C.18 DOM Process Editor

[2708] Document object model (DOM) source documents, and particularly Office document modules, comprise the blueprints, process, external data sources and linkages, and materials for building the resulting presentation; the presentation content is usually the ultimate end product. The blueprints and process often are immaterial to the presentation and represent proprietary and confidential material. This DOM object model complexity and diverse accessibility creates an opportunity for the knowledge expander search engine.

[2709] Effective DOM and metadata searches use the object hierarchy structure as variously described as a binary tree, category structure, or hive. In any event, the entry point is the root or base, containing a potentially infinite number of subcategories, each with a potentially infinite number of leaf items. See FIG. C-9. The structure can be pruned, deleted, or rearranged. The items represent object-oriented information, from entire subdocuments, to relational databases, layered graphics with vector elements, to simple plain-text, to a single binary numerical element.

[2710] The process requires a parse of all branches to each and every leaf. This process is not recursive, just extensive. Each path is examined for context, each leaf for content, all nodes for external references, and everything must be viewed within the context of sources and methods, not just obvious content. The obvious content is what the user created and sees, but as you now know, that is a minor portion of the data contained within the document object structure. This is a paradigm shift is shown in the hierarchy below:

DOM Deconstruct Table

For each document (the file and structure); Access the root; For each limb; For each branch; For each sub-branch; For each leaf (item); and Process each leaf.

IPR2023-00973
International Business Machines Corporation v. Digital Doors, Inc.
IBM's Exhibit 1002, Vol 5 of 9
Ex. 1002, Page 2060

[2711] Preservation of the path to each leaf is important as it defines the access to that data element. The existence and/or null value of the leaf represents a security control point. The model defines, with supplemental external knowledge of the object model, potential search opportunities. The model and the content are not separate from external knowledge of sources and methods. The model and the content are part of a contextual analysis of the source document or data stream itself. The leaf the significant search control point. It is possible to review and alter the contents of the leaf within the context of the purpose of the leaf to retain functional access with multi-level SC or sec-con sensitivity.

C.19 Five Informational Attributes

[2712] The five information attributes of SC or sec-con sensitivity in context to processing include the leaf, purpose, sources and methods, ownership, date or timeliness, and content. The entity must establish protocols which rate or prioritize the five information attributes on each root, branch and leaf in the DOM source document. With the system initialized in this manner, the processing of the DOM document within the parameters of the knowledge expander search is accomplished.

[2713] Purpose: How does the purpose of the leaf provide context, purpose, or informational reference to the document as a whole or the individual leaf? Does it provide source, destination, authorship, viability, validity, verification, or integrity to the document as a whole or the individual leaf? Consider the value of processes imbedded in the document as cell formulae, a help file, or other complex routing wizard. Does it show linkages or references to other documents? What is its status or position within the document? What is its element position, as a headline, footnote, or redlined status? These seemingly minor details transcend actual content but provide clues to the following attributes.

[2714] Sources and Method: Intelligence agencies stress the confidentially of the sources and methods used to gather information. The information itself might or might not be important, but the

ongoing care of the sources and methods is important for future information gathering activities and retention of any status quo until action is initiated. In addition, the viability, validity, verification, or integrity of the document is predicated by the viability, validity, verification, or integrity of the sources and methods used to create it. In terms of the Office document, this type of information is both contextual, leaf content, and metadata. To presume that the SC search uses only doc content at the leaf misses the value of metadata and the inherent value of the object-oriented document format. For example, authorship, source, source dates, editing dates, deletions, redlining, notes, footnotes, MS hidden text, links, and other structural elements in the source doc describe when, how, where, and who created the document. This speaks to the viability, validity, verification, or integrity of the document as a whole, and can compromise past, ongoing, or future data collection efforts and operations.

[2715] Ownership: Ownership is reflected both in leaf-level content—that is obvious when a document is presented or published—but also in the metadata. Ownership is also a characteristic of file storage properties, in ring rights, file storage position, linkages, SMB or network file access rights, and HTML references. Ownership, particular the number of links, the times access and edited, numbers of hits, and the level of churning, suggests the relative importance and merit in the document.

[2716] Date-Timeliness: Date or timeliness reflects currency. The dates, in terms of edit times, access times, and frequencies suggest the relative importance and merit in the document. Touch and other file-level commands can only mask the overt date and timestamp of a file, not its purpose or content, true timeliness, or merit. This information is spread through the metadata and leaf content. In some hierarchical structures, this information is stored in tables or other structures apart from the immediate document root. When a document is a relational data structure, as in Access or SQL, hidden system fields and hidden security data define edit and deletion times. It is also important to recognize

that in databases, records which are deleted by the user are only marked as deleted but persist until the database is purged, packed, cleaned, compressed, or otherwise processed in a maintenance mode. When relational technology with transactional logs and rollback facilities are enabled, data can be recreated or dated despite many types or natural of instigated disasters. This supplemental metadata defines date and timeliness too.

[2717] Security: Security of content can be compared to erecting a barrier around that content and may be viewed as an important SC sensitivity issue. However, when content becomes a collection of simple data elements along with data objects, dispersed and distributed sources, effected by embedded events and triggered methods, a search which ignores the security content characteristic fails to acknowledge that the SC sensitivity may be impacted by such omission.

[2718] While content is king in most search systems, it is not the only critical aspect of a source document. In terms of the knowledge expander processing of an Office document, each leaf must be processed and assessed for its metadata. Note again that each leaf may be another object-oriented structure in its own right or a simple element. It will need to be processed and assessed accordingly.

C.20 Select Content Introns and Exons

[2719] Terminology employed in connection with the operation DNA (deoxyribonucleic acid) provides an appropriate metaphor for the MS Office document object model or any other DOM model. While the DOM is separate from an MS Office binary file, it defines the purpose of that file and maps its activation. The DOM "genes" are expressed into the file binaries only as specifically referenced, and frequently diverge from the pure MS Office application as genes from other OLE (object linking and embedding) applications are embedded into the document. The DOM and the expressed document can mutate for better or worse, and both backwards and forwards the document is adaptable just like DNA,

with unforeseen consequences including the profound security flaws evident within the MS Office workflow.

[2720] In genetics, an intron is any non-coding or non-activating sequence of DNA initially copied into RNA but cut from the final RNA transcript or unknown as to singular or recombinant purposes. Introns are excluded or ignored in the DNA process. An exon is a coding or activating sequence with a known purpose that is actually used or one that is unknown as to purpose but nonetheless still used. DNA is, of course, the blueprint for life. RNA is the functional transcript of the DNA blueprint used for cell division and replication. Exons are the useful portions in the DNA cycle.

[2721] In the object model, the DOM is metaphorically the DNA blueprint for an MS Office document whereas the actual Word, Excel, or Outlook message is an expression of the RNA as a functional transcript. Correspondingly, the SC select content or sec-con intron is any document branch, leaf, or node element with a non-coding, non-activated, or even unknown control utility for the document. From a select content - search (or sec-con - search) standpoint, each and every intron represents a non-qualified element that is a potential search term that may lead to an expanded knowledge expander supple doc compilation. Rather than ignoring SC or sec-con introns as most common search engines do, the current knowledge expander search engine employs the SC or sec-con introns to expand the scope of the search. A SC or sec-con exon is any document branch, leaf, or node element serving an end purpose. Each SC or sec-con exon in a MS Office document becomes a certifiable data element.

[2722] Unless each such SC or sec-con intron and SC or sec-con exon in the source document DOM is vetted for credentials, which vetting includes a prioritized taxonomic label or tag, the

knowledge expander search, whether through conventional search engines or the novel search engines described herein, will be incomplete. This is effective for DOM, HTML. XML, databases, and any structured file binaries. The standard 2-phrase process transforms into a 3-phase process where DOM node elements are coded either as exons or introns, and thereafter processed accordingly for inclusion or exclusion.

[2723] The improved accuracy of 3-phase scanning of documents within the context of an object model is apparent. While the traditional 2-phase method find SC or sec-con introns and SC or sec-con extrons within a source document, it also miscodes several other sequences as introns. The accuracy of such process will always include statistically measurable false negatives and positives, thereby missing true threats and removing non-threats. The 3-phase process improved on the 2-phase process with granular deconstruction of the document and subsequent recoding of both false positives and false negatives to yield a higher rate of accuracy. SC or sec-con introns are added to the search term list in the knowledge expander search engine and are scalable numerically. Better DOM maps mean better intron handling.

[2724] FIG. C-11 shows the General DOM Editor program 1022 in a flow chart form. Step 1024 is the initialization that is employed by the security entity or SC or sec-con sensitivity supervisor to set up the program. Step 1026 obtains the DOM layout or blueprint from the DOM vendor. Step 1028 notes that for each root, branch and leaf in the DOM, the information attributes must be prioritized with the SC select content or sec-con and organizational informational attributes (a taxonomic routine with prioritization). SC or sec-con introns are identified and SC or sec-con exons are classified, placed in a hierarchical structure and labeled. This step, of course, uses a content filter to identify the SC or sec-con exons. A contextual filter or algorithm is used to taxonomically classify SC or sec-con exons at a higher

priority level. For example, when "Bin" is next to "Laden" the SC or sec-con exon combination -- Bin Laden-- is classified TS or the top level for the SC or sec-con H-tax class.

[2725] Step 1030 obtains the source document DOM. Step 1032 maps the DOM source document as a binary file populated with content data and meta data as a subset of the DOM blueprint. Step 1034 identifies SC or sec-con exons and SC or sec-con Introns. Step 1036 labels or tags SC or sec-con exons per the tax class (taxonomic classification) and per priority, to be included in the further processing of the item and identifies SC or sec-con introns to be used as search terms in the knowledge expander search. Multiple tags and overlapping tags are possible and a ruled-based system is employed to upcode multiple tags and overlapping tags to the next higher tax class - priority level. Step 1036 converts SC or sec-con exons at each root, branch and leaf into SC or sec-con level save doc, form and format (for example, a safe DOM template), and generates a save blueprint or map, drops (or alternatively stores in a remainder store) all low priority SC or sec-con exons, and expands the search term list with the SC or sec-con introns and the top group of the SC exons. Step 1038 processes the save DOM doc, that is, the top level SC or sec-con exons and all SC or sec-con introns as search terms through public and/or private databases, indices, search engines, etc. A divergent search uses SC or sec-con intron. A convergent search uses SC or sec-con exon. Supplemental documents are gathered form the search, the filter H- tax class priority tag process is repeated on the supple docs, the SC or sec-con introns are identified and selected top priority SC or sec-con exons are identified and the search and a second tier supple docs compilation is processed. Supple docs are stored and a relational map is generated both with the search terms and the supple docs.

[2726] FIG. C-12A shows a flow chart of a basic application for a DOM Editor -knowledge expander search for MS Office document. Step 1042 initializes the system. Step 1044 obtains the

source DOM document and notes that all processing occurs after a spam and virus filter. Step 1046 notes that the program creates or is provided with a security safe or clean DOM document and map. All levels of SC are labeled or tagged and saved in the "save doc" routine. This hierarchical taxonomic (H-tax) tagging labels all SC or sec-con words, terms, etc. and locates and maps exons and introns in the source doc. Step 1048 notes that a template is opened and SC or sec-con exons and SC or sec-con introns (non-standard SC or sec-con and unknown terms, characters, words, etc.) are copied from the source doc into the clean DOC. A clean .DOC template (Word) or whatever the new document type is opened for the specific application. The Normal.DOC or New Spreadsheet.XLS on the MS Office distribution CD is safe. In Visio, for example, start with a new chart. Older documents saved as templates tend to accumulate unanticipated metadata. If one must use a non-standard template, clean it up. View it as both a printed document, as a binary file, and as a document object. Write protect the templates, or store the templates as non-modifiable networked volume. If the templates are used throughout the organization, create a network store for them and configure each user's installation of MS Office to look there for the templates. Search the network for duplicate copies of these templates and eliminate them.

[2727] If changes from any version of MS Office to another version are made — this can be a regularly upgrade or a even a downgrade—create new documents and cut-and-paste parts of prior documents into new ones. Lose the older files and templates. If you receive or open an Office document in either an older or newer version, create new documents and cut-and-paste parts of prior documents into new ones consistent with the MS Office version that you use.

[2728] Step 1050 disables edit controls and step 1052 copies SC or sec-con exon and SC or sec-con intron content. The point is one must edit cleanly. This is not a single step but rather a process, both

one time and ongoing. Disable versioning in step 1050 to prevent a buildup of past versions of the document. With versioning, prior sessions will be stored as document.doc 1, document.doc 2, and so on. These tend to get entwined with the latest version. If workflow with InfoPath, Outlook, or other collaborative workflow tools creates duplicate copies of the source document file for each user. Step 1050 includes the concept that the system is configured to store a single network copy instead. Preserve an audit trail and backup with a system backup rather than versioning. Disable change tracking in step 1050 to curtail the buildup of additions, deletions, and changes that transcend the publishing intent of the document. If redlining is necessary, establish guidelines for periodically accepting changes to purge change log. Use the command to save the document without the change log with File/Save or File/Save As. Do not use nor rely on fast saves, timed saves, or file recovery after a MS Office crash to purge the dirty metadata. After a crash, reopen the document, save the document under a new name. Close the Office application. Delete the old file precipitating the crash. Rename the new file under the old name. Reopen the Office application.

[2729] Step 1054 locates text in footnotes, hidden text, etc and labels or tags that content as SC or sec-con exons or SC or sec-con introns and maps those data elements to the SC or sec-con save doc and copies the elements into the Clean DOC. Use comments instead of hidden text. It is documented as a feature so it can be found rather than accidentally uncovered. Hidden text with a font color change or font size change looks like an artifact that most users will ignore or delete. Avoid the use of headers, footers, footnotes, endnotes, inserts for table of contents, index and the like. These appear only in the printed output unless specifically viewed from the View pulldown menu. Such links also create a lot of dirty metadata beyond what is visible even during editing that persists until changes are accepted. Remove references from the source document. This is subtle, but very important when documents are

specifically posted or even inadvertently listed on web sites. References include other files, documents, hyperlinks, and other possible embedded formatted materials. These references create the ability to infer quite a lot about the purpose of the document from other related documents in the same directory, by the same authors, and the types of other documents. For example, a spreadsheet stored with a report that is not overtly included in the report suggests that is source material that has not been reviewed with an eye towards privacy, security, or client privilege.

[2730] Paste and copy images, cut text, formatted text, pie charts, record sets, slides, waterfalls, milestones, organizational charts as plain text or an image rather than formatted Office objects. If the embed commend is used, all the metadata baggage from the other Office application is now added to the metadata in the target document. Since that metadata baggage is not native to the target document application, it is inaccessible and truly hidden. Tools, such as Metadata Assistant will not find Excel metadata within a Word Document, Word metadata within an Excel spreadsheet, and none of them within an Outlook note or message.

[2731] Step 1056 notes that a clean map for the meta data cleared DOM document must be created.

[2732] Step 1058 executes the intron search and/or granular search routine, gathers and compiles supple. docs and the processes those supple docs through the granular filters discussed earlier to locate, with the hierarchical taxonomic filter process tags new words, terms, symbols, which are related to the original SC select content or sec-con, thereby expanding the knowledge base of the meaning of the SC or sec-con source document.

