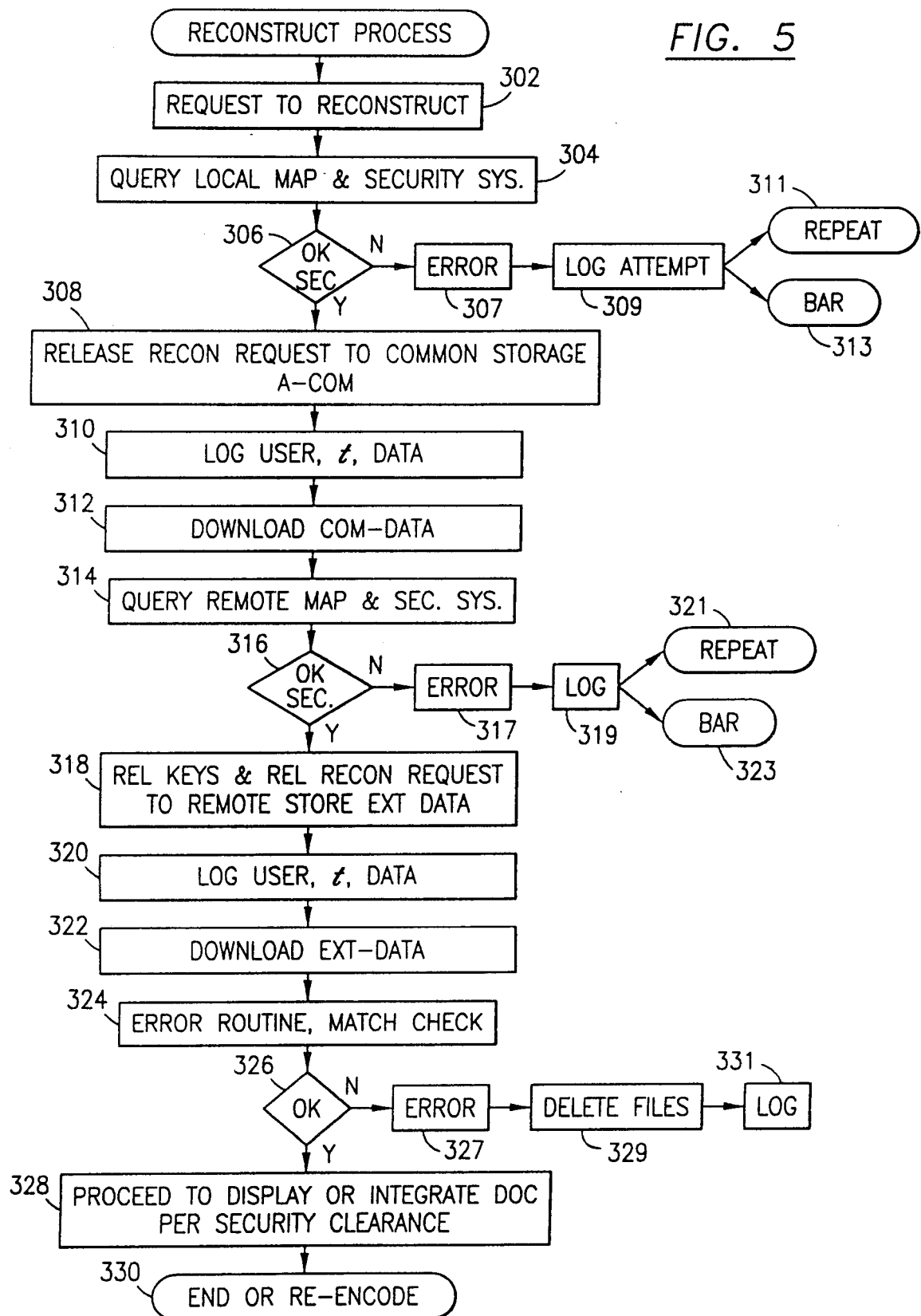


FIG. 4





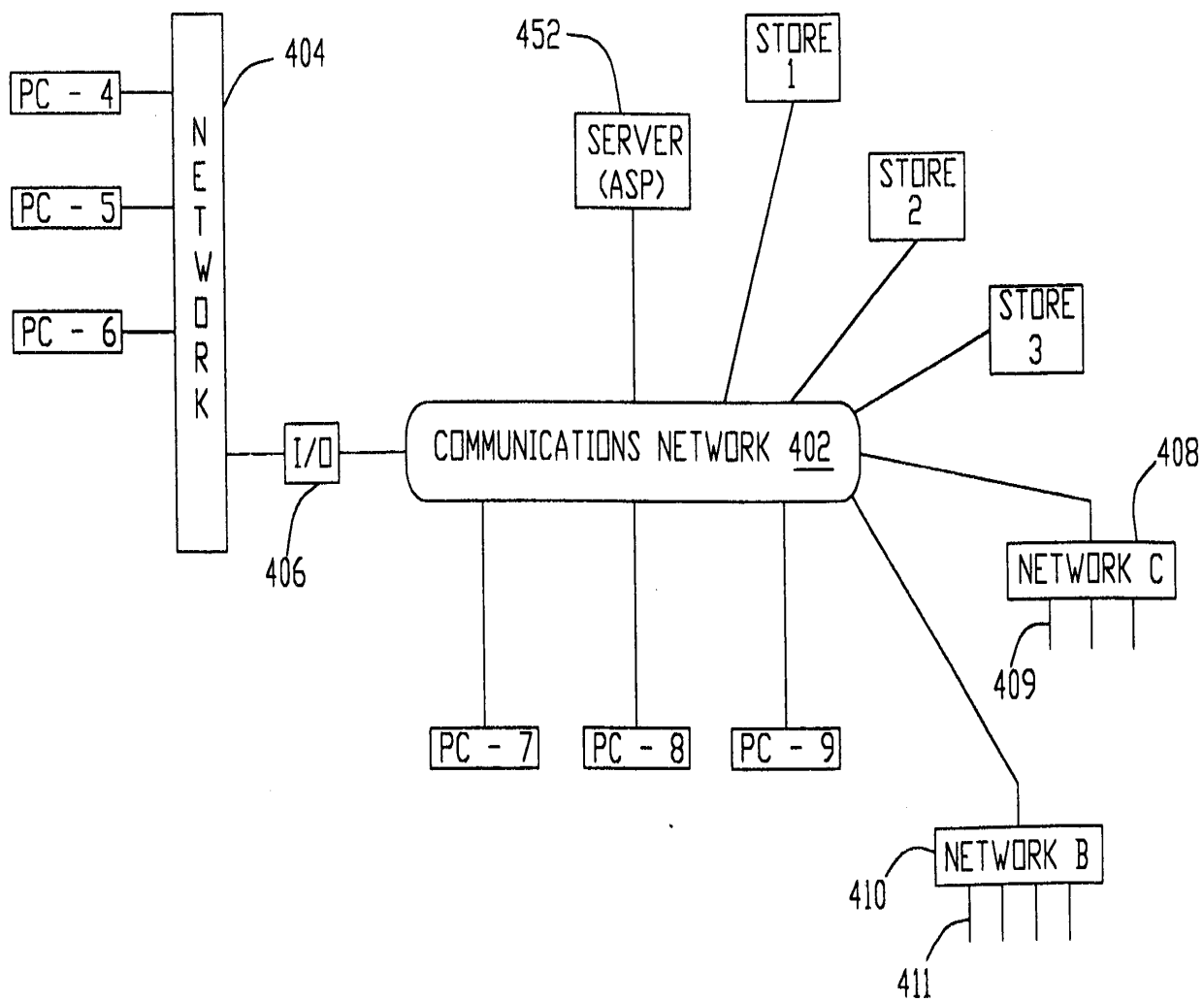


FIG.6

FIG. 7

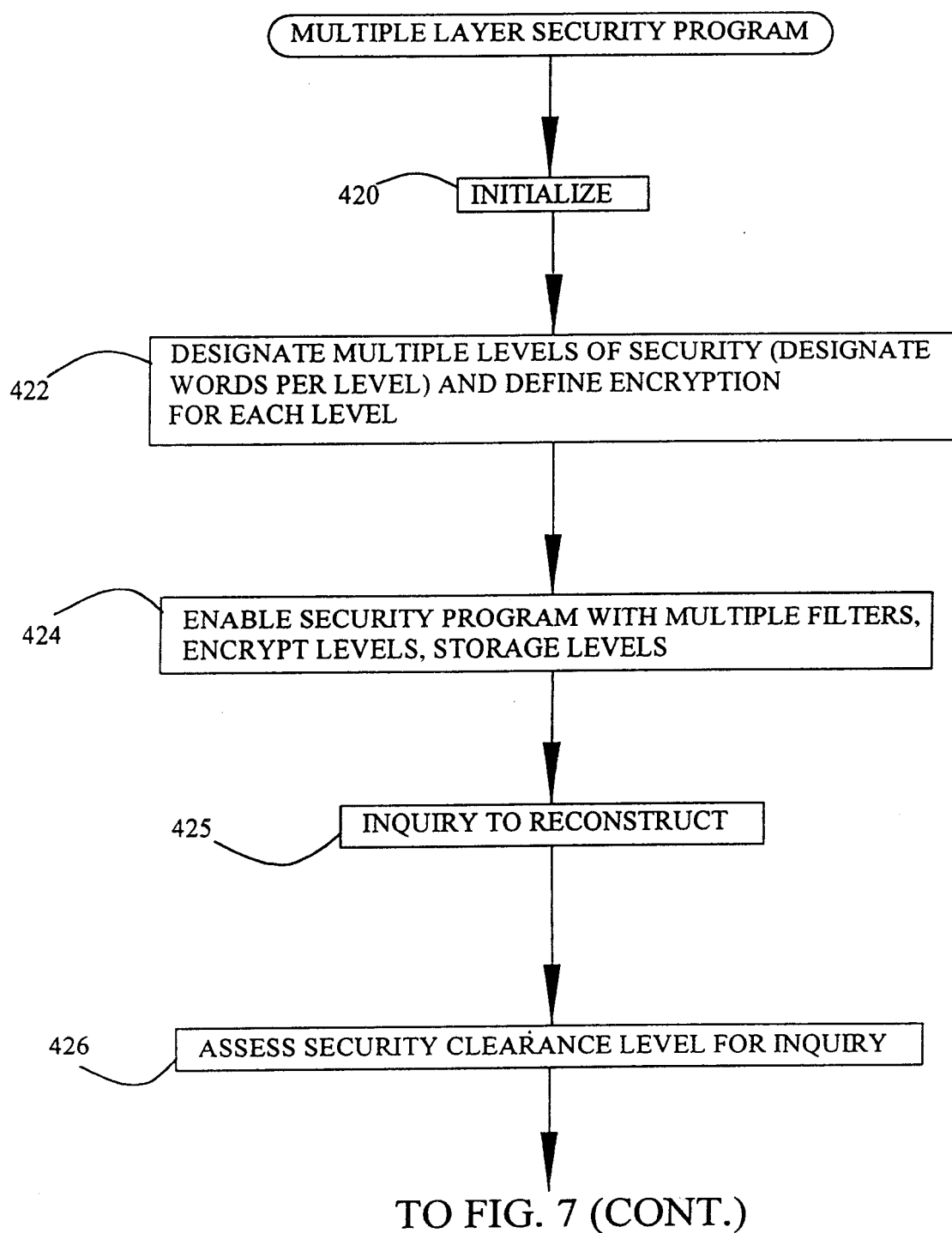


FIG. 7 (CONT.)

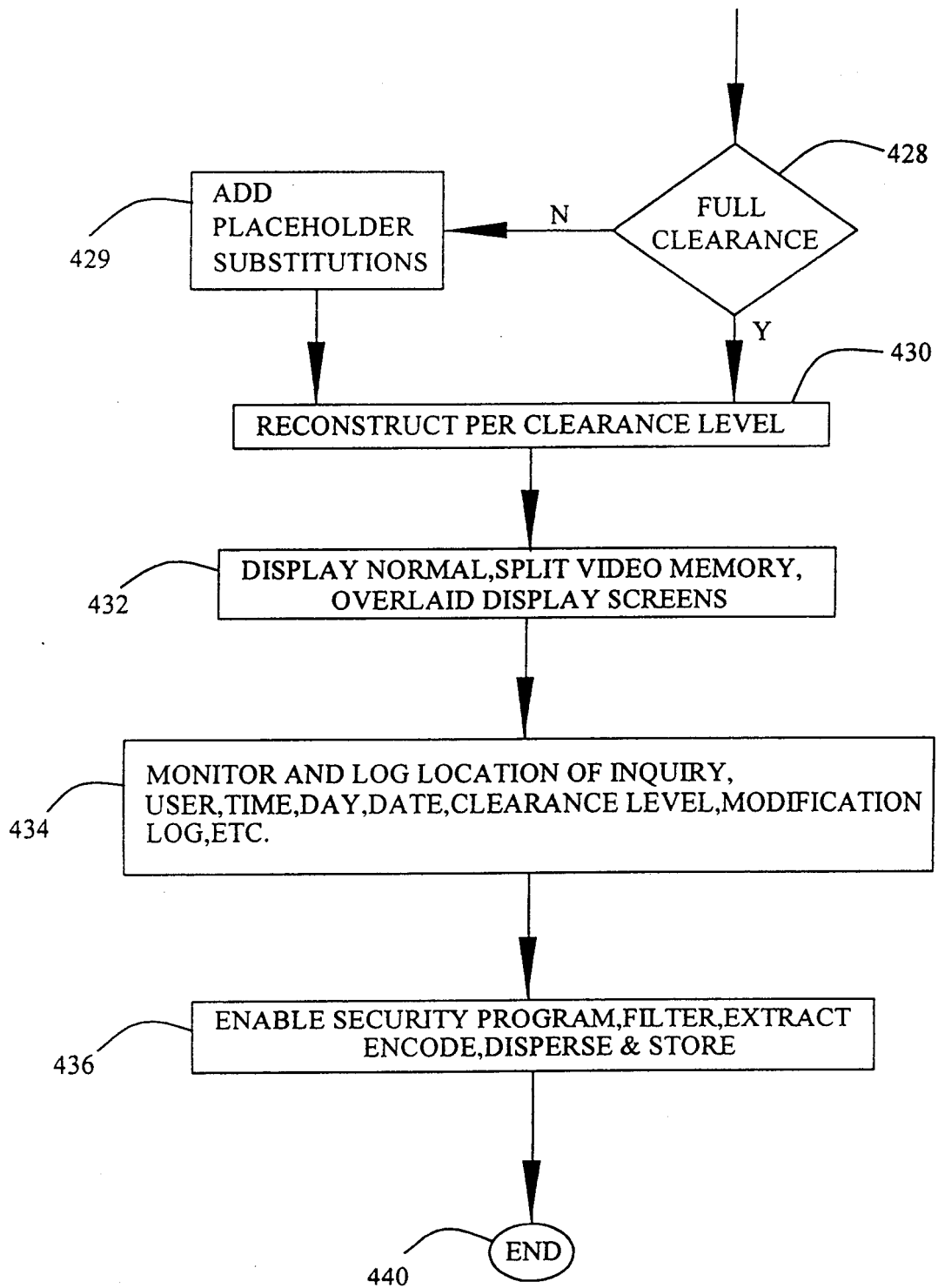


FIG. 8

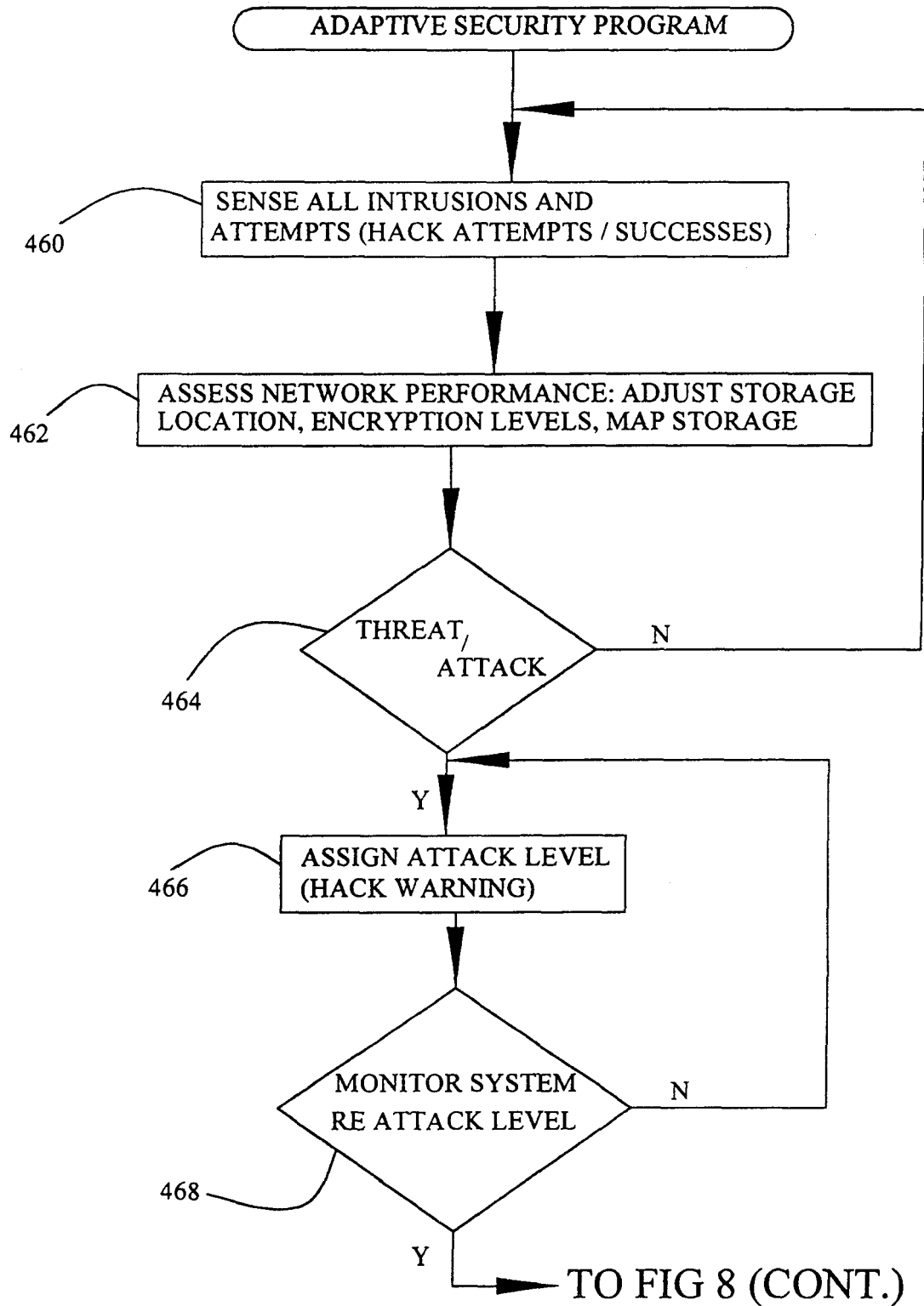


FIG. 8 (CONT.)

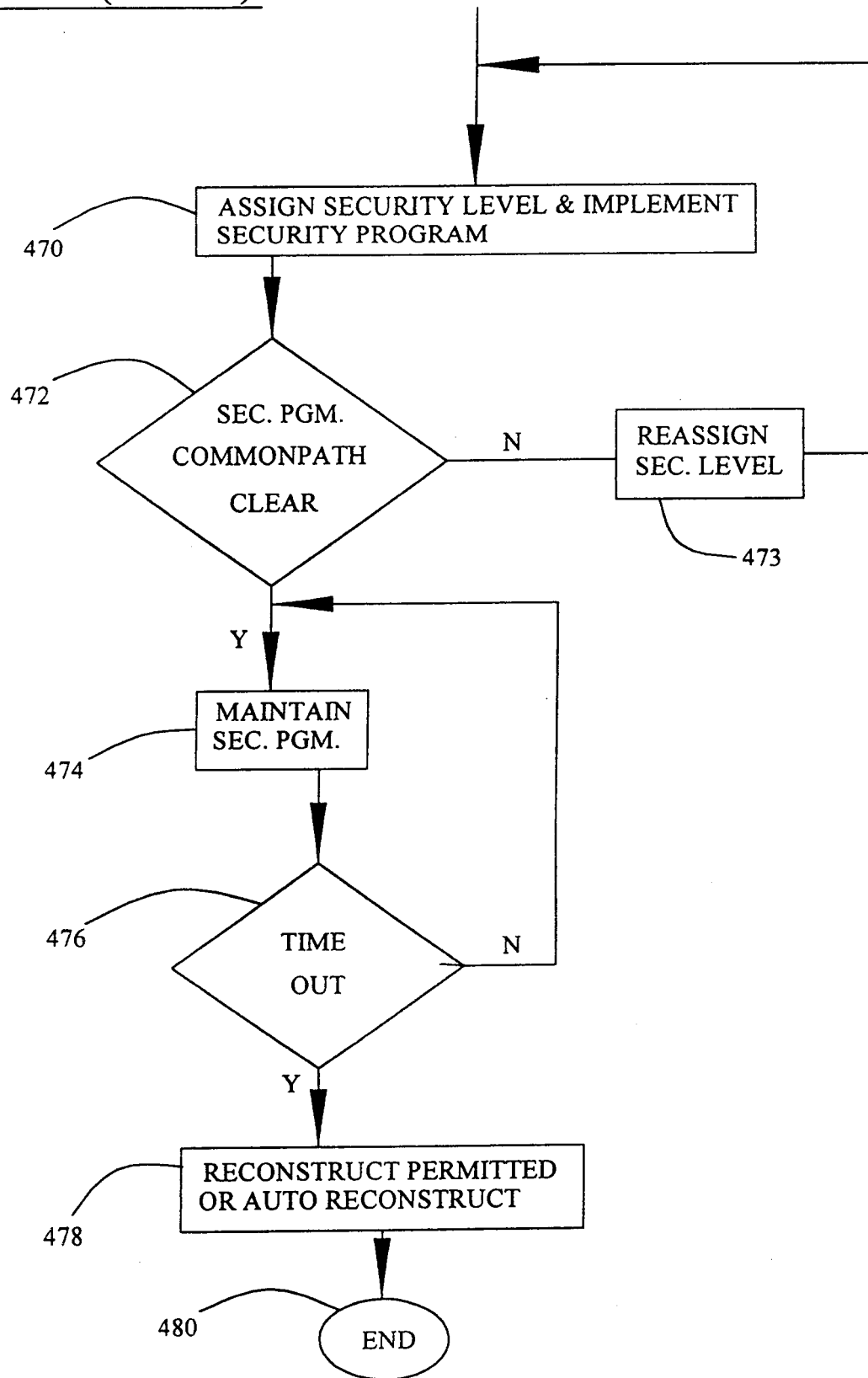


FIG. 9

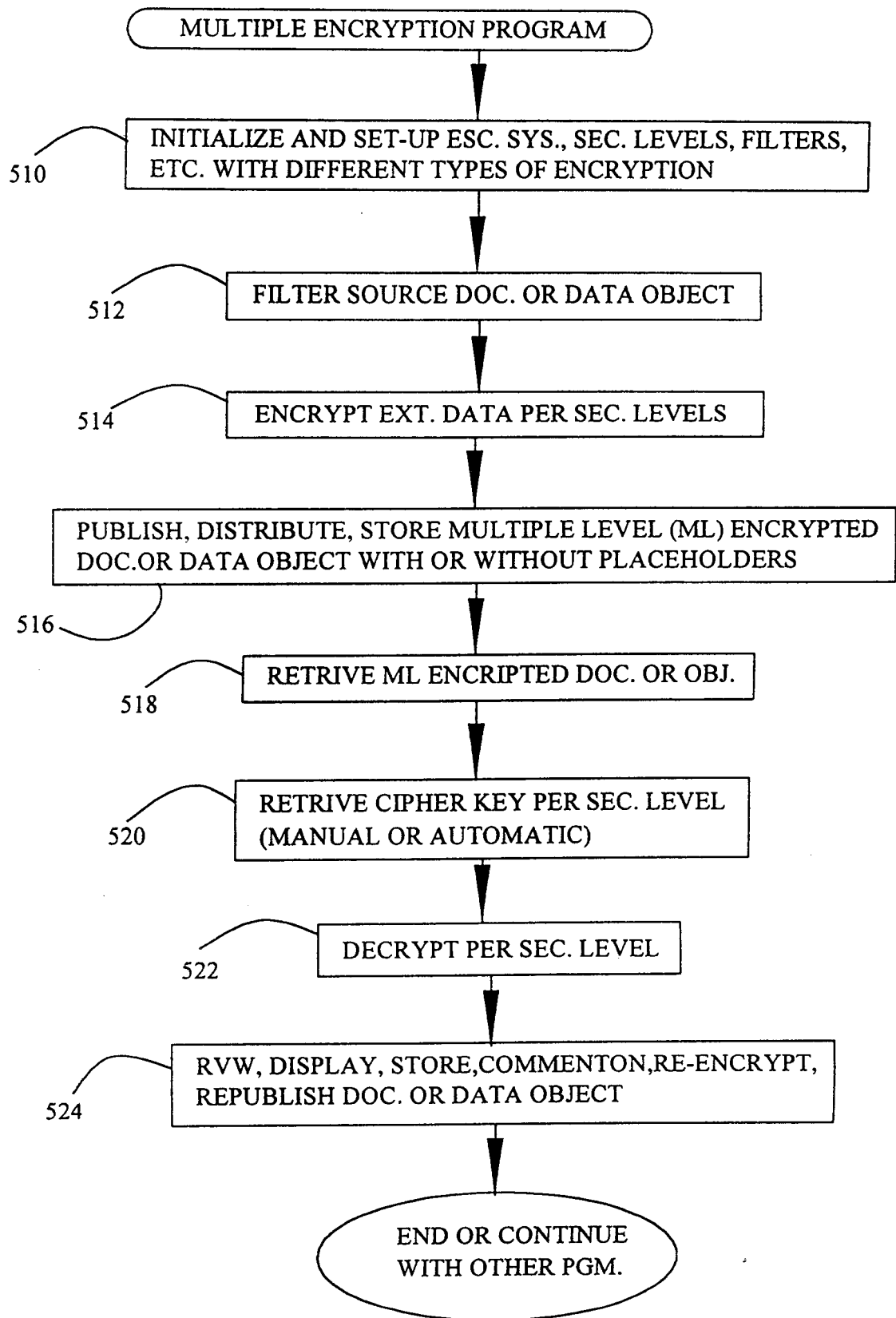
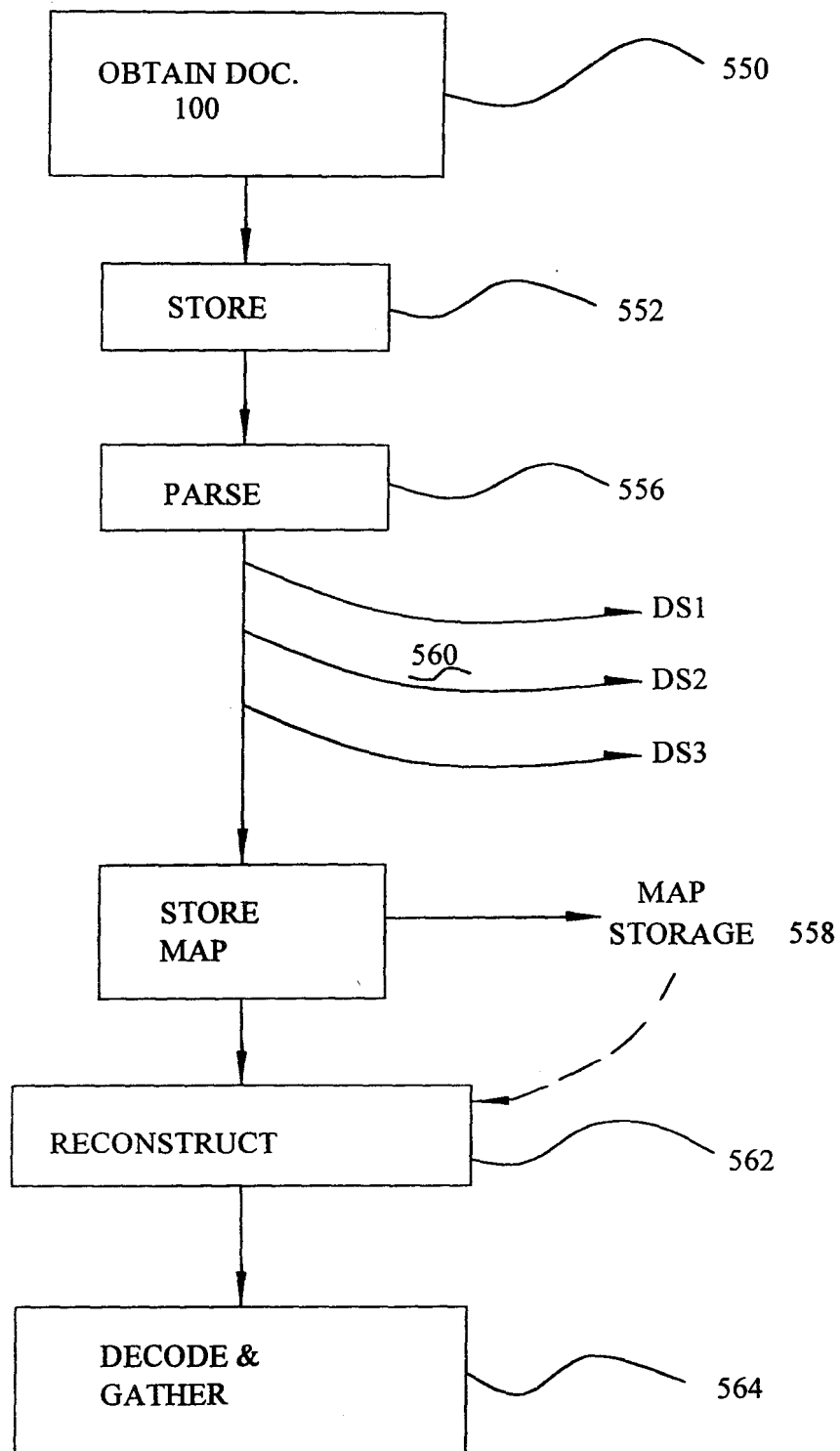