C.21 Hierarchical Taxonomic Class Examples

[2733] Various type of classification systems (taxonomic systems) may be employed. For

example, a dictionary classifies all words as nouns, verbs, adverbs, etc. This is one taxonomic system. A prioritized H-tax system classifies nouns into a name subclass and this name subclass may be priority or sensitivity level 1. Geographic locations (class nouns) may be priority 2. The operator of the present knowledge expander search process may place a high priority or sensitivity on "noun" class, thereby converting the simple taxonomic structure into a hierarchical taxonomic system. Identifying categories and subcategories for SC or sec-con sensitive words, etc. or critical data, creating a compilation of pre-existing data, comparing the compiled pre-existing data to the target data and labeling or tagging the SC or sec-con terms is one of many important aspects of the present invention. Table 1 in FIG. C-12B provides categorical identifiers for personal identity. These categories, which may be utilized to identify a person, are not meant to be all encompassing but are mainly provided as examples.

[2734] After categories are identified for the critical data, it is important to create the hierarchical taxonomic system against which the target data is tested. Ranking or qualifying the categories at SC or sec-con sensitivity levels is next. Table 2 in FIG. C-12C is a general attempt to quantify the categories for personal identification from a high risk value beginning with "name" to a low risk value ending with "personal interests". Again, the Ranked Identity Category Table 2 is not meant to be limiting but is meant to be an example. Individuals skilled in identifying a person may alter the ranking of the identity categories in Table 2, FIG. C-12C.

[2735] The present invention can be employed to use a hierarchical taxonomic system for a business. Table 3 in FIG. C-12D set forth below provides examples of categorical identifiers for a manufacturing business. Again, this list is not meant to be exhaustive or complete, but is only provided as an example of the types of categories and subcategories which a manufacturing business would employ in order to establish the risk monitor of the present invention.

EX. 1002, Page 2070

[2736] With this list, the manufacturing business may assign a SC or sec-con sensitivity level to each category (class, subclass and sub-subclass) thereby creating a prioritized hierarchical taxonomic system.

C.22 Knowledge Expander (KE) Basic Program

[2737] As discussed earlier, the information life cycle or knowledge expander search module can be configured with many different modules in order to achieve the objective of the operator. The knowledge expander or KE basic program 3001 in FIG. C-13 is one basic implementation of the expander search program. FIG. C-13, In step 3002, the operator or user sets various filters and sets the search targets. The search targets may be publicly available search engines or private data bases, data collections, indices or any item that the user wants the KE search to access. Filters are described earlier as hierarchical taxonomic filters or taggers, content, contextual and other types of filters. Filters are used to identify class, subclass and priority in the hierarchical taxonomic or H-tax system, to apply contextual rules or algorithms ("bomb" within 10 words of "arab"), and content (select content SC or sec-con verses non-matching SC or sec-con). Step 3004 obtains the source data or the source is input by the operator. Data input may be from a client computer in a server-client computer system. The source data may be a data stream, a source document or other item. Step 3004 contemplates that if a document is utilized, the document is deconstructed to its basic data elements and appropriately mapped. See the discussion above in connection with DOM branch, leaf and tree deconstruction. In step 3006, the hierarchical taxonomic classification (H-tax) occurs and each data element in the input document is tagged based upon the classification system which has been prioritized by the user (or the user uses a pre-set prioritized H-tax). A note to deconstruct the source document into data elements (see DOM deconstruction into its object hierarchical structure above) is found in step 3006. In step 3008, for non-matching data elements, a search is conducted through the search targets. Non-matching data elements

form the input doc are those which do not match SC or sec-con. In step 3010, the system gathers the documents from the search (supplemental documents) and repeats the H-tax tagging operation for b number of supple docs. A relationship mapping function and display function is activated if c number of hits occur within the H-tax top priority range. In other words, if the search for non-matching data elements returns 50 select content or SC or sec-con terms and of those 50 SC or sec-con terms in the supple docs, 20 SC or sec-con terms fall within priority ranges 1-5 of the hierarchical taxonomic classification set by the user (n priority H-tax levels), then the system and process maps the results and displays the representations of the H-tax recovered from the supple docs c is less than 20. If less than b number of H-tax tags are noted in the supplemental documents, the system repeats steps 3006 and 3008 and gathers a second tier of supplemental documents.

[2738] Steps 3012, 3014, 3016 are optional. As an option to be set by the user or as an option to be set by the system operator as a default, step 3012 changes the H-tax top range bandwidth from n priorities to be searched to m priorities. This change may be needed to expand the search bandwidth from b to b-10 to b+20. A reduction (m less than n) is needed if too many supple docs are recovered by the search. If too few are recovered, then m is made greater than n priorities in the H-tax. Option 3014 changes the output supplemental document bandwidth to b + y if too few supple docs are recovered. Of course, the output supplemental bandwidth could be reduced with b - y. Optional step 3016 mixes n number of select content search terms with the no-match data element before the search. This effectively is a convergent filter. By adding the known SC or sec-con to the search terms (initially, search terms are generated from the input doc based upon priority H-tax), the search is biased or is set to converge on the known SC or sec-con added to the search term group. By using the no-match (NOT AND) function, the KE search diverges to gather a wider range of docs. Of course, the user may always employ

common search engines in addition to the search plans set forth herein. Step 3018 repeats the process until b supplement documents or c hits (SC or sec-con sensitivity matches) are noted within the H-tax top range. Step 3020 maps, displays, stores and ends the program.

[2739] FIG. C-14 shows an expansive or expansion unknown search engine 3031. Step 3032 initializes the program with preferably user input, sets up the hierarchical taxonomic H-tax classification system along with a priority or sensitivity level assigned to each level and branch and leaf in the H-tax system. Select content SC or sec-con filter modules for content and contextual range or algorithm tests are also set. At least some select content should fall within the prioritized hierarchical taxonomic system. The select content SC or sec-con encompasses words, terms and data objects that the user wants to expand his or her knowledge base with the search engine. The user sets a no-match search bandwidth nms and sets search targets such as search engines, public or private databases, data compilations, indices, data collections and data structures or whatever. Step 3034 obtains a source or data stream or input document. Step 3036 processes each data element (which may include a document deconstruction) with the H-tax, content and context filters, and tags each data element with an H-tax marker. Multiple, singular, and a default "unknown" H-tax classification indicators are linked or tagged on every data element. The system in step 3036 may upgrade or downgrade the priority or sensitivity H-tax level for a particular word, term, etc., due to contextual rules in the context filter. In step 3038, the system conducts a search for nms number of not matching or unknown data elements. If nms is 10, the system takes the top 10 priority H-tax supple SC or sec-con terms obtained from the input doc and uses the top 10 supple SC or sec-con as search terms in the target data collections. The search is conducted through search targets identified in the set-up step 3032. The no-match search 3038 is sometimes identified as step A herein. Step 3040 gathers supplemental documents. Sometimes, step 3040 is step B herein. In

step 3042, the system processes the supplemental documents through the H-tax tagger. The supple docs are classified with the H-tax. This is sometimes step C. In step 3044, the system determines if p hits have been noted in the H-tax top range levels. If YES, the system stops and maps the select content SC or sec-con sensitivity sel. levels to the H-tax mapping structure and displays that SC or sec-con hierarchical representation map to the user. Further, the system in step 3044 maps the supplemental documents to the H-tax map structure and displays that to the user. Sometimes, step 3044 is step D herein. In step 3046, if p number of hits are NOT identified in step 3044, steps A,B,C, D are again executed and repeated unless the repeat cycle is more than R. The nms bandwidth may automatically change (increase) or the n priority H-tax may change to m H-tax levels to increase the supple docs or the hit count for supple SC or sec-con . The same techniques may be used in reverse if too many supple docs are recovered. The system ends after step 3046.

[2740] FIG. C-15 shows knowledge expander KE search options 3051. Step 3052 is an option to add a noise filter after the H-tax tagger step 3036 in the expansive unknown search engine routine 3031. The noise filter reduces the number of unknown data element and operates on the unknown tags for those unknown data elements. For example, terms "and" and "or" and "the" may be deleted by the noise filter. Optional step 3054 adds to step D, if p hits is equal to zero, then the system resets the no-match bandwidth nms + u and repeats step A,B,C,D and repeats the entire process until p hits in step D or R iterative cycles have been noted (counted). In optional step 3056, a convergence filter is added to the expansive, unknown search engines 3031 by adding w select content SC or sec-con search terms to the no-match search step A. In optional step 3058, a divergence filter is added by changing, either increasing or decreasing, nms value if p hits do not exceed p + x. In optional step 3059, a content filter is added to detect temporal relationships such as time and date ranges. Time may be time of length of

search or time may be a time-date range limit on recovered supple docs. The temporal contextual filter (time and date is a matter of context) would be added to step 3036 the H-tax step. In optional step 3060, the H-tax map is output to the user so the user sees the classification and the prioritization of that classification. In step 3062 the operator can change the repeat cycle R, the time the search runs, the number of cycles, and the search target databases, data sets, spreadsheets or public or private search engines. In optional step 3064, the operator can limit the supplemental documents based upon a temporal factor such as time, the total number of SC or sec-con terms located in the supplemental documents, and the total number of supplemental documents.

C.23 Secured Metasearch Engine Based on Granular Data Control

[2741] As an overview, the secured metasearch engine technology is based on granular data control. The engine is part of the KE engine described above in sections C.9 - C.22. The secured metasearch engine technology enables secured searches and distribution of secured search results including secured information sharing with multi level security (MLS) search capabilities across domains. Data is explored not only by content but also context and concept. Search should occur across domains, with information shared and delivered across domains and through the extraction and integration of both private and public data sources including the Internet. Stovepipes and silos, independent efforts at information collection and intelligence analysis, and air gaps or security guards divide information domains and prevent secured information sharing. Centralization and consolidation of data gives rise to data overload, a problem in part addressed by new web-like searching techniques, but also opens the door to security leaks.

[2742] The security of current data mining and search operations as well as the security of the multi level distribution of the search results to users with different access levels is questionable.

EX. 1002, Page 2075

Furthermore, the current data mining and search is rigid because the starting point for each and every effort requires an index or search terms and the mining is completely content-based. When connecting the dots, it is essential that search be possible without preconceptions of utility, purpose, or cultural bias. Effective search techniques, called "metasearch" herein, comprises more than web-like textual (and other formats such as audio or video, but also compound meta-formats) search technology. It includes data mining, textual and contextual search, aggregation, inference, and data-to-data interaction all based on granular data control subject to security compliance.

[2743] Metasearch generally means the usage of multiple web-based search engines based on keywords with results combined into a single unified report; this is better described as a confederated search or federated search. Each web-based search engine is rigid in terms of its reliance on preexisting indexes; it is usually fast but limited in terms of most likely usage bias. However, the combined results reinforce the preexisting answers based on the implicit search question.

[2744] In contrast, the Secured Metasearch Engine (sections C.9 - C.22) is designed for searching the unknowns and expands the base of information, as well as conducts the search operations across different domains with different security levels. The Secured Metasearch Engine results provides two distinct and fundamental directions, search convergence and search divergence, both of which are critical to the process of connecting-the-dots. Failure to consider both convergence and divergence leads to incomplete results.

[2745] Search divergence is the process of expanding the content, context, and concept beyond the strict scope of the fundamental search. Search convergence is the process of validating, substantiating, and establishing the integrity of the fundamental search. Divergence is the expansion of the search query or data mining operation. There is a need to find outliers useful to expand the scope

of the users knowledge and infer new information and intelligence. Some information and intelligence operations require exploration without preconception. Herein, outliers with the least priority, relevance, or ranking frequently provide previously unknown references or interconnections that are purposefully hidden. This is a search divergence because the base search query primes the process but effectively we already know the highest ranking results and reject those results while iterating the search for non-ranking items.

[2746] The Security Metasearch Engine starts with known keywords and indexes, but accepts primarily information that is new or different from the direct response to the implicit question, that is the base search query. Validation and integrity is not important to divergence. The search engine is looking for all related metadata, references, links, and relationships without regard to accuracy. Exact matches are in effect usually ignored, but all new references are added into a secondary query yielding subsequent results (supple docs and supple search terms). The subsequent results in turn yield yet more new references. This subsequent query yields subsequent results, which is repeated indefinitely. The iterative results create an asymptotic adjacency list model, which may include a networking relatedness. The networking relatedness is often viewed as flow charts showing betweenness, closeness, and connectedness. The networking relatedness may also be a social network relatedness.

[2747] This expansion of the base search query is the process by which the user discovers more dots. Connecting dots the user already knows is pointless and does not expand the user's knowledge; the user wants to expand the set of dots and generate new content, new context, and new concepts. The Secured Metasearch Engine starts with old and/or limited information, but generates new information. The theory of six degrees of separation has some legitimacy, however there is a difference between accidental and active relatedness.

[2748] Divergence is also critical to enabling the Secured Metasearch Engine to foster security by exploring the purpose and usage of information beyond the immediate and obvious preconceptions (i.e. foresee reflexivity) of semantic and pragmatic meaning. See beyond the immediate security perception for other possible cross-domain requirements and enable information sharing. The Secure Metasearch Engines is connecting known dots with new dots, the true concept of "connecting the dots". The new dots lack integrity and substantiation. They are not ignored or dismissed outliers because they can reveal the outlines of previously unknown, undiscovered, unforeseen, uninvestigated and unrevealed situations.

[2749] The search process is really a metasearch, applying techniques of data mining, textual and contextual search, aggregation, inference, and data-to-data interaction, and the integration is the establishment of relationships. However, some of the new dots will be false and noise. At this point, a search convergence is useful to establish likelihood and risk for the new information and integrity and substantiation of the difference between accidental and active relatedness.

[2750] The Convergence Search is described herein. Convergence is the usual web-like search engine or data mining operation. It is rigid. The user starts with known keywords and indexes—search terms—as the base search query and accept hits with the highest relevancy. This information is used aggregately to confirm or deny the integrity of the initial search. The user gets back what the user expects with priority, relevance, or ranking focusing the hits to the content most consistent to the search term context. Outliers are naturally rejected and filtered out. Search convergence might entail a physical inventory, database report verification, an independent party confirmation, or a drone flyover to substantiate the information. The result is in direct response to the implicit question, that is the base search query. The user positions and substantiates the dots the user already knows. The user starts with

old information, and the user gets back old information. However, the benefit provides by the Secured Metasearch Engine is that it contextualizes these convergent results with a higher level of relevancy to the user's specific purposes based on tools which manage and control granular data. Those include tools include: (1) metafilters for automatic categorization; and (2) sensitivity level taxonomy. These tools deliver " fine adjustments " to the search process and find the most appropriate results for the user prioritized according to the highest relevancy.

[2751] The combination of divergence and convergence operations provides additional information. The Secure Metasearch Engines performs three key functions. (1) First, it selects new data elements of value and recognizes unknowns for automated iterative divergent search. (2) Second, the combined divergence search delivers "fine adjustments" to the divergence search process and finds the most appropriate results for the user prioritized according to the highest relevancy. (3) The Secure Meta search Engine categorizes all aggregated results to sensitivity level and enables distribution subject to MLS-compliance cross domain. While the Secure Metasearch Engines primarily focus on unstructured information, it can be integrated with structured data sources too because it is actually easier to extract context and concept from structured data.