FIG. 10



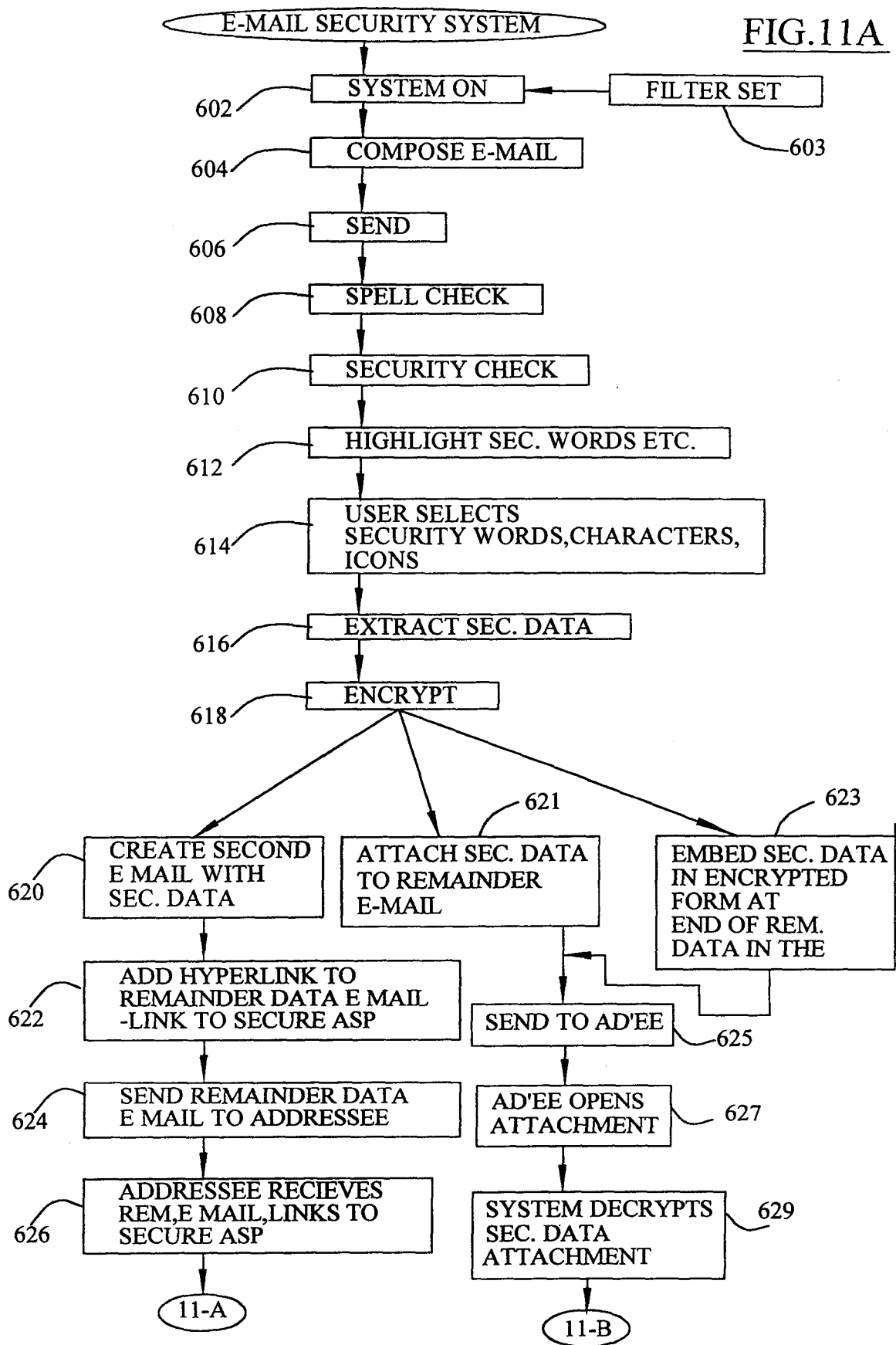


FIG.11B

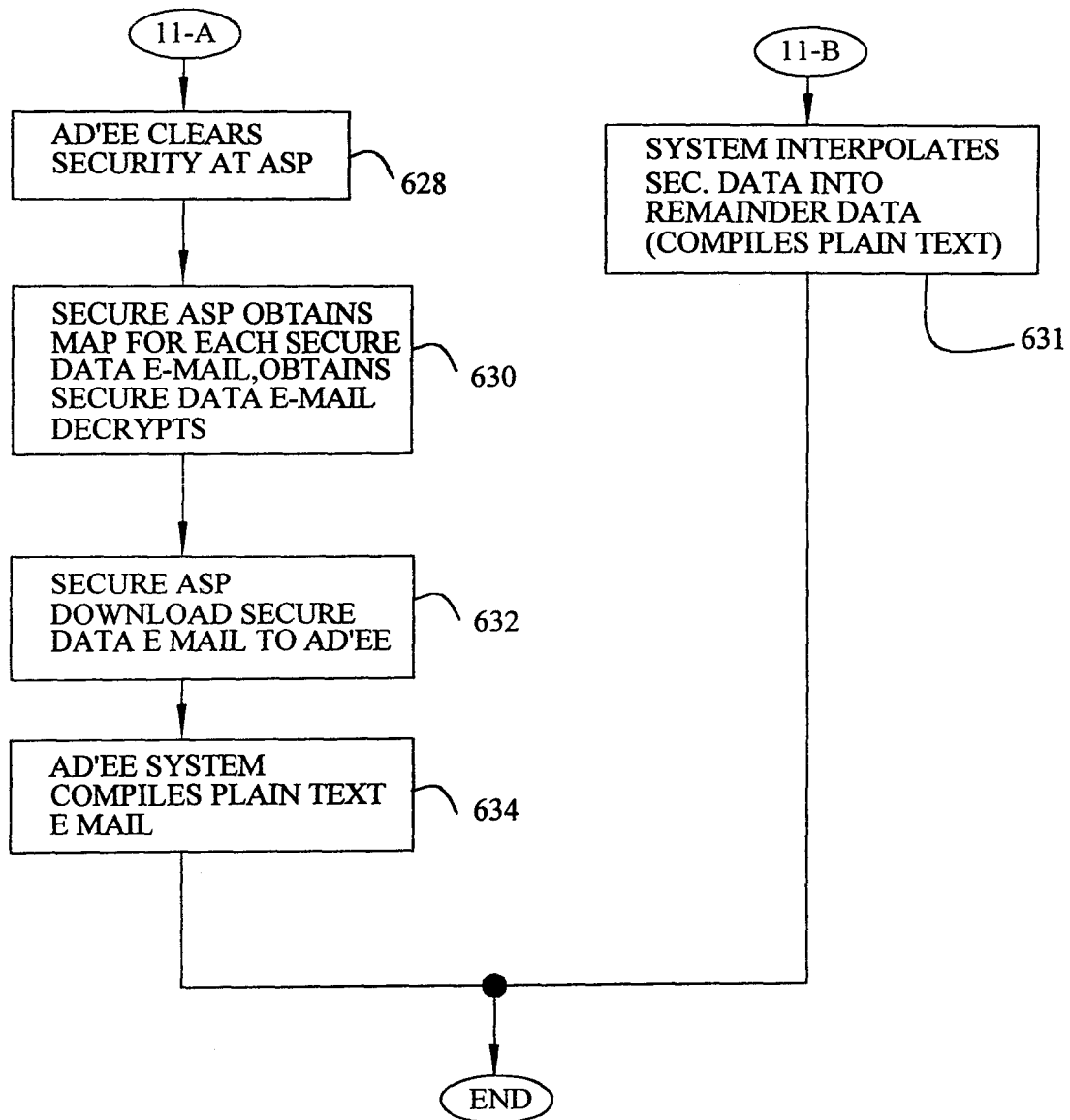


FIG.12A

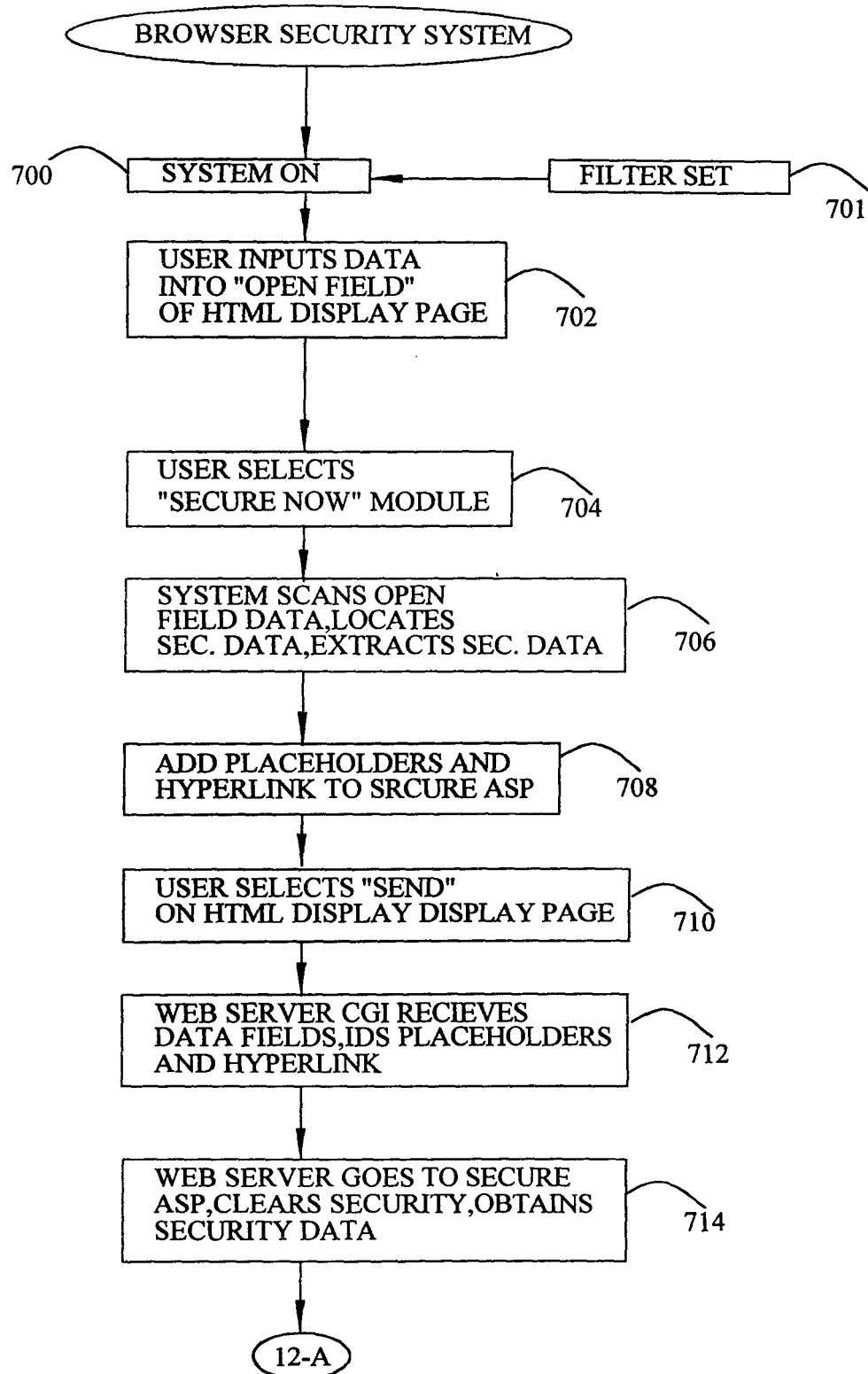
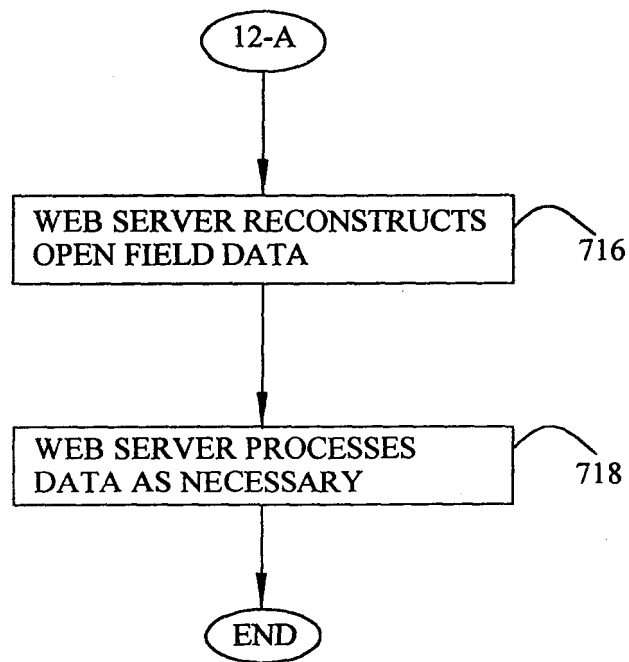
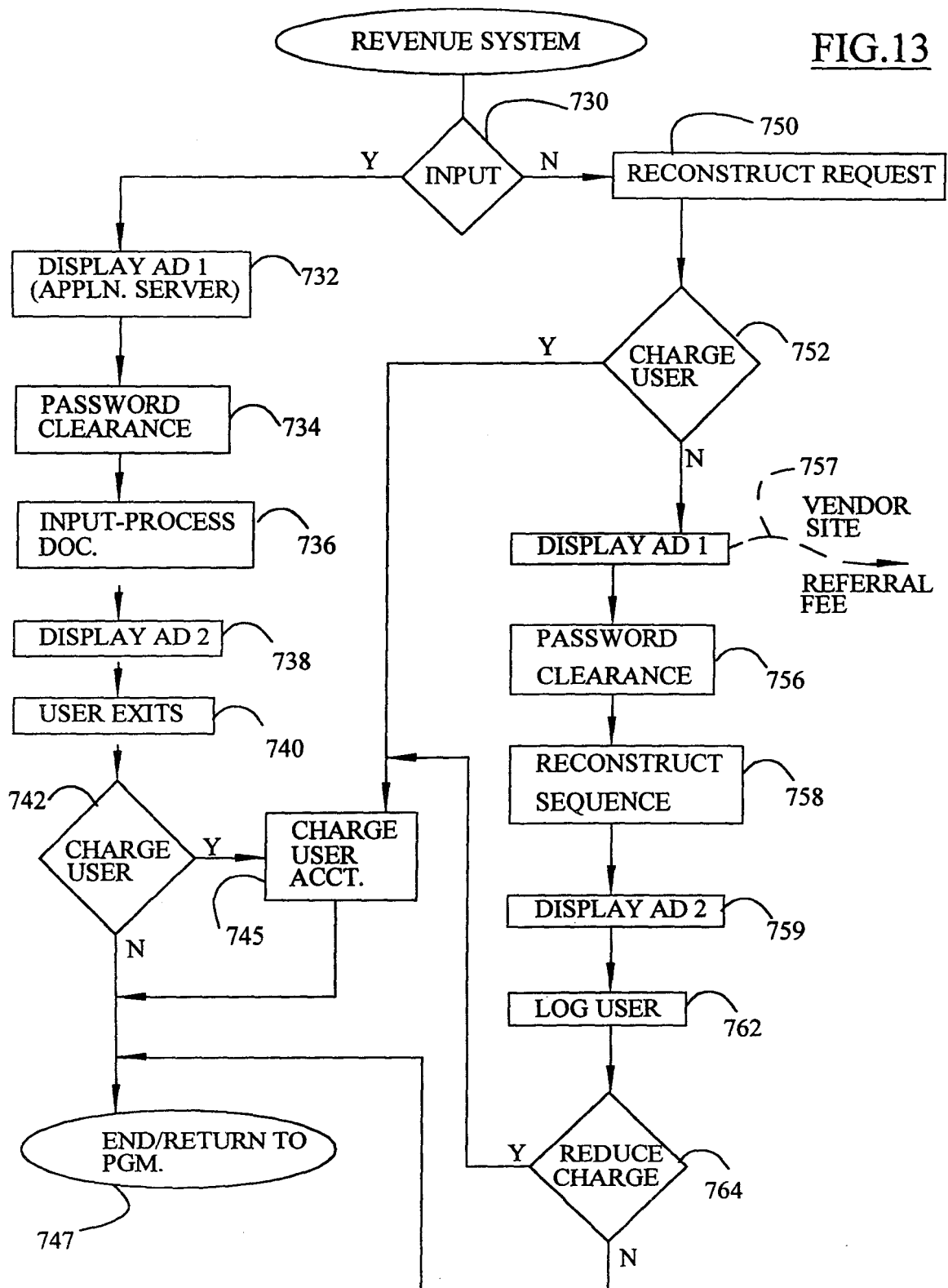


FIG.12B





DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled Data Security System and Method Adjunct to E-mail, Browser or Telecom Program the specification of which

(check one) ☐ is attached hereto.

☒ was filed on May 23, 2002

as Application Serial No. 10/155,525

and was amended on February 22, 2006
(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 (a-d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below any foreign application for patent or inventor's certificate, or any PCT international application having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)

Priority Claimed

<u> </u> (Number)	<u> </u> (Country)	<u> </u> (Day/Month/Year Filed)	☐ Yes	☐ No
<u> </u> (Number)	<u> </u> (Country)	<u> </u> (Day/Month/Year Filed)	☐ Yes	☐ No

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

<u>09/916,397</u> (Application Serial No.)	<u>07/27/01</u> (Filing Date)	<u>pending</u> (Status) (patented, pending, abandoned)
<u>10/008,209</u> (Application Serial No.)	<u>12/6/01</u> (Filing Date)	<u>pending</u> (Status)
<u>10/008,218</u> (Application Serial No.)	<u>12/6/01</u> (Filing Date)	<u>pending</u> (Status) (patented, pending, abandoned)

I hereby claim the benefit under Title 35, United States Code, §119(e) of any United States provisional application(s) listed below:

60/260,398, filed Jan. 9, 2001 60/287,813, filed May 2, 2001 60/267,944, filed February 12, 2001
(Provisional Application No.) (Provisional Application No.) (Provisional Application No.)

60/247,242, filed November 12, 2000 60/247,232, filed November 13, 2000
(Provisional Application No.) (Provisional Application No.)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

Robert C. Kain, Jr., Reg. No. 30,648; Martin Fleit, Reg. No. 16,900; Jon A. Gibbons, Reg. No. 37,333; Jose Gutman, Reg. No. 35,171; and Steve Bongini, Reg. No. 40,917; Paul D. Bianco, Reg. No. 43,500.

Send Correspondence to: Robert C. Kain, Jr., **Customer Number 004897**
Fleit, Kain, Gibbons, Gutman & Bongini, P.L.
750 Southeast Third Avenue, Suite 100
Ft. Lauderdale, Florida 33316-1153
Direct Telephone Calls to: Robert C. Kain, Jr., (954) 768-9002

Ron M. Redlich

Full name of sole or first inventor


Inventor's signature

07-03-2006
Date

Miami Beach, FL

Residence

U.S.

Citizenship

4201 Collins Avenue, Apt. 2103

Post Office Address

Miami Beach, FL 33140

Martin A. Nemzow

Full name of second joint inventor, if any


Inventor's signature

07-03-2006
Date

Miami Beach, FL

Residence

U.S.

Citizenship

2915 Flamingo Drive

Post Office Address

Miami Beach, FL 33140

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Ron M. Redlich, et al.

Serial No.:

Filed: Herewith

Confirmation No.:

For: Data Security System and Method Adjunct to E-mail, Browser, Telecom or Encryption Program

TRANSMITTAL

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

I HEREBY CERTIFY that the below listed documents are being electronically filed on March 7, 2007 in the Patent and Trademark Office.

- X Patent application (spec.88 pgs., pp. 1-88; claims 44, 9 pgs., pp 89-97; abst. 1 pg., p. 98.)
- X Seventeen (17) sheets drawings - formal
- X Declaration and Power of Attorney for Patent Application (2 pgs.)
- X Please charge Deposit Account No. 03-1231 in the amount of \$1,425.00
- X Please charge any underpayments or credit any overpayments to Deposit Account No. 03-1231.

Respectfully submitted,

By /Robert C. Kain, Jr./

Robert C. Kain, Jr.

Reg. No. 30,648

FLEIT, KAIN, GIBBONS, GUTMAN, BONGINI & BIANCO, P.L.

750 S.E. Third Avenue, Suite 100

Ft. Lauderdale, Florida 33316-1153

Telephone: (954) 768-9002

Facsimile: (954) 768-0158

Electronic Patent Application Fee Transmittal

Application Number:				
Filing Date:				
Title of Invention:	Data Security System and Method Adjunct to E-mail, Browser, Telecom or Encryption Program			
First Named Inventor/Applicant Name:	Ron M. Redlich			
Filer:	Robert C. Kain			
Attorney Docket Number:	6851-02-cip4-con			
Filed as Small Entity				
Utility Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	75	75
Utility Search Fee	2111	1	250	250
Utility Examination Fee	2311	1	100	100
Pages:				
Claims:				
Claims in excess of 20	2202	24	25	600
Independent claims in excess of 3	2201	4	100	400
Miscellaneous-Filing:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				1425

Electronic Acknowledgement Receipt

EFS ID:	1571012
Application Number:	11682941
International Application Number:	
Confirmation Number:	9976
Title of Invention:	Data Security System and Method Adjunct to E-mail, Browser, Telecom or Encryption Program
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	04897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-02-cip4-con
Receipt Date:	07-MAR-2007
Filing Date:	
Time Stamp:	11:21:06
Application Type:	Utility

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	\$ 1425
RAM confirmation Number	1566
Deposit Account	031231
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 and 1.17	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part /.zip	Pages (if appl.)
1	Specification	6851-02-cip4-con-pa-spec.pdf	177367	no	88
Warnings:					
Information:					
2	Claims	6851-02-cip4-con-pa-clms.pdf	26684	no	9
Warnings:					
Information:					
3	Abstract	6851-02-cip4-con-pa-abstrc.pdf	16703	no	1
Warnings:					
Information:					
4	Drawings	6851-02-cip4-con-drawings.pdf	317437	no	17
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
5	Oath or Declaration filed	6851-02-cip4-con-Dec-ss-070306.pdf	93187	no	2
Warnings:					
Information:					
6	Miscellaneous Incoming Letter	6851-02-cip4-con-pa-transmittal-elec-filing-030707.pdf	21255	no	1
Warnings:					
Information:					
7	Fee Worksheet (PTO-06)	fee-info.pdf	8588	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			661221		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronic Acknowledgement Receipt

EFS ID:	1571012
Application Number:	11682941
International Application Number:	
Confirmation Number:	9976
Title of Invention:	Data Security System and Method Adjunct to E-mail, Browser, Telecom or Encryption Program
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	04897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-02-cip4-con
Receipt Date:	07-MAR-2007
Filing Date:	
Time Stamp:	11:21:06
Application Type:	Utility

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	\$ 1425
RAM confirmation Number	1566
Deposit Account	031231
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 and 1.17	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part /.zip	Pages (if appl.)
1	Specification	6851-02-cip4-con-pa-spec.pdf	177367	no	88
Warnings:					
Information:					
2	Claims	6851-02-cip4-con-pa-clms.pdf	26684	no	9
Warnings:					
Information:					
3	Abstract	6851-02-cip4-con-pa-abstrc.pdf	16703	no	1
Warnings:					
Information:					
4	Drawings	6851-02-cip4-con-drawings.pdf	317437	no	17
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
5	Oath or Declaration filed	6851-02-cip4-con-Dec-ss-070306.pdf	93187	no	2
Warnings:					
Information:					
6	Miscellaneous Incoming Letter	6851-02-cip4-con-pa-transmittal-elec-filing-030707.pdf	21255	no	1
Warnings:					
Information:					
7	Fee Worksheet (PTO-06)	fee-info.pdf	8588	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			661221		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 11/682,941

Confirmation No.: 9976

Filed: March 7, 2007

For: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program

INFORMATION DISCLOSURE STATEMENT

Mail Stop IDS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

As a means of complying with the duty of disclosure set forth in 37 C.F.R. §1.56, applicant, through the undersigned attorney, files this Information Disclosure Statement pursuant to 37 C.F.R. §1.97.