[2752] There are multiple starting points to the metasearch process. One or more candidate data streams, news feeds, or documents can be dragged from the desktop into a queue. These items may be monitored for changes and then fed into the Secure Metasearch Engine for granular data selection and metatag categorization with the output result that search terms are generated and metasearch terms are also generated. A document or data stream automatically sets the context of the search and is explored for likely search terms/ key words. No index or bias is necessary to begin the process. The resulting search terms of interest are fed into the next search cycle, which may include also one or more URLs for

further exploration.Indexes and search terms do not define the implicit question or establish parameters for an effective answer because they represent a single dimension of information. Metafilters are used to control the granular data elements in order to fine-tune the search. The metafilters add both context and concepts to the initial search and all subsequent exploration. Such metafilters may be: (1) Categories of the granular data elements in a document ("name" "location" "date" "amount"); (2) sensitivity levels of the data elements ("top Secret" "Private" "level 9"); (3) phrases, ("Mohammed Atta" "United Nations"); and (4) Group Lists, (Groups of words which represent a concept or a context –"Nuclear" + "Submarine").

[2753] Generation of keywords / search terms for conducting the continuing searches is done by controlling of data at the granular data level. Control of data at the granular data level is enabled by combining different filters. The Secure Metasearch Engine recognizes complex content and context by implementing a combination of filters / sieves. Those combinations of different filters/ sieves create different permutations of resulting keywords for the search. The different keywords for the continuing searches are selected automatically based on: (1) the words entered into each filter/ metafilter; and (2) the configuration of the different filters/ metafilters combinations. As an example in one embodiment, all the content of a document is: (1) categorized, i.e. each individual word (or phrase) in the document is tagged by category, "name" "location" "date" etc.; (2) the individual words are also tagged by sensitivity tags "secret " "confidential" "Private" "level 3 sensitivity" etc.; and (3) all the above is presented in a matrix format. The filters will automatically select which words in the matrix will be used as keywords for the continuing search. Different keywords /search terms will be selected based on the different filters or combination of filters used. The entries for such filters may be machine or user defined. The combination and selection of different filters may create different permutation and results.

The filters may include the "Word Lists", "Phrases list", and "Word Group Lists" which limit the range or area from which the keywords may be selected. The ideal combination of filters to control granular content for automatic production of keywords may be found also by trial and error. Artificial intelligence tools may be integrated.

[2754] Linear adjacent selections may be used as keywords. However, unknown content can slip through this sieve without an explicit human intervention, therefore the Secured Metasearch Engine automates this sieve by creating permutations of both categorized and unknown words and phrases. These permutations are used as new search terms. The likelihood of random combinations (included in the class of the NP! problem space) is so low, that emphasis is focused instead on linear adjacent selections. This result in is a small and focused problem space that can be solved on a typical personal computer and ads disproportionate value. For example, a Google search of "Mohammed Atta" returns "Khalid Sheikh Mohammed" as a disconnected string of categorized and unknown words out of the box; that means parts of the phrase "Khalid Sheikh Mohammed" are recognized without any special configuration, but not as a contextual phrase. Permutations of linear adjacent selections do however create the complete connected phrase and automatically submit the complete phrase for a divergent metasearch, thereby creating new and previously unrecognized relationships to connect the-dots.

[2755] The engine can be set for automated contextual pruning with flexibility to discover codes. Many divergent mining and search efforts will expose unknown, deceitfully hidden, and statistically irrelevant relationships. For example, a Google search of "Mohammed Atta" also shows meetings at Aleppo. The relevant thread for Aleppo is that it is Syrian university town with social connections to Hamburg and the 9/11 hijackers associates. However, Aleppo is also a common Lebanese street name, and the original shoemaker character in the Pinocchio story by C. Collodi. The name was changed to

Geppetto in the Disney children's movie. While it is tempting just to prune this track, it is also important to explore associative contexts, because the use of codes can mask more sinister meanings. The 9/11 hijackers communicated within the seemingly innocuous context of weddings, guest lists, and dates. So while contextual pruning is easier after the fact, it can be very important before the fact when the use of codes and false contexts are not so clear.

[2756] In conclusion, although stovepipes and silos, independent efforts at information collection and intelligence analysis, and air gaps or security guards among domains prevent information sharing, the Secure Metasearch Engine enables security with information sharing including Multi Level Security (MLS) search capabilities across domains. It overcomes security leaks consistent with the needs to both protect national security interests but also enable cross-domain information sharing. The Secured Metasearch Engine technology is based on granular data control. It enables secured searches and distribution of secured search results including secured information sharing with Multi Level Security (MLS) search capabilities across domains. Data is explored not only by content but also context and concept. Search should occur across domains, with information shared and delivered across domains and through the extraction and integration of both private and public data sources including the Internet.

D.1 Secure Editor, DOM Editor (General) and DOM Editor -

Basic Applied as Extractor Modules

[2757] The Secure Editor can be used to generate SC or sec-con data for a search and can also be used to locate and extract security or sec-con data and SC data before storage of the sec-con or SC data in the distributed storage sites. The Secure Editor in FIG. D-20 diagrammatically illustrates an editor which may be employed to secure sensitive word/objects in a source document. In a current working embodiment, the secure editor is a standalone application or a module to add into other applications for plain text and

media creation, editing, and sensitivity level tagging. Other types of tagging, wherein the editor supplements the initial group or subset of security sensitive (or select content) words, characters, icons and data objects by categorization, taxonomy classification, privacy, security, compliance, and semiotic meaning, are also available. The editor supports a full range of document management and can be integrated into a unified infrastructure, from creation, editing, document markup, tagging, tag conversion, tag removal, context sensitivity level redaction, context reconstitution, and support for complex process work flows. The architecture assures separation of data from metadata so that no security lapses are introduced into the traditional word processing and document management cycle.

[2758] FIG. D-20 is a basic flow chart for one embodiment of the Secure Editor module. Editor program 972a begins with obtaining the source document 974a. Of course, the source document may be any type of document as explained later herein. Step or function 976a obtains one or more filters for one or more security or sensitivity levels. Step 978 screens or processed the source document with the filter(s). For example, the source document in FIG. B-8A in window 991 has text regions 993, 994, 995 and 996. In step 979, the Secure Editor displays, in situ (in the displayed document), the filtered identified material and conforms the precursor document to the security level protocols for the system within which the Secure Editor is employed as an information processing tool. FIG. B-8B shows that the address data 993 is marked TS (top secret), region 994 is displayed in color A for TS coding (please note that the addressee data may also be so marked) and is "red-lined" or struck out. Region 995 is displayed as presented in the source document and is labeled U (unclassified) and region 996 is shown in color B, is redlined and is labeled S. Labels TS, S, C (classified) and U are the established security labeling protocol used by the organization employing the Secure Editor. Other labeling schemes may be employed. Color is used to assist the user to select (and in some non-standard cases, deselect) the

sensitive data marked by the editor. Redline is used to inform the user that the filter(s) will extract the marked data. Labels are used to permit the entity using the editor to employ standard tear line protocol. Any data beneath a security classification of the user is under the tear line and the data is permitted to be distributed to the lower security cleared user. Of course, electronic distribution of secure data need not use the hard copy or print version of the tear line. However, this nomenclature referring to the tear line is used in the prior art systems.

[2759] Step 980a (FIG. D-20) accepts the user's manual changes (typically upgrades) to the precursor document. These manual changes are displayed, redlined, colored and labeled. Step 982a inserts the security label TS, S, C and U has discussed above. Step 984a notes that the system takes certain meta data such as author, date-time, version history, change history, etc. and converts this meta data into ordinary text, marks that data at the necessary security level and labels the data. Step 986a permits the user to add (or omit) placeholders into the final document. FIG. B-8C shows placeholders as black lines or as XXXXX symbols (or other symbols) wherein the sensitive text is not shown but some replacement markers are shown. The byline in region 1003 shows "sanitized document." The byline 1003 in FIG. B-8B lists the security level and the color representation.

[2760] Step 988a (FIG. D-20) activates the filter, extracts the sensitive or SC data and temporarily stores the extracted data. Step 990a displays the filtered document and the user may view the filtered document at each security level. Therefore, the user, before transmitting a secured email (or letter) may look at the source (FIG. B-8A), may look at the TS level without the redline strike out but with security labels and colors, may look at the T level revealing regions 996 and 994 but not regions 993 and 994 (which are TS coded regions), and look at U versions as shown in FIG. B-8C. Step 992a disperses the extracted data and the remainder data or disperses partial versions of the document (those partial versions

formatted and containing only data at or above the target security level (all TS level data (which includes TS, S, C and U data), or all S data (comprising S, C and U) or all C data and U data)).

[2761] One feature of the present invention is that in step 979a, the security level protocol determines whether single words are granularly classified (TS, S, etc.) or whether a line is classified, or whether an entire paragraph is classified (see FIG. B-8B). If a commercial/privacy filter is used to exclude all social security numbers, the organizational protocol is set at a granular level to exclude just social security numbers. Different group protocols use algorithms to mark, filter and extract adjunctive security sensitive (or select content) words, characters, icons and data objects near the target security sensitive words, characters, icons and data objects. The sensitive words may be security sensitive (or select content) words, characters or data objects defined by compliance with law, regulation or policy, privacy, national, organizational or private security concerns. For example, Bin Laden is the target sensitive word in FIG. B-8B and this classifies the entire paragraph as TS level. The other words in the paragraph are adjunctive word/objects.

[2762] Several steps are prudent to enable MS Office document protection. The first step is have a network guard (see FIG. D-16) that filters all incoming and outgoing traffic for MS Office document files and quarantines them. Spam and virus filtering is necessary to preclude system, resource, and file exploits. URL filtering, quarantine lists, black lists, white lists represent the minimum responsible approach. Ingress files can harbor viruses, etc. Outgress files can harbor privileged information at any and all levels of the DOM. With a means to filter and check every node for purpose, content, metadata, formats, structure, comments, links, and so on, there is no other way to vet the integrity of the file.

[2763] FIG. D-24 shows the General DOM Editor program 1022a in a flow chart form. Step 1024a is the initialization that is employed by the security entity to set up the program. Step 1026a

obtains the DOM layout or blueprint from the DOM vendor. Step 1028a notes that for each root, branch and leaf in the DOM, the information attributes must be prioritized with th the security organizational informational attributes. For example, the audio files of potential Bn Laden voice prints may be critical at TS and S levels but be completely excluded at C and U levels. Therefore, any audio files below C and U are security introns which are excluded or ignored.

[2764] Step 1030a obtains the source document DOM. Step 1032a maps the DOM source document as a binary file populated with content data and meta data as a subset of the DM blueprint. Step 1034a identifies security exons to be included in the further processing of the item and identifies security introns to be ignored or excluded in the processing. Step 1036a converts security exons at each root, branch and leaf int security safe form and format (for example, a safe DOM template), and generates a safe blueprint or map for the precursor DOM and discards all security introns. Step 1038a processes the content of the safe DOM with security filters discussed above. It also processes all data objects (exons) from the safe DOM with granular filters. Data is dispersed as necessary and retrieved and re-assembled as necessary with a safe map.

[2765] FIG. D-25 shows a flow chart of a basic application for a DOM Editor for MS Office document. Step 1042a initializes the system. Step 1044a obtains the source DOM document and notes that all processing occurs after a spam and virus filter. Step 1046a notes that the program creates or is provided with a security safe DOM document and map. Step 1048a notes that a template is opened. A clean .DOT template (Word) or whatever the new document type is opened for the specific application. The Normal.DOT or New Spreadsheet.XLS on the MS Office distribution CD is safe. In Visio, for example, start with a new chart. Older documents saved as templates tend to accumulate unanticipated metadata. If one must use a non-standard template, clean it up. View it as both a printed document, as

a binary file, and as a document object. Write protect the templates, or store the templates as non-modifiable networked volume. If the templates are used throughout the organization, create a network store for them and configure each user's installation of MS Office to look there for the templates. Search the network for duplicate copies of these templates and eliminate them.

[2766] Step 1050a disables edit controls and step 1053a copies content. The point is one must edit cleanly. This is not a single step but rather a process, both one time and ongoing. Disable versioning in step 1050a to prevent a buildup of past versions of the document. With versioning, prior sessions will be stored as document.doc 1, document.doc 2, and so on. These tend to get entwined with the latest version. If workflow with InfoPath, Outlook, or other collaborative workflow tools creates duplicate copies of the source document file for each user. Step 1050a includes the concept that the system is configured to store a single network copy instead. Preserve an audit trail and backup with a system backup rather than versioning. Disable change tracking in step 1050a to curtail the buildup of additions, deletions, and changes that transcend the publishing intent of the document. If redlining is necessary, establish guidelines for periodically accepting changes to purge change log. Use the command to save the document without the change log with File/Save or File/Save As. Do not use nor rely on fast saves, timed saves, or file recovery after a MS Office crash to purge the dirty metadata. After a crash, reopen the document, save the document under a new name. Close the Office application. Delete the old file precipitating the crash. Rename the new file under the old name. Reopen the Office application.

[2767] Step 1054a locates text in footnotes, hidden text, etc and either discards or ignores the subtext because those items are considered security introns or copies them into a safe DOM text form and disables functions, if necessary. Step 1056a notes that a clean map for the security cleared DOM document must be created. Step 1058a executes the editor or granular filter and dispersal routine as

necessary. The distribution or push of partial security cleared versions of the text can be included in step 1058a.

D.2 Applications of the Secure and SC Data Systems

[2768] The secure data storage systems in Part B, combined with the search engine or KE engine in Part C can be deployed in various applications, some of which are described in this Part D.

D.3 Automatic Features

[2769] 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.

[2770] 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.

[2771] 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

EX. 1002, Page 2088

or month. It may be n seconds after the user stops typing on a keyboard. It may be a timed back-up feature.

D.4 Multiple Security Levels

[2772] 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 (or select content) 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.

[2773] 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.

[2774] 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. Partial reconstruction of the plaintext also includes a concept that the security sensitive (or select content) items or materials may be subject to different types 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.

[2775] 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.

[2776] FIGs. D-1 through D-5 are omitted as shown in the drawings.

[2777] FIG. D-6 is an exemplary computer network diagram showing various user communities. It should be noted that select content SC data stores may be grouped for different portions of the same enterprise. Therefore, rather than have security groups as discussed herein, the system could provide SC interest groups in an enterprise. An "SC interest group" is the same as a security level group. 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. D-6 as PC-4, PC-5 and PC-6. Of course, Network A could be coupled to other PCs not illustrated in FIG. D-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.

[2778] 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 communicated via e-mail. Further, the network may be any telecommunications network including wire, cable, cellular, wireless, satellite, IR or RF systems.

[2779] FIG. D-7a 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 or SC 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 or SC level 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. D-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

[2780] Further, designation step 422 will include identifying the words, phrases, icons or data objects subject to security or SC 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

EX. 1002, Page 2092

Medium network storage	all family names, all client names
Low, encrypt and separate store in local memory	all items not in dictionary

[2781] 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

[2782] In FIG. D-7a, step 424 executes or enables the security program or SC levels 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.

Example: 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.

[2783] 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.

[2784] 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. B-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.

[2785] 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 .....

[2786] 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.

[2787] The following Security Level Access Placeholder Table is another example of the type

EX. 1002, Page 2094

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].

[2788] 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.

D.5 Sharing Data with Different Security Levels - Data Mining

[2789] The present invention can be configured to overcome obstacles to intelligence sharing and data sharing between parties by enabling the parties to identify granular critical data and control the release the granular critical electronic data subject to a sharing arrangement with other parties. In some instances, the controlled release process is designed to implement an agreed upon plan to share secured data or SC data based upon arms length negotiations between the parties. The invention enables a party to release specific granular data such as a name, address, or date without releasing the entire "classified" document. In a commercial context, this is akin to data mining in that the inquiring party seeks limited data (not the entire data file, record or document) and is willing to pay for the "mined" data. As an example of a security intelligence system, a local police chief may release granular critical data about a suspect to a federal agency, when in return the federal authority will release further intelligence "mined" or obtained for the secured data storage, about the suspect. The controlled release of data from the higher security level party (the FBI) may be an intelligence document or a granular part of it (a partial

EX. 1002, Page 2095

reconstruction provided to the local police). The rational behind this implementation of the invention is that there are many obstacles for sharing intelligence and information. There are even many more hurdles when it comes to sharing of raw intelligence. The invention creates a leveled playing field in which the different parties must share and exchange information in order to achieve their objectives.

[2790] The invention can be configured to resolve the major challenges facing government by enabling sharing of information between its different organizations in relationship to fighting terrorism. The invention for example can enable organizations, connected to the Homeland Security Department, to search data bases of various other government, state and local organizations, eliminating the fear of the "source" organizations, owning or controlling the source or plaintext documents that their proprietary data or granular critical data is released without their specific permission. The invention enables open negotiations between the parties regarding what data to release and for what consideration. When several organizations are seeking access to a specific document, the invention and can allow a controlled release of different granular data to different parties for different considerations and benchmarks.

[2791] The invention's mechanism of controlled release of the located document/data enables other parties to search their documents without the fear that sensitive information will be released to the searching party. This invention is designed to foster sharing of documentation between different parties, taking into consideration the need to limit the access of other parties to the total content of the owner's document.

[2792] The invention is a machine and process and its purposes and advantages may be as follows: (a) To automatically control selection of data objects within a data stream and release them in a controlled method only to authorized parties. (b) To automatically separate data objects within a data stream into two or more digital data streams according to the importance and categorization of contents,

through extraction and removal of the prioritized content and its replacement by appropriate placeholders. (c) To automatically control selected contents in E-mail, and enable its release in a controlled method only to authorized parties. (d) To enable users to leverage the growth in computer and telecommunications connectivity and electronic commerce by reducing security risks. (e) To enable users to release documents, digital files, and data streams into closed and opened digital networks with the confidence that important, identifying, and critical contents in that documents, digital files, and data streams is secure and will be seen only by authorized parties. (f) To enable real time simultaneous customization and personalization of selected contents within a data stream to different parties, allowing instant display of the selected content or part of it based on, and tailored made to the status of the user or receiving party. (g) To secure the important and critical contents of a document or digital file by transporting said contents into a separated data stream and removing said data stream to a removed storage memory, while eradicating any copies, temporary caches, or traces of the removed extracts on the original computer or machine. (h) To enable instant return transfer to the display or to another display all or part of extracted content instantly with verification of authorized user. (i) To create a projection of the original document, digital file, data objects within a data stream, or variations of it through combined projection of the splinted data streams, while maintaining separation between the data streams. (j) To create an alternative method for security, instead of encryption, which is secure, cost effective, less time-consuming, and flexible. (k) To enable automatic timed removal of specific content items, automatically or manually selected from a document, digital file, or data objects within a data stream. (l) To enable an automatic timed reconstruction (reconstitution) of the said document, digital file, or data objects within a data stream.

[2793] Another object of this invention is as a system and method for automatically creating

EX. 1002, Page 2097

customized and personalized versions of a document, data object, or data stream. In real time, simultaneous versions of the original are created and altered, then disseminated based on the status of the different users and their access privileges. The system and method enables content management and control by automatically locating content items prioritized by importance, transporting them to a secure memory, and releasing them under explicit controls or preset rules.

[2794] Another object of the invention is as a system and method for control, analysis and management of important and prioritized information within documents, files, data object, and data streams. The system and method, enables the processing of all data objects at the time in which they are created or imported into the system. The early stage processing, enables early stage inventorying of prioritized contents as well as early stage pattern recognition. Extracting critical information, such as credit card numbers, last names, first names, social security numbers, phones numbers, transaction dollar amounts and addresses, enables the system and method to aggregate data in categories and analyze the data in different optional methodologies including pattern recognition.

[2795] Another object of the invention is as a system and method for comprehensive monitoring of various activities including business activities in real time. With this level of detail, the system and method becomes a management information tool and information/data command and control center. The said system and method can include an alert system, which in effect creates a real time apparatus for command and control of the systems activities. In real time, and at any point in time, the user can get a comprehensive view of different activities including: (a) How many transactions are being processed, their content, their context, identity of the involved parties identity, their profiles, and the personnel involved. (b) How much money is being transacted. (c) When, in terms of dates, relevant to the transaction. (d) Where, in terms of geographical location, the transactions are taking place. (e) Where, in terms of geographical

location, monies or goods are being transferred. (f) Which departments in the organization are involved.

D.6 Multilevel Security through Sanitization with Reconstruction of Sanitized Content

[2796] A multilevel security (MLS) or SC level technology secures the targeted, filtered content with extraction and dispersal to storage, bypassing the use of classification labels, in order to achieve stronger security of the source document or data or better understanding of the SC material. During the process of developing security or SC technologies for defending critical infrastructure, it was discovered that the business model was too complex and there was a need to redefine and create new systems and methods for doing business. As a result, one aspect of the present invention provides a system and codifies methods and business processes to automatically identify, extract, store critical data (as an input security system) and permit reconstruction of critical data only in the presence of certain security clearances (as the output of the security system) or as established by the SC policy release rules.

[2797] The invention is a method and process to establish a stronger multilevel security (or MLS) architecture and product, than is currently available. The invention introduces multilevel security through sanitization of critical content of a source or plaintext document (or data object) with the unique ability to reconstruct all or part of the original document in conformance to the classification level of the user. A user with top classification may view the entire document, while a user with a lower level classification will view a sanitized document, tailor made automatically for his clearance level. The invention secures the targeted filtered content of a document, file, or data stream, through extraction and dispersal to storage, bypassing the common use of classification labels in order to achieve stronger security. The invention enables secure document storage and secure message transfers between users and networks with different security classification levels while protecting the information on a need to know basis.

[2798] Currently multilevel security MLS systems are using multiple PCs for each user, and using

physically separate systems for processing data at each classification level. The inventive system, in several embodiments, eliminates the need for the use of multiple computers. All the documents in the user's PC are automatically secured with a granular classification process generally described above with identification of special security data, extraction from the source document or data object, and then separate storage of the security data. The classified granular content is dispersed to different secure, distributed storage locations. The classification level of a user will determine his right and ability to access and release the stored critical extracted content from the various storage locations for reconstruction. A user with top classification will view the entire document, while a user with a lower level classification will view a sanitized document, tailor made automatically for his clearance level.

[2799] Types of government security levels are: Top Secret (TS); Secret (S); Confidential (C); and Unclassified (UC). Business identifies security levels as: Restricted to Management (R, for example, attorney-client privilege); Proprietary (P); Sensitive (S); and Public (P). These MLS security levels may be supplemented with "need to know" classification labels, organizational limits (Army, Navy, DoD) and time limits. Prior art security systems identified each file with: owner, size, date and time of creation and security attributes. The Bell Lapadula (BPL) security model uses concepts such as domination of the MLS security level over both a process and the subject (a data object). Some examples of various processes are read, execute, overwrite, append, write, kill (delete), etc. Some examples of process rules under the BPL model are: NRU - No Read Up (a lower security level cannot read a document at a higher security level); NWD - No Write Down (a higher level cannot write down to a lower MLS level).

[2800] The invention herein does not use the "classification labels" of the prior art. Instead it creates a situation in which the user gets access rights to specific distributed storage locations based upon his MLS level, each access right can be classified with a different classification level. With respect to the editor

described later herein, security labels (for example ("e.g."), TS, S, C and UC labels) are added or inserted into the filtered but not disassembled document. As explained later, the insertion of these SL labels conforms the current inventive system to the prior art methodology and protocol. However, the current inventive system does not use the SL labels for processing purposes. The current system uses a granular or filter approach to make secure the sensitive data in a particular document. SC labels, matching the relevancy of the SC data may be employed rather than security level tags.

[2801] FIG. D-7b diagrammatically illustrates a multiple level security system accessed by users having different security clearances (which also represents a data mining system and operation). A MLS SC data system uses different SC policy rules permitting access to different SC levels of interest. Source data 100 passes through security program 200. Critical, important data objects or elements are extracted and dispersed into storage 801. In the illustrated embodiment, storage 801 has four security levels SL1 - SL4, level SL4 being the most secure data requiring the highest security clearance. Levels SL1 - SL4 may refer to SC relevancy levels or organizational levels. Between each level is an MLS or multiple level security guard. The guard (physical or software configured) limits transfer of data objects there between. Upon a request or inquiry from user 1, 2 or 3, each having a security clearance s1, s2 or s3, respectively, the query or request for access to data Q1, Q2, or Q3 is sent to security clearance process 803. The process 803 detects and confirms the user's clearance level and passes a cleared query to storage 801. Cleared data (an entire document/data object or a portion thereof or simply one secured data (i.e., a name)), is sent as Data 1, 2 or 3 to clearance process 803. If clearance is still valid, data 1, 2 or 3 is sent to the respective user.

[2802] FIG. D-7b can be a data mining system in that the user is permitted to mine the "cleared" data from storage 801. Data mining may be a monetary charge associated with the clearance function in process 803.

[2803] In a secured system, the documents in the user's PC may be in "declassified" to his security level 99.9% of the time. The "declassified" or available documents are reconstituted through a controlled release of the critical data from storage, and re-classified only when the user presents his identification and his classification level is being verified. Reclassification is automatic at the user's PC. The result is that the user's PC or workstation can operate in classified and un-classified modes. It is unclassified when the documents are declassified and when the documents are reconstituted the user is working in a classified mode.

[2804] The invention introduces a new paradigm whereby computers that are classified as secret or top secret, in actuality will contain 99.9% of the time declassified documents. This capability strengthens substantially the security of such classified systems.

[2805] The invention can resolve the major challenges facing government in enabling sharing of information between its different organizations in relationship to conducting military operations as well as fighting terrorism. The invention for example can enable organizations connected to the Department of Defense (DOD) or the Homeland Security Department to search into data bases of various other government, state and local organizations, eliminating the fear of the organizations owning the documents that their proprietary data or granular critical data would be released without their specific permission. The invention's mechanism of controlled release of the located document/data enables other parties to search their documents without the fear that sensitive information will be released to the searching party. This invention is designed to foster sharing of documentation between different parties, taking into consideration the need to limit the access of other parties to the total content of the owner's document. The invention enables overcoming the obstacles of existing multiple level security MLS systems by enabling sharing of sensitive data, and granular data between parties in a much more flexible way which also enables much greater access to information not enabled by the current MLS systems. The invention includes a controlled release

mechanism for release of data in conformance to benchmarks, which can include submitting of access identification, the giving of consideration, submitting of other information, etc.

[2806] The invention creates better collaboration between users and organizations based on a better flow of information. It enables better efficiency enabling easier communication between users and networks with different levels of classification while maintaining the highest levels of security. The invention enables a much better management of documents in storage and in transport including e-mail. The invention introduces automation to the sanitization process and an automatic reconstruction process. The automation will avoid human error both intentionally as well as unintentionally. The automation will enable a substantial reduction in costs, furthermore the ability to create a multilevel security environment in one PC or workstation will save costs of purchasing operating and maintaining multiple machines as is the current practice.

[2807] The challenge of many organizations is in getting mission critical and time sensitive information speedily to the users who need it. In many cases the needed non- classified or low-level classified information is stored in systems but is not provided to the user who needs it, because the information is in documents which are highly classified. This creates situations in which users are unable to access information, which they need to accomplish their tasks, because of a technological classification barrier. This over classification of information results in hampering critical tasks and activities, as well as creating system redundancies inefficiencies. The DoD (Department of Defense) multiple level security (MLS) was based upon the Bell-Lapadula (BPL) Model. Many believe that the BLP security model is superior to other models. The Bell-Lapadula Model and the existing MLS uses labels to classify users and subject matter. A professional attacker will use his efforts to change or damage the labels in- order to compromise the machines secured information.

[2808] The architecture or the present invention extracts and physically separates data whereby

content is being recognized not by labels by automatically based on the semantic content of the plaintext. In some embodiments of the present invention, labels are added to the granular, filtered document to conform to known organizational protocols. These labels are displayed but not used by the system in processing.

[2809] In the DoD's MLS, data of multiple security levels are processed and transferred by the system, which separates the varying security levels and controls access to the data. In the prior art MLS system, some applications process only one level of data at a time, (for example, when a user edits a document with a word processing tool, the data in the document are treated as if they were a single level, the classification of the document itself). Other applications treat individual data elements at their actual levels. For example, a word processor enforces paragraph and page MLS classification labels, or an MLS data base brings together data elements of different security levels to allow an analyst a multilevel view of the information.

[2810] The vulnerabilities of MLS: The components in the MLS system contain the data in their memories and disks, and the data could be compromised if adequate physical security is not maintained. An attacker who gets access to the system might be able to locate the data or its copies. MLS guards control the flow of information across security boundaries. These MLS guards are known. One concern with the Bell-Lapadula Model and the existing MLS is the use of labels to classify users and subject matter. A professional attacker will use all his efforts to change or damage the labels in- order to compromise the machines secured information. The invention introduces an architecture whereby content is being recognized not by labels by automatically based on the semantic contents of the plain text. The invention sanitizes and enables reconstitution upon valid authentication. It is the only architecture and system which enables both sanitization and reconstitution according to user's verified access identification. The conventional way of classifying documents with high classification (TS), limits the low level clearance users (C) from accessing substantially

EX. 1002, Page 2104

un-classified information "granular data" which is in the classified document. Furthermore, the invention enables maximum sharing of unclassified information which lies dormant in classified documents. Top security- secret information is dispersed to distributed storage in many locations. The invention is designed to avoid any one point of failure. The theory behind the architecture is the creation of substantial lines of defense in depth. The attacker will need to break through many obstacles before accessing all the dispersed data of the document. Additional levels of security are provided with multi-type encryption. The system and process introduces the capability to encrypt different parts of a document with different types of encryption. Multi type encryption creates a major barrier to an attacker. Should he wish to break the encryption, he would need many super computers. Should the attacker look for implementation mistakes, even if he finds few, he will still not get access to the total plain text. The inventive system provides flexibility. The system and process delivers flexibility to accommodate changing circumstances. By controlling the level of the granularity, the user can boost the level of security according to changing circumstances. For example, if a competitor becomes a partner the user enables him access to more storage locations, by changing the matrix.