Notice of Related Cases

<u>Our Ref.</u>	<u>Reg./Serial No.</u>	<u>Filed/Registered</u>
Redlich	7,146,644	Dec. 6, 2006
Redlich	7,140,044	Nov. 21, 2006
Redlich	7,103,915	Sept. 5, 2006
-02-div1	11/465,309	Aug. 17, 2006
-02-div2	11/465,350	Aug. 17, 2006
-02-con	11/465,388	Aug. 17, 2006
-02-cip4	10/155,525	May 23, 2002

-02-cip5	10/390,807	March 19, 2004
-02-cip6	10/277,196	Dec. 31, 2002
-02-cip7	10/998,366	Nov. 26, 2003
-02-cip8	10/998,365	Nov. 26, 2004
-02-cip9	10/998,363	Nov. 26, 2004
-03	10/396,088	Mar. 25, 2003
-07	11/614,186	Dec. 21, 2006

IDS References

Patent No.	Inventor	Issue Date
5,941,944	Messerly	Aug. 24, 1999
6,505,150	Nunberg et al.	Jan. 7, 2003
6,594,654	Salam et al.	Jul. 15, 2003
6,999,959	Lawrence et al.	Feb. 14, 2006
7,031,961	Pitkow et al.	Apr. 18, 2006
7,120,625	Kagimasa et al.	Oct. 10, 2006
6,978,262	Tsai	Dec. 20, 2005
7,007,008	Goel et al.	Feb. 28, 2006
7,043,492	Neal et al.	May 9, 2006
7,085,766	Keith, Jr.	Aug. 1, 2006
7,113,954	Vogel	Sep. 26, 2006
6,192,472	Garay et al.	Feb. 20, 2001
6,148,342	Ho	Nov. 14, 2000
6,094,483	Fidrich et al.	Jul. 25, 2000
6,055,544	DeRose et al.	Apr. 25, 2000

5,996,011	Humes	Nov. 30, 1999
5,905,980	Masuichi et al.	May 18, 1999
5,832,212	Cragun et al.	Nov. 3, 1998
5,485,474	Rabin	Jan. 16, 1996
5,933,498	Schneck et al	Aug. 3, 1999
US2002/0073313	Brown et al.	Jun. 13, 2002
WO 00/75779-A2	Lambert	Dec. 14, 2000
6,925,454	Lam et al.	Aug. 2, 2005
6,874,139	Krueger et al.	Mar. 29, 2005
US2005/0288939-A1	Peled et al.	Dec. 29, 2005

-“Protecting Privacy using the Decentralized Label Model” A. Myers, Cornell Univ.
1/1/2000.

-Mimesweeper Product Data sheet, Resoft Int’l LLC., Nov. 12, 2001 re-
soft.com/product/mimeswep.

-Complete Content Security for Internet Gateways and Mail Servers, Aladdin, July
2000.

-Aladdin Product announcement for e-Safe Appliance, Aladdin Knowledge Sys.,
Ltd., Nov. 8, 2001, Aks.com/news/2001/e-safe.

-Mail Attender 4.1x product white paper by Sherpa Software, Oct., 2001.

-Ingrian i100, Content Security Appliance (2 pages)

-Element-Wise XML Encryption, Hiroshi Maruyama and Takeshi Imamura, IBM
Research, Tokyo Research Laboratory (4 pages)

-Survival Information Storage Systems by Jay J. Wylie, Michael W. Bigrigg, John
D. Strunk, Gregory R. Ganger, Han Kiliccote Pradeep K. Khosla (8 pages)

-ZD Net Interactive Week - IBS, SAP: XML to Boost Security, integration.

-Myers, A.C. "Mostly-Static Decentralized Information Flow Control" M.I.T.

Doctoral Thesis January, 1999.

-MIMESweeper-Content Security for E-mail, Web Browsing & Webmail, November
12, 2001.

The examiner in Patent No. 7,103,915 cited the following references:

U.S. Patent No. 5,960,080 to Fahlman
U.S. Patent No. 5,581,682 to Anderson
U.S. Patent No. 6,389,542 to Flyntz
U.S. Patent No. 6,602,298 to Kirshenbaum
U.S. Patent No. 6,078,907 to Lamm
U.S. Patent No. 6,598,161 to Kluttz
U.S. Patent No. 5,036,315 to Gurley
The 1996 book, Applied Cryptography, by Schneier
The Uniform Resource Locator article "FOLD OC"

The examiner in Patent No. 7,140,044 cited the following references:

U.S. Patent No. 5,960,080 to Fahlman
U.S. Patent No. 5,581,682 to Anderson
U.S. Patent No. 6,389,542 to Flyntz
U.S. Patent No. 6,078,907 to Lamm
U.S. Patent No. 6,598,161 to Kluttz
U.S. Patent No. 5,036,315 to Gurley
U.S. Patent No. 5,532,950 to Moses
The 1996 book, Applied Cryptography, by Schneier
The Uniform Resource Locator article "FOLD OC"

The examiner in Patent No. 7,146,644 cited the following references:

U.S. Patent No. 5,960,080 to Fahlman
U.S. Patent No. 5,581,682 to Anderson
U.S. Patent No. 6,389,542 to Flyntz
U.S. Patent No. 6,078,907 to Lamm
U.S. Patent No. 6,301,668 to Gleichauf
U.S. Patent No. 6,598,161 to Kluttz
U.S. Patent No. 5,036,315 to Gurley
U.S. Patent No. 5,532,950 to Moses
U.S. Patent No. 6,714,977 to Fowler
The 1996 book, Applied Cryptography, by Schneier
The Uniform Resource Locator article "FOLD OC"

Wylie "Survivable Information Storage Systems"

The examiner in Serial No. 10/155,192 cited the following references:

U.S. Patent No. 6,073,165 to Narasimhan
U.S. Patent No. 5,960,080 to Fahlman
U.S. Patent No. 6,602,298 to Kirshenbaum
U.S. Patent No. 6,487,538 to Gupta
U.S. Patent No. 6,771,290 to Hoyle
Published U.S. Application 2002/0116641 to Mastrianni

The examiner in Serial No. 10/155,525 cited the following references:

U.S. Patent No. 6,073,165 to Narasimhan
U.S. Patent No. 5,960,080 to Fahlman
U.S. Patent No. 6,602,298 to Kirshenbaum
U.S. Published Patent Application 2002/0116641 to Mastrianni
U.S. Published Patent Application 2004/0054630 to Ginter
Microsoft Word "Learning Microsoft Word 7.0"

The examiner in Serial No. 10/277,196 cited the following references:

U.S. Patent No. 5,960,080 to Fahlman
U.S. Patent No. 5,581,682 to Anderson
U.S. Patent No. 6,253,203 to O'Flaherty
U.S. Patent No. 6,598,161 to Kluttz
U.S. Patent No. 6,044,375 to Shmueli
U.S. Patent No. 6,662,189 to Oyanagi
U.S. Patent No. 5,036,315 to Gurley

This Information Disclosure Statement is filed in accordance with 37 C.F.R. §1.97, and this statement shall not be construed as a representation that a search was made, has been made, or that the information cited above is, or is considered to be, material to patentability as defined in §1.56(b), or that no other material information, as defined in 37 C.F.R. §1.56(b), exists. Translations of the pertinent portions of foreign language patents or publications listed above are supplied if existing translations are readily available to the applicant or the applicant's attorney. A concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR §1.56(c) most knowledgeable about the content of the information, of each patent, publication, or other information

listed that is not in the English language is provided either in the patent specification or in the enclosed attachment.

Respectfully submitted,

By /Robert C. Kain, Jr./

Robert C. Kain, Jr.

Reg. No. 30,648

Fleit, Kain, Gibbons, Gutman, Bongini & Bianco, P.L.

750 Southeast Third Avenue

Suite 100

Ft. Lauderdale, Florida 33316-1153

Telephone: 954-768-9002

Facsimile: 954-768-0158

\\Tiger\data share\RCK\CLIENTS\Redlich\6851-02-cip4-con-IDS.wpd

INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)	Docket Number (Optional) 6851-02-cip4-con	Application Number 11/682,941
Title: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program	Applicant(s) Ron M. Redlich, et al.	
	Filing Date 03/07/2007	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	7,103,915	9/5/2006	Redlich et al.	726	27	
	7,140,044	11/21/2006	Redlich et al.	726	27	
	7,146,644	12/5/2006	Redlich et al.	726	27	
	6,925,454	8/2/2005	Lam et al.	706	45	
	6,874,139	3/29/2005	Krueger et al.	717	127	
	US2005/0288939	12/29/2005	Peled et al.	705	1	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	-“Protecting Privacy using the Decentralized Label Model” A. Myers, Cornell Univ. 1/1/2000.	
	-Mimesweeper Product Data sheet, Resoft Int’l LLC., Nov. 12, 2001 re-soft.com/product/mimeswep.	
	-Complete Content Security for Internet Gateways and Mail Servers, Aladdin, July 2000.	
	-Aladdin Product announcement for e-Safe Appliance, Aladdin Knowledge Sys., Ltd., Nov. 8, 2001, Aks.com/news/2001/e-safe.	

EXAMINER

DATE CONSIDERED

INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>	Docket Number (Optional) 6851-02-cip4-con	Application Number 11/682,941
Title: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program	Applicant(s) Ron M. Redlich, et al.	
	Filing Date 03/07/2007	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,192,472	2/20/2001	Garay et al	713	165	
	6,148,342	11/14/2000	Ho	709	225	
	6,094,483	7/25/2000	Fridrich et al	380	28	
	6,055,544	4/25/2000	DeRose et al.	707	104	
	5,996,011	11/30/1999	Humes	709	225	
	5,905,980	5/18/1999	Masuichi et al	707	1	
	5,832,212	11/3/1998	Cragun et al	395	188.01	
	5,485,474	1/16/1996	Rabin	371	37.1	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	-Mail Attender 4.1x product white paper by Sherpa Software, Oct., 2001	
	MIMesweeper-Content Security for E-mail, Web Browsing & Webmail, November 12, 2001	

EXAMINER

DATE CONSIDERED

INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>	Docket Number (Optional) 6851-02-cip4-con	Application Number 11/682,941
Title: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program	Applicant(s) Ron M. Redlich, et al.	
	Filing Date 03/07/2007	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	5,960,080	9/28/1999	Fahlman	380	4	
	6,602,298	8/05/2003	Kirshenbaum	715	502.2	
	6,487,538	11/26/2002	Gupta	705	24	
	6,771,290	8/03/2004	Hoyle	345	745	
	US2002/0116641	8/22/2002	Mastrianni	713	201	
	US2004/0054630	3/18/2004	Ginter	705	53	
	5,933,498	8/3/1999	Schneck et al.	380	4	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	Ingrian i100, Content Security Appliance (1 pages)	
	Element-Wise XML Encryption, Hiroshi Maruyama and Takeshi Imamura, IBM Research, Tokyo Research Laboratory (4 pages)	
	Survival Information Storage Systems by Jay J. Wylie, Michael W. Brigg, John D. Strunk, Gregory R. Ganger, Han Kilocote Pradeep K. Khosla (8 pages)	
	ZD Net Interactive Week - IBS- SAP: XML to Boost Security Integration (1 page)	
	Myers, A.C. "Mostly-Static Decentralized Information Flow Control" M.I.T. Doctoral Thesis January, 1999	

EXAMINER

DATE CONSIDERED

INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)	Docket Number (Optional) 6851-02-cip4-con	Application Number 11/682,941
Title: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program	Applicant(s) Ron M. Redlich, et al.	
	Filing Date 03/07/2007	Group Art Unit

U.S. PATENT DOCUMENTS

Exami ner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,078,907	6/20/2000	Lamm	705	40	
	6,598,161	7/22/2003	Kluttz	713	166	
	5,036,315	7/30/1991	Gurley	340	721	
	5,532,950	7/02/1996	Moses	364	724.19	
	6,301,668	10/09/2001	Gleichauf	713	201	
	6,714,977	3/30/2004	Fowler	709	224	
	US2002/0073313	6/13/2002	Brown et al	713	165	
	WO 00/75779	12/14/2000	Lambert			
	5,581,682	12/3/1996	Anderson et al	395	792	
	6,389,542	5/14/2002	Flyntz	713	201	
	6,073,165	6/6/2000	Narasimhan et al	109	206	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER

DATE CONSIDERED

INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>	Docket Number (Optional) 6851-02-cip4-con	Application Number 11/682,941
Title: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program	Applicant(s)	
	Filing Date 03/07/2007	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,253,203	6/26/2001	O'Flaherty	707	9	
	6,044,375	3/28/2000	Shmueli	707	101	
	6,662,189	12/9/03	Oyanagi	707	102	
	5,941,944	08/24/1999	Messerly	709	203	
	6,505,150	01/07/2003	Numberg et al.	704	1	
	6,594,654	07/15/2003	Salam et al.	707	3	
	6,999,959	02/14/2006	Lawrence et al.	707	5	
	7,031,961	04/18/2006	Pitkow et al.	707	4	
	7,120,625	10/10/2006	Kagimasa et al.	707	3	
	6,978,262	12/20/2005	Tsai	707	3	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER

DATE CONSIDERED

INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>	Docket Number (Optional) 6851-02-cip4-con	Application Number 11/682,941
Title: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program	Applicant(s)	
	Filing Date 03/07/2007	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	7,007,008	02/28/2006	Goel et al.	707	3	
	7,043,492	05/09/2006	Neal et al.	707	101	
	7,085,766	08/01/2006	Keith, Jr.	707	101	
	7,113,954	09/26/2006	Vogel	707	101	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER

DATE CONSIDERED

Electronic Acknowledgement Receipt

EFS ID:	1578949
Application Number:	11682941
International Application Number:	
Confirmation Number:	9976
Title of Invention:	Data Security System and Method Adjunct to E-mail, Browser, Telecom or Encryption Program
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	4897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-02-cip4-con
Receipt Date:	09-MAR-2007
Filing Date:	
Time Stamp:	12:48:29
Application Type:	Utility

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed	6851-02-cip4-con-IDS.pdf	26729	no	6

Warnings:

Information:					
This is not an USPTO supplied IDS fillable form					
2	Information Disclosure Statement (IDS) Filed	6851-02-cip4-con-IDS-Form-PTO-1449a.pdf	46916	no	6
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
Total Files Size (in bytes):			73645		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
11/682,941	03/07/2007	2131	1425	6851-02-cip4-con	44	7

CONFIRMATION NO. 9976

4897

ROBERT C. KAIN, JR.
750 SOUTHEAST THIRD AVENUE
SUITE 100
FT LAUDERDALE, FL 33316-1153

FILING RECEIPT

Date Mailed: 03/20/2007

Receipt is acknowledged of this regular Patent Application. It will be considered in its order and you will be notified as to the results of the examination. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please mail to the Commissioner for Patents P.O. Box 1450 Alexandria Va 22313-1450. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections (if appropriate).**

Applicant(s)

Ron M. Redlich, Miami Beach, FL;
Martin A. Nemzow, Miami Beach, FL;

Power of Attorney:

Martin Fleit--16900 Paul Bianco--43500
Robert Kain Jr--30648
Jose Gutman--35171
Jon Gibbons--37333
Stephen Bongini--40917

Domestic Priority data as claimed by applicant

This application is a CON of 10/155,525 05/23/2002 PAT 7,191,252
which is a CIP of 10/008,209 12/06/2001 PAT 7,140,044
and is a CIP of 10/008,218 12/06/2001 PAT 7,146,644
which is a CIP of 09/916,397 07/27/2001 PAT 7,103,915
which claims benefit of 60/287,813 05/02/2001
and claims benefit of 60/267,944 02/12/2001
and claims benefit of 60/260,398 01/09/2001
and claims benefit of 60/247,242 11/13/2000
and claims benefit of 60/247,232 11/13/2000

Foreign Applications

If Required, Foreign Filing License Granted: 03/19/2007

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is

US11/682,941

Projected Publication Date: 06/28/2007

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program

Preliminary Class

726

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all

applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
11/682,941	03/07/2007	2131	1425	6851-02-cip4-con	44	7

CONFIRMATION NO. 9976

4897

ROBERT C. KAIN, JR.
750 SOUTHEAST THIRD AVENUE
SUITE 100
FT LAUDERDALE, FL 33316-1153

FILING RECEIPT

Date Mailed: 03/20/2007

Receipt is acknowledged of this regular Patent Application. It will be considered in its order and you will be notified as to the results of the examination. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please mail to the Commissioner for Patents P.O. Box 1450 Alexandria Va 22313-1450. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections (if appropriate).**

Applicant(s)

Ron M. Redlich, Miami Beach, FL;
Martin A. Nemzow, Miami Beach, FL;

Power of Attorney:

Martin Fleit--16900 Paul Bianco--43500
Robert Kain Jr--30648
Jose Gutman--35171
Jon Gibbons--37333
Stephen Bongini--40917

Domestic Priority data as claimed by applicant

This application is a CON of 10/155,525 05/23/2002 PAT 7,191,252
which is a CIP of 10/008,209 12/06/2001 PAT 7,140,044
and is a CIP of 10/008,218 12/06/2001 PAT 7,146,644
which is a CIP of 09/916,397 07/27/2001 PAT 7,103,915
which claims benefit of 60/287,813 05/02/2001
and claims benefit of 60/267,944 02/12/2001
and claims benefit of 60/260,398 01/09/2001
and claims benefit of 60/247,242 11/13/2000
and claims benefit of 60/247,232 11/13/2000

Foreign Applications

If Required, Foreign Filing License Granted: 03/19/2007

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is

US11/682,941

Projected Publication Date: 06/28/2007

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program

Preliminary Class

726

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all

applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(c) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/682,941	03/07/2007	Ron M. Redlich	6851-02-cip4-con

CONFIRMATION NO. 9976

4897
ROBERT C. KAIN, JR.
750 SOUTHEAST THIRD AVENUE
SUITE 100
FT LAUDERDALE, FL333161153

Title: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program

Publication No. US-2007-0150965-A1

Publication Date: 06/28/2007

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publicly available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently <http://www.uspto.gov/patft/>.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently <http://pair.uspto.gov/>. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 703-305-3028.

Pre-Grant Publication Division, 703-605-4283

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich

Serial No 11/682,941

Group Art 2131

Confirmation No.: 9976

Filed: March 7, 2007

For: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program

INFORMATION DISCLOSURE STATEMENT

Mail Stop IDS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

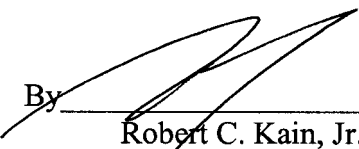
As a means of complying with the duty of disclosure set forth in 37 C.F.R. §1.56, applicant, through the undersigned attorney, files this Information Disclosure Statement pursuant to 37 C.F.R. §1.97.

Patent No.	Inventor	Issue Date
6,922,696	Lincoln et al.	Jul. 26, 2005
7,031,961	Pitkow et al.	Apr. 18, 2006

This Information Disclosure Statement is filed in accordance with 37 C.F.R. §1.97, and this statement shall not be construed as a representation that a search was made, has been made, or that the information cited above is, or is considered to be, material to patentability as defined in §1.56(b), or that no other material information, as defined in 37 C.F.R. §1.56(b), exists. Translations of the

pertinent portions of foreign language patents or publications listed above are supplied if existing translations are readily available to the applicant or the applicant's attorney. A concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR §1.56(c) most knowledgeable about the content of the information, of each patent, publication, or other information listed that is not in the English language is provided either in the patent specification or in the enclosed attachment.

Respectfully submitted,

By 

Robert C. Kain, Jr.
Reg. No. 30,648
Fleit, Kain, Gibbons, Gutman, Bongini & Bianco, P.L.
750 Southeast Third Avenue
Suite 100
Ft. Lauderdale, Florida 33316-1153
Telephone: 954-768-9002
Facsimile: 954-768-0158

G:\RCK\CLIENTS\Redlich\6851-02-cip4-con.wpd

INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)	Docket Number (Optional) 6851-02-CIP4-CON	Application Number 11/482,941
Title: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program	Applicant(s) Ron M. Redlich	
	Filing Date March 7, 2007	Group Art Unit 2131

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,922,696	07/26/2005	Lincoln et al.	707	101	
	7,031,961	04/18/2006	Pitkow et al.	707	4	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER

DATE CONSIDERED

Electronic Acknowledgement Receipt

EFS ID:	2638517
Application Number:	11682941
International Application Number:	
Confirmation Number:	9976
Title of Invention:	Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	4897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-02-cip4-con
Receipt Date:	26-DEC-2007
Filing Date:	07-MAR-2007
Time Stamp:	12:40:26
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed	6851-02-cip4-con-ids-1449.pdf	60526 6fd614469419b96b0135e58c3209915658830383	no	3

Warnings:

Information:

Total Files Size (in bytes):

60526

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 11/682,941

Group Art 2131

Confirmation No.: 9976

Filed: March 7, 2007

For: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program

INFORMATION DISCLOSURE STATEMENT

Mail Stop IDS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

As a means of complying with the duty of disclosure set forth in 37 C.F.R. §1.56, applicant, through the undersigned attorney, files this supplemental Information Disclosure Statement pursuant to 37 C.F.R. §1.97 which represents foreign search results.

Patent No.	Inventor	Issue Date
6,078,907	Lamm	Jun. 20, 2000
6,253,203	O'Flaherty et al.	Jun. 26, 2001
5,960,080	Fahlman et al.	Sep. 28, 1999

-Published Canadian Patent Application CA 2 345 148 June 4, 2000.

-"Processing of confidential information in distributed systems by fragmentation" by

J. Fabre, Computer Communications Vol. 20, pp. 177-188 (1997).

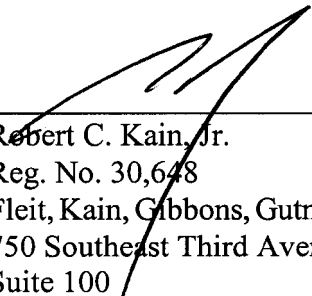
-“Secure External References in Multimedia Email Messages” B. Wiegel, ACM, pp. 11-18, Mar. 14, 1996.

-“Element-Wise XML Encryption” H. Maruyama et al., IBM Research, Tokyo Res. Lab. Ap. 19, 2000.

This Information Disclosure Statement is filed in accordance with 37 C.F.R. §1.97, and this statement shall not be construed as a representation that a search was made, has been made, or that the information cited above is, or is considered to be, material to patentability as defined in §1.56(b), or that no other material information, as defined in 37 C.F.R. §1.56(b), exists. Translations of the pertinent portions of foreign language patents or publications listed above are supplied if existing translations are readily available to the applicant or the applicant's attorney. A concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR §1.56(c) most knowledgeable about the content of the information, of each patent, publication, or other information listed that is not in the English language is provided either in the patent specification or in the enclosed attachment.

Respectfully submitted,

By



Robert C. Kain, Jr.
Reg. No. 30,648
Fleit, Kain, Gibbons, Gutman, Bongini & Bianco, P.L.
750 Southeast Third Avenue
Suite 100
Ft. Lauderdale, Florida 33316-1153
Telephone: 954-768-9002
Facsimile: 954-768-0158

G:\RCK\CLIENTS\Redlich\6851-02-cip4-con-Supple-IDS-030408.wpd

INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)	Docket Number (Optional) 6851-02-cip4-con	Application Number 11/682,941
Title: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program	Applicant(s) Ron M. Redlich, et al.	
	Filing Date March 7, 2007	Group Art Unit 2131

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,078,907	06/20/2000	Lamm	705	40	
	6,253,203	06/26/2001	O'Flaherty et al.	707	9	
	5,960,808	09/28/1999	Fahlman et al.	380	4	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO
	CA 2 345 148	06/04/2000	Canada			X

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	"Processing of confidential information in distributed systems by fragmentation" by J. Fabre, Computer Communications Vol. 20, pp. 177-188 (1997)	
	"Secure External References in Multimedia Email Messages" B. Wiegel, ACM, pp. 11-18, Mar. 14, 1996	
	"Element-Wise XML Encryption" H. Maruyama et al., IBM Research, Tokyo Res. Lab. Ap. 19, 2000	

EXAMINER

DATE CONSIDERED

Electronic Acknowledgement Receipt

EFS ID:	2953912
Application Number:	11682941
International Application Number:	
Confirmation Number:	9976
Title of Invention:	Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	4897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-02-cip4-con
Receipt Date:	05-MAR-2008
Filing Date:	07-MAR-2007
Time Stamp:	16:04:12
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed	6851-02-cip4-con-Supple-ID S-1449-030408.pdf	159719 3dd8b57523a98aff418934bd19e5fed30c8dd21d	no	3

Warnings:

Information:

Total Files Size (in bytes):

159719

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 11/682,941

Confirmation No.: 9976

Group Art 2131

Filed: March 7, 2007

For: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program

INFORMATION DISCLOSURE STATEMENT

Mail Stop IDS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

As a means of complying with the duty of disclosure set forth in 37 C.F.R. §1.56, applicant, through the undersigned attorney, files this Information Disclosure Statement pursuant to 37 C.F.R.

§1.97. Applicant's related cases are listed below.