[2811] The system and process integrates the Internet for dispersal and hiding of contents. If a party needs more information it could be released granularly. There is no need to release the whole secret document. The system and process does not use labeling but rather extracts the critical to storage (bu the system may label sensitive text to conform to known protocols). The system avoids situations, in which, attackers may manipulate the labels or the labeling system. Furthermore, the release of information is based on changing circumstances (time, location-GPS, event).

[2812] The invention is a machine and process and its purposes and advantages may be as follows: (a) To automatically control selection of data objects within a data stream and release them in a controlled method only to authorized parties. (b) To automatically separate data objects within a data stream into two

or more digital data streams according to the importance and categorization of contents, through extraction and removal of the prioritized content and its replacement by appropriate placeholders. (c) To automatically control selected contents in E-mail, and enable its release in a controlled method only to authorized parties. (d) To enable users to leverage the growth in computer and telecommunications connectivity and electronic commerce by reducing security risks. (e) To enable users to release documents, digital files, and data streams into closed and opened digital networks with the confidence that important, identifying, and critical contents in that documents, digital files, and data streams is secure and will be seen only by authorized parties. (f) To enable real time simultaneous customization and personalization of selected contents within a data stream to different parties, allowing instant display of the selected content or part of it based on, and tailored made to the status of the user or receiving party. (g) To secure the important and critical contents of a document or digital file by transporting said contents into a separated data stream and removing said data stream to a removed storage memory, while eradicating any copies, temporary caches, or traces of the removed extracts on the original computer or machine. (h) To enable instant return transfer to the display or to another display all or part of extracted content instantly with verification of authorized user. (i) To create a projection of the original document, digital file, data objects within a data stream, or variations of it through combined projection of the splinted data streams, while maintaining separation between the data streams. (j) To create an alternative method for security, instead of encryption, which is secure, cost effective, less time-consuming, and flexible. (k) To enable automatic timed removal of specific content items, automatically or manually selected from a document, digital file, or data objects within a data stream. (l) To enable an automatic timed reconstruction (reconstitution) of the said document, digital file, or data objects within a data stream.

[2813] The invention differs from the current implementations of multilevel security MLS systems based on the Bell-Lapadula Model, and the prior art use of labels to classify users and subject matter. A

professional attacker will use all his efforts to change or damage the labels in- order to compromise the machines secured information. The present invention introduces an architecture whereby content is being recognized not by labels by automatically based on the semantic contents of the plain text. The invention enables overcoming the obstacles of existing multiple level security systems by enabling sharing of sensitive data, and granular data between parties in a much more flexible way which also enables much greater access to information not enabled by the current MLS systems. The invention includes a controlled release mechanism for release of data in conformance to benchmarks, which can include submitting of access identification, the giving of consideration, submitting of other information, etc. The invention creates better collaboration between users and organizations based on a better flow of information. It enables better efficiency enabling easier communication between users and networks with different levels of classification while maintaining the highest levels of security. The invention enables a much better management of documents in storage and in transport including e-mail. The invention introduces automation to the sanitization process and an automatic reconstruction process. The automation will avoid human error both intentionally as well as unintentionally. The automation will enable a substantial reduction in costs, furthermore the ability to create a multilevel security environment in one PC or workstation will save costs of purchasing operating and ,maintaining multiple machines as is the current practice.

D.7 Multiple Independent Levels of Security (MILS)

[2814] FIGs. D-16, D-17 and D-18 diagrammatically illustrate a computer system configured as a multiple independent levels of security (MILS) system. Although the general operation and layout of the MILS system is well known, the incorporation of the inventive system, that is, granular filtration, extraction and re-assembly is unique to the inventive system. In the following MILS system 910, the dispersion and retrieval operation of the present application is discussed using, as an example, one of the most common

environments for protecting classified data, that is, Multiple Independent Levels of Sensitivity (MILS). The MLS system, discussed in connection with security levels, can be implemented with SC based upon either relevancy or based upon enterprise units who have permission (policy rights) to access the SC data.

[2815] As is known in a MILS configuration, each level (TS - top secret; S - secret, U - unclassified) of classified data is isolated from other levels by confining it to set of components dedicated to a single classification level. Data labels are not used within the system, since its components are Commercial-Off-The-Shelf (COTS) products that are not able to handle data labels. The level of the system TS, S or U (top secret, secret or unclassified) establishes an implied sensitivity label. Data is explicitly labeled only in guards 926, 932 (the Dispersal and Re-assembly guard computers) and other MLS devices that connect the MILS system to systems at other sensitivity levels, that connect the TS system to the S system and to the U system. Data transfer between levels is accomplished manually (sneaker net), or through a few, high assurance and closely protected MLS devices, such as guards, digital diodes, etc. A user with the authority to access multiple levels of data is required to use a separate set of interface equipment to access each MILS system. In some cases, keyboard-video-mouse (KVM) switches are permitted.

[2816] Figure D-16 shows an implementation of the present invention in a MILS environment. Two similarly configured domains 911, 915 are shown (upper region consisting of sub-networks 912, 913 and 914 and lower network 915), presumably under different administrative control. Each domain has three networks, one for each of three classification levels. Each network includes a plurality of workstations (only one station being shown in the figure), a Dispersion and Reassembly (D&R) server 926, 932, (a MLS device connected to all networks), and database servers TS, S and U data servers (928, 929 and 930 in the upper domain and 934 in the lower domain) to support the D&R server's proxy document server functionality.

[2817] The user interface components of the present invention reside on the user workstations W St-

EX. 1002, Page 2108

U (920), W St-S (918) and W St-TS (916). Dispersion and reassembly functionality is hosted in the D&R servers 926, 932. Digital signatures (encryption) protects the integrity of user data between the user interface at 916, 918, 920 and the D&R server 926. Encryption provides a level of discretionary access controls that prevents disclosure in cases where others have the appropriate clearance ut lack the formal "need to know" level to view the classified information.

[2818] The present example discusses an e-mail and a file server to help clarify its operation in a MILS environment. The system may be configured to handle other documents, images, etc. In the e-mail example, a Top Secret user 916 will prepare a multi-level message and send it to a Secret user 922b, and the recipient 922b will only be able to read the "Secret Level" and below parts. In the file server example, a Top Secret user 916 will prepare a multi-level document and post it to a file server, then a Secret user 922b will retrieve it, getting only the Secret and below parts. These are both downgrading examples. Movement of data within a level and to higher level conforms to existing security rules, for example, Bell-LaPadulla rules.

[2819] The path an e-mail message takes from a Top Secret workstation 916 in one domain 911 to a Secret workstation 922b in the other domain 915. It would work similarly if both sender and receiver were in the same domain; the local D&R server 926 would perform the functions of both D&R servers 926, 932 in this example. The D&R server 926 hosts an e-mail server that is customized to perform D&R functions, as described below.

[2820] An e-mail originator on a Top Secret workstation 916 composes an e-mail using MS Outlook. Originator marks sections of the message with TS, S, and U levels (explained herein), and the system on workstation 916 compartment tags the email document using a combination of the automatic features described earlier and manual tagging (user based), as allowed by the security policy of the accrediting organization. Originator 916 digitally signs and sends the message to the mail server on the D&R system

926.

[2821] The Disperser component of the D&R mail server 926 verifies that the originator 916, identified by e-mail address and authenticated by the digital signature key, has the authority to downgrade messages to the requested levels. The Disperser within Server 926 separates the message according to the originator's tags. The Disperser writes the message sections tagged higher than Unclassified to the Secret and Top Secret servers 929, 928. The unclassified part becomes the base message map stored in server 930 and contains pointers to the higher-level components. The pointers map the re-assembly path when the document is fully or partially re-assembled. This base message map is the only step in the process that requires downgrading. A guard 926 is used to provide increased assurance that the downgrading is done correctly (see FIG. D-17, guard 936). The originator's identity is provided to the guard as part of the downgrade credentials. The Disperser forwards the base message and message map, to the D&R e-mail server 932 of the addressee, using its Top Secret network path c. Other paths 924a, b and c link the same security levels in either domain. Using the TS path prevents downgrading if the target server 932 is not a D&R server. Alternately, the D&R servers 926, 932 could authenticate each other before transferring messages.

[2822] The target D&R e-mail server 932 determines the clearance of the addressee 922b from its network address and looks up the addressee's compartment authorization in its own tables. It then removes links from the base message and map to all message components that are not dominated by the addressee (as defined by Bell-LaPadula). The target D&R e-mail server 932 then retrieves the data for the remaining message components from S database server 929 via guard server 926, constructs or re-assembles the message that the addressee is cleared to read (secret level, not top secret level), and places the message in the addressee's inbox 922b that is at the security level of the highest component in the message. These steps are executed for each addressee. The addressees 922b connect to their local D&R e-mail servers 932 and

download unread e-mail.

[2823] A similar method is used for document serving, such as would be used for file service, web service, ftp service, etc. The document creators tag their documents, sign them digitally, and post them to a D&R file server 926, 932, which is actually a proxy using storage in the database servers 928,929, 930, 934, and others not numbered. The server 926, 932 disperses the message components to its database servers on the MILS networks.

[2824] The following describes the path a document takes from its creation (or modification) in a Top Secret workstation 922a in one domain 915 to a reader on a Secret workstation 918 in another domain 911. The D&R server 932 hosts file servers that are customized to perform D&R functions, as described. The document posting process follows: A document is created on a Top Secret workstation 922a using MS Word, Excel, etc. The originator 922a marks sections of the document with TS, S, and U, and compartment tags using a combination of automatic and manual tagging features, as allowed by the organization's security policy. Originator at 922a digitally signs and sends the document to the file server on the D&R system 932.

[2825] The Disperser component of the D&R file server 932 verifies that the originator 922a, identified by the digital signature, has the authority to downgrade documents to the requested levels. The Disperser in server 932 separates the document according to the originator's tags, creating a base document at the lowest tagged level (U - Db or S - Db) that contains pointers to the more classified components (TS - Db 934). The base document is encrypted using an algorithm appropriate to its level. The Disperser writes the document sections to the file servers (U - Db or S - Db or TS - Db 934) according to their tags. This is the only place in the system where downgrading is performed. A guard 932 is in the downgrade path to provide additional assurance that data is not leaked. The user identity derived from the originator's 922a digital signature on the tagged message will be provided to the guard 932 as part of the downgrade

credentials. The disperser places references to the document in the directory of each file server 932, 926 for which a version of the document can be built (e.g., if there is no unclassified data in the document, a reference to the document will not be placed in the unclassified directory).

[2826] The document retrieval process follows. A user on a workstation 916 logs onto its local D&R proxy document server 926. The strength of user authentication is application specific and determined during system accreditation. The user 916 locates a document and requests that it be downloaded for reading, specifying a requested sensitivity level and compartment. The Re-assembler component of the D&R server 926 loads and decrypts the base document. The Re-assembler in server 926 verifies that the requestor 916 dominates the requested security level and compartment, based on the level of the network over which the request was received and the contents of its compartment authorization table. The Re-assembler in server 926 constructs the document to the authorized security and compartment level. The Re-assembler provides the document to the requestor. The re-assembly function does not violate Bell-LaPadula and does not require downgrade authority.

D.8 MLS Server and Workstation Components

[2827] FIGs. D-17 and D-18 diagrammatically illustrate the server and workstation. Figure D-17 shows the D&R Server 926 hosted on a DigitalNet CTS-400 system, which is currently evaluated. It consists of the CTX-400 hardware and the STOP 6.0 operating system. The disperser part 937 of the D&R server 926 has the most security critical functions, since it must move data contrary to the Bell-LaPadula security policy. It maintains a table of user downgrade authorizations 938 keyed by the originator's public digital signature key 939 and downgrade authority 941. A guard 936 is also included, which may employ a version of automated tagging system of the present invention to identify sensitive data. The double check of the security label tag for each part of the message/document provided by the guard 936 is particularly important since the

downgrade labels are applied in a single-level system.

[2828] The re-assembly side (in re-assembler 942) requires no policy violation, but requires its own table of user compartment authorizations 944 because the MILS systems do not have the ability to label data. The table 944 is keyed by e-mail address (for e-mail routing) or user identity 945 from the user authentication process (for file service). Authorized compartments 946 are coupled to email user id 945.

[2829] The components of the user workstations are shown in Figure D-18. A MILS workstation 916 is a single-level component, that is, it is coupled to a single security level network. The user interface will in some cases be installed on existing workstations 916 and in other cases new workstations procured for this use. The workstations include an operating system Windows 2000, a graphical user interface Windows GUI, WS Office as a document processor, digital signature system rated at EAL 4 and a rated user interface.

D.9 Flexibility of the Present MLS Approach

[2830] The late-binding techniques or retrieval and reassembly features used in the present invention is a compelling feature, because it provides solutions to some of the most significant problems of sharing data in modern warfare and international coalition operations. A single comprehensive document can include data sensitive to many different environments, yet by tagging its components correctly, maximally useful versions can be provided to readers with widely different authorizations, and without having to identify them all ahead of time.

[2831] For example, in a coalition environment, countries or classes of countries, or agencies within countries can be assigned non-hierarchical and hierarchical labels and then a single document, suitably tagged, can be securely distributed to all of them using a properly configured and administrated infrastructure of the present invention.

[2832] In the presently configured MILS embodiment, the tagging protocol is, at a minimum,

confirmed by the guard in the D&R servers. In prior art systems, only the guard tags documents. In the presently configured system, the thin client applications program on the workstation tags the document segments but the guard confirms this preliminary tagging. One feature which seems to be important in certain security systems is that the re-assembly map be cleaned or scrubbed to match the then current security level where the map is stored. This theory, carried forward, would include the concept that the re-assembly map, stored in each version of the secured document, only point to the next level storage location. Hence, if all portions TS extracts, S extracts, C (classified) extracts and U (remainder) document are dispersed into, for example TS 928, S 929, C (not shown) and U 930, then the document in U 930 only includes a pointer to the location of C extracts and the C extracts only includes a pointer to the S extracts and the S extracts includes only a pointer to the TS extract location. The downgrade discussed above refers to the location of the higher secured extract.

D.10 Multiple Extraction Filters and Application Outline

[2833] There is a need to construct filters which supplement the initial list or compilation of security sensitive (sec-con) or select content (SC) words, characters, icons and data objects (herein "word/objects"). The need arises either due to the fact that the initial security or SC word/object list is incomplete, or that the author of the initial list is concerned that the list is too limited or in order to defeat a attack or an inference engine "reverse engineering" the sanitized document and ascertaining not only the filter (a type of code) but also the sensitive word/object removed from the source document. Further, the incorporation of a filter generator enhances the current user friendliness of the program. In its current embodiment, the program is configured as an editor to screen and sanitize a source document. The user selects, at his option, functional aspects which include: compliance with laws (an application of a type of filter, e.g. HIPAA, GLB, Oxley-Sarbanes, EU privacy, executive orders); privacy (another type of filter which excludes, for example, social

security numbers, see also, EU policy); search for and supplement filter; pay per view (which enables the user to buy missing sensitive information (for commercial purposes); survival (which creates a distributed and dispersed copy of the user's document and other stored documents and items using predetermined storage facilities); security (which triggers the various security routine discussed herein); and storing (which permits the user to select which of the several storage options the extracted sensitive or SC data/objects should be employed in the dispersal.