The examiner in Serial No. 11/465309 cited the following references:

U.S. Patent No. 6,845,448 to Chaganti (Jan. 2005; 713/166)
U.S. Patent No. 6,941,459 to Hind (Sept., 2005; 713/167)
U.S. Patent No. 7,010,681 to Fletcher (Mar. 2006; 713/154)

The examiner in Serial No. 10/396,088 cited the following references:

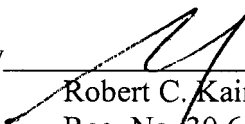
U.S. Patent No. 6,922,696 to Lincoln
U.S. Patent No. 7,031,961 to Pitkow
U.S. Patent No. 7,089,428 to Farley
U.S. Patent No. 7,188,107 to Moon

Related Cases

<u>Our Ref.</u>	<u>Serial No.</u>	<u>Filed</u>
-02-div1	11/465309	08.17.2006
-02-div2	11/465350	08.17.2006
-02-con	11/465388	08.17.2006
-02-cip4-con	11/682941	03.07.2007
-02-cip5	10/390,807	March 19, 2004
-02-cip7	10/998,366	Nov. 26, 2003
-02-cip8	10/998,365	Nov. 26, 2004
-02-cip9	10/998,363	Nov. 26, 2004
-02-cip10	11/829207	09.06.2007
-03	10/396,088	Mar. 25, 2003

This Information Disclosure Statement is filed in accordance with 37 C.F.R. §1.97, and this statement shall not be construed as a representation that a search was made, has been made, or that the information cited above is, or is considered to be, material to patentability as defined in §1.56(b), or that no other material information, as defined in 37 C.F.R. §1.56(b), exists. Translations of the pertinent portions of foreign language patents or publications listed above are supplied if existing translations are readily available to the applicant or the applicant's attorney. A concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR §1.56(c) most knowledgeable about the content of the information, of each patent, publication, or other information listed that is not in the English language is provided either in the patent specification or in the enclosed attachment.

Respectfully submitted,

By 
Robert C. Kain, Jr.
Reg. No. 30,648
Kain & Associates, Attorneys at Law, P.A.
750 Southeast Third Avenue
Suite 100
Ft. Lauderdale, Florida 33316-1153
Telephone: 954-768-9002
Facsimile: 954-768-0158

INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>	Docket Number (Optional) 6851-02-CIP4-CON	Application Number 11/682,941
Title: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program	Applicant(s) Ron M. Redlich	
	Filing Date March 7, 2007	Group Art Unit 2131

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,845,448	01/2005	Chaganti	713	166	
	6,941,459	09/2005	Hind	713	167	
	7,010,681	03/2006	Fletcher	713	154	
	6,922,696	07/2005	Lincoln	707	101	
	7,031,961	04/2006	Pitkow	707	4	
	7,089,428	05/2006	Farley	370	231	
	7,188,107	03/2007	Moon	707	5	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER

DATE CONSIDERED

G:\RCK\CLIENTS\Redlich\6851-02-cip4-con-Form-PTO-1449-Master.wpd

Electronic Acknowledgement Receipt

EFS ID:	4739012
Application Number:	11682941
International Application Number:	
Confirmation Number:	9976
Title of Invention:	Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	04897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-02-cip4-con
Receipt Date:	05-FEB-2009
Filing Date:	07-MAR-2007
Time Stamp:	12:00:05
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed (SB/08)	6851-02-cip4-con-IDS-020409- update-pendng-IDS.pdf	81082 7f52236962e90bc9faa1d540d6fb913310554828	no	3

Warnings:

Information:

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

(19)  Canadian Intellectual Property Office

An Agency of
Industry Canada

Office de la Propriété
Intellectuelle
du Canada

Un organisme
d'Industrie Canada

(11) CA 2 345 148

(13) A1

(40) 06.04.2000

(43) 06.04.2000

(12)

(21) 2 345 148

(51) Int. Cl. 7: G06F 1/00

(22) 24.09.1999

(85) 22.03.2001

(86) PCT/CA99/00891

(87) WO00/19296

(30) 2,246,006 CA 25.09.1998

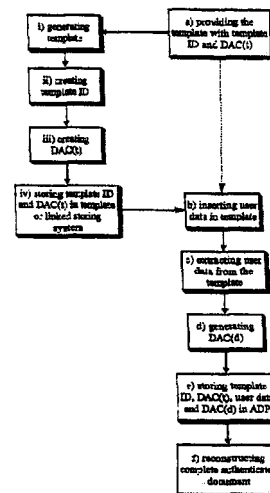
(71) SILANIS TECHNOLOGY INC.,
305-3333 C^{te} Vertu, ST-LAURENT, Q1 (CA).

(72) MILCZAREK, ED (CA).
PETROGIANNIS, TOMMY (CA).
SILVESTER, Joseph (CA).

(74) ROBIC

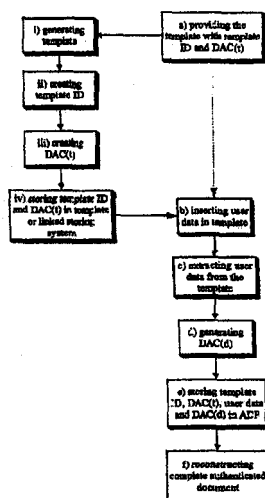
(54) PROCEDE D'AUTHENTIFICATION SEPARÉE D'UN MODELE ET DE DONNEES D'UTILISATEUR
(54) METHOD FOR THE SEPARATE AUTHENTICATION OF A TEMPLATE AND USER DATA

(57) A method for the separate authentication of a template and of data inserted therein. A template is provided with a template ID and a template Data Authentication Code (DAC(t)). User data is inserted in the template, and then extracted to be handled separately. A DAC(d) is generated on the user data by itself, and stored in an Approval Data packet with the template ID, DAC(t) and the user data. The complete document with the template and the user data can later be reconstructed. The method may be useful for many industries that rely on templates as a means for collecting data.





(72) MILCZAREK, ED, CA
(72) PETROGIANNIS, TOMMY, CA
(72) SILVESTER, Joseph, CA
(71) SILANIS TECHNOLOGY INC., CA
(51) Int. Cl.⁷ G06F 1/00
(30) 1998/09/25 (2,246,006) CA
(54) PROCEDE D'AUTHENTIFICATION SEPARÉE D'UN MODELE
ET DE DONNEES D'UTILISATEUR
(54) METHOD FOR THE SEPARATE AUTHENTICATION OF A
TEMPLATE AND USER DATA



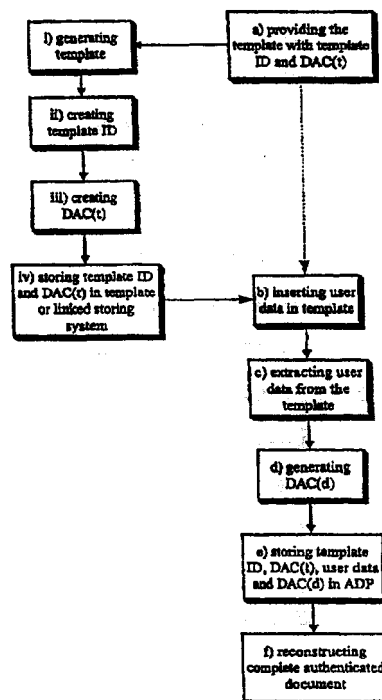
(57) A method for the separate authentication of a template and of data inserted therein. A template is provided with a template ID and a template Data Authentication Code (DAC(t)). User data is inserted in the template, and then extracted to be handled separately. A DAC(d) is generated on the user data by itself, and stored in an Approval Data packet with the template ID, DAC(t) and the user data. The complete document with the template and the user data can later be reconstructed. The method may be useful for many industries that rely on templates as a means for collecting data.



PCTWORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁷ : G06F 1/00	A1	(11) International Publication Number: WO 00/19296
		(43) International Publication Date: 6 April 2000 (06.04.00)
(21) International Application Number: PCT/CA99/00891 (22) International Filing Date: 24 September 1999 (24.09.99) (30) Priority Data: 2,246,006 25 September 1998 (25.09.98) CA (71) Applicant: SILANIS TECHNOLOGY INC. [CA/CA]; Suite 305, 3333, Côte Vertu, St. Laurent, Québec H4R 2N1 (CA). (72) Inventors: SILVESTER, Joseph; 282, place des Cèdres, Dollard-des-Ormeaux, Québec H9G 1W1 (CA). MIL-CZAREK, Ed; 5135 des Cajoux, Pierrefonds, Québec H9J 3C4 (CA). PETROGIANNIS, Tommy; 4560 Cumberland Avenue, Montréal, Québec H4B 2L4 (CA). (74) Agent: ROBIC; 55, St. Jacques, Montréal, Québec H2Y 3X2 (CA).		(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Published <i>With international search report.</i>
(54) Title: METHOD FOR THE SEPARATE AUTHENTICATION OF A TEMPLATE AND USER DATA		
(57) Abstract A method for the separate authentication of a template and of data inserted therein. A template is provided with a template ID and a template Data Authentication Code (DAC(t)). User data is inserted in the template, and then extracted to be handled separately. A DAC(d) is generated on the user data by itself, and stored in an Approval Data packet with the template ID, DAC(t) and the user data. The complete document with the template and the user data can later be reconstructed. The method may be useful for many industries that rely on templates as a means for collecting data.		



WO 00/19296

PCT/CA99/00891

I

METHOD FOR THE SEPARATE AUTHENTICATION OF A TEMPLATE AND USER DATA

5 FIELD OF THE INVENTION

The present invention relates to the secure handling of data and more particularly concerns a method for separately authenticating a template and user data inserted in the template.

10 BACKGROUND OF THE INVENTION

There are many computer systems that have been designed to create, store, approve, revise or verify data electronically. Many of the documents that have been created through these systems have relied on a pre-existing template as a means of assembling data. This facilitates the means of data entry and allows the user to store the data and the template on one document. The use of the template also contributes to a less time-consuming process of entering information on an electronic document, a process that may contribute to fewer costs than those associated with paper-based data collection.

20 While there exist a great number of systems that may facilitate the creation, serial approval, storage and authentication of documents or of templates, there is no known system to date that can enable users to separate user data from template information. Current systems allow users to create templates and enter data in them. The data therefore becomes bound to the template in a single document. However, such systems do not have the capacity to enable users to securely approve, store and authenticate each portion separately, to approve multiple templates or, alternatively, opt to recreate the complete document.

Existing systems vary in the scope of the functions they can perform.
30 Some are particularly limited, such as U.S. patent no. 4,933,969 to

WO 00/19296

PCT/CA99/00891

2

Marshall et al., which primarily addresses authentication and storage. This mechanism stores information and protects against unauthorized modifications. While this type of data authentication system contributes greatly to ensuring the security and integrity of data, it lacks the capacity
5 for the generation, approval and secure storage of both template information and user data.

Other systems offer certain types of electronic functions that are related to the generation and authentication of electronic signatures. For example, U.S. patent no. 5,195,133 to Kapp et al. describes a system
10 designed to generate a completed payment document, which can be signed by a customer, and then capture that customer's signature in digital form. The principal feature of this mechanism is that it seeks to ensure that a signature approving a particular document was, in fact, captured at the time of the completion of the transaction to which it relates and was not
15 obtained on some other occasion and merely reproduced for the particular transaction in question. The Kapp et al. patent creates a digital record of the transaction and captures a digital representation of the signature at the time the transaction is completed. This system then uses this digital record to encrypt the digital representation of the signature. However, it does not
20 offer any possibility of generating or approving a template document separately from the user data or the electronic approval.

Other technology provides for the creation of an electronic signature for a particular signer only, and cannot be used for any document other than the one for which the signature was given (U.S. patent no. 5,689,567).
25 U.S. patent no. 5,606,609 to Houser and Adler is a system designed to verify the integrity or signer of electronic documents. This is accomplished by embedding and encrypting security information in the electronic document at a location selected by the signer. When the electronic document is subsequently displayed, the technology decrypts the security
30 information and verifies the identity of the signer. In another mechanism,

WO 00/19296

PCT/CA99/00891

3

another method operates to authenticate and verify users on a network (U.S. patent no. 5,706,427). The possible applications of any of the aforementioned systems, albeit useful for certain purposes, are nonetheless limited as they do not allow for the creation, approval or authentication of
5 template information distinct from the user data.

While each of the aforementioned systems can be useful for electronic business processes, they all have certain deficiencies. These mechanisms lack the capacity to enable the user to generate, approve, store and authenticate template information separately from user data, with the
10 possibility of subsequently merging the two later in a complete document. Current technology operates such that any user data entered on the template becomes bound to the template in one document. The present invention allows users to access either the template data, multiple templates and/or the user data as independent files. Moreover, the
15 technology ensures that no unauthorized modifications can be made to either file or to the complete document. This therefore accords the user greater flexibility in accessing each file without compromising the security or authenticity of the data.

The Remote Template Approval ("RTA") can serve as a vital tool
20 facilitating electronic business processes. Many industries, such as insurance for example, which rely on templates and standard forms as a means of gathering information or selling and marketing services can greatly benefit from this technology. The RTA would enable those marketing these services to securely store and access user data separately from the
25 templates, while individual template information could be generated, accessed or modified for each subsequent user or purchaser. This would represent an efficient way of gathering, storing and authenticating client and template information. In addition, it would offer an easy and secure medium through which users or consumers could submit information and
30 purchase services on-line.

WO 00/19296

PCT/CA99/00891

4

Clearly then, as electronic business transactions become even more prevalent, the need to generate and store template information and user data as separate entities will become more pronounced as well. As this occurs, the need for the Remote Template Approval mechanism will expand
5 with it.

SUMMARY OF THE INVENTION

The present invention provides a system and method designed to facilitate remote template approval. This system will enable users to
10 separate user data from template information and authenticate and verify each portion separately. Thus, by virtue of this method, users will be able to approve template information separately from the data added to the template. Preferably, this invention will also enable users to securely recreate the complete document composed of both data and template and
15 verify its authenticity. Such a process would represent a marked improvement over existing systems which enable users to add data to existing templates in such a fashion as to bind the data to the template in one document. The present invention allows the user to securely access the template and the data as distinct records, or to, optionally, access the
20 complete document.

Accordingly, the present invention provides a method for the separate authentication of a template and of user data inserted therein, comprising the steps of:

- a) providing the template, said template having a corresponding template ID
25 and template Document Authentication Code, hereinafter referred to as DAC(t), linked thereto;
- b) inserting the user data in the template;
- c) extracting the user data from the template;
- d) generating a user data Document Authentication Code, hereinafter
30 referred to as DAC(d), based on the user data; and

WO 00/19296

PCT/CA99/00891

5

e) storing the template ID, DAC(t), the user data and DAC(d) in an Approval Data Packet, hereinafter referred to as ADP.

There is also provided a method for the separate authentication of a template having entry fields and user data inserted into said fields, comprising the steps of:

a) selecting a template ID and a corresponding template Document Authentication Code, hereinafter referred to as DAC(t), linked to the template;

b) entering the user data;

10 c) linking the user data to the fields of the template;

d) generating a user data Document Authentication Code, hereinafter referred to as DAC(d), based on the user data; and

e) storing the template ID, DAC(t), the user data and DAC(d) in an Approval Data Packet, hereinafter referred to as ADP.

15 The present invention further provides a method for the separate authentication of a template and of user data inserted therein, comprising the steps of:

a) providing the template, said template having a corresponding template ID and template Document Authentication Code, hereinafter referred to as DAC(t), linked thereto;

20 b) inserting the user data in the template;

c) generating a complete document Document Authentication Code, hereinafter referred to as DAC(c), based on the template with the user data therein;

25 d) extracting the user data from the template;

e) generating a user data Document Authentication Code, hereinafter referred to as DAC(d), based on the user data; and

f) storing the template ID, DAC(t), the user data, DAC(c) and DAC(d) in an Approval Data Packet, hereinafter referred to as ADP.

WO 00/19296

PCT/CA99/00891

6

Also provided is a method for the separate authentication of a template and of user data inserted therein by multiple users, comprising the steps of:

- a) authenticating a template and user data from a first user according to the last method described above; and
- b) for each subsequent user of the multiple users, performing the substeps of:
 - i) retrieving the template and DAC(c);
 - ii) inserting user data from previous users in the template;
 - 10 iii) generating for the template with the user data from previous users therein a new complete document Document Authentication Code, hereinafter referred to as DAC(nc);
 - iv) comparing DAC(nc) with DAC(c), and proceeding only if DAC(nc) is equal to DAC(c);
 - 15 v) inserting data from the current user in the template;
 - vi) generating a DAC(c), based on the template with the user data from the previous users and current user therein;
 - vii) extracting the user data from the previous users and current user from the template;
 - 20 viii) generating a DAC(d), based on the user data extracted in step vii); and
 - ix) storing the user data, DAC(c) and DAC(d) in ADP.

The present invention can have numerous applications. For example, it could enable users to create and approve one document on one system (e-mail for example), with the target template indicated in the ADP, and

25 send it to another system, which may be the same system or a completely different one. The message can then be entered into the actual template document with all the proper formatting and no need to convert the document.

WO 00/19296

PCT/CA99/00891

7

This invention would be useful for many industries that rely on templates as a means of collecting data. The same template could be generated for each new user and the data collected could be stored separately or could also be combined with the template to create a completed document. This method would allow users to re-generate the template for each subsequent user.

The present invention and its advantages will be better understood upon reading the following non-restrictive description of embodiments thereof with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a flow chart representing the main steps of a method for the separate authentication of a template and of user data inserted therein in accordance with a preferred embodiment of the present invention.

FIG. 2 is a flow chart detailing step f of the method of FIG. 1.

FIG. 3 is a flow chart representing the main steps of a method for the separate authentication of a template and of user data inserted therein in accordance with an alternative embodiment of the invention.

FIG. 4 is a flow chart representing the main steps of a method for the separate authentication of a template and of user data inserted therein in accordance with another embodiment of the invention.

FIG. 5 is a flow chart detailing step g of the method of FIG. 4.

FIG. 6 is a flow chart detailing another variant for step g of the method of FIG. 4.

FIG. 7 is a flow chart representing the main steps of a method for the separate authentication of a template and of user data inserted therein in accordance with yet another embodiment of the invention.

DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION

Referring to FIGs. 1 and 2, the steps of a method for the separate authentication of a template and user data inserted in the template are shown. This method allows the secure handling of the template and user data independently, without having to store the user data inside the template.

The first step a) of the method of FIG. 1 consists of providing the template itself. A template ID, identifying the particular template chosen, and a template Document Authentication code, DAC(t), are both linked to the template. DAC(t) is a code characterizing precisely the template's content, and is preferably generated through a one-way hash function. If the template is not pre-existing, step a) may include the substep of generating the template, creating the template ID and DAC(t) and storing the last two in an appropriate location, which can for example be inside the template itself or in a linked storage system.

The second step b) consists of inserting the user data in the template. The term "user data" is understood as encompassing any relevant information that may be entered in a template, including a user signature and the date of signing. The method may therefore be used in the context of the remote approval of a document. The template preferably has specific fields where the user data may be received.

The user data is then extracted from the template in accordance with step c), and in the next step d) a user data Authentication Code (DAC(d)) is generated, based on the user data itself independently of the template.

Step e) consists of storing the template ID, DAC(t), the user data and DAC(c) in an Approval Data Packet (ADP) which may be encrypted for security. The user data may alternatively be stored elsewhere and a link to its location may be provided in the ADP.

Referring to FIGs. 1 and 2, there is shown an optional step f) of reconstructing a complete document including both the template and the

AMENDED SHEET

Printed 15-09-2000

WO 00/19296

PCT/CA99/00891

9

user data. In accordance with this additional step, the template ID and DAC(t) are first retrieved from the ADP, and the template corresponding to the template ID is accessed and opened. A new DAC (DAC(nt)) is generated on the opened template, and compared to DAC(t). Corrective action is to be
5 taken if they don't match. If they do match, the user data and DAC(d) are also retrieved. A DAC(nd) is generated on the user data and compared to DAC(d). If they also match, the user data may then be inserted in the template.

In an alternate embodiment of the invention, illustrated in FIG. 3, the
10 method described above may be performed without actually accessing the template. In this embodiment, a template ID and the corresponding DAC(t) are selected, and the user data is entered, preferably in answer to prompts for particular information. The user data entered is then linked to corresponding fields in the template, so that a complete document including
15 both the template and the user data may later be reconstructed.

Referring to FIGs. 4, 5 and 6, there is shown yet another embodiment of the invention. In this particular embodiment, a step is added between steps b) and c) of FIG. 1 where a DAC(c) is generated based on the template with the user data therein, before the user data is extracted from
20 the template. This DAC(c) is stored in the ADP with the other relevant information. In this manner, when reconstructing the complete document, additional substeps of generating a DAC(nc) on the complete document once the user data is inserted in the template and comparing this DAC(nc) with DAC(c) may be performed, as shown in FIG. 5. Alternatively, only the
25 DACs of the complete documents may be compared, completely bypassing the verifications of the separate template and user data, as illustrated in FIG. 6.

Referring to FIG. 7, there is shown another embodiment of the invention where multiple users insert user data sequentially in a single
30 template. The method includes the steps of:

a) authenticating a template and user data from a first user according to the method of FIG. 4. In this manner, an ADP is created containing the template ID, DAC(t), the user data, DAC(d) and DAC(c).

b) for each subsequent user of the multiple users, the following substeps
5 are performed:

i) retrieving the template and DAC(c) from the ADP;

ii) inserting user data from previous users in the template. The document thereby generated corresponds to the complete document of the previous iteration;

10 iii) generating for the template with the user data from previous users therein a new complete document Document Authentication Code (DAC(nc));

iv) comparing DAC(nc) with DAC(c), and proceeding only if DAC(nc) is equal to DAC(c);

15 v) inserting data from the current user in the template;

vi) generating a DAC(c), based on the template with the user data from the previous users and current user therein;

vii) extracting the user data from the previous users and current user from the template;

20 viii) generating a DAC(d), based on the user data extracted in step vii); and

ix) storing the user data, DAC(c) and DAC(d) in ADP. DAC(c) and DAC(d) thereby replace the previously stored values of these variables.

25 An additional step of reconstructing the complete document, which in this case corresponds to the document generated in the last iteration of step b), may also be performed, either in the manner illustrated in FIG. 5 or FIG. 6.

WO 00/19296

PCT/CA99/00891

11

Of course, numerous changes could be made to the preferred embodiment disclosed hereinabove without departing from the scope of the invention as defined in the appended claims.

WHAT IS CLAIMED IS:

1. A method for the separate authentication of a template and of user data inserted therein, comprising the steps of:
 - 5 a) providing the template, said template having a corresponding template ID and template Document Authentication Code, hereinafter referred to as DAC(t), linked thereto;
 - b) inserting the user data in the template;
 - c) extracting the user data from the template;
 - 10 d) generating a user data Document Authentication Code, hereinafter referred to as DAC(d), based on the user data; and
 - e) storing the template ID, DAC(t), the user data and DAC(d) in an Approval Data Packet, hereinafter referred to as ADP.
- 15 2. The method according to claim 1, wherein step a) comprises the substeps of:
 - i) generating the template;
 - ii) creating the template ID;
 - iii) creating DAC(t); and
 - 20 iv) storing the template ID and DAC(t) in a location linked to the template.
3. The method according to claim 2, wherein substep a)iii) comprises generating DAC(t) from a one-way hash function.
- 25 4. The method according to claim 2, wherein, in substep a) iv), the location linked to the template is inside said template.
5. The method according to claim 2, wherein, in substep a) iv), the location
30 linked to the template is a linked storage system.

6. The method according to claim 1, wherein step e) further comprises encrypting the ADP.

7. The method according to claim 1, further comprising an additional step f) of reconstructing an authenticated complete document, said complete document including the template and the user data.

8. The method according to claim 7, wherein step f) comprises the substeps of:

- i) retrieving the template ID and DAC(t) from the ADP;
- ii) opening the template corresponding to said template ID;
- iii) generating for said template a new template Document Authentication Code, hereinafter referred to as DAC(nt);
- iv) comparing DAC(nt) with DAC(t), and proceeding only if DAC(nt) is equal to DAC(t);
- v) retrieving the user data and DAC(d) from the ADP;
- vi) generating for said user data a new user data Document Authentication Code, hereinafter referred to as DAC(nd);
- vii) comparing DAC(nd) with DAC(d), and proceeding only if DAC(nd) is equal to DAC(d); and
- viii) inserting the user data in the template.

9. The method according to claim 1, wherein the template has entry fields, and wherein said step of inserting user data includes the step of inserting user data into said entry fields.

10. The method according to claim 9, wherein step b) further comprises prompting the user for the user data.

11. The method according to claim 9, wherein step e) further comprises encrypting the ADP.

12. The method according to claim 9, further comprising an additional step f) of reconstructing an authenticated complete document, said complete document including the template and the user data.

13. The method according to claim 12, wherein step f) comprises the substeps of:

- 10 i) retrieving the template ID and DAC(t) from the ADP;
ii) opening the template corresponding to said template ID;
iii) generating for said template a new template Document
Authentication Code, hereinafter referred to as DAC(nt);
iv) comparing DAC(nt) with DAC(t), and proceeding only if DAC(nt) is
15 equal to DAC(t);
v) retrieving the user data and DAC(d) from the ADP;
vi) generating for said user data a new user data Document
Authentication Code, hereinafter referred to as DAC(nd);
vii) comparing DAC(nd) with DAC(d), and proceeding only if DAC(nd)
20 is equal to DAC(d); and
viii) inserting the user data in the template.

14. The method according to claim 1, wherein said method further includes step b1) generating a complete Document Authentication Code, hereinafter referred to as DAC(c), based on the template with the user data therein.

15. The method according to claim 14, wherein step a) comprises the substeps of:

- i) generating the template;

WO 00/19296

PCT/CA99/00891

16

18. The method according to claim 15, wherein, in substep a) iv), the location linked to the template is a linked storage system.

19. The method according to claim 14, wherein step f) further comprises
5 encrypting the ADP.

20. The method according to claim 14, further comprising an additional step
g) of reconstructing an authenticated complete document, said complete
document including the template and the user data.

10

21. The method according to claim 20, wherein step g) comprises the
substeps of:

- i) retrieving the template ID, DAC(t) and DAC(c) from the ADP;
- ii) opening the template corresponding to said template ID;
- 15 iii) generating for said template a new template Document
Authentication Code, hereinafter referred to as DAC(nt);
- iv) comparing DAC(nt) with DAC(t), and proceeding only if DAC(nt) is
equal to DAC(t);
- v) retrieving the user data and DAC(d) from the ADP;
- 20 vi) generating for said user data a new user data Document
Authentication Code, hereinafter referred to as DAC(nd);
- vii) comparing DAC(nd) with DAC(d), and proceeding only if DAC(nd)
is equal to DAC(d);
- viii) inserting the user data in the template;
- 25 ix) generating for the template with the user data therein a new
complete document Document Authentication Code, hereinafter referred to
as DAC(nc); and
- x) comparing DAC(nc) with DAC(c), and proceeding only if DAC(nc) is
equal to DAC(c).