[2834] The filter routine diagrammatically illustrated in FIG. D-19 is useful in compiling a filter which separates both the sensitive word/objects and contextual and semiotic and taxonomic aspects of the initial list of security sensitive (or select content) word/objects. The filter works in conjunction with a compilation of data, typically located on a network which could be private or public. In low level security or SC situations, the filter may access Internet databases to gather additional data for the filter. In more secure or SC systems, the filter could access a secure or SC data base (one located at the same security level as the user) and build or compile the additional word/objects. The filter program 950a in FIG. D-19 begins with step 952a which compiles the initial list of security sensitive (or select content) word/objects. In 954a, the initial list is supplemented with dictionaries, phone books, corporate records (to obtain subsidiary data and trade names) and thesaurus data. Each of these represent different compilations of data and the added data is added to the initial list of sensitive word/objects. In 956a, a search is conducted on a network, usually through a search engine, to gather excerpts near and abut the keywords. These keywords are the initial sensitive word/objects. Statistical algorithms are applied to gather non-common word/objects which are associate with the keywords as found in the additional data compilations. The goal of the adaptive filter is to obtain contextual, semiotic and taxonomic words, characters or data objects from the compilation of additional data related to the security sensitive (or select content) words, characters or data objects. Semiotic

is a general philosophical theory of signs and symbols (read language and words and objects) that especially deals with their function. Semiotics include syntactics, semantics and pragmatics. Syntactics is the formal relationship between signs. Semantics is the meaning of signs and pragmatics is the relationship between signs and their users, such as the relationship of sentences to their environment. Taxonomy is the scientific classification and categorization of items. Therefore as an example, a search through the Internet on Google search engine under "Bin Laden" may shw a number of uncommon (non-dictionary words) within 200 words of the target "Bin Laden." This search string would gather documents form the Google search and copy 200 words on either side of "Bin Laden" and then extract only non-dictionary words into a supplemental list. This type of filter algorithm looks for contextual matters close or near to the target. The search is semiotic and statistical in nature. Additionally, the initial supplemental list would identify the Bin Laden is an arab and this classification (a taxonomic aspect) can be used to expand the list for the filter. The algorithm may include a simple command to gather all 10 words on either side of Bin Laden. This is a pure contextual search and the "10 word" aspect is a statistical number. From the supplemental list, all pronouns, prepositions and conjunctions may be eliminated. Spiders or robots may be used in the gathering of the contextual and semiotic filter data. The contextual, semiotic and taxonomic words, characters or data objects from the compilation of additional data is all related to the initial list of security sensitive (or select content) words, characters or data objects.

[2835] Step 958a compiles the adaptive filter. The above noted contextual, semiotic and taxonomic filter is adaptive since it can be used to expand (and potentially contract or reduce) and adapt an existing list of sensitive word/objects to a larger list which better protects the source document and inhibits the operation of an inference engine. Step 959a repeats the filter gathering and compilation for various levels of security. Higher security may require a broader search (1000 uncommon words near Bin Laden and add all Arabic and

sub-Asian continent cities). Orthogonal security groups (those groups having the same level, e.g. S Secret, with each other but being different organizations, e.g, Department of Defense compared to the FBI) often have different methods to keep data secret between compartments.

[2836] The adaptive filter can be set to automatically gather additive sensitive word/objects. The system, with a basic filter, may identify a sensitive word in a paragraph being scanned by the initial filter. This sensitive word may be a special word in the existing filter or may be a non-common word not found in the initial filter. The adaptive filter system may then obtain this "unknown" or "special" word, and conduct a search through a compilation or data base of additional words, etc. Any new word/objects falling within the contextual, semiotic and taxonomic words, characters or data objects from the compilation of additional data (database) related to said security sensitive (or select content) words, characters or data objects are then added to the filter. The expanded filter is then used to screen the source document.

[2837] Step 960a compiles a supplemental filter with random words, phrases, etc. in order to further defeat an inference engine reverse engineering assault on the secured and sanitized document. In some sense, the production and use of a random filter is an encryption technique since the resultant filtered product, in order to be understood by others, must be reverse filtered or decrypted to reveal the document at the appropriate security level. Nonsense words may be added to this supplemental filter. Step 962a applies the primary filter (with the security word/objects and the additive word/objects from the contextual et al. filter) to the source document. Step 964a extracts the sensitive word/objects per security level. It is noted that several filters are used, on one for each security level, whether hierarchical or orthogonal. The extracted word/objects are stored or th partially extracted document per security level is stored in the corresponding security cleared data base or storage. Step 966a applies the supplemental filter to the remainder or lowest classified document. Step 968a stores the supplemental random filter to permit the low level user to decrypt

the document. Step 970a publishes, distributes or pushes the document to others having a need to know. The pointer to the location of the supplemental filter decoder is encrypted and stored in the filtered remainder document. This permits the low level person to decode the remainder document.

D.11 Multiple Security Features for Data

[2838] FIG. D-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. Multiple levels, types 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.

[2839] Step 510 in FIG. D-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. B-4 and D-7a, 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. D-9 is necessary.

[2840] FIG. D-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. D-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.

[2841] 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.

[2842] 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; end code

[2843] 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. B-1A, B-1B and B-2.

[2844] To some extent, the present system can also be utilized for key management and encryption systems.

[2845] 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. D-

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.

[2846] 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.

[2847] To achieve a very high level of security, the system can optionally incorporate a two-man 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.

[2848] 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.

[2849] 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.

[2850] 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.

[2851] 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 dispersement 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.

[2852] It should be noted that various aspects of the methodology and program described above in connection with FIGS. B-1A through B-4 and D-6 through D-9 can be incorporated into the parsing methodology and program in order to enhance or modify the system.

D.12 Adaptive Data Security - Event Responsive System

[2853] 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.

[2854] The output of the electronic attack or hacking monitor loaded into PC 142 (FIG. B-2) for example, or loaded into PC-6 acting as a server for Network A 404 in FIG. D-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

[2855] 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.

[2856] FIG. D-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.

[2857] 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.

[2858] 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.

[2859] There are various methodologies that may be utilized in the adaptive system. The tables in FIGS. D-8 A (Standard Automatic Defenses Matrix Table), D-8B (Optional Automatic Defenses Matrix Table), D-8C (Security Meter Module Table), D-8D (Normal Work Mode Table), D-8E (Threat Made Table), and D-8F (Attack Mode Table) sets forth these various security methodologies.

[2860] Another object of the system and method is to enhance the survivability of a system, network, or an organization through distribution of critical information. The objective is to enable a network or organization to carry on its critical missions even while under attacked or damaged. Survivability is the ability of a system to execute its mission and provide critical operational services during and after a successful intrusion or damage. Providing critical operational services includes maintaining availability of information and data such as credit card numbers, names, phone numbers, transaction amounts, shipment details without compromising the security of the information and data.

[2861] The invention is designed to enable a network to adapt to ongoing attack and react in a way that permits critical missions to continue. With the current state of the art, when firewalls or other security measures are compromised, no real obstacles curtail or hinder intruders. The system and method is very adaptable and flexible to provide additional layers of security, privacy, anonymity, redundancy, and backup through the selection, extraction, storage, transportation, and reconstruction processes. The dynamic architecture of the invention enables it to conduct an automatic real time configuration of its extraction/transport/recovery activities, in response to the challenge of attacks.

[2862] The invention's survivability modes enable: (a) Presetting of rules for computer or network functioning under attack or alert. (b) An automatic assessment of damage and automatic reaction to enable functionality of critical missions.

D.13 Email, Web-based and Other Types of Applications

[2863] FIGS. D-11A and D-11B diagrammatically illustrate a flowchart showing the key components of one embodiment of the present invention, that is, an e-mail security system. A similar system may be deployed to capture select content Sc data in real time FIG. D-11A is linked to FIG. D-11B via jump points D-11-A and D-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. The extract stores may be SC stores. A singular security or SC relevancy level is identified in FIG. D-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 (or select content) 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. D-11A and D-11B primarily relate to identification of security or SC data, the same is true regarding the use of securing e-mail data with a parsing algorithm.

[2864] The e-mail security or SC 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 or SC filter identifying one or more security sensitive (or select content SC relevant) 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 or SC check on the plaintext document or composed e-mail generated in step 604. The filter is used in step 604. In step 612, security or SC 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 or SC words for data to be extracted out. The highlighting step facilitates this selection. In step 616, the system extracts the security or SC data and, preferably, in step 618, the security or SC 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.

[2865] After encryption step 618, the e-mail security or SC 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 or SC 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 or SC 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.

[2866] A second e-mail having encrypted security or SC 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 ASP or SC application service provider ASP. See the discussion of FIG. B-2 above. The ASP represents a data storage facility for the secured or SC 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 or SC data is sent to the ASP. In step 626, the addressee receives the remainder e-mail which includes a hyperlink to the secured or SC data ASP. The system jumps at jump step D-11-A from FIG. D-11-A to FIG. D-11-B.

[2867] 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 the SC system, the SC data is stored in the SC storage and this data capture is logged into the system. In step 630, the secured or SC data ASP obtains a map for each secured or SC data e-mail (since the original e-mail may be broken up into a plurality of extracted, secured or SC data e-mails) obtains all secured or SC data e-mail and decrypts the same. In step 632, the secured or SC ASP downloads the secured or SC data as an e-mail to the addressee. In step 634, the addressee system compiles the original plaintext e-mail 100. In the SC mode, the SC data in added to the remainder data and the user-viewer is permitted to see additional SC content associated with that relevancy level. In this sense, the SC email is a knowledge expander permitted the user-viewer to enhance his or her knowledge with additional SC content. A reconstruction program may be necessary to decode the secured or SC data and insert the data into the document via the placeholders.

[2868] 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 or SC system described above may include many of the features discussed earlier in connection with the other figures. For example, both the security or SC data and the remainder e-mail data can be encrypted prior to transmission to the addressee and the secured or SC 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. B-3.

[2869] 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 or SC sites.

[2870] Another implementation of the secured or SC e-mail system attaches the encrypted and secured or SC data to the remainder e-mail data as indicated in step 621. For an SC email system, the addressee may add the SC sent with the email to the addressee's SC database. E-mail attachments are well known. Alternatively, the encrypted secured or SC 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 or SC data attachment or the embedded data attachment. In step 631, the recipient's system integrates the now decrypted secured or SC data with the remainder data. Of course, this a compilation step. Place holders or other position indicators are customarily utilized. Appending the encrypted security or SC data is generally equivalent to attaching a file to the original e-mail which constitutes, after extraction, the remainder data. Including the encrypted security or SC data is adding the security or SC 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). All SC data may be added to the addressee's SC store. Relevancy of the SC is based upon SC relevancy markers transmitted with the email, similar to the security levels for the MLS secure email system.

[2871] It should be appreciated that the e-mail or SC security system may work automatically or may be selected manually by the user. The highlighting or special distinguishing manner for the security or SC words in step 612 is optional. By highlighting the security or SC 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 or SC data ASP, enter security clearance data, download the secure or SC data and integrate

the secure or SC data in the remainder data e-mail (or SC data structure). 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 or SC data and the remote storage locations handling the secure or SC 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 or SC 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.

[2872] FIGS. D-12A and D-12B diagrammatically illustrate a flowchart showing the key components of one embodiment of the system and the invention which implements the security or SC system on a web browser. Jump point 12-A links FIG. D-12A to FIG. D-12B. The system, at step 700 is ON. The filters establishing either the parsing or the identification of security or SC 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 ON SC operator) 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 or SC data and extracts security or SC data. In step 708, place holders are added to replace the extracted security or SC data in the remainder data and a hyperlink is added to the open field remainder data providing a link to the secure or SC data ASP. In the SC system, the placeholders show the addressee critical terms subject to the SC knowledge expander feature. 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

EX. 1002, Page 2134

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 or SC data ASP. In step 714, the web server receiving the data from user's browser goes to the secure or SC data ASP, inputs and clears any security level, and obtains the secured or SC 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 the above figures may be implemented on the browser system.

[2873] The credit card scrubber or financial data scrubber operates in a similar manner to the email and browser data security system described above. A similar system can be designed to comply with privacy laws or other governmental regulations. A credit card number is similar to a social security number and patent name, address and phone are common personal identifiers that some privacy laws require extraction and special handling. The credit card or financial data or social security number 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 detects17 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. In an SC system, the CC data may be data mined by affiliated companies. 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. An SC system requires SC relevancy clearances set by the policy administrator. 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 ques 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.

[2874] FIG. D-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. D-13 shows two basic systems, one at the data input stage and the second at the data output or reconstruction phase. Release of the reconstructed document or portions thereof are based upon security clearance or SC relevancy and compensation. "Compensation" includes an exchange of information, particularly for the SC storage system. 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. D-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. Swapping SC content may include an evaluator module that tests the "proposed" SC data file and determines whether the proposed SC data file is worthy or being

exchanged for an existing SC data file.

[2875] 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 or SC 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.

[2876] 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 or SC 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.

[2877] 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.

D.14 Portable Computing Device Environment

[2878] The invention can be applied to portable computing devices to secure files and data objects in such devices. The invention extracts, disperses, via a controlled release of data segments to storage locations, and permits reconstruction utilizing security protocols to provide a security or SC system for data based upon the location of the portable device, typically detected by a global position signal generator (GPS) or based upon triangulation data from several broadcast points. In an SC system, the sensitive data may be made available to the user-viewer for a period of time or as long as the user is in a geographic territory. Beyond that time-space limit, the SC data is removed from the user's portable data device. Scrubbing security or SC icons from maps, credit card data or financial data from text, a data object or data stream is part of the portable security system.

[2879] As used herein, the term "portable computing device" means a laptop computer, a PC with a movable feature, such as a PC mounted in a car, plane, truck or trailer, PDAs or personal data assistants, mobile or cellular phones configured with a memory, a processor and some type of GPS or locator system to determine where the phone or cellular unit is located within a territory and digital pagers having similar electronic systems.

[2880] The present invention can be linked with a location sensing circuit, such as a global position sensor or system (GPS) or other type of location sensing system, such as a system which utilizes triangulated signals. The concept is a location based access oriented security (or SC relevancy) such as an automated trigger (which activates the security or SC program discussed hereinabove when the portable computing

device is beyond a predetermined region); an automated safety system; a trip wire; an interlock; a method to disable systems, activity or access to data; and means to limit functionality or access in whole or in granular parts. The portable security system operates on text, data objects, images or other digitally configured data objects. Security access (or relevancy access) is limited by a location way point (in relation to a reference point) or a calculated range (using satellite GPS, high altitude services, or earth-based range finding GLS (geographic location services)) about a way point with physical means or mathematical calculations to define a geographic area by equations or geometric shapes or aggregated ranges (the shapes including rectangles, solids, cubes, circles, oval, spherical region or other areas defined by algorithms). Physical and logical access or entry control to weapons, devices, vehicles, computers, equipment, tools, data, networks, local access, remote access beyond a physical location (reference point), can be enabled or disabled with the system of the present invention. The regions (sometimes identified as a single predetermined region or a plurality of predetermined regions), can consist of complex definitions of three dimensional areas of arbitrary shape and sizes, as long as those regions can be defined by algorithms. The region can also be defined as an area circumscribed internally by a perimeter or by an area external to that perimeter. In other words, access can be denied if the portable device is within a certain region as compared with denying access when the device is beyond a predetermined regions. The claims are meant to cover both situations.