30

WO 00/19296

PCT/CA99/00891

17

22. The method according to claim 20, wherein step g) comprises the substeps of:

- i) retrieving the template ID, the user data and DAC(c) from the ADP;
- ii) opening the template corresponding to said template ID;
- 5 iii) inserting the user data in the template;
- iv) generating for the template with the user data therein a new complete document Document Authentication Code, hereinafter referred to as DAC(nc); and
- v) comparing DAC(nc) with DAC(c), and proceeding only if DAC(nc) is
10 equal to DAC(c).

23. A method for the separate authentication of a template and of user data inserted therein by multiple users, comprising the steps of:

- a) authenticating a template and user data from a first user according to the
15 method of claim 14; and
- b) for each subsequent user of the multiple users, performing the substeps of:
 - i) retrieving the template and DAC(c);
 - ii) inserting user data from previous users in the template;
 - 20 iii) generating for the template with the user data from previous users therein a new complete document Document Authentication Code, hereinafter referred to as DAC(nc);
 - iv) comparing DAC(nc) with DAC(c), and proceeding only if DAC(nc) is equal to DAC(c);
 - 25 v) inserting data from the current user in the template;
 - vi) generating a DAC(c), based on the template with the user data from the previous users and current user therein;
 - vii) extracting the user data from the previous users and current user from the template;

WO 00/19296

PCT/CA99/00891

18

- viii) generating a DAC(d), based on the user data extracted in step vii); and
- ix) storing the user data, DAC(c) and DAC(d) in ADP.

5 24. The method according to claim 23, further comprising an additional step c) of reconstructing an authenticated complete document, said complete document including the template and the user data from all of the multiple users.

10 25. The method according to claim 24, wherein step c) comprises the substeps of:

- i) retrieving the template ID, DAC(t) and DAC(c) from the ADP;
- ii) opening the template corresponding to said template ID;
- iii) generating for said template a new template Document
- 15 Authentication Code, hereinafter referred to as DAC(nt);
- iv) comparing DAC(nt) with DAC(t), and proceeding only if DAC(nt) is equal to DAC(t);
- v) retrieving the user data and DAC(d) from the ADP;
- vi) generating for said user data a new user data Document
- 20 Authentication Code, hereinafter referred to as DAC(nd);
- vii) comparing DAC(nd) with DAC(d), and proceeding only if DAC(nd) is equal to DAC(d);
- viii) inserting the user data in the template;
- ix) generating for the template with the user data therein a new
- 25 complete document Document Authentication Code, hereinafter referred to as DAC(nc); and
- x) comparing DAC(nc) with DAC(c), and proceeding only if DAC(nc) is equal to DAC(c).

1 / 7

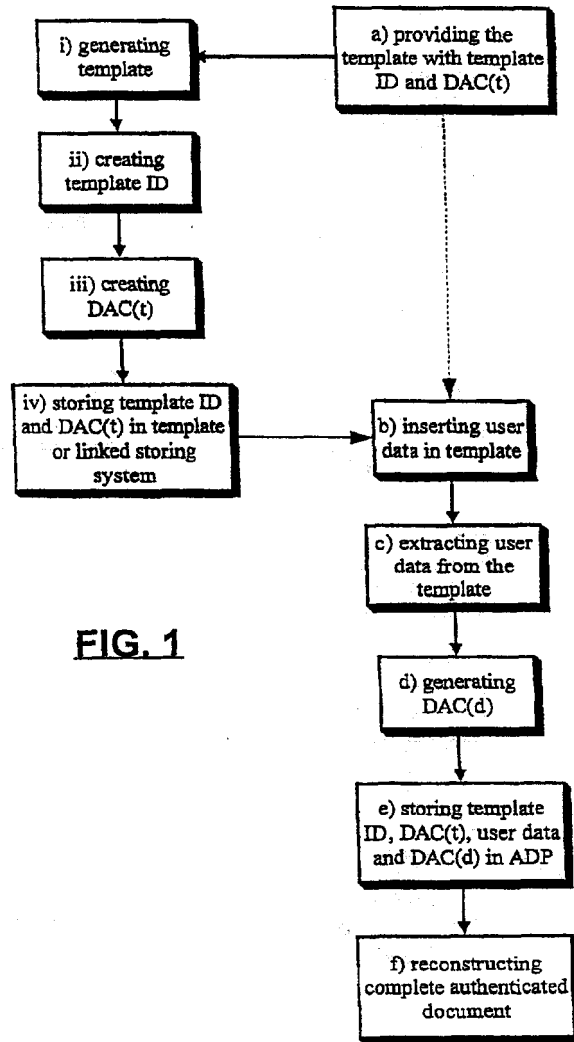
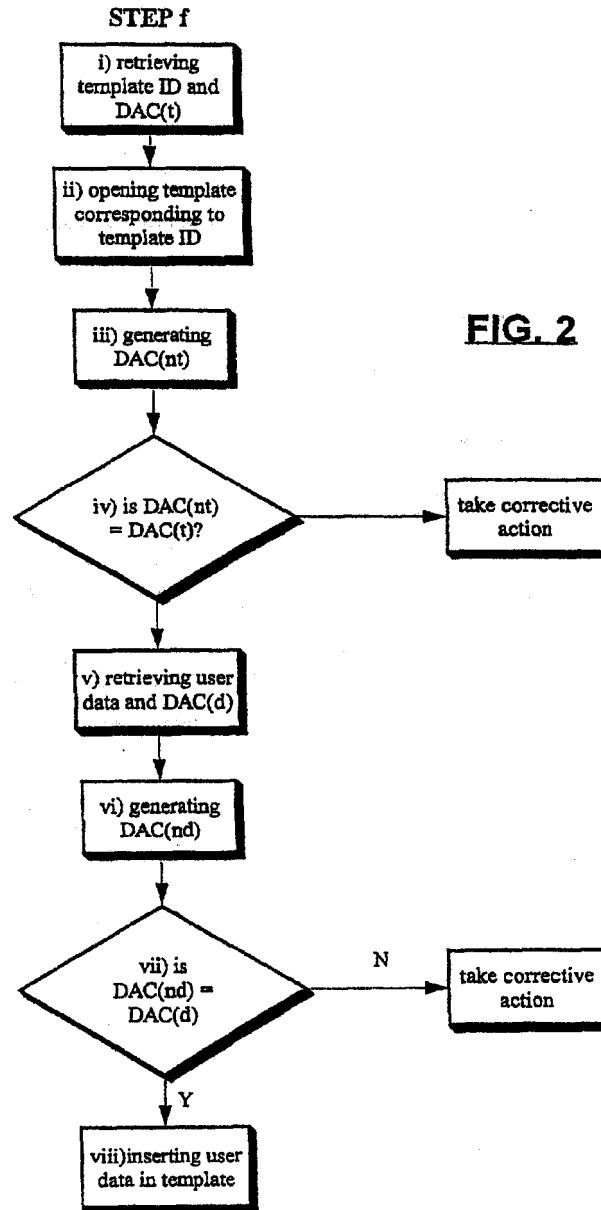
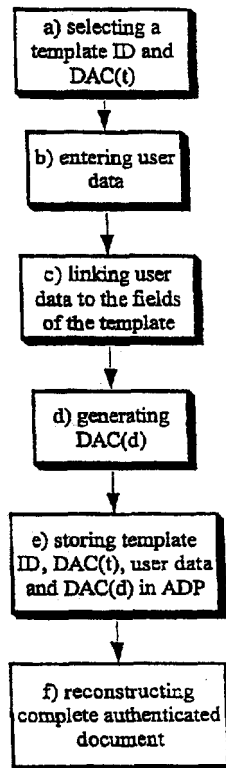


FIG. 1

2 / 7



3 / 7

**FIG. 3**

4 / 7

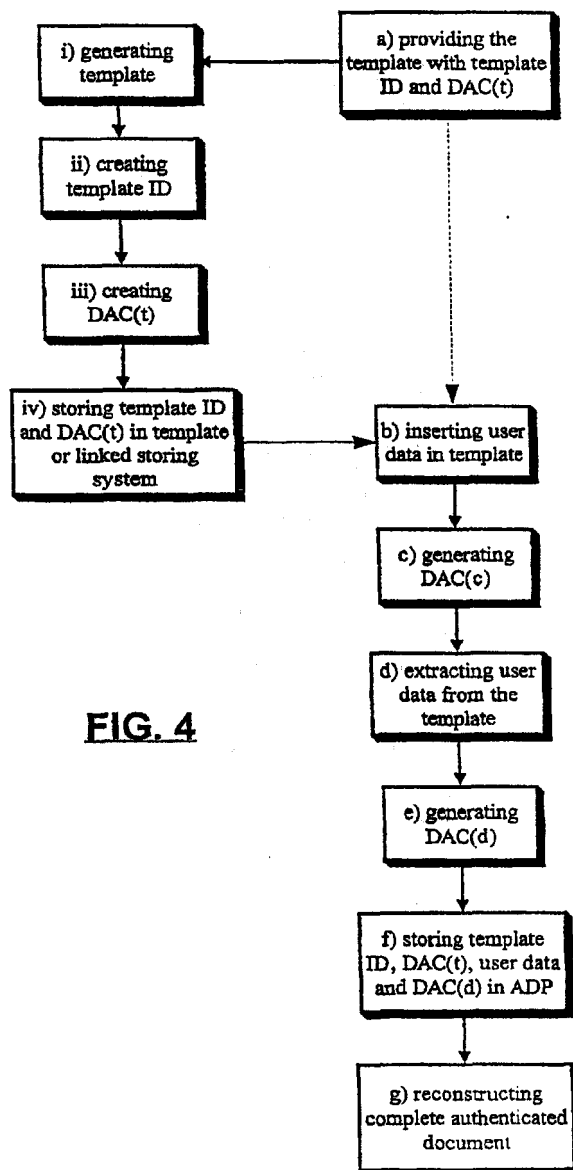
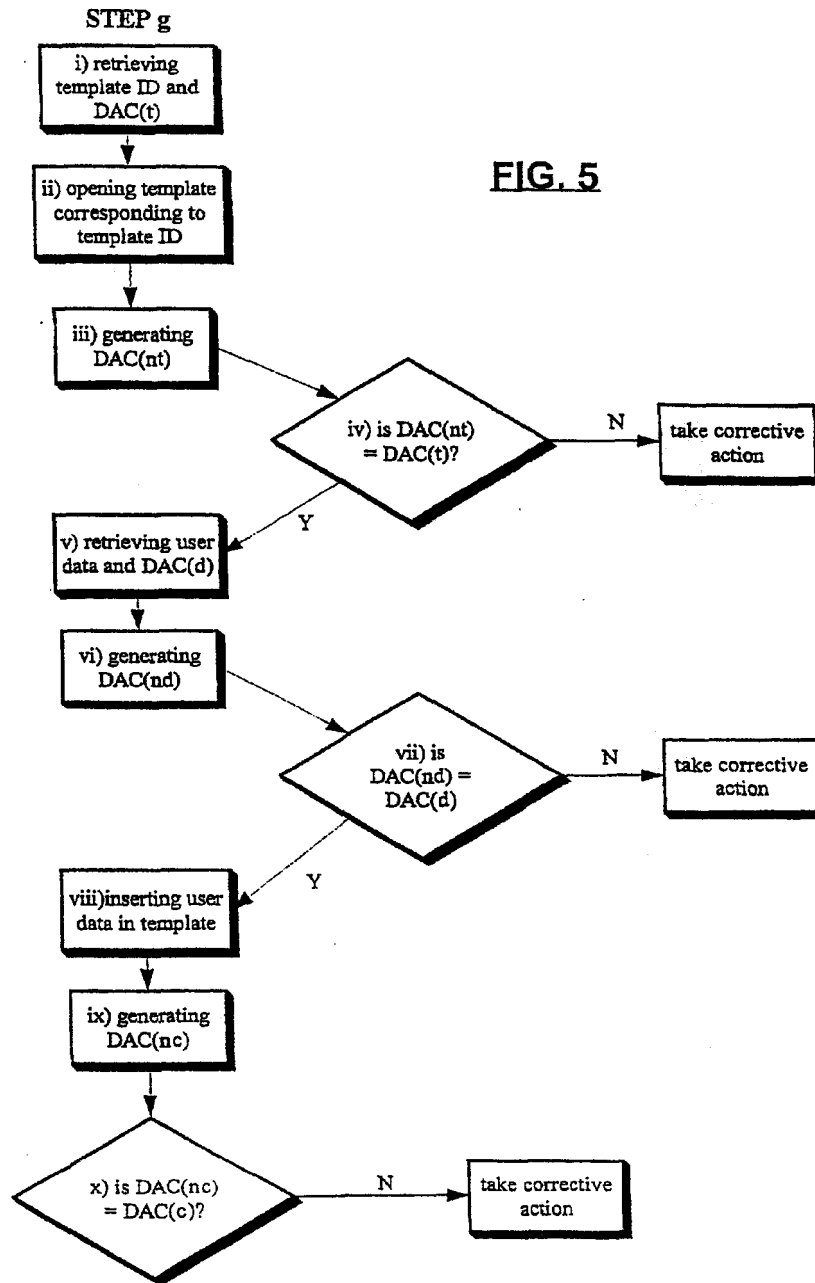
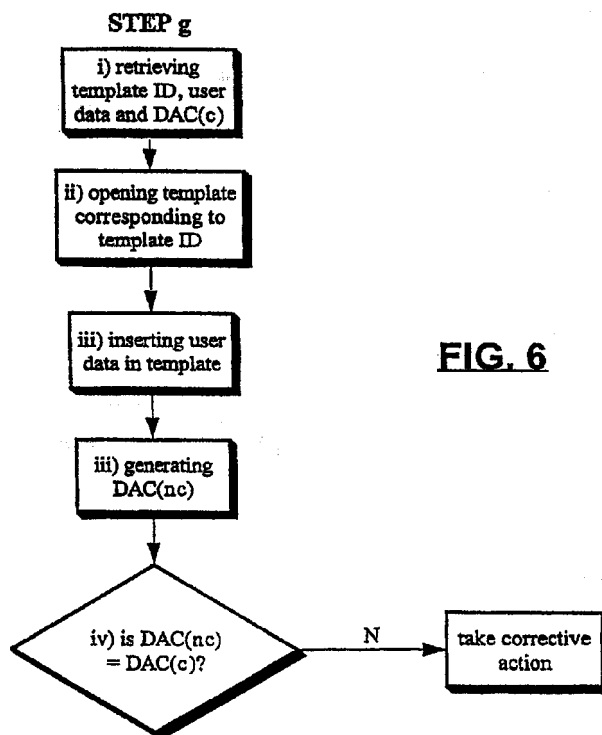


FIG. 4

5 / 7

FIG. 5



**FIG. 6**

WO 00/19296

PCT/CA99/00891

7 / 7

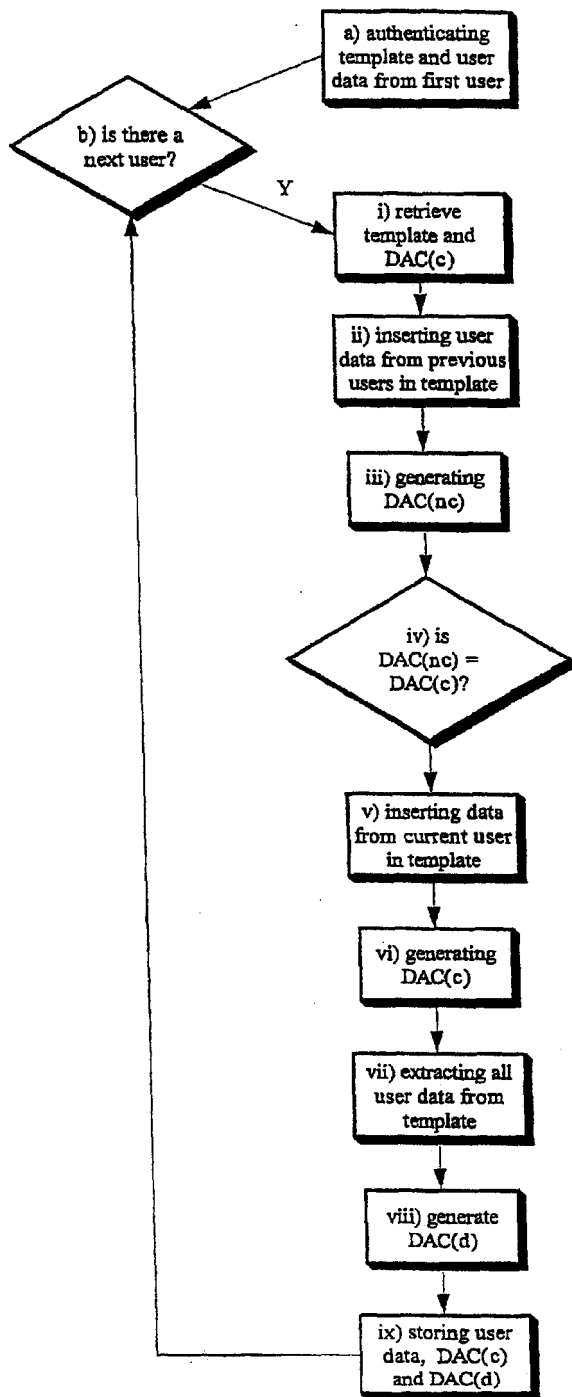


FIG. 7

Electronic Acknowledgement Receipt

EFS ID:	5043330
Application Number:	11682941
International Application Number:	
Confirmation Number:	9976
Title of Invention:	Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	04897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-02-cip4-con
Receipt Date:	26-MAR-2009
Filing Date:	07-MAR-2007
Time Stamp:	17:06:24
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed (SB/08)	6851-02-cip4-con-IDS-Supple- F1449-032409.pdf	71923 7ed2ce09ce5d1547bc6257657c928e593ac b24ae	no	3

Warnings:

Information:

This is not an USPTO supplied IDS fillable form					
2	Information Disclosure Statement (IDS) Filed (SB/08)	Pr-Art-Secure-External.pdf	1060497	no	8
			9ab51ddd72a1c4fe818829f9fbf8942e9a1c29b		
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Information Disclosure Statement (IDS) Filed (SB/08)	Pr-Art-Proces-Confid-Info.pdf	812445	no	12
			687b4d764bade290dde95a47f4c85b8aac2c26c6		
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
4	Information Disclosure Statement (IDS) Filed (SB/08)	Pr-Art-Canada-2345148-Silanis. pdf	1113678	no	28
			52f3e78f2267c62b1f79ceb703fa830d01646c99		
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
Total Files Size (in bytes):			3058543		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 11/682,941

Confirmation No.: 9976

Examiner Kim Y Vu

Filed: March 7, 2007

Group Art 2131

For: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program

INFORMATION DISCLOSURE STATEMENT

Mail Stop IDS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

As a means of complying with the duty of disclosure set forth in 37 C.F.R. §1.56, applicant, through the undersigned attorney, files this Information Disclosure Statement pursuant to 37 C.F.R. §1.97. The prior art cited below was cited in a pending, non-U.S. patent application as being technical background.

-“Secure External References in Multimedia Email Messages” by B. Wiegel, German National Research Center, Mar. 14, 1996.

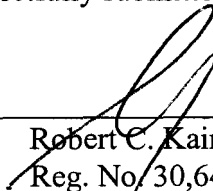
-“Process of Confidential Information in Distributed Systems by Fragmentation” by J. Fabre, Computer Communications 20:177 - 188, 1997.

-Canadian Patent Publication by S. Lanis, CA 2345148, April 6, 2000.

This Information Disclosure Statement is filed in accordance with 37 C.F.R. §1.97, and this statement shall not be construed as a representation that a search was made, has been made, or that the information cited above is, or is considered to be, material to patentability as defined in §1.56(b), or that no other material information, as defined in 37 C.F.R. §1.56(b), exists. Translations of the pertinent portions of foreign language patents or publications listed above are supplied if existing translations are readily available to the applicant or the applicant's attorney. A concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR §1.56(c) most knowledgeable about the content of the information, of each patent, publication, or other information listed that is not in the English language is provided either in the patent specification or in the enclosed attachment.

Respectfully submitted,

By



Robert C. Kain, Jr.

Reg. No. 30,648

Kain & Associates, Attorneys at Law, P.A.

750 Southeast Third Avenue

Suite 100

Ft. Lauderdale, Florida 33316-1153

Telephone: 954-768-9002

Facsimile: 954-768-0158

G:\RCK\CLIENTS\Redlich\6851-02-cip4-con-IDS-Supple-032409.wpd

INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>	Docket Number (Optional) 6851-02-cip4-con	Application Number 11/682,941
Title: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program	Applicant(s) Ron M. Redlich, et al.	
	Filing Date March 7, 2007	Group Art Unit 2131

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	-“Secure External References in Multimedia Email Messages” by B. Wiegel, German National Research Center, Mar. 14, 1996.	
	-“Process of Confidential Information in Distributed Systems by Fragmentation” by J. Fabre, Computer Communications 20:177 - 188, 1997.	
	-Canadian Patent Publication by S. Lanis, CA 2345148, April 6, 2000.	

EXAMINER

DATE CONSIDERED

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**CHANGE OF
CORRESPONDENCE ADDRESS**
*Application*Address to:
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Application Number	11/682,941
Filing Date	3/7/2007
First Named Inventor	
Art Unit	
Examiner Name	
Attorney Docket Number	6851-02-cip4-con

Please change the Correspondence Address for the above-identified patent application to:

The address associated with
Customer Number:

004897

ORFirm or
Individual Name

Address

City

State

Zip

Country

Telephone

Email

This form cannot be used to change the data associated with a Customer Number. To change the data associated with an existing Customer Number use "Request for Customer Number Data Change" (PTO/SB/124).

I am the:



Applicant/Inventor

Assignee of record of the entire interest.
Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).Attorney or agent of record. Registration Number 30,648.

Registered practitioner named in the application transmittal letter in an application without an executed oath or declaration. See 37 CFR 1.33(a)(1). Registration Number _____.

Signature

Typed or Printed
Name

Robert C. Kain, Jr.

Date 10/28/2009

Telephone

954-768-9002

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

*Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	6357473
Application Number:	11682941
International Application Number:	
Confirmation Number:	9976
Title of Invention:	Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	04897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-02-cip4-con
Receipt Date:	29-OCT-2009
Filing Date:	07-MAR-2007
Time Stamp:	16:12:00
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Change of Address	6851-02-cip4-con-change-address-sb0122_fill.pdf	315497 5e2fc2c725ff3506bc97353ea80a6a913745d419	no	2

Warnings:

Information:

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/682,941	03/07/2007	Ron M. Redlich	6851-02-cip4-con	9976

4897 7590 04/09/2010

ROBERT C. KAIN, JR.
KAIN & ASSOCIATES, ATTORNEYS AT LAW, P.A.
900 SOUTHEAST THIRD AVENUE, SUITE 205
FT LAUDERDALE, FL 33316

EXAMINER

DALENCOURT, YVES

ART UNIT	PAPER NUMBER
----------	--------------

2457

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

04/09/2010

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

rkain@complexip.com
ekotler@complexip.com

Office Action Summary	Application No. 11/682,941	Applicant(s) REDLICH ET AL.	
	Examiner YVES DALENCOURT	Art Unit 2457	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 March 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-44 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-44 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) ☒ Notice of References Cited (PTO-892) | 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) ☐ Notice of Informal Patent Application |
| 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>3/9/2007;12/26/2007;3/5/2008;2/5/2009;3/26/2009</u> . | 6) ☐ Other: _____ |

DETAILED ACTION

This office action is responsive to communication filed on 03/07/2007.

Priority

The status of the continuation applications on page 1 of the specification needs to be updated.

Claim Objections

Claims 24 – 25, and 30 are objected to because of the following informalities: It is suggested to delete “operable“. Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1 – 7, 16 – 30, and 36 - 44 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 1 is rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory “process” under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a

different state or thing. See page 10 of In Re Bilski 88 USPQ2d 1385. The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter, and therefore do not qualify as a statutory process. The method steps recited in claim 1 is broad enough that the claims could be completely performed mentally, verbally or without a machine nor is any transformation apparent.

Claims 2 – 7 are necessarily rejected as being dependent upon the rejection of claim 1.

Claims 16 – 30 and 36 - 44 relate to a computer readable medium containing instructions; the specification describes non-statutory types of computer readable media in paragraph. The computer readable medium may include computer readable information in a transitory state medium such as a network link and/or a network interface, including a wired network or a wireless network that allow a computer to read such computer readable information [0096]. As such, the claims lack the necessary physical articles or objects to constitute a machine or a manufacture within the mean of 35 USC §101. They are clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. They are, at best, functional descriptive material per se. It is recommended to limit the claims to the physical embodiments described in paragraph [0096].

It is suggested to amend the claims by inserting before computer readable medium --- **non-transitory** --- in order to differentiate the claims from being non-statutory subject matter.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1 – 44 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 - 90 of U.S. Patent No. 7,322,047. Although the conflicting claims are not identical, they are not patentably distinct from each other because they are both performing the steps of extracting,

encrypting, and reconstructing fully or partially in put data with minor variations in the claimed language between the instant application and U.S. Patent No. 7,322,047 for the purpose of achieving the same end results.

Claims 1 – 44 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 - 73 of U.S. Patent No. 7,103,915. Although the conflicting claims are not identical, they are not patentably distinct from each other because they are both performing the steps of extracting, encrypting, and reconstructing fully or partially in put data with minor variations in the claimed language between the instant application and U.S. Patent No. 7,103,915 for the purpose of achieving the same end results.

Claims 1 – 44 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 - 85 of U.S. Patent No. 7,191,252. Although the conflicting claims are not identical, they are not patentably distinct from each other because they are both performing the steps of extracting, storing, and reconstructing fully or partially input data with minor variations in the claimed language such as reconstructing input data in the instant application as opposed to reconstructing email data in patent for the purpose of achieving the same end results.

Claims 1 – 44 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 - 73 of U.S. Patent No. 7,140,044. Although the conflicting claims are not identical, they are not patentably distinct from each other because they are both performing the steps of extracting,

encrypting, and reconstructing fully or partially in put data with minor variations in the claimed language between the instant application and U.S. Patent No. 7,140,044 for the purpose of achieving the same end results.

Claims 1 – 44 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 - 67 of U.S. Patent No. 7,146,644. Although the conflicting claims are not identical, they are not patentably distinct from each other because they are both performing the steps of extracting, encrypting, and reconstructing fully or partially in put data with minor variations in the claimed language between the instant application and U.S. Patent No. 7,146,644 for the purpose of achieving the same end results.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Fahlman et al (US 5,960,080) discloses a method for transforming message containing sensitive information.