[2881] FIG. D-14 diagrammatically illustrates a portable computing device 810 at location B. The portable computing device 810 includes, in the illustrated embodiment, a GPS system (or a receiver system) 812 coupled to a bus 814 and further coupled to memory 816, a processor 818 and an input/output system 820. Input/output 820 is coupled to, among other things, a key board or key pad, a display, and possibly a transmitter and receiver subsystem. As is known, GPS Systems detect satellite positioning signals and generate an output indicative of the location of the GPS system. In the illustrated embodiment, this location

is location B in FIG. D-14.

[2882] A simple implementation of the present security or SC system provides that upon detection of d1 from location A, defined by building 822, certain security events occur, e.g., automatic extraction and a denial of reconstruction rights. In one example, GPS subsystem 812 continually monitors the location of portable device 810. When the location of device 810 exceeds a predetermined distance (d1-limit), the program operating in memory 816, operable by processor 818, either extracts data and stores the extracted data as discussed in detail above or prohibits reconstruction of data as requested by the operator of portable device 810. Alternatively, automatic extraction may occur without prohibiting reconstruction due to device 810 being located beyond the predetermined region d1-limit. The portable computing device 810 in FIG. D-14 may have many other electronic components such as those shown in FIG. B-2 in connection with computer 165. Alternatively, the security or SC system can be configured in a reverse manner such that the extraction of security or SC information is triggered when portable 810 is within a predetermined region (less than d1-max) close to location A and building 822, that is, the security or SC system disclosed above is triggered to extract information when distance d1 is less than d1-max.

[2883] The security or SC system can also be configured such that GPS or locator system 812 detects a variable distance such as distance d2 between truck 824 and location B of portable device 810. In this sense, the location of portable device 810 is obtained by GPS circuit 812 and further some type of communications must be established between truck 824 at location C and the portable device 810. For example, the receiver coupled to input/output 820 receives this information from location of truck 824 and location C. This reference location C is then processed in conjunction with the location data from GPS circuit 812 by processor 818 and memory 816. The same results as discussed above in conjunction with fixed reference location A can be achieved with a variable reference location C. Truck 826 at variable location D

EX. 1002, Page 2140

enables the system to provide an additional level of security. In other words, within distance d2 (d2-limit), the operator of portable device 810 may be able to reconstruct information upon request. However, if portable device 810 intrudes upon or is less than distance d3 (d3-max) the distance between location B and location D, the security system may trigger an immediate extraction routine thereby disbursing, on a granular basis, the secured or SC words, data objects or whatever and further prohibit reconstruction. Of course, the security or SC system could be configured simply to extract the information and permit reconstruction. Otherwise, the security or SC system could be configured to simply extract information and prohibit reconstruction. In this manner, the security or SC system discussed in conjunction with the portable computing device 810 can have multiple triggers or location established events enabling the security or SC program to extract security or SC information or disabling the security or SC program to prohibit reconstruction based upon a fixed location A or one or more variable locations C, D.

[2884] Another configuration of the present invention utilizes triangulation to obtain location B for the portable computing device 810. In a triangulation situation, the receiver system 812 for the locator receives signals from one or more fixed locations, and preferably three locations diagrammatically illustrated by tower T1, T2 and T3 in FIG. D-14. The triangulation of signals to obtain location B is known in the art. However, the combination of such location position coupled to extraction of security or SC data and/or reconstruction of security or SC data based upon certain location parameters is part of the present invention.

[2885] For illustration purposes only, the present security or SC system for the portable computing device 810 can remotely store extracted security or SC information. Remote store 828 coupled to receiving tower T1 illustrates this concept.

[2886] FIG. D-15 diagrammatically illustrates a basic flow chart for the portable security or SC system program utilized in connection with portable computing device 810. Decision step 830 determines

whether a certain event has occurred. This event may include a power ON for the portable computing device, may be a "save document" command, may be a screen ON event or may be a timed function. For example, if the portable computing device 810 is continually ON, the program may periodically poll the locator circuit (GPS 812) and determine whether location B is within or beyond the predetermined regions (d-max or d-limit). Step 832 activates the GPS or the triangulation circuit to obtain current location data. This may include locating variable locations C, D. Step 833 obtains territory limits for various security levels or SC relevancy levels. As discussed earlier, security or SC level SL1 is public or non-confidential information, security or SC SL2 confidential or proprietary information, level SL3 is secret information and level SL4 is top secret or SC information. This system can be configured such that various territories or predetermined regions correspond to respective ones of the security or SC levels SL1-SL4.

[2887] Decision step 834 determines whether location B of portable computing device 810 is within or without the predetermined territory limits or predetermined region. If YES, the system determines in decision step 836 whether the user has initiated a reconstruction request. If not, the system returns to a point preceding decision step 830, the detect event function or step. If YES, the system, in step 838, reconstructs the document only if location B is beyond a predetermined region. Of course, a negative operation could occur in that reconstruction would be prohibited if location B was within a predetermined region. The claims appended hereto are meant to cover both within a region and without a region and independently, extract or permit reconstruction. Step 840 secures the reconstructed file again as necessary.

[2888] Returning to decision step 834, if location B is not within the predetermined regions or territories defined by security or SC levels SL1-SL4, the NO branch is taken and decision step 842 determines whether portable computing device 810 has any unsecured files. If YES, the system executes step 844 which is extract and store the security or SC sensitive words, data objects etc. in accordance with security

or SC levels SL2-SL4. As stated above, the storage could be on media in a local drive or can be remotely distributed to memory segments designated as a remote extract store. If the NO branch is taken from decision step 842, the system executes decision step 846 which determines whether the user has requested a reconstruction of data. If not, the program ends or returns to the event detection step 830. If YES, the system executes step 848 which determines whether a lower security or SC clearance is available within the current territory, determines whether the user has the proper pass code to access the reconstruction and process the reconstruction or whether the system prohibits all reconstruction. Partial reconstruction for lower security or SC items may be permitted. For example, reconstruction at top secret or SC level SL4 may be prohibited when distance d2 is greater than d2-limit but reconstruction at a lower security or SC level such as confidential level SL2 may be permitted beyond limit d2-limit. In this sense, the present invention can be configured to generate extraction for various security or SC levels at various predetermined regions based upon a fixed reference point or a variable reference point. Alternatively, reconstruction can be permitted or denied based on a plurality of security or SC levels and a plurality of corresponding regions or distances. The term "mobile predetermined region" is sometimes utilized in conjunction with variable regions d2 and d3.

[2889] As an example, the data object retained by portable computing device 810 may be a map having security or SC sensitive icons on the map. These icons are extracted if location B is less than a predetermined defined distance d3-limit between variable location D and location B. If location B is beyond d3-minimum, the map can be viewed by the operator on portable device 810. If location B is less than distance d3-minimum, the security or SC icons are removed from the map. In a similar sense, security or SC sensitive credit card characters can be extracted from plain text documents carried on portable computing device 810 when device 810 is a certain distance beyond d1-limit from fixed reference point A. This location A may be a bank headquarters. Encrypting and decrypting the data based upon the geographic event is also

EX. 1002, Page 2143

contemplated by the present invention. Of course, portable device 810 may be a plurality of portable devices linked via a hard wire network or via a wireless network. The same security or SC program disclosed above in herein can be utilized with one computer or a series of computers. Further, portable computing device 810 can include a plurality of memory segments (see FIG. B-3A) and may include a plurality of display screens as discussed above in conjunction with FIG. B-3. The extraction and storage and reconstruction of streaming data is possible as is operation on voice data. Additionally, the portable computing device may set off an audible and/or visual alarm prior to extraction of data. For variable territories or predetermined regions, step 832 or 833 may include gathering information regarding the variable location of vehicles 824, 826 prior to determining the territorial limits for various security or SC levels SL2, SL3 and SL4.

E.1 General System Comments

[2890] It is important to know that the embodiments illustrated herein and described herein 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. The section titles are not meant to limit the detailed description of the system and process described therein.

[2891] 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.

[2892] 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.

[2893] 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. 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.

[2894] 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
CIO	Chief Information Officer or system administrator
comm.	communications, typically telecommunications
comp	computer
CPU	central processing unit
DB or db	data base or structured data file
D & R	dispersion and re-construct or re-assemble
Distrib	distribution or transmission of data (information) files
DS	data storage
doc	document
dr	drive, e.g., computer hard drive
e	encryption
ext-data	extracted data
F	floppy computer drive or flash drive memory
H-tax	hierarchical taxonomic system, a prioritized classification system
I/O	input/output
I-com	Internet storage for common or remainder data
id	identify
I-ext	Internet storage for extracted data
KE	knowledge expander, such as a knowledge expander search
loc	location
MLS	multilevel security
mem	memory
mod	module or software-firmware-hardware function
obj	object, for example, a data object
opt	optional
PC	personal computer or any other type of general computer
pgm	program
re	regarding or relating to
recon	reconstruct

rel	release
req	request
rev	review
SC	select content -- e.g., words, terms, images, sound that is of particular interest to the user
sec	security
sec-con	security sensitive content
sec. level	TS top secret, S secret, C classified, UC unclassified
sel	SC sensitivity level, sometimes SC sel. level
sel cont	select content
sel levels	SC levels, hierarchical taxonomic classification levels of SC
sch	search
SL	security level (sometimes S1 for sec. Level 1, S2 is Level 2, etc., also, for example, TS is Top Secret, S is Secret, C is Classified, U is Unclassified))
supple	supplemental
supple doc	supplemental document of data object
sys	system
sys-admin	CIO or system operator
t	time
tax	taxonomic or classification system
tele-com	telecommunications system or network
unkn	unknown item or data element or data object
URL	Uniform Resource Locator, x pointer, or other network locator
W St	computer work station

[2895] "Data," as used herein, includes any data object, e.g., text, image, icons, audio, video, still images, etc. and data is sometimes referred to herein as a "data object." A source document is either a document, any data structure, or a data stream. Since a data stream has a start bit or term and an end bit or term, the data stream is structured data, and reference to a "document" refers to any document, data structure, or data stream. Likewise a "supplemental document" is any document, data structure, or data stream. The select content (SC) is any critical or security sensitive word, character, image, or data object 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 SC words, letters, images, icons, partial versions of the foregoing or any other granular aspect of the source document.

[2896] FIG. C-16 diagrammatically illustrates a personal computer or PC computer system 140, a second PC or computer 142, and a third PC -3. Similar numerals designate similar items in FIGs. C-16 and B-2. PCs 140, 142 and PC-3 are connected together via a network 145 (LAN or WAN) and connected to one or more private databases or data structures which are represented by Db A. The LAN 145 is also connected to an input/output device 146 that may be generally described as a router or an I/O device 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. The ASP provides various tools to the user on computer 142 such a Google search through other data bases, indices and data structures. Internet 150 also includes various computer memory storage devices such as computer storage B 154a, computer storage C 156a accessible through Gate C 157a (via password or other control device) and computer storage D 158a accessible via Gate D 159a. Access to computer storage C and D is permitted via, in one instance, security level clearance modules or Gate C and D 157a, 159a. Maps to the computer stores C and D may require security level clearance.

[2897] 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 F media (flash or 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.

[2898] One methodology of implementing the present invention utilizes filters on the PC or on removable memory F. The present invention may also be embodied utilizing an Application Service Provider (ASP) on server 152 and in a client-server network. The user or operator on the PC 142 calls up an ASP on system 152 and operates the KE process on the computer system 152. Filters and rules may be located with a uniform research locator or URL to find filters, data collections, target files from computer store B, C and D. In a client-server environment, server 152 acts as a server generally cooperating with data operations with 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. C-16. The claims appended hereto are meant to cover the alternative embodiments.

[2899] As an example of a client-server or web-based implementation of the present invention, the user at computer 140 may define the SC 2018 as described above, and input data via keyboard 161 or load source data from F drive 162 or CD-ROM drive 160 into RAM 166. Alternatively, the data stream on LAN 145 may be monitored by PC 140. In any event, whether the source data is input via keyboard 161 or copied or accessed in or from F drive 162 or CD-RW drive 160, the source data is filtered as discussed above in connection with FIGs. C-1 - C-2. Prior to filtering, it is appropriate for the user at computer 140 to identify the hierarchical taxonomic system and the location of SC filters and My Group Profiles. Off site data storage and processes are available permitting activation of 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 SC filter and H-tax classes pursuant to input selected by the user. The client compute may (a) filter the source doc 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 154a, 156a. Either the PC or

the server could conduct the knowledge expander search and return the compiled data, supple docs, and map results to the PC.

[2900] The claims appended hereto are meant to cover modifications and changes within the scope and spirit of the present invention.

[2901] What is claimed is:

1. A method of organizing and processing data in a distributed computing system having select content represented by one or more predetermined words, characters, images, data elements or data objects, said distributed computing system having a plurality of select content data stores in a server cloud for respective ones of a plurality of security designated data and scarcity designated data, each with respective access controls thereat, said plurality of select content data stores and server cloud operatively coupled over a communications network, the method of organizing and processing data comprising:

extracting and storing said security designated data and said scarcity designated data in respective select content data stores of said server cloud;

withdrawing some or all of said security designated data and said scarcity designated data in said respective select content data stores only in the presence of said respective access controls applied to said select content data stores in said server cloud.

2. A method of organizing and processing data as claimed in claim 1 including applying a monetization algorithm to said security designated data and said scarcity designated data based upon non-secure availability of said security designated data and said scarcity designated data and generating and assigning either a financial value to said security designated data and said scarcity designated data or generating and assigning a risk-release value to said security designated data and said scarcity designated data.

3. A distributed computer system for organizing and processing data having select content represented by one or more predetermined words, characters, images, data elements or data objects, said distributed computing system having a plurality of select content data stores in a server cloud for respective ones of a plurality of security designated data and scarcity designated data, each with respective access controls thereat, said plurality of select content data stores and server cloud operatively coupled over a communications

network, comprising:

means for identifying plurality of select content data stores for respective ones of a plurality of security designated data and scarcity designated data in said server cloud,

a processor activating at least one of said select content data stores in a server cloud there by permitting access to said select content data stores and respective security designated data and scarcity designated data based upon an application of one or more of said access controls thereat;

said processor having means for applying a reconstruction data process employing said respective access control to combine one or more of said security designated data and scarcity designated data in said server cloud.

4. A distributed computer system for organizing and processing data as claimed in claim 3 including means for applying a monetization algorithm to said security designated data and said scarcity designated data based upon non-secure availability of said security designated data and said scarcity designated data and means for generating and assigning either a financial value to said security designated data and said scarcity designated data or generating and assigning a risk-release value to said security designated data and said scarcity designated data.

Abstract

Distributed computer system processes data having select content (SC) represented by one or more predetermined words, characters, etc. The system has a plurality of SC data stores in a server cloud for respective security designated (Sec-D) data and scarcity designated (S-D) data, each with respective access controls thereat. The SC data stores are is operatively coupled on a network. An identification module for identifying SC data stores for the Sec-D data and S-D data in the server cloud. A processor activates an SC data stores in the server cloud thereby permitting access to the SC data stores and respective Sec-D data and S-D data based upon an application of one or more of said access controls thereat. The processor has a reconstruction module operating as a data process employing the respective access controls to combine one or more of the Sec-D data and S-D data.

G:\RCK\CLIENTS\Redlich\Patents\6851-08-CIP-pa.wpd

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
12/453,124	04/29/2009	Ron M. Redlich	6851-08-cip

CONFIRMATION NO. 8996

4897
ROBERT C. KAIN, JR.
750 SOUTHEAST THIRD AVENUE
SUITE 100
FT LAUDERDALE, FL 333161153

FORMALITIES LETTER

OC000000036341969

Date Mailed: 06/12/2009

NOTICE OF INCOMPLETE REPLY (NONPROVISIONAL)

Filing Date Granted

The U.S. Patent and Trademark Office has received your reply on 05/27/2009 to the Notice to File Missing Parts (Notice) mailed 05/19/2009 and it has been entered into the nonprovisional application. The reply, however, does not include the following items required in the Notice.

The period of reply remains as set forth in the Notice. You may, however, obtain EXTENSIONS OF TIME under the provisions of 37 CFR 1.136(a) accompanied by the appropriate fee (37 CFR 1.17(a)).

A complete reply must be timely filed to prevent ABANDONMENT of the above-identified application. Replies should be mailed to: Mail Stop Missing Parts, Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450.

- The oath or declaration is unsigned.
- Surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of $130 was not received.

The application is informal since it does not comply with the regulations for the reason(s) indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- A substitute specification in compliance with 37 CFR 1.52, 1.121(b)(3), and 1.125, is required. The substitute specification must be submitted with markings and be accompanied by a clean version (without markings) as set forth in 37 CFR 1.125(c) and a statement that the substitute specification contains no new matter (see 37 CFR 1.125(b)). The specification, claims, and/or abstract page(s) submitted is not acceptable and cannot be scanned or properly stored because:
  - The application papers (including any electronically submitted papers) are not in compliance with 37 CFR 1.52 because pages 1-110 contain text that is unreadable or of insufficient clarity.
    Application papers (including any electronically submitted papers) must be presented in a form having sufficient clarity and contrast between the background of the paper and the writing thereon to permit the Office to electronically reproduce the papers by use of digital imaging and optical character recognition. See 37 CFR 1.52(a)(1)(v).
- Replacement drawings in compliance with 37 CFR 1.84 and 37 CFR 1.121(d) are required. The drawings submitted are not acceptable because:
  - The drawings must be reasonably free from erasures and must be free from alterations, overwriting, interlineations, folds, and copy marks. See Figure(s) all.

Applicant is cautioned that correction of the above items may cause the specification and drawings page count to exceed 100 pages. If the specification and drawings exceed 100 pages, applicant will need to submit the required application size fee.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is $**2020** for a small entity

- $**130** Surcharge.
- The fee for submitting a specification and drawing containing more than 100 pages has not been paid in full. Applicant owes $**1890** for **313** pages in excess of **750** pages for a small entity in compliance with 37 CFR 1.27.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/rgreen/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Attorney's Docket No. 6851-08-cip

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich

Serial No. 12453124
Confirmation No. 8996

Filed: April 29, 2009

Group 2444

For: Digital information infrastructure and method

Entity Status Change Request

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

Sir:

Applicant requests a change in entity status. Applicant inadvertently paid large entity fees when filing the above identified patent application. Applicant is an individual and requests that the entity status be changed to small entity.

Respectfully submitted,

By /rck/

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

Certificate of E-Filing

I hereby certify that this correspondence is being e-filed with the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on June 8, 2009.

Robert C. Kain, Jr.
Reg. No. 30,648

G:\RCK\CLIENTS\Redlich\6851-08-cip-entity-pto-060809.wpd

Best Available Copy

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

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

Serial No. 12/453,124
Confirmation No. 8996

Filed: April 29, 2009 Group 2444

For: Digital Information Infrastructure and Method

TRANSMITTAL LETTER

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

Sir:

Please find enclosed for filing:

X Submission of Replacement Formal Drawings (1 pg.)

X Fifty-nine (59) sheets formal drawings

X Please credit any overpayments or charge any underpayments to Deposit Account No. 03-1231

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, FL 33316-1153
Telephone: 954-768-9002
Facsimile: 954-768-0158

G:\RCK\CLIENTS\Redlich\6851-08-cip-transmittal-replacement-drawings.wpd

06/05/2009 VVAN11 00000007 031231 12453124

01 FC:1011 330.00 DA
02 FC:1111 540.00 DA
03 FC:1311 220.00 DA
04 FC:1081 3510.00 DA

Adjustment date: 06/16/2009 SDIRETA1
06/05/2009 VVAN11 00000007 031231 12453124
01 FC:1011 330.00 CR
02 FC:1111 540.00 CR
03 FC:1311 220.00 CR
04 FC:1081 3510.00 CR

06/16/2009 SDIRETA1 00000008 031231 12453124

01 FC:2011 165.00 DA
02 FC:2111 270.00 DA
03 FC:2311 110.00 DA
04 FC:2081 2700.00 DA
05 FC:2051 65.00 DA

Best Available Copy

Kain & Associates
Attorneys at Law

Complex I P . com

Patent - Trademark - Copyright - Computer Law
Trade Secret - Domain Disputes

750 Southeast Third Avenue, Suite 100
Fort Lauderdale, Florida 33316-1153
Telephone: (954) 768-9002
Facsimile: (954) 768-0158

www.ComplexIP.com
Robert C. Kain, Jr. rkain@ComplexIP.com
Darren Spielman dspielman@ComplexIP.com

June 9, 2009
Via Facsimile Only - 1-571-273-6500
Number of Pages - 3

Director of Patents and Trademarks
Attention: Refund Section
Mail Stop 16
P.O. Box 1450
Alexandria, VA 22313-1450

Re: Refund to Deposit Account No. 03-1231

Dear Sir:

Enclosed is a copy of the June 8, 2009 Deposit Account Statement for Account No. 03-1231.

There are an incorrect charges to the above identified account. The charges posted on 6/05/2009 for Serial No. 12453124, Attorney Docket Nbr. 6851-08-cip are all posted as large entities. This is a small entity and we request a refund of one-half of each amount charged (total charged $4,600.00).

Please credit Deposit Account No. 03-1231 in the appropriate amount. A copy of Entity Status Change Request is also enclosed.

If you have any questions, please contact the undersigned.

Sincerely,

Ellen Kotler, Office Manager
for the Firm.

/elk
encls.

G:\RCK\FORMS\PATENT\REFUND.LTR.wpd

Deposit Account Statement

United States Patent and Trademark Office

Deposit Account Statement

Requested Statement Month:	June 2009
Deposit Account Number:	031231
Name:	KAIN & ASSOCIATES
Attention:	ATT: ELLEN KOTLER
Street Address 1:	750 SOUTHEAST THIRD AVE.
Street Address 2:	SUITE 100
City:	FT.LAUDERDALE
State:	FL
Zip:	33316-1153
Country:	UNITED STATES

DATE	SEQ	POSTING REF TXT	ATTORNEY DOCKET NBR	FEE CODE	AMT	BAL
06/05	16	12453124	6851-08-CIP	1011	$330.00	$4,379.70
06/05	19	12453124	6851-08-CIP	1081	$3,510.00	$869.70
06/05	18	12453124	6851-08-CIP	1311	$220.00	$649.70
06/05	17	12453124	6851-08-CIP	1111	$540.00	$109.70

START BALANCE	SUM OF CHARGES	SUM OF REPLENISH	END BALANCE
$4,709.70	$4,600.00	$.00	$109.70

Need Help? | USPTO Home Page | Finance Online Shopping Page | Alerts Page

Attorney Docket No. 6851-08-cip

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Ron M. Redlich

Serial No. 12/453,124

Confirmation No. 8996

Filed: April 29, 2009

For: Digital Information Infrastructure and Method

Response to Incomplete Reply (Nonprovisional Application)

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

Sir:

This is a response to the Notice of Incomplete Reply of Nonprovisional application, (copy enclosed) dated June 12, 2009.

1. On May 27, 2009, formal replacement drawings were electronically filed in the U.S. Patent and Trademark Office.

2. On June 8, 2009, fees totaling $4,600.00 were charged to applicant's attorneys' deposit account. Applicant disputed this amount since the U.S. Patent and Trademark Office charged large entity fees whereas applicant is a small entity. On June 16, 2009, the large entity fees were credited back to applicant's attorneys' deposit account and small entity fees were charged to the deposit account.

3. On June 10, 2009, a Response to the Notice to File Missing Parts; a submission of substitute

specification; a substitute specification; and a copy of the executed declaration and power of attorney for patent application were filed via Express Mail. A copy of the stamped return receipt postcard is attached showing receipt in the U.S. Patent and Trademark Office on June 10, 2009.

4. Applicant requests that the U.S. Patent and Trademark Office withdraw the Notice dated June 12, 2009 since the Notice does not refer to the June 10, 2009 filing by applicant.

Respectfully submitted,

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

By _____
Robert C. Kain, Jr.
Reg. No. 30,648
Suite 100
750 S.E. Third Avenue
Ft. Lauderdale, Florida 33316-1153
(954) 768-9002
Facsimile: 954-768-0158

Certificate of E-Filing

I hereby certify that this correspondence is being e-filed with the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on June 17, 2009.

_____
Robert C. Kain, Jr.
Reg. No. 30,648

G:\RCK\CLIENTS\Redlich\6851-08-cip-response-to-incomplete-reply-061609.wpd

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
12/453,124	04/29/2009	Ron M. Redlich	6851-08-cip

CONFIRMATION NO. 8996

4897
ROBERT C. KAIN, JR.
750 SOUTHEAST THIRD AVENUE
SUITE 100
FT LAUDERDALE, FL 333161153

FORMALITIES LETTER



Date Mailed: 06/12/2009

NOTICE OF INCOMPLETE REPLY (NONPROVISIONAL)

Filing Date Granted

The U.S. Patent and Trademark Office has received your reply on 05/27/2009 to the Notice to File Missing Parts (Notice) mailed 05/19/2009 and it has been entered into the nonprovisional application. The reply, however, does not include the following items required in the Notice.

The period of reply remains as set forth in the Notice. You may, however, obtain EXTENSIONS OF TIME under the provisions of 37 CFR 1.136(a) accompanied by the appropriate fee (37 CFR 1.17(a)).

A complete reply must be timely filed to prevent ABANDONMENT of the above-identified application. Replies should be mailed to: Mail Stop Missing Parts, Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450.

- The oath or declaration is unsigned.
- Surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of $130 was not received.

The application is informal since it does not comply with the regulations for the reason(s) indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- A substitute specification in compliance with 37 CFR 1.52, 1.121(b)(3), and 1.125, is required. The substitute specification must be submitted with markings and be accompanied by a clean version (without markings) as set forth in 37 CFR 1.125(c) and a statement that the substitute specification contains no new matter (see 37 CFR 1.125(b)). The specification, claims, and/or abstract page(s) submitted is not acceptable and cannot be scanned or properly stored because:
  - The application papers (including any electronically submitted papers) are not in compliance with 37 CFR 1.52 because pages 1-110 contain text that is unreadable or of insufficient clarity.
    Application papers (including any electronically submitted papers) must be presented in a form having sufficient clarity and contrast between the background of the paper and the writing thereon to permit the Office to electronically reproduce the papers by use of digital imaging and optical character recognition. See 37 CFR 1.52(a)(1)(v).
- Replacement drawings in compliance with 37 CFR 1.84 and 37 CFR 1.121(d) are required. The drawings submitted are not acceptable because:
  - The drawings must be reasonably free from erasures and must be free from alterations, overwriting, interlineations, folds, and copy marks. See Figure(s) all.

Applicant is cautioned that correction of the above items may cause the specification and drawings page count to exceed 100 pages. If the specification and drawings exceed 100 pages, applicant will need to submit the required application size fee.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is **$2020** for a small entity

- **$130** Surcharge.
- The fee for submitting a specification and drawing containing more than 100 pages has not been paid in full. Applicant owes **$1890** for **313** pages in excess of **750** pages for a small entity in compliance with 37 CFR 1.27.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

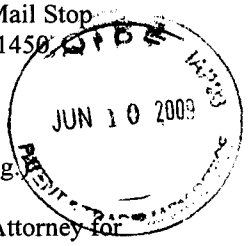
/rgreen/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

June 10, 2009

Kindly Date Stamp and Return to Acknowledge Receipt
File No 6851-08-cip - Redlich

I HEREBY CERTIFY that the below listed documents are being deposited with the United States Postal Service "Express Mail Post Office to Address," Mailing Label No. EL039210521US under 37 C.F.R. 1.10 on June 10, 2009 and are addressed to Mail Stop Missing Parts, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.



X Notice to File Missing Parts (2 pgs.)
X Submission of Substitute Specification (1 pg.)
X Substitute Patent application (1006 pgs.)
X Copy of signed Declaration and Power of Attorney for Patent Application (2 pgs.)
X Transmittal Letter (1 pg.)

Electronic Acknowledgement Receipt

EFS ID:	5530253
Application Number:	12453124
International Application Number:	
Confirmation Number:	8996
Title of Invention:	Digital information infrastructure and method
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	04897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-08-cip
Receipt Date:	17-JUN-2009
Filing Date:	29-APR-2009
Time Stamp:	09:53:49
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	Supplemental Response or Supplemental Amendment	6851-08-cip-response-to-incomplete-reply-061609.pdf	43227 e1d8817b8b9cc4e72e9aefdbf1722233780fb942	no	2

Warnings:	
Information:	

2	Miscellaneous Incoming Letter	6851-08-cip-pto-notice-061209.pdf	77583 0201dee7fd22db338a8f4df98a8a6e38b89e6ab7	no	2
Warnings:					
Information:					
3	Miscellaneous Incoming Letter	6851-08-cip-pto-postcard-061009.pdf	15652 41fd6bfd253780f613b9c19c89410d37835d7791	no	1
Warnings:					
Information:					
			Total Files Size (in bytes):	136462	

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 NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
12/453,124	04/29/2009	2444	3310	6851-08-cip	4	2

CONFIRMATION NO. 8996

UPDATED FILING RECEIPT

4897
ROBERT C. KAIN, JR.
750 SOUTHEAST THIRD AVENUE
SUITE 100
FT LAUDERDALE, FL 333161153

OC00000036607128

Date Mailed: 07/01/2009

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. 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 submit a written request for a Filing Receipt Correction. 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**

Applicant(s)

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

Power of Attorney:
Robert Kain Jr--30648

Domestic Priority data as claimed by applicant

This application is a CIP of 11/746,440 05/09/2007
which claims benefit of 60/883,522 01/05/2007

Foreign Applications

If Required, Foreign Filing License Granted: 05/15/2009

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 12/453,124**

Projected Publication Date: 10/08/2009

Non-Publication Request: No

Early Publication Request: No
** **SMALL ENTITY** **

Title

Digital information infrastructure and method

Preliminary Class

709

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 AssetsControl, 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
12/453,124	04/29/2009	Ron M. Redlich	6851-08-cip

CONFIRMATION NO