Evan R. Kirshenbaum (US 6,602,298) discloses methods of storing and retrieving communications, information, and documents.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to YVES DALENCOURT whose telephone number is (571)272-3998. The examiner can normally be reached on M-F 8-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on (571) 272-4001. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/YVES DALENCOURT/
Primary Examiner, Art Unit 2457

Notice of References Cited	Application/Control No. 11/682,941		Applicant(s)/Patent Under Reexamination REDLICH ET AL.	
	Examiner YVES DALENCOURT		Art Unit 2457	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-7,103,915	09-2006	Redlich et al.	726/27
*	B	US-7,140,044	11-2006	Redlich et al.	726/27
*	C	US-7,146,644	12-2006	Redlich et al.	726/27
*	D	US-7,191,252	03-2007	Redlich et al.	709/246
*	E	US-7,322,047	01-2008	Redlich et al.	726/27
*	F	US-6,602,298	08-2003	Kirshenbaum, Evan R.	715/234
*	G	US-5,960,080	09-1999	Fahlman et al.	380/252
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes 	Application/Control No. 11682941	Applicant(s)/Patent Under Reexamination REDLICH ET AL.
	Examiner YVES DALENCOURT	Art Unit 2457

SEARCHED			
Class	Subclass	Date	Examiner
709	206, 218, 219, 244, 246	03/28/2010	YD
726	26, 27	03/28/2010	YD
713	166, 189	03/28/2010	YD

SEARCH NOTES		
Search Notes	Date	Examiner
WEST(see attached text search)	03/28/2010	YD

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

--	--

<i>Index of Claims</i> 	Application/Control No. 11682941	Applicant(s)/Patent Under Reexamination REDLICH ET AL.
	Examiner YVES DALENCOURT	Art Unit 2457

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant			☐ CPA			☐ T.D.			☐ R.1.47		
CLAIM		DATE									
Final	Original	03/24/2010									
	1	✓									
	2	✓									
	3	✓									
	4	✓									
	5	✓									
	6	✓									
	7	✓									
	8	✓									
	9	✓									
	10	✓									
	11	✓									
	12	✓									
	13	✓									
	14	✓									
	15	✓									
	16	✓									
	17	✓									
	18	✓									
	19	✓									
	20	✓									
	21	✓									
	22	✓									
	23	✓									
	24	✓									
	25	✓									
	26	✓									
	27	✓									
	28	✓									
	29	✓									
	30	✓									
	31	✓									
	32	✓									
	33	✓									
	34	✓									
	35	✓									
	36	✓									

<i>Index of Claims</i> 	Application/Control No. 11682941	Applicant(s)/Patent Under Reexamination REDLICH ET AL.
	Examiner YVES DALENCOURT	Art Unit 2457

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant		☐ CPA		☐ T.D.		☐ R.1.47			
CLAIM		DATE							
Final	Original	03/24/2010							
	37	✓							
	38	✓							
	39	✓							
	40	✓							
	41	✓							
	42	✓							
	43	✓							
	44	✓							

WEST Search History for Application 11682941

Creation Date: 2010032816:54

Prior Art Searches

Query	DB	Op.	Plur.	Thes.	Date
secur\$3 near3 data and extract\$3 near3 security near3 sensitive near3 word\$1	PGPB, USPT, EPAB, JPAB, DWPI, TDBD	OR	YES		03-28-2010
(extract\$3 or censor\$3 or delet\$3) adj7 (word\$1 or character\$1)	PGPB, USPT, EPAB, JPAB, DWPI, TDBD	OR	YES		03-28-2010
(restor\$3 or reconstruct\$3) adj7 (data or message\$1 or email\$1 or content)	PGPB, USPT, EPAB, JPAB, DWPI, TDBD	OR	YES		03-28-2010
(secur\$3 near3 data and extract\$3 near3 security near3 sensitive near3 word\$1) and ((extract\$3 or censor\$3 or delet\$3) adj7 (word\$1 or character\$1))	PGPB, USPT, EPAB, JPAB, DWPI, TDBD	OR	YES		03-28-2010
((restor\$3 or reconstruct\$3) adj7 (data or message\$1 or email\$1 or content)) and (secur\$3 near3 data and extract\$3 near3 security near3 sensitive near3 word\$1 and (extract\$3 or censor\$3 or delet\$3) adj7 (word\$1 or character\$1))	PGPB, USPT, EPAB, JPAB, DWPI, TDBD	OR	YES		03-28-2010
encrypt\$3 adj7 (retriev\$3 or extract\$3)adj7 (data or information)	PGPB, USPT, EPAB, JPAB, DWPI, TDBD	OR	YES		03-28-2010
		OR	YES		03-28-2010

(encrypt\$3 adj7 (retriev\$3 or extract\$3)adj7 (data or information)) and ((restor\$3 or reconstruct\$3) adj7 (data or message\$1 or email\$1 or content) and secur\$3 near3 data and extract\$3 near3 security near3 sensitive near3 word\$1 and (extract\$3 or censor\$3 or delet\$3) adj7 (word\$1 or character\$1))	PGPB, USPT, EPAB, JPAB, DWPI, TDBD				
(reasembl\$3 or restor\$3 or recostruct\$3) adj7 (message\$1 or email or e-mail or mail)	PGPB, USPT, EPAB, JPAB, DWPI, TDBD	OR	YES		03-28-2010
709/206, 218, 219, 244, 246.ccls.	PGPB, USPT, EPAB, JPAB, DWPI, TDBD	OR	YES		03-28-2010
726/26, 27.ccls.	PGPB, USPT, EPAB, JPAB, DWPI, TDBD	OR	YES		03-28-2010
713/166, 189.ccls.	PGPB, USPT, EPAB, JPAB, DWPI, TDBD	OR	YES		03-28-2010
(713/166, 189.ccls.) and (encrypt\$3 adj7 (retriev\$3 or extract\$3)adj7 (data or information) and (restor\$3 or reconstruct\$3) adj7 (data or message\$1 or email\$1 or content) and secur\$3 near3 data and extract\$3 near3 security near3 sensitive near3 word\$1 and (extract\$3 or censor\$3 or delet\$3) adj7 (word\$1 or character\$1))	PGPB, USPT, EPAB, JPAB, DWPI, TDBD	OR	YES		03-28-2010
(713/166, 189.ccls.) and ((reasembl\$3 or restor\$3 or recostruct\$3) adj7 (message\$1 or email or e-mail or mail))	PGPB, USPT, EPAB, JPAB, DWPI, TDBD	OR	YES		03-28-2010
(encrypt\$3 adj7 (retriev\$3 or extract\$3)adj7 (data or information) and (restor\$3 or reconstruct\$3) adj7 (data or message\$1 or email\$1 or content) and secur\$3 near3 data and extract\$3 near3 security	PGPB, USPT, EPAB, JPAB,	OR	YES		03-28-2010

near3 sensitive near3 word\$1 and (extract\$3 or censor\$3 or delet\$3) adj7 (word\$1 or character\$1)) and (726/26, 27.ccls.)	DWPI, TDBD				
(encrypt\$3 adj7 (retriev\$3 or extract\$3)adj7 (data or information) and (restor\$3 or reconstruct\$3) adj7 (data or message\$1 or email\$1 or content) and secur\$3 near3 data and extract\$3 near3 security near3 sensitive near3 word\$1 and (extract\$3 or censor\$3 or delet\$3) adj7 (word\$1 or character\$1)) and (709/206, 218, 219, 244, 246.ccls.)	PGPB, USPT, EPAB, JPAB, DWPI, TDBD	OR	YES		03-28-2010

INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)	Docket Number (Optional) 6851-02-CIP4-CON	Application Number 11/482,941
Title: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program	Applicant(s) Ron M. Redlich	
	Filing Date March 7, 2007	Group Art Unit ~~2457~~ 2457

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,922,696	07/26/2005	Lincoln et al.	707	101	
	7,031,961	04/18/2006	Pitkow et al.	707	4	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER

/Yves Dalencourt/

DATE CONSIDERED

03/28/2010

G:\RCK\CLIENTS\Redlich\6851-02-div2-Form PTO-1449-1.wpd

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /Y.D./

Ex. 1002, Page 215

INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>	Docket Number (Optional) 6851-02-cip4-con	Application Number 11/682,941
Title: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program	Applicant(s) Ron M. Redlich, et al.	
	Filing Date March 7, 2007	Group Art Unit 2457

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,078,907	06/20/2000	Lamm	705	40	
	6,253,203	06/26/2001	O'Flaherty et al.	707	9	
	5,960,808	09/28/1999	Fahlman et al.	380	4	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO
	CA 2 345 148	06/04/2000	Canada			X

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	"Processing of confidential information in distributed systems by fragmentation" by J. Fabre, Computer Communications Vol. 20, pp. 177-188 (1997)	
	"Secure External References in Multimedia Email Messages" B. Wiegel, ACM, pp. 11-18, Mar. 14, 1996	
	"Element-Wise XML Encryption" H. Maruyama et al., IBM Research, Tokyo Res. Lab. Ap. 19, 2000	

EXAMINER /Yves Dalencourt/

DATE CONSIDERED 03/28/2010

G:\RCK\CLIENTS\Redlich\6851-02-cip4-con-Supp-Form-PTO-1449.wpd

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /Y.D./

INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>	Docket Number (Optional) 6851-02-CIP4-CON	Application Number 11/682,941
Title: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program	Applicant(s) Ron M. Redlich	
	Filing Date March 7, 2007	Group Art Unit ~~21~~ 2457

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,845,448	01/2005	Chaganti	713	166	
	6,941,459	09/2005	Hind	713	167	
	7,010,681	03/2006	Fletcher	713	154	
	6,922,696	07/2005	Lincoln	707	101	
	7,031,961	04/2006	Pitkow	707	4	
	7,089,428	05/2006	Farley	370	231	
	7,188,107	03/2007	Moon	707	5	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER /Yves Dalencourt/

DATE CONSIDERED 03/28/2010

G:\RCK\CLIENTS\Redlich\6851-02-cip4-con-Form-PTO-1449-Master.wpd

INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)	Docket Number (Optional) 6851-02-cip4-con	Application Number 11/682,941
Title: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program	Applicant(s) Ron M. Redlich, et al.	
	Filing Date March 7, 2007	Group Art Unit ~~2457~~ 2457

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	-“Secure External References in Multimedia Email Messages” by B. Wiegel, German National Research Center, Mar. 14, 1996.	
	-“Process of Confidential Information in Distributed Systems by Fragmentation” by J. Fabre, Computer Communications 20:177 - 188, 1997.	
	-Canadian Patent Publication by S. Lanis, CA 2345148, April 6, 2000.	

EXAMINER /Yves Dalencourt/

DATE CONSIDERED

03/28/2010

G:\RCK\CLIENTS\Redlich\6851-02-cip4-con-Form-PTO-1449-supple.wpd

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /Y.D./

INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)	Docket Number (Optional) 6851-02-cip4-con	Application Number 11/682,941
Title: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program	Applicant(s) Ron M. Redlich, et al.	
	Filing Date 03/07/2007	Group Art Unit 2457

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	7,103,915	9/5/2006	Redlich et al.	726	27	
	7,140,044	11/21/2006	Redlich et al.	726	27	
	7,146,644	12/5/2006	Redlich et al.	726	27	
	6,925,454	8/2/2005	Lam et al.	706	45	
	6,874,139	3/29/2005	Krueger et al.	717	127	
	US2005/0288939	12/29/2005	Peled et al.	705	1	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	-“Protecting Privacy using the Decentralized Label Model” A. Myers, Cornell Univ. 1/1/2000.	
	-Mimesweeper Product Data sheet, Resoft Int’l LLC., Nov. 12, 2001 re-soft.com/product/mimeswep.	
	-Complete Content Security for Internet Gateways and Mail Servers, Aladdin, July 2000.	
	-Aladdin Product announcement for e-Safe Appliance, Aladdin Knowledge Sys., Ltd., Nov. 8, 2001, Aks.com/news/2001/e-safe.	

EXAMINER /Yves Dalencourt/ DATE CONSIDERED 03/28/2010

INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>	Docket Number (Optional) 6851-02-cip4-con	Application Number 11/682,941
Title: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program	Applicant(s) Ron M. Redlich, et al.	
	Filing Date 03/07/2007	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,192,472	2/20/2001	Garay et al	713	165	
	6,148,342	11/14/2000	Ho	709	225	
	6,094,483	7/25/2000	Fridrich et al	380	28	
	6,055,544	4/25/2000	DeRose et al.	707	104	
	5,996,011	11/30/1999	Humes	709	225	
	5,905,980	5/18/1999	Masuichi et al	707	1	
	5,832,212	11/3/1998	Cragun et al	395	188.01	
	5,485,474	1/16/1996	Rabin	371	37.1	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	-Mail Attender 4.1x product white paper by Sherpa Software, Oct., 2001	
	MIMesweeper-Content Security for E-mail, Web Browsing & Webmail, November 12, 2001	

EXAMINER

DATE CONSIDERED

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /Y.D./

INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>	Docket Number (Optional) 6851-02-cip4-con	Application Number 11/682,941
Title: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program	Applicant(s) Ron M. Redlich, et al.	
	Filing Date 03/07/2007	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	5,960,080	9/28/1999	Fahlman	380	4	
	6,602,298	8/05/2003	Kirshenbaum	715	502.2	
	6,487,538	11/26/2002	Gupta	705	24	
	6,771,290	8/03/2004	Hoyle	345	745	
	US2002/0116641	8/22/2002	Mastrianni	713	201	
	US2004/0054630	3/18/2004	Ginter	705	53	
	5,933,498	8/3/1999	Schneck et al.	380	4	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	Ingrian i100, Content Security Appliance (1 pages)	
	Element-Wise XML Encryption, Hiroshi Maruyama and Takeshi Imamura, IBM Research, Tokyo Research Laboratory (4 pages)	
	Survival Information Storage Systems by Jay J. Wylie, Michael W. Brigrigg, John D. Strunk, Gregory R. Ganger, Han Kiloccote Pradeep K. Khosla (8 pages)	
	ZD Net Interactive Week - IBS- SAP: XML to Boost Security Integration (1 page)	
	Myers, A.C. "Mostly-Static Decentralized Information Flow Control" M.I.T. Doctoral Thesis January, 1999	

EXAMINER

DATE CONSIDERED

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /Y.D./

INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>	Docket Number (Optional) 6851-02-cip4-con	Application Number 11/682,941
Title: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program	Applicant(s) Ron M. Redlich, et al.	
	Filing Date 03/07/2007	Group Art Unit

U.S. PATENT DOCUMENTS

Exami ner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,078,907	6/20/2000	Lamm	705	40	
	6,598,161	7/22/2003	Kluttz	713	166	
	5,036,315	7/30/1991	Gurley	340	721	
	5,532,950	7/02/1996	Moses	364	724.19	
	6,301,668	10/09/2001	Gleichauf	713	201	
	6,714,977	3/30/2004	Fowler	709	224	
	US2002/0073313	6/13/2002	Brown et al	713	165	
	WO 00/75779	12/14/2000	Lambert			
	5,581,682	12/3/1996	Anderson et al	395	792	
	6,389,542	5/14/2002	Flyntz	713	201	
	6,073,165	6/6/2000	Narasimhan et al	109	206	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER

DATE CONSIDERED

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /Y.D./

INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>	Docket Number (Optional) 6851-02-cip4-con	Application Number 11/682,941
Title: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program	Applicant(s)	
	Filing Date 03/07/2007	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,253,203	6/26/2001	O'Flaherty	707	9	
	6,044,375	3/28/2000	Shmueli	707	101	
	6,662,189	12/9/03	Oyanagi	707	102	
	5,941,944	08/24/1999	Messerly	709	203	
	6,505,150	01/07/2003	Numberg et al.	704	1	
	6,594,654	07/15/2003	Salam et al.	707	3	
	6,999,959	02/14/2006	Lawrence et al.	707	5	
	7,031,961	04/18/2006	Pitkow et al.	707	4	
	7,120,625	10/10/2006	Kagimasa et al.	707	3	
	6,978,262	12/20/2005	Tsai	707	3	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER

DATE CONSIDERED

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /Y.D./

INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>	Docket Number (Optional) 6851-02-cip4-con	Application Number 11/682,941
Title: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program	Applicant(s)	
	Filing Date 03/07/2007	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	7,007,008	02/28/2006	Goel et al.	707	3	
	7,043,492	05/09/2006	Neal et al.	707	101	
	7,085,766	08/01/2006	Keith, Jr.	707	101	
	7,113,954	09/26/2006	Vogel	707	101	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER	/Yves Dalencourt/	DATE CONSIDERED	03/28/2010
----------	-------------------	-----------------	------------

\\Tiger\data\share\IRCK\CLIENTS\Redlich\6851-02-cip4-con-IDS-Form-PTO-1449.wpd

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875					Application or Docket Number 11/682,941		Filing Date 03/07/2007		☐ To be Mailed	
APPLICATION AS FILED – PART I										
(Column 1)			(Column 2)			SMALL ENTITY ☒ OR		OTHER THAN SMALL ENTITY		
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	OR	RATE (\$)	FEE (\$)			
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A				
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A				
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A				
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X \$	=		X \$	=			
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X \$	=		X \$	=			
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).									
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))										
* If the difference in column 1 is less than zero, enter "0" in column 2.					TOTAL		TOTAL			
APPLICATION AS AMENDED – PART II										
(Column 1)			(Column 2)			SMALL ENTITY OR		OTHER THAN SMALL ENTITY		
AMENDMENT	03/31/2010	CLAIMS REMAINING AFTER AMENDMENT	MINUS	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	* 16	Minus	** 20	= 0	X \$26 =	0		X \$	=
	Independent (37 CFR 1.16(h))	* 1	Minus	*** 3	= 0	X \$110 =	0		X \$	=
☐ Application Size Fee (37 CFR 1.16(s))										
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))										
						TOTAL ADD'L FEE	0		TOTAL ADD'L FEE	
(Column 1)			(Column 2)			SMALL ENTITY OR		OTHER THAN SMALL ENTITY		
AMENDMENT	09/21/2010	CLAIMS REMAINING AFTER AMENDMENT	MINUS	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	* 9	Minus	** 20	= 0	X \$26 =	0		X \$	=
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0	X \$110 =	0		X \$	=
☐ Application Size Fee (37 CFR 1.16(s))										
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))										
						TOTAL ADD'L FEE	0		TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.										

Legal Instrument Examiner:
/GLENN BURNS JR/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.
Serial No. 11/682,941
Confirmation No.: 9976
Filed: March 7, 2007

Examiner Dalencourt
Group Art 2457

For: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program

AMENDMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This amendment responds to the Office Action dated April 9, 2010. Applicant files herewith a request for extension of time pursuant to 37 CFR §1.136 (\$555.00) for a three month extension of time. Since the six month period ended on Saturday October 9, 2010 and Monday, October 11 is a federal holiday (Columbus Day) and the USPTO is closed, the presentation of this amendment October 11 is proper. Applicant also files herewith a Terminal Disclaimer and requests that the extension of time fee (\$555.00) and the terminal disclaimer fee (\$70.00) be charged to Deposit Account No. 03-1231 (total \$625.00). Please debit or credit any underpayment or overpayment to Deposit Account No. 03-1231. This Amendment includes:

- a. Transmittal (1 pg., p. 1)
- b. Claims (9 pgs., pp. 2 - 10)
- c. Remarks (2 pgs., pp. 11 - 12)
- d. Request for Extension of Time (1 pg.)
- e. Terminal Disclaimer (4 pgs.)

[space left blank]

REMARKS

This amendment responds to the Office Action dated April 9, 2010.

With respect to claims 24, 25 and 30, Applicant has deleted the term “operable” as suggested by the Examiner. See Office Action, pg. 2, claim objections.

With respect to the computer medium claims 16 - 30 and 36 - 44, Applicant has amended independent claims 16, 23, 36 and 41 to add the term “non-transitory” as suggested by the Examiner. See Office Action pgs. 3 - 4, Section 101 rejection. Since the dependent claims all relate back to the amended independent claims, allowance is requested.

With respect to the double patenting rejection, Applicant submits herewith a Terminal disclaimer. See Office Action pgs. 4 - 6.

With respect to the Section 101 rejection of claims 1 - 7 (Office Action pgs. 2 - 3) wherein the Examiner states that these claims are not (a) tied to particular machine, or (b) transform underlying subject matter (such as an article or material) to a different state or thing, Applicant respectfully submits that the currently amended claims do transform digital data, as an article, into something other than the digital data that was input into the computer network. Claim 1 has been amended to recite:

1. (currently amended) In a computer network which processes digital data, A a method of securing digital input data having security sensitive digital content, represented by one or more security sensitive words, characters, images, data elements or data objects therein, comprising:

extracting said security sensitive digital content from said input data to obtain a plurality of extract data grouped into different security levels;

encrypting said extracted data for each said security level and one of digitally appending, adding or inserting said encrypted extracted data with remainder input data to form a composite;

responsive to a data request, digitally reconstructing fully or partially said input data from said composite with decryption of said extracted data only in the presence of a respective predetermined security clearance, required for each said security level.

First, the method now operates in a computer network which processes digital data. Second, the extraction step transforms the digital input data into another thing. The encryption step further transforms the various extracts of digital data into essentially undecipherable data, which undecipherable data is then "appending, adding or inserting said encrypted extracted data with remainder input data to form a composite." The composite is a transformed version of the digital input data. Further transformation occurs in that digital reconstruction is permitted, either fully or partially. The partial reconstruction is a changed set of digital data than the input digital data.

Therefore, it is respectfully submitted that the amended claims 1 and 8 do transform data and are within the boundaries of Section 101 of the Patent Statute. Withdrawal of the rejection and allowance of the claims is respectfully requested.

Other than the double patenting rejection, the Examiner did not reject claims 8 - 15 and 31 - 37.

No new matter is added to this case by the amendments to the various claims.

Withdrawal of all the rejections and allowance of all the claims is respectfully requested.

Respectfully submitted,

By /Robert Kain/
Robert C. Kain, Jr.
Reg. No. 30,648
Kain & Associates, Attorneys at Law, P.A.
900 Southeast Third Avenue, Suite 205
Ft. Lauderdale, Florida 33316-1153
Telephone: 954-768-9002
Facsimile: 954-768-0158

G:\RCK\CLIENTS\Redlich\Patents\6851-02-cip4-con-Amdt-1st-20101011.wpd

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 11/682,941

Confirmation No.: 9976

Examiner Dalencourt

Filed: March 7, 2007

Group Art 2457

For: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program

REQUEST FOR EXTENSION OF TIME

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is a request for extension of time pursuant to 37 CFR §1.136. Please charge \$555.00 for a three month extension of time pursuant to 37 CFR §1.17(a) to Deposit Account No. 03-1231 and please debit or credit any underpayment or overpayment to Deposit Account No. 03-1231. Applicant is a small entity.

Respectfully submitted,

By____/Robert Kain_____
Robert C. Kain, Jr.
Reg. No. 30,648
Kain & Associates, Attorneys at Law
900 Southeast Third Avenue
Suite 205
Ft. Lauderdale, Florida 33316-1153
Telephone: 954-768-9002
Facsimile: 954-768-0158

G:\RCK\CLIENTS\Redlich\6851-02-cip4-con-Req-Extend-Time-20101011.wpd

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 11/682,941

Confirmation No.: 9976

Examiner Dalencourt

Filed: March 7, 2007

Group Art 2457

For: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program

TERMINAL DISCLAIMER

Commissioner for Patents
Alexandria, VA 22313-1450

Sir:

Petitioner, Digital Doors, Inc., a Florida corporation, having its principal place of business at 4201 Collins Avenue, Suite 2103, Miami Beach, FL 33140, represents that it is the owner by assignment of all rights to (i) the captioned application and (ii) the following:

U.S. Patent No. 7,103,915, Serial No. 09/916,397, filed July 27, 2001;
U.S. Patent No. 7,140,044, Serial No. 10/008,209, filed December 6, 2001;
U.S. Patent No. 7,146,644, Serial No. 10/008,218, filed December 6, 2001;
U.S. Patent No. 7,349,987, Serial No. 10/155,192, filed May 23, 2002;
U.S. Patent No. 7,191,252, Serial No. 10/155,525, filed May 23, 2002;
U.S. Patent No. 7,313,825, Serial No. 10/390,807, filed March 19, 2003;
U.S. Patent No. 7,322,047, Serial No. 10/277,196, filed December 31, 2002;
U.S. Patent No. 7,546,334, Serial No. 10/998,365 filed November 26, 2004;
U.S. Patent No. 7,552,482, Serial No. 11/465,309, filed August 17, 2006;
Serial No. 10/998,363, filed November 26, 2004;
Serial No. 10/998,366, filed November 26, 2004;
Serial No. 10/998,365 filed November 26, 2004 (see U.S. Patent No. 7546334);
Serial No. 11/465,350 filed August 17, 2006;
Serial No. 11/465,388 filed August 17, 2006;
Serial No. 11/682,941 filed March 7, 2007 (captioned case);

Serial No. 11/829,207 filed September 6, 2007; and
Serial No. 12/403,850, filed March 13, 2009

The captioned application was assigned to Digital Doors, Inc. and the assignment was filed with the original parent application. The evidentiary document accompanying or referred to in the instant terminal disclaimer has been reviewed by the undersigned and it is certified that to the best of assignee, Digital Doors, Inc.'s knowledge and belief, title is in the assignee. Assignee is a small entity.

Petitioner, Digital Doors, Inc., hereby disclaims the terminal part of any patent granted on the above identified application, which would extend beyond the expiration date of any patent granted on any application listed below or any of the below-listed patents:

U.S. Patent No. 7,103,915, Serial No. 09/916,397, filed July 27, 2001;
U.S. Patent No. 7,140,044, Serial No. 10/008,209, filed December 6, 2001;
U.S. Patent No. 7,146,644, Serial No. 10/008,218, filed December 6, 2001;
U.S. Patent No. 7,349,987, Serial No. 10/155,192, filed May 23, 2002;
U.S. Patent No. 7,191,252, Serial No. 10/155,525, filed May 23, 2002;
U.S. Patent No. 7,313,825, Serial No. 10/390,807, filed March 19, 2003;
U.S. Patent No. 7,322,047, Serial No. 10/277,196, filed December 31, 2002;
U.S. Patent No. 7,546,334, Serial No. 10/998,365 filed November 26, 2004;
U.S. Patent No. 7,552,482, Serial No. 11/465,309, filed August 17, 2006;
Serial No. 10/998,363, filed November 26, 2004;
Serial No. 10/998,366, filed November 26, 2004;
Serial No. 10/998,365 filed November 26, 2004 (see U.S. Patent No. 7546334);
Serial No. 11/465,350 filed August 17, 2006;
Serial No. 11/465,388 filed August 17, 2006;
Serial No. 11/829,207 filed September 6, 2007; and
Serial No. 12/403,850, filed March 13, 2009

AND, except as provided below, hereby agrees that any patent so granted on the above identified applications shall be enforceable only for and during such period and that the listed patents remain commonly owned. Petitioner, Digital Doors, Inc., is a small entity.

Petitioner does not disclaim any terminal part of any patent granted on the above identified application prior to the expiration date of the full statutory term of any patent granted on:

U.S. Patent No. 7,103,915, Serial No. 09/916,397, filed July 27, 2001;
U.S. Patent No. 7,140,044, Serial No. 10/008,209, filed December 6, 2001;
U.S. Patent No. 7,146,644, Serial No. 10/008,218, filed December 6, 2001;
U.S. Patent No. 7,349,987, Serial No. 10/155,192, filed May 23, 2002;
U.S. Patent No. 7,191,252, Serial No. 10/155,525, filed May 23, 2002;
U.S. Patent No. 7,313,825, Serial No. 10/390,807, filed March 19, 2003;
U.S. Patent No. 7,322,047, Serial No. 10/277,196, filed December 31, 2002;
U.S. Patent No. 7,546,334, Serial No. 10/998,365 filed November 26, 2004;
U.S. Patent No. 7,552,482, Serial No. 11/465,309, filed August 17, 2006;
Serial No. 10/998,363, filed November 26, 2004;
Serial No. 10/998,366, filed November 26, 2004;
Serial No. 10/998,365 filed November 26, 2004 (see U.S. Patent No. 7546334);
Serial No. 11/465,350 filed August 17, 2006;
Serial No. 11/465,388 filed August 17, 2006;
Serial No. 11/829,207 filed September 6, 2007; and
Serial No. 12/403,850, filed March 13, 2009

IN THE EVENT that any latter patent: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid, is statutorily disclaimed in whole or terminally disclaimed under 37 C.F.R. §1.321(a), has all claims canceled by a reexamination certificate, is reissued, or is otherwise terminated prior to the expiration of its statutory term as presently shortened by any terminal disclaimer, except for the separation of legal title stated above.

Petitioner expressly reserves and does not waive the right to extend the term of any patent granted on:

U.S. Patent No. 7,103,915, Serial No. 09/916,397, filed July 27, 2001;
U.S. Patent No. 7,140,044, Serial No. 10/008,209, filed December 6, 2001;
U.S. Patent No. 7,146,644, Serial No. 10/008,218, filed December 6, 2001;
U.S. Patent No. 7,349,987, Serial No. 10/155,192, filed May 23, 2002;
U.S. Patent No. 7,191,252, Serial No. 10/155,525, filed May 23, 2002;
U.S. Patent No. 7,313,825, Serial No. 10/390,807, filed March 19, 2003;
U.S. Patent No. 7,322,047, Serial No. 10/277,196, filed December 31, 2002;
U.S. Patent No. 7,546,334, Serial No. 10/998,365 filed November 26, 2004;
U.S. Patent No. 7,552,482, Serial No. 11/465,309, filed August 17, 2006;
Serial No. 10/998,363, filed November 26, 2004;
Serial No. 10/998,366, filed November 26, 2004;
Serial No. 10/998,365 filed November 26, 2004 (see U.S. Patent No. 7546334);
Serial No. 11/465,350 filed August 17, 2006;
Serial No. 11/465,388 filed August 17, 2006;
Serial No. 11/829,207 filed September 6, 2007; and

Serial No. 12/403,850, filed March 13, 2009

OR ANY patent granted on the above identified application under any statute which permits such an extension of term.

I hereby declare that all statements made herein of our own knowledge are true, and that all statements made on information and belief are believed to be true; and further, that these statements were made with the knowledge that willful false statements, and the like so made, are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Dated: Oct. 11, 2010

Digital Doors, Inc.
By: ___/Robert C. Kain/_____
Robert C. Kain, Jr., Reg. No. 30,648
Kain & Associates
900 Southeast Third Avenue, Suite 205
Ft. Lauderdale, Florida 33316-1153
(954) 768-9002
Attorney of Record for Petitioner

G:\RCK\CLIENTS\Redlich\6851-02-cip4-con-Terminal-Disclaim-20101011.wpd

Electronic Patent Application Fee Transmittal

Application Number:	11682941			
Filing Date:	07-Mar-2007			
Title of Invention:	Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program			
First Named Inventor/Applicant Name:	Ron M. Redlich			
Filer:	Robert C. Kain			
Attorney Docket Number:	6851-02-cip4-con			
Filed as Small Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 3 months with \$0 paid	2253	1	555	555

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				555

Electronic Acknowledgement Receipt

EFS ID:	8599736
Application Number:	11682941
International Application Number:	
Confirmation Number:	9976
Title of Invention:	Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	04897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-02-cip4-con
Receipt Date:	11-OCT-2010
Filing Date:	07-MAR-2007
Time Stamp:	16:09:48
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Electronic Funds Transfer
Payment was successfully received in RAM	\$555
RAM confirmation Number	10760
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	----------------------------------	------------------	------------------

1	Amendment/Req. Reconsideration-After Non-Final Reject	6851-02-cip4-con- Amdt-1st-20101011-trans.pdf	19277	no	1
			25af7708d5cf636d00c0f54d4c7ada1eab07bb49		
Warnings:					
Information:					
2	Claims	6851-02-cip4-con- Amdt-1st-20101011-clms.pdf	29873	no	9
			cd5f9ee626dd7e1865b680fb13fd5ea955802fd4		
Warnings:					
Information:					
3	Applicant Arguments/Remarks Made in an Amendment	6851-02-cip4-con- Amdt-1st-20101011-rem.pdf	21493	no	2
			b1c0bc7825ccd449602e083223e881cb3816c757		
Warnings:					
Information:					
4	Extension of Time	6851-02-cip4-con-Req-Extend- Time-20101011.pdf	20827	no	1
			01c8a8d4da73a1f84b55f0f848ab2e44a3ed0084		
Warnings:					
Information:					
5	Terminal Disclaimer Filed	6851-02-cip4-con-Terminal- Disclaim-20101011.pdf	27421	no	4
			501152145956ed513e8a63802a3d28fb7763f577		
Warnings:					
Information:					
6	Fee Worksheet (PTO-875)	fee-info.pdf	30280	no	2
			824ce6b93bba74ebb454106a6039c94577f9d0eb		
Warnings:					
Information:					
Total Files Size (in bytes):			149171		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875					Application or Docket Number 11/682,941		Filing Date 03/07/2007		☒ To be Mailed			
APPLICATION AS FILED – PART I												
(Column 1)			(Column 2)		SMALL ENTITY ☒ OR			OTHER THAN SMALL ENTITY				
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	OR	RATE (\$)	FEE (\$)	OR	RATE (\$)	FEE (\$)		
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A			N/A			
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A			N/A			
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A			N/A			
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X \$	=		X \$	=		X \$	=		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X \$	=		X \$	=		X \$	=		
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).											
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))												
* If the difference in column 1 is less than zero, enter "0" in column 2.												
APPLICATION AS AMENDED – PART II												
(Column 1)			(Column 2)		(Column 3)			SMALL ENTITY OR			OTHER THAN SMALL ENTITY	
AMENDMENT	10/11/2010	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	* 44	Minus	** 44	= 0	X \$26 =	0		X \$	=		
	Independent (37 CFR 1.16(h))	* 7	Minus	*** 7	= 0	X \$110 =	0		X \$	=		
	☐ Application Size Fee (37 CFR 1.16(s))											
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))											
					TOTAL ADD'L FEE	0		TOTAL ADD'L FEE				
(Column 1)			(Column 2)		(Column 3)			SMALL ENTITY OR			OTHER THAN SMALL ENTITY	
AMENDMENT	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	*	Minus	**	=	X \$	=		X \$	=		
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X \$	=		X \$	=		
	☐ Application Size Fee (37 CFR 1.16(s))											
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))											
					TOTAL ADD'L FEE			TOTAL ADD'L FEE				
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.												

Legal Instrument Examiner:
/NICHELE PETERSON/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 10/13/2010

NPETERSO	SALE	#00000001	Mailroom Dt:	10/11/2010	031231	11682941
		01	FC : 2814	70.00	DA	

CLAIMS

1. (currently amended) In a computer network which processes digital data, A a method of securing digital input data having security sensitive digital content, represented by one or more security sensitive words, characters, images, data elements or data objects therein, comprising:

extracting said security sensitive digital content from said input data to obtain a plurality of extract data grouped into different security levels;

encrypting said extracted data for each said security level and one of digitally appending, adding or inserting said encrypted extracted data with remainder input data to form a composite;

responsive to a data request, digitally reconstructing fully or partially said input data from said composite with decryption of said extracted data only in the presence of a respective predetermined security clearance, required for each said security level.

2. (original) A method as claimed in claim 1 including displaying said security sensitive content in a distinguishing manner prior to extracting.

3. (currently amended) A method as claimed in claim 2 including permitting one of user selection and user confirmation of said security sensitive digital content.

4. (original) A method as claimed in claim 1 including providing multiple levels of encryption and corresponding multiple levels of security clearance.

5. (original) A method as claimed in claim 4 including providing multiple levels of encryption with different encryption keys corresponding to said multiple levels of security clearance.

6. (original) A method as claimed in claim 4 wherein said remainder data is encrypted with said multiple levels of encryption.

7. (currently amended) A method as claimed in claim 6 wherein the step of digital reconstruction includes decrypting one or both of said extracted data and remainder data with respect to one of more of said multiple levels of encryption based upon one or more of said multiple levels of security clearance.

8. (original) A method of securing input data having security sensitive content, represented by one or more security sensitive words, characters, images, data elements or data objects therein, the method of securing data deployed in a client-server computer system with at least one server computer operatively coupled to at least one client computer over a communications network, said client computer having a decryption routine, the method comprising:

extracting said security sensitive content from said input data to obtain a plurality of extract data grouped into different security levels;

encrypting said extracted data for each said security level and one of appending, adding or inserting said encrypted extracted data with remainder input data to form a composite; and

transmitting said composite to said at least one client computer.

9. (original) A method as claimed in claim 8 wherein said one client computer is one of a plurality of client computers and the method includes, at one of said client computers, displaying said security sensitive content in a distinguishing manner prior to extracting.

10. (original) A method as claimed in claim 9 including, at one of said client computers, permitting one of user selection and user confirmation of said security sensitive content prior to extracting.

11. (original) A method as claimed in claim 8 including providing multiple levels of encryption and corresponding multiple levels of security clearance.

12. (original) A method as claimed in claim 8 including providing multiple levels, types or keys for encryption for said different levels of security clearance.

13. (original) A method as claimed in claim 11 wherein said remainder data is encrypted with said multiple levels of encryption.

14. (original) A method as claimed in claim 8 wherein said extracting said security sensitive content and encrypting said extracted data and transmitting said composite to said at least one client computer occurs at said server computer.

15. (original) A method as claimed in claim 8 wherein said one client computer is one of a plurality of client computers and the method includes said extracting said security sensitive content and encrypting said extracted data occurs at one of said client computers, and transmitting said composite to another client computer occurs via said server computer.

16. (currently amended) A non-transitory computer readable medium containing programming instructions for a method of securing input data having security sensitive content, represented by one or more security sensitive words, characters, images, data elements or data objects therein, comprising:

extracting said security sensitive content from said input data to obtain a plurality of extract data grouped into different security levels;

encrypting said extracted data for each said security level and one of appending, adding or inserting said encrypted extracted data with remainder input data to form a composite;

responsive to a data request, reconstructing fully or partially said input data from said composite with decryption of said extracted data only in the presence of a respective predetermined security clearance, required for each said security level.

17. (original) A computer readable medium containing programming instructions for the method as claimed in claim 16 including displaying said security sensitive content in a distinguishing manner prior to extracting.

18. (original) A computer readable medium containing programming instructions for the method as claimed in claim 17 including permitting one of user selection and user confirmation of said security sensitive content.

19. (original) A computer readable medium containing programming instructions for the method as claimed in claim 16 including providing multiple levels of encryption and corresponding multiple levels of security clearance.

20. (original) A computer readable medium containing programming instructions for the method as claimed in claim 19 including providing multiple levels of encryption with different encryption keys corresponding to said multiple levels of security clearance.

21. (original) A computer readable medium containing programming instructions for the method as claimed in claim 19 wherein said remainder data is encrypted with said multiple levels of encryption.

22. (original) A computer readable medium containing programming instructions for the method as claimed in claim 21 wherein the step of reconstruction includes decrypting one or both of said extracted data and remainder data with respect to one of more of said multiple levels of encryption based upon one or more of said multiple levels of security clearance.

23. (currently amended) A non-transitory computer readable medium containing programming instructions for a method of securing input data having security sensitive content, represented by one or more security sensitive words, characters, images, data elements or data

objects therein, the method of securing data deployed in a client-server computer system with at least one server computer operatively coupled to at least one client computer over a communications network, said client computer having a decryption routine, the programming instructions comprising:

extracting said security sensitive content from said input data to obtain a plurality of extract data grouped into different security levels;

encrypting said extracted data for each said security level and one of appending, adding or inserting said encrypted extracted data with remainder input data to form a composite; and

transmitting said composite to said at least one client computer.

24. (currently amended) A computer readable medium containing programming instructions for a method as claimed in claim 23 ~~operable~~ wherein said one client computer is one of a plurality of client computers and the programming instructions include, at one of said client computers, displaying said security sensitive content in a distinguishing manner prior to extracting.

25. (currently amended) A computer readable medium containing programming instructions for a method as claimed in claim 24 ~~operable~~ wherein, at one of said client computers, permitting one of user selection and user confirmation of said security sensitive content prior to extracting.

26. (original) A computer readable medium containing programming instructions for a method as claimed in claim 23 including providing multiple levels of encryption and corresponding multiple levels of security clearance.

27. (original) A computer readable medium containing programming instructions for a method as claimed in claim 23 including providing multiple levels, types or keys for encryption for said different levels of security clearance.

28. (original) A computer readable medium containing programming instructions for a method as claimed in claim 26 wherein said remainder data is encrypted with said multiple levels of encryption.

29. (original) A computer readable medium containing programming instructions for a method as claimed in claim 23 wherein said extracting said security sensitive content and encrypting said extracted data and transmitting said composite to said at least one client computer occurs at said server computer.

30. (currently amended) A computer readable medium containing programming instructions for a method as claimed in claim 23 ~~operable~~ wherein said one client computer is one of a plurality of client computers and the programming instructions include extracting said security sensitive content and encrypting said extracted data at one of said client computers, and transmitting said composite to another client computer occurs via said server computer.

31. (original) A method of securing input data passing through a browser, said input data having security sensitive content, represented by one or more security sensitive words, characters, images, data elements or data objects therein, the method deployed in a distributed computer system with a plurality of extract stores, each having a security level and a clearance therefor, comprising:

extracting said security sensitive content from said input data to obtain extracted data for respective security levels;

facilitating the storage of said extracted data in respective ones of said extract stores; and

forwarding any remainder input data to a target destination in said distributed computer system and requiring predetermined security clearances to access said extract stores.

32. (original) A method as claimed in claim 31 including filtering said data while extracting.

33. (original) A method as claimed in claim 32 including defining the filter with a group of security sensitive content and the method includes one of storing said filter or destroying said filter after storing said extracted data.

34. (original) A method as claimed in claim 33 including encrypting one or both of said extracted data and said remainder data.

35. (original) A method as claimed in claim 31 wherein the extracting step operates on credit data, financial data or account data.

36. (currently amended) A non-transitory computer readable medium containing programming instructions for securing input data passing through a browser, said input data having security sensitive content, represented by one or more security sensitive words, characters, images, data elements or data objects therein, the programming instructions operably deployed in a distributed computer system with a plurality of extract stores, each having a security level and a clearance therefor, comprising:

extracting said security sensitive content from said input data to obtain extracted data for respective security levels;

facilitating the storage of said extracted data in respective ones of said extract stores; and

forwarding any remainder input data to a target destination in said distributed computer system and requiring predetermined security clearances to access said extract stores.

37. (original) A computer readable medium containing programming instructions for securing input data as claimed in claim 36 including filtering said data while extracting.

38. (original) A computer readable medium containing programming instructions for securing input data as claimed in claim 37 including defining the filter with a group of security sensitive content and the programming instructions include one of storing said filter or destroying said filter after storing said extracted data.

39. (original) A computer readable medium containing programming instructions for securing input data as claimed in claim 38 including encrypting one or both of said extracted data and said remainder data.

40. (original) A computer readable medium containing programming instructions for securing input data as claimed in claim 36 wherein the extracting step operates on credit data, financial data or account data.

41. (currently amended) A non-transitory computer readable medium containing programming instructions for securing data passing through a browser, said data having one or more security sensitive words, characters or icons, used in conjunction with a distributed computer system with a plurality of remote memories respectively designated as corresponding extract stores, each having a respective security level and clearance, comprising:

extracting said security sensitive words, characters or icons from said data to obtain extracted data for respective security levels and remainder data therefrom;

facilitating the storage of said extracted data in respective ones of said extract stores; and

forwarding said remainder data to a targeted destination in said distributed computer system and requiring a respective predetermined security clearance for access to corresponding extract stores.

42. (original) A medium with programming instructions as claimed in claim 41 including filtering said data while extracting.

43. (original) A medium with programming instructions as claimed in claim 42 including defining the filter with a group of security sensitive words, characters or icons and the method includes one of storing said filter or destroying said filter after storing said extracted data.

44. (original) A medium with programming instructions as claimed in claim 43 including encrypting one or both of said extracted data and said remainder data.

Application Number 	Application/Control No. 11/682,941	Applicant(s)/Patent under Reexamination REDLICH ET AL.	
Document Code - DISQ		Internal Document – DO NOT MAIL	

TERMINAL DISCLAIMER	☐ APPROVED	☒ DISAPPROVED
Date Filed : 10/11/10	This patent is subject to a Terminal Disclaimer	

Approved/Disapproved by:
Felicia D. Roberts Improper language: - Page 2: The enforceable clause is improper. It only states that the "listed patents" remain commonly owned. It does not mention the listed applications. - Page 3: "except for the separation of legal title stated above" is not acceptable language. - Page 3-4: extensions and conditions are unacceptable language. Please use the forms at the end of Chapter 1400 of the MPEP or the form paragraphs in 1490, or language that is clear and complies with the TD rules.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

11/682,941

03/07/2007

Ron M. Redlich

6851-02-cip4-con

9976

4897

7590

12/27/2010

ROBERT C. KAIN, JR.

KAIN & ASSOCIATES, ATTORNEYS AT LAW, P.A.

900 SOUTHEAST THIRD AVENUE, SUITE 205

FT LAUDERDALE, FL 33316

EXAMINER

DALENCOURT, YVES

ART UNIT

PAPER NUMBER

2457

NOTIFICATION DATE

DELIVERY MODE

12/27/2010

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

rkain@complexip.com

ekotler@complexip.com

Office Action Summary	Application No. 11/682,941	Applicant(s) REDLICH ET AL.	
	Examiner YVES DALENCOURT	Art Unit 2457	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 11 October 2010.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-44 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-44 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) ☐ Notice of References Cited (PTO-892) | 4) ☐ Interview Summary (PTO-413) |
| 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) ☐ Information Disclosure Statement(s) (PTO/SB/08) | 5) ☐ Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) ☐ Other: _____ |

DETAILED ACTION

This office action is responsive to amendment filed on 10/11/2010.

Response to Amendment

The Examiner has acknowledged the amended claims 1, 3, 7, 16, 23, 24, 30, 36, and 41.

Response to Arguments

Applicant's arguments, see amendment, filed 10/11/2010, with respect to the rejection(s) of claim(s) 1 - 44 under 35 USC § 101 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, and since the Terminal Disclaimer has been disapproved, the double patenting rejection is maintained.

The Terminal Disclaimer has been disapproved because of improper language:

On page 2 of the TD, the enforceable clause is improper because it only states that the "listed patents" remain commonly owned without mentioning the listed applications. Also, Applicant needs to delete "except for the separation of legal title stated above. Petitioner expressly reserves and does not waive the right to extend the term of any patent granted on OR ANY patent granted on the above identified filed application under any statute which permits such an extension of term" (pages 3 – 4).

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory

Art Unit: 2457

obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1 – 44 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 - 90 of U.S. Patent No. 7,322,047. Although the conflicting claims are not identical, they are not patentably distinct from each other because they are both performing the steps of extracting, encrypting, and reconstructing fully or partially in put data with minor variations in the claimed language between the instant application and U.S. Patent No. 7,322,047 for the purpose of achieving the same end results.

Claims 1 – 44 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 - 73 of U.S. Patent No. 7,103,915. Although the conflicting claims are not identical, they are not patentably distinct from each other because they are both performing the steps of extracting, encrypting, and reconstructing fully or partially in put data with minor variations in the

claimed language between the instant application and U.S. Patent No. 7,103,915 for the purpose of achieving the same end results.

Claims 1 – 44 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 - 85 of U.S. Patent No. 7,191,252. Although the conflicting claims are not identical, they are not patentably distinct from each other because they are both performing the steps of extracting, storing, and reconstructing fully or partially input data with minor variations in the claimed language such as reconstructing input data in the instant application as opposed to reconstructing email data in patent for the purpose of achieving the same end results.

Claims 1 – 44 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 - 73 of U.S. Patent No. 7,140,044. Although the conflicting claims are not identical, they are not patentably distinct from each other because they are both performing the steps of extracting, encrypting, and reconstructing fully or partially in put data with minor variations in the claimed language between the instant application and U.S. Patent No. 7,140,044 for the purpose of achieving the same end results.

Claims 1 – 44 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 - 67 of U.S. Patent No. 7,146,644. Although the conflicting claims are not identical, they are not patentably distinct from each other because they are both performing the steps of extracting, encrypting, and reconstructing fully or partially in put data with minor variations in the

claimed language between the instant application and U.S. Patent No. 7,146,644 for the purpose of achieving the same end results.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to YVES DALENCOURT whose telephone number is (571)272-3998. The examiner can normally be reached on M-F 8-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on (571) 272-4001. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/YVES DALENCOURT/
Primary Examiner, Art Unit 2457

Index of Claims *1168294 1*	Application/Control No. 11682941	Applicant(s)/Patent Under Reexamination REDLICH ET AL.
	Examiner YVES DALENCOURT	Art Unit 2457

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant				☐ CPA				☐ T.D.				☐ R.1.47			
CLAIM		DATE													
Final	Original	03/24/2010	12/14/2010												
	1	✓	✓												
	2	✓	✓												
	3	✓	✓												
	4	✓	✓												
	5	✓	✓												
	6	✓	✓												
	7	✓	✓												
	8	✓	✓												
	9	✓	✓												
	10	✓	✓												
	11	✓	✓												
	12	✓	✓												
	13	✓	✓												
	14	✓	✓												
	15	✓	✓												
	16	✓	✓												
	17	✓	✓												
	18	✓	✓												
	19	✓	✓												
	20	✓	✓												
	21	✓	✓												
	22	✓	✓												
	23	✓	✓												
	24	✓	✓												
	25	✓	✓												
	26	✓	✓												
	27	✓	✓												
	28	✓	✓												
	29	✓	✓												
	30	✓	✓												
	31	✓	✓												
	32	✓	✓												
	33	✓	✓												

<i>Index of Claims</i> *1168294 1*	Application/Control No. 11682941	Applicant(s)/Patent Under Reexamination REDLICH ET AL.
	Examiner YVES DALENCOURT	Art Unit 2457

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant				☐ CPA				☐ T.D.				☐ R.1.47			
CLAIM		DATE													
Final	Original	03/24/2010	12/14/2010												
	34	✓	✓												
	35	✓	✓												
	36	✓	✓												
	37	✓	✓												
	38	✓	✓												
	39	✓	✓												
	40	✓	✓												
	41	✓	✓												
	42	✓	✓												
	43	✓	✓												
	44	✓	✓												

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 11/682,941

Confirmation No.: 9976

Examiner Dalencourt

Filed: March 7, 2007

Group Art. 2457

For: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program

RESPONSE TO FINAL OFFICE ACTION

Commissioner for Patents
Alexandria, VA 22313-1450

Sir:

This response (1 pg.) and the enclosed Terminal Disclaimer (3 pgs.) respond to the Office Action dated December 27, 2010. Applicant paid the Terminal Disclaimer fee with the last amendment.

Digital Doors, Inc.

Dated: Jan. 3, 2011

By: ___/Robert C. Kain/_____
Robert C. Kain, Jr., Reg. No. 30,648
Kain & Associates
900 Southeast Third Avenue, Suite 205
Ft. Lauderdale, Florida 33316-1153
(954) 768-9002
Attorney of Record for Petitioner

G:\RCK\CLIENTS\Redlich\6251-02-cip1-con-Resp-final-OA-20110103.wpd

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 11/682,941

Confirmation No.: 9976

Examiner Dalencourt

Filed: March 7, 2007

Group Art 2457

For: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program

TERMINAL DISCLAIMER

Commissioner for Patents
Alexandria, VA 22313-1450

Sir:

Petitioner, Digital Doors, Inc., a Florida corporation, having its principal place of business at 4201 Collins Avenue, Suite 2103, Miami Beach, FL 33140, represents that it is the owner by assignment of all rights to (i) the captioned application and (ii) the following:

U.S. Patent No. 7,103,915, Serial No. 09/916,397, filed July 27, 2001;
U.S. Patent No. 7,140,044, Serial No. 10/008,209, filed December 6, 2001;
U.S. Patent No. 7,146,644, Serial No. 10/008,218, filed December 6, 2001;
U.S. Patent No. 7,349,987, Serial No. 10/155,192, filed May 23, 2002;
U.S. Patent No. 7,191,252, Serial No. 10/155,525, filed May 23, 2002;
U.S. Patent No. 7,313,825, Serial No. 10/390,807, filed March 19, 2003;
U.S. Patent No. 7,322,047, Serial No. 10/277,196, filed December 31, 2002;
U.S. Patent No. 7,546,334, Serial No. 10/998,365 filed November 26, 2004;
U.S. Patent No. 7,552,482, Serial No. 11/465,309, filed August 17, 2006;
Serial No. 10/998,363, filed November 26, 2004;
Serial No. 10/998,366, filed November 26, 2004;
Serial No. 10/998,365 filed November 26, 2004 (see U.S. Patent No. 7546334);
Serial No. 11/465,350 filed August 17, 2006;
Serial No. 11/465,388 filed August 17, 2006;
Serial No. 11/682,941 filed March 7, 2007 (captioned case);
Serial No. 11/829,207 filed September 6, 2007; and
Serial No. 12/403,850, filed March 13, 2009

The captioned application was assigned to Digital Doors, Inc. and the assignment was filed with the original parent application. The evidentiary document accompanying or referred to in the instant terminal disclaimer has been reviewed by the undersigned and it is certified that to the best of assignee, Digital Doors, Inc.'s knowledge and belief, title is in the assignee. Assignee is a small entity.

Petitioner, Digital Doors, Inc., hereby disclaims the terminal part of any patent granted on the above identified application, which would extend beyond the expiration date of any patent granted on any application listed below or any of the below-listed patents:

U.S. Patent No. 7,103,915, Serial No. 09/916,397, filed July 27, 2001;
U.S. Patent No. 7,140,044, Serial No. 10/008,209, filed December 6, 2001;
U.S. Patent No. 7,146,644, Serial No. 10/008,218, filed December 6, 2001;
U.S. Patent No. 7,349,987, Serial No. 10/155,192, filed May 23, 2002;
U.S. Patent No. 7,191,252, Serial No. 10/155,525, filed May 23, 2002;
U.S. Patent No. 7,313,825, Serial No. 10/390,807, filed March 19, 2003;
U.S. Patent No. 7,322,047, Serial No. 10/277,196, filed December 31, 2002;
U.S. Patent No. 7,546,334, Serial No. 10/998,365 filed November 26, 2004;
U.S. Patent No. 7,552,482, Serial No. 11/465,309, filed August 17, 2006;
Serial No. 10/998,363, filed November 26, 2004;
Serial No. 10/998,366, filed November 26, 2004;
Serial No. 10/998,365 filed November 26, 2004 (see U.S. Patent No. 7546334);
Serial No. 11/465,350 filed August 17, 2006;
Serial No. 11/465,388 filed August 17, 2006;
Serial No. 11/829,207 filed September 6, 2007; and
Serial No. 12/403,850, filed March 13, 2009

AND, except as provided below, hereby agrees that any patent so granted on the above identified applications shall be enforceable only for and during such period and that the listed patents and patent applications remain commonly owned. Petitioner, Digital Doors, Inc., is a small entity.

Petitioner does not disclaim any terminal part of any patent granted on the above identified application prior to the expiration date of the full statutory term of any patent granted on:

U.S. Patent No. 7,103,915, Serial No. 09/916,397, filed July 27, 2001;

U.S. Patent No. 7,140,044, Serial No. 10/008,209, filed December 6, 2001;
U.S. Patent No. 7,146,644, Serial No. 10/008,218, filed December 6, 2001;
U.S. Patent No. 7,349,987, Serial No. 10/155,192, filed May 23, 2002;
U.S. Patent No. 7,191,252, Serial No. 10/155,525, filed May 23, 2002;
U.S. Patent No. 7,313,825, Serial No. 10/390,807, filed March 19, 2003;
U.S. Patent No. 7,322,947, Serial No. 10/277,196, filed December 31, 2002;
U.S. Patent No. 7,546,334, Serial No. 10/998,365 filed November 26, 2004;
U.S. Patent No. 7,552,482, Serial No. 11/465,309, filed August 17, 2006;
Serial No. 10/998,363, filed November 26, 2004;
Serial No. 10/998,366, filed November 26, 2004;
Serial No. 10/998,365 filed November 26, 2004 (see U.S. Patent No. 7,546,334);
Serial No. 11/465,350 filed August 17, 2006;
Serial No. 11/465,388 filed August 17, 2006;
Serial No. 11/829,207 filed September 6, 2007; and
Serial No. 12/403,850, filed March 13, 2009

IN THE EVENT that any latter patent: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid, is statutorily disclaimed in whole or terminally disclaimed under 37 C.F.R. §1.321(a), has all claims canceled by a reexamination certificate, is reissued, or is otherwise terminated prior to the expiration of its statutory term as presently shortened by any terminal disclaimer.

I hereby declare that all statements made herein of our own knowledge are true, and that all statements made on information and belief are believed to be true; and further, that these statements were made with the knowledge that willful false statements, and the like so made, are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Dated: Jan. 3, 2011

Digital Doors, Inc.
By: ____/Robert C. Kain/_____
Robert C. Kain, Jr., Reg. No. 30,648
Kain & Associates
900 Southeast Third Avenue, Suite 205
Ft. Lauderdale, Florida 33316-1153
(954) 768-9002
Attorney of Record for Petitioner

G:\RCK\CLIENTS\Rediff\0831-02-cipl-con-Terminat-Disclaim-20110103.wpd

Electronic Acknowledgement Receipt

EFS ID:	9152796
Application Number:	11682941
International Application Number:	
Confirmation Number:	9976
Title of Invention:	Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	04897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-02-cip4-con
Receipt Date:	03-JAN-2011
Filing Date:	07-MAR-2007
Time Stamp:	16:19:40
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment After Final	6851-02-cip4-con-Resp-final-OA-20110103.pdf	63901 adf7dedab92c482ab882c811d2e49b29987a8f53	no	1

Warnings:

Information:

2	Terminal Disclaimer Filed	6851-02-cip4-con-Terminal-Disclaim-20110103.pdf	213603 f3ec186a042ffa9db9d83bb83c18e5d6bfa835aa	no	3
Warnings:					
Information:					
Total Files Size (in bytes):				277504	
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					

Application Number 	Application/Control No. 11/682,941	Applicant(s)/Patent under Reexamination REDLICH ET AL.	
Document Code - DISQ		Internal Document – DO NOT MAIL	

TERMINAL DISCLAIMER	☒ APPROVED	☐ DISAPPROVED
Date Filed : 03 JAN 2011	This patent is subject to a Terminal Disclaimer	

Approved/Disapproved by:
JAB



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

4897 7590 02/04/2011

ROBERT C. KAIN, JR.
KAIN & ASSOCIATES, ATTORNEYS AT LAW, P.A.
900 SOUTHEAST THIRD AVENUE, SUITE 205
FT LAUDERDALE, FL 33316

EXAMINER

DALENCOURT, YVES

ART UNIT

PAPER NUMBER

2457

DATE MAILED: 02/04/2011

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

11/682,941

03/07/2007

Ron M. Redlich

6851-02-CIP4-CON

9976

TITLE OF INVENTION: DATA SECURITY SYSTEM AND METHOD ADJUNCT TO A BROWSER, TELECOM OR ENCRYPTION PROGRAM

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	\$755	\$300	\$0	\$1055	05/04/2011

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

**Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

4897 7590 02/04/2011

ROBERT C. KAIN, JR.
KAIN & ASSOCIATES, ATTORNEYS AT LAW, P.A.
900 SOUTHEAST THIRD AVENUE, SUITE 205
FT LAUDERDALE, FL 33316

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

11/682,941 03/07/2007 Ron M. Redlich 6851-02-CIP4-CON 9976

TITLE OF INVENTION: DATA SECURITY SYSTEM AND METHOD ADJUNCT TO A BROWSER, TELECOM OR ENCRYPTION PROGRAM

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
-------------	--------------	---------------	---------------------	----------------------	------------------	----------

nonprovisional YES \$755 \$300 \$0 \$1055 05/04/2011

EXAMINER	ART UNIT	CLASS-SUBCLASS
----------	----------	----------------

DALENCOURT, YVES 2457 726-027000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

- (1) the names of up to 3 registered patent attorneys or agents OR, alternatively, 1 _____
- (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2 _____
- 3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

- ☐ Issue Fee
- ☐ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies _____

4b. Payment of Fee(s); (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

11/682,941

03/07/2007

Ron M. Redlich

6851-02-CIP4-CON

9976

4897

7590

02/04/2011

EXAMINER

DALENCOURT, YVES

ART UNIT

PAPER NUMBER

2457

DATE MAILED: 02/04/2011

ROBERT C. KAIN, JR.
KAIN & ASSOCIATES, ATTORNEYS AT LAW, P.A.
900 SOUTHEAST THIRD AVENUE, SUITE 205
FT LAUDERDALE, FL 33316

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 608 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 608 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Notice of Allowability	Application No.	Applicant(s)	
	11/682,941	REDLICH ET AL.	
	Examiner	Art Unit	
	YVES DALENCOURT	2457	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 01/03/2011.
2. ☒ The allowed claim(s) is/are 1-44.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: ____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date ____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date ____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|--|--|
| <ol style="list-style-type: none"> 1. ☐ Notice of References Cited (PTO-892) 2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 3. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date ____ 4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material | <ol style="list-style-type: none"> 5. ☐ Notice of Informal Patent Application 6. ☒ Interview Summary (PTO-413),
Paper No./Mail Date <u>01/27/2011</u>. 7. ☒ Examiner's Amendment/Comment 8. ☐ Examiner's Statement of Reasons for Allowance 9. ☐ Other ____. |
|--|--|

YVES DALENCOURT/
Primary Examiner, Art Unit 2457

DETAILED ACTION

This office action is responsive to amendment filed on 01/03/2011.

Response to Amendment

The Examiner has acknowledged the amended claims 1, 3, 7, 16, 23, - 25, 30, 36, and 41. The objection of claims 24 – 25 and the 35 U.S.C. 101 rejection of claims 1 – 7, 16 – 30, and 36 – 44 have been withdrawn. The Double Patenting rejection has been withdrawn based on the approved terminal disclaimer filed on 01/03/2011.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Robert C. Kain, Jr. on 01/27/2011.

The application has been amended as follows:

In claims 1, 8, 16, and 23, delete "from" (claim 1, line 7; claim 8, line 9; claim 16, line 8; and claim 23, line 11), and insert --- form ---.

Allowable Subject Matter

Claims 1 – 44 are allowed.

The following is an examiner's statement of reasons for allowance: The closest prior art (US 5,960,080) discloses transforming an original message into a final message by including an untrusted service includes the steps of identifying at least one sensitive term from the original message; replacing the at least one sensitive term with a standard token to create a sanitized message; storing the at least one sensitive term; transmitting the sanitized message to a provider of the untrusted service; performing the untrusted service on the sanitized message to create a serviced message; merging the serviced message with the at least one sensitive term stored in the storing step to create the final message. Such prior art fails to disclose, among other limitations, in combination the steps of encrypting said extracted data for each said security level and one of appending, adding or inserting said encrypted extracted data with remainder input data to form a composite; responsive to a data request, reconstructing fully or partially said input data from said composite with decryption of said extracted data only in the presence of a respective predetermined security clearance, required for each said security level.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to YVES DALENCOURT whose telephone number is (571)272-3998. The examiner can normally be reached on M-F 8-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on (571) 272-4001. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/YVES DALENCOURT/
Primary Examiner, Art Unit 2457

<i>Index of Claims</i> 	Application/Control No. 11682941	Applicant(s)/Patent Under Reexamination REDLICH ET AL.
	Examiner YVES DALENCOURT	Art Unit 2457

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☒ Claims renumbered in the same order as presented by applicant					☐ CPA					☒ T.D.					☐ R.1.47				
CLAIM		DATE																	
Final	Original	03/24/2010	12/14/2010	01/26/2011															
	1	✓	✓	=															
	2	✓	✓	=															
	3	✓	✓	=															
	4	✓	✓	=															
	5	✓	✓	=															
	6	✓	✓	=															
	7	✓	✓	=															
	8	✓	✓	=															
	9	✓	✓	=															
	10	✓	✓	=															
	11	✓	✓	=															
	12	✓	✓	=															
	13	✓	✓	=															
	14	✓	✓	=															
	15	✓	✓	=															
	16	✓	✓	=															
	17	✓	✓	=															
	18	✓	✓	=															
	19	✓	✓	=															
	20	✓	✓	=															
	21	✓	✓	=															
	22	✓	✓	=															
	23	✓	✓	=															
	24	✓	✓	=															
	25	✓	✓	=															
	26	✓	✓	=															
	27	✓	✓	=															
	28	✓	✓	=															
	29	✓	✓	=															
	30	✓	✓	=															
	31	✓	✓	=															
	32	✓	✓	=															
	33	✓	✓	=															
	34	✓	✓	=															
	35	✓	✓	=															
	36	✓	✓	=															

<i>Index of Claims</i> 	Application/Control No. 11682941	Applicant(s)/Patent Under Reexamination REDLICH ET AL.
	Examiner YVES DALENCOURT	Art Unit 2457

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☒ Claims renumbered in the same order as presented by applicant					☐ CPA					☒ T.D.					☐ R.1.47				
CLAIM		DATE																	
Final	Original	03/24/2010	12/14/2010	01/26/2011															
	37	✓	✓	=															
	38	✓	✓	=															
	39	✓	✓	=															
	40	✓	✓	=															
	41	✓	✓	=															
	42	✓	✓	=															
	43	✓	✓	=															
	44	✓	✓	=															

Bib Data Sheet Maintenance

Application No*:	11682941	Search	Clear
Foreign Priority claimed:	☐ yes ☒ no		
35 USC 119(a-d) conditions met:	☐ yes ☒ no		
Verified and Acknowledged:	YVES DALENCOURT		☐ Met after Allowance
	Examiner's Signature	Initials	
TITLE:	Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program		Update

Please enter amendment.

/YD/

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich, et al.

Serial No. 11/682,941

Confirmation No.: 9976

Examiner Dalencourt

Filed: March 7, 2007

Group Art. 2457

For: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program

RESPONSE TO FINAL OFFICE ACTION

Commissioner for Patents
Alexandria, VA 22313-1450

Sir:

This response (1 pg.) and the enclosed Terminal Disclaimer (3 pgs.) respond to the Office Action dated December 27, 2010. Applicant paid the Terminal Disclaimer fee with the last amendment.

Digital Doors, Inc.

Dated: Jan. 3, 2011

By: ___/Robert C. Kain/_____
Robert C. Kain, Jr., Reg. No. 30,648
Kain & Associates
900 Southeast Third Avenue, Suite 205
Ft. Lauderdale, Florida 33316-1153
(954) 768-9002
Attorney of Record for Petitioner

G:\RCK\CLIENTS\Redlich\6251-02-cip1-con-Resp-final-OA-20110103.wpd

WEST Search History for Application 11682941

Creation Date: 2011012620:42

Prior Art Searches

Query	DB	Op.	Plur.	Thes.	Date
secur\$3 near3 data and extract\$3 near3 security near3 sensitive near3 word\$1	PGPB, USPT, EPAB, JPAB, DWPI, TDBD	OR	YES		03-28-2010
(extract\$3 or censor\$3 or delet\$3) adj7 (word\$1 or character\$1)	PGPB, USPT, EPAB, JPAB, DWPI, TDBD	OR	YES		03-28-2010
(restor\$3 or reconstruct\$3) adj7 (data or message\$1 or email\$1 or content)	PGPB, USPT, EPAB, JPAB, DWPI, TDBD	OR	YES		03-28-2010
(secur\$3 near3 data and extract\$3 near3 security near3 sensitive near3 word\$1) and ((extract\$3 or censor\$3 or delet\$3) adj7 (word\$1 or character\$1))	PGPB, USPT, EPAB, JPAB, DWPI, TDBD	OR	YES		03-28-2010
((restor\$3 or reconstruct\$3) adj7 (data or message\$1 or email\$1 or content)) and (secur\$3 near3 data and extract\$3 near3 security near3 sensitive near3 word\$1 and (extract\$3 or censor\$3 or delet\$3) adj7 (word\$1 or character\$1))	PGPB, USPT, EPAB, JPAB, DWPI, TDBD	OR	YES		03-28-2010
encrypt\$3 adj7 (retriev\$3 or extract\$3)adj7 (data or information)	PGPB, USPT, EPAB, JPAB, DWPI, TDBD	OR	YES		03-28-2010
		OR	YES		03-28-2010

(encrypt\$3 adj7 (retriev\$3 or extract\$3)adj7 (data or information)) and ((restor\$3 or reconstruct\$3) adj7 (data or message\$1 or email\$1 or content) and secur\$3 near3 data and extract\$3 near3 security near3 sensitive near3 word\$1 and (extract\$3 or censor\$3 or delet\$3) adj7 (word\$1 or character\$1))	PGPB, USPT, EPAB, JPAB, DWPI, TDBD				
(reasembl\$3 or restor\$3 or recostruct\$3) adj7 (message\$1 or email or e-mail or mail)	PGPB, USPT, EPAB, JPAB, DWPI, TDBD	OR	YES		03-28-2010
709/206, 218, 219, 244, 246.ccls.	PGPB, USPT, EPAB, JPAB, DWPI, TDBD	OR	YES		03-28-2010
726/26, 27.ccls.	PGPB, USPT, EPAB, JPAB, DWPI, TDBD	OR	YES		03-28-2010
713/166, 189.ccls.	PGPB, USPT, EPAB, JPAB, DWPI, TDBD	OR	YES		03-28-2010
(713/166, 189.ccls.) and (encrypt\$3 adj7 (retriev\$3 or extract\$3)adj7 (data or information) and (restor\$3 or reconstruct\$3) adj7 (data or message\$1 or email\$1 or content) and secur\$3 near3 data and extract\$3 near3 security near3 sensitive near3 word\$1 and (extract\$3 or censor\$3 or delet\$3) adj7 (word\$1 or character\$1))	PGPB, USPT, EPAB, JPAB, DWPI, TDBD	OR	YES		03-28-2010
(713/166, 189.ccls.) and ((reasembl\$3 or restor\$3 or recostruct\$3) adj7 (message\$1 or email or e-mail or mail))	PGPB, USPT, EPAB, JPAB, DWPI, TDBD	OR	YES		03-28-2010
(encrypt\$3 adj7 (retriev\$3 or extract\$3)adj7 (data or information) and (restor\$3 or reconstruct\$3) adj7 (data or message\$1 or email\$1 or content) and secur\$3 near3 data and extract\$3 near3 security	PGPB, USPT, EPAB, JPAB,	OR	YES		03-28-2010

near3 sensitive near3 word\$1 and (extract\$3 or censor\$3 or delet\$3) adj7 (word\$1 or character\$1)) and (726/26, 27.ccls.)	DWPI, TDBD				
(encrypt\$3 adj7 (retriev\$3 or extract\$3)adj7 (data or information) and (restor\$3 or reconstruct\$3) adj7 (data or message\$1 or email\$1 or content) and secur\$3 near3 data and extract\$3 near3 security near3 sensitive near3 word\$1 and (extract\$3 or censor\$3 or delet\$3) adj7 (word\$1 or character\$1)) and (709/206, 218, 219, 244, 246.ccls.)	PGPB, USPT, EPAB, JPAB, DWPI, TDBD	OR	YES		03-28-2010

Web Images Videos Maps News Shopping Gmail more ▼

Scholar Preferences | Sign in

Google scholar

{restoring and reconstructing) and (data or me Search Advanced Scholar Search

Scholar Articles and patents anytime include citations Create email alert

Results 1 - 10 of about 444. (0.15 sec)

[BOOK] The CPM dictionary: the single source for acronyms, terms, and abbreviations in business continuity, security and emergency management

P Kirvan - 2004 - books.google.com

... policy Audit Trail: Chronological record of system activities that can be used to **reconstruct**, review, and ... Self-Signed SSL: Type of single sign-on that provides authentication and **data** encryption through a ... is, or has; 2) use of a system to ensure that a file or **message** supposed to ...

Cited by 1 - Related articles - Library Search - All 3 versions

[BOOK] Dictionary of Information Security

R Stæde - 2006 - books.google.com

... to combine parts of multiple Syngress books, as well as their own **content**, into a ... contact Matt Pedersen, Director of Sales and Rights, at Syngress Publishing; **email** matt@syngress ... He initiated the Rockwell computer and **data security** program in 1977 and continued to administer ...

Cited by 9 - Related articles - Library Search - All 12 versions

[PDF] from smallblue-greenworld.co.uk

[CITATION] Resource discovery and Security in Distributed systems

L. Larsen - 2007 - Citeseer

All 3 versions

Electromagnetic pulse (EMP) hardened information infrastructure with extractor, cloud dispersal, secure storage, content analysis and classification and method ...

RM Redlich... - US Patent App. 20,100,250,497, 2010 - freepatentsonline.com

... the structured **data** fields from, to, cc, bcc and subject, but the body of the **email message** is unstructured ... 10 diagrammatically illustrates a chart showing the key components of the parsing, dispersion, multiple storage and **reconstruction** (under **security clearance**) of **data**. ...

Cached

[PDF] Design & Implementation Aspects of Mobile Agents

T Kapoor, P Ali - cs.kent.edu

... Some of these issues will be addressed in detail, as **data** is available, with respect to the 3 mobile agent ... proxy is transferred, it keeps the agent id and its address, and uses that information to **restore** the correct ... The receiver is responsible for **reconstructing** and resuming the agent ...

Related articles - View as HTML

[PDF] from kent.edu

Monitoring Information Systems to Enforce Computer Security Policies

SW Graham, SE Mills... - 1993 - cit.dtic.mil

... An inaccurate **message** could result in a failed mission, civilian casualties, or have significant political ramifications ... This gives the system administrator the ability to recreate the actions of a user in the event of a computer **security** breach and **restore** the original **data** if needed ...

All 5 versions

[PDF] from dtic.mil

[PDF] Dialectics of Information Security

D Pargov - Information & Security, 2000 - kms2.isn.ethz.ch

... An International Journal **e-mail**: infosec@mbox.digsys.bg ... The same is valid for **data** processing methods. ... mechanisms create new abilities for deception, blackmail and sabotage, the creation and manipulation of "truths", through monitoring and manipulating **message** traffic. ...

All 9 versions

[PDF] from ethz.ch

[CITATION] Network security bible

E Cole, R Krutz... - 2005 - Wiley-India

Cited by 47 - Related articles - Library Search - All 7 versions

[PDF] Security and trust management in collaborative computing

S Yang - 2003 - etd.fcla.edu

... Once two organizations choose a contract template and agree upon the **content**, the contract notary stores the contract. The ... The Collaboration Protocol Agreement (CPA), a part of the ebXML [34], is a system-level agreement for **data** ... Although it covers critical **message** ...

Cited by 1 - Related articles - View as HTML - Library Search - All 3 versions

[PDF] from fcla.edu

[CITATION] Security Guards for the Future Web

N Reed, D Bryson, J Garries, S Gosnell, B Heaton... - 2004 - Citeseer

Cited by 1 - Related articles - Library Search - All 20 versions

[PDF] from dtic.mil

Create email alert

Google

Result Page: 1 2 3 4 5 6 7 8 9 10 Next

{restoring and reconstructing) and (c Search

Go to Google Home - About Google - About Google Scholar

©2011 Google

Search Notes 	Application/Control No. 11682941	Applicant(s)/Patent Under Reexamination REDLICH ET AL.
	Examiner YVES DALENCOURT	Art Unit 2457

SEARCHED			
Class	Subclass	Date	Examiner
709	206, 218, 219, 244, 246	03/28/2010	YD
726	26, 27	03/28/2010	YD
713	166, 189	03/28/2010	YD

SEARCH NOTES		
Search Notes	Date	Examiner
WEST(see attached text search)	03/28/2010	YD
WEST (updated text search)	01/26/2011	YD
GoogleScholarSearch	01/26/2011	YD

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner
WEST(updated text search 709/246)		01/26/2011	YD

--	--

INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)	Docket Number (Optional) 6851-02-CIP4-CON	Application Number 11/682,941
Title: Data Security System and Method Adjunct to a Browser, Telecom or Encryption Program	Applicant(s) Ron M. Redlich	
	Filing Date March 7, 2007	Group Art Unit ~~2457~~ 2457

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date if Appropriate
	6,845,448	01/2005	Chaganti	713	166	
	6,941,459	09/2005	Hind	713	167	
	7,010,681	03/2006	Fletcher	713	154	
	6,922,696	07/2005	Lincoln	707	101	
	7,031,961	04/2006	Pitkow	707	4	
	7,089,428	⁸ 05/2006	Farley	370	231	
	7,188,107	03/2007	Moon	707	5	

Change(s) applied

to document,

/MAH/

3/16/2011

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER /Yves Dalencourt/

DATE CONSIDERED 03/28/2010

G:\RCK\CLIENTS\Redlich\6851-02-cip4-con-Form-PTO-1449-Master.wpd

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail** **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Robert C. Kain, Jr.
 900 Southeast Third Avenue
 Suite 205
 Ft. Lauderdale, Florida 33316

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

Robert C. Kain, Jr.	(Depositor's name)
/rck/	(Signature)
04/29/2011	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/682,941	03/07/2007	Ron M. Redlich	6851-02-cip4-con	9976

TITLE OF INVENTION:

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	\$755	\$300	\$0	\$1055	05/04/2011

EXAMINER	ART UNIT	CLASS-SUBCLASS

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. Use of a Customer Number is required.

2. For printing on the patent front page, list

- (1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
- (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1. Robert C. Kain, Jr.

2. _____

3. _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

Digital Doors, Inc.

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Miami Beach, Florida

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

- ☒ Issue Fee
- ☒ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 031231 (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature /rck/

Date 04/29/2011

Typed or printed name Robert C. Kain, Jr.

Registration No. 30648

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Electronic Patent Application Fee Transmittal

Application Number:	11682941			
Filing Date:	07-Mar-2007			
Title of Invention:	DATA SECURITY SYSTEM AND METHOD ADJUNCT TO A BROWSER, TELECOM OR ENCRYPTION PROGRAM			
First Named Inventor/Applicant Name:	Ron M. Redlich			
Filer:	Robert C. Kain			
Attorney Docket Number:	6851-02-CIP4-CON			
Filed as Small Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl issue fee	2501	1	755	755
Publ. Fee- early, voluntary, or normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				1055

Electronic Acknowledgement Receipt

EFS ID:	9983018
Application Number:	11682941
International Application Number:	
Confirmation Number:	9976
Title of Invention:	DATA SECURITY SYSTEM AND METHOD ADJUNCT TO A BROWSER, TELECOM OR ENCRYPTION PROGRAM
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	04897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-02-CIP4-CON
Receipt Date:	29-APR-2011
Filing Date:	07-MAR-2007
Time Stamp:	06:55:27
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Electronic Funds Transfer
Payment was successfully received in RAM	\$ 1055
RAM confirmation Number	9519
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	----------------------------------	------------------	------------------

1	Issue Fee Payment (PTO-85B)	6851-02-cip4-con-issue-fee-transmittal-042911.pdf	65046 de7a1f87d98cbef410b1b759238e1d8d8fd16749	no	1
Warnings:					
Information:					
2	Fee Worksheet (PTO-875)	fee-info.pdf	32028 d2cf1e1844ab961c920c095a0313394b6ef4ca16	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			97074		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/682,941	06/07/2011	7958268	6851-02-CIP4-CON	9976

4897 7590 05/18/2011

ROBERT C. KAIN, JR.
KAIN & ASSOCIATES, ATTORNEYS AT LAW, P.A.
900 SOUTHEAST THIRD AVENUE, SUITE 205
FT LAUDERDALE, FL 33316

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment is 1032 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

Ron M. Redlich, Miami Beach, FL;
Martin A. Nemzow, Miami Beach, FL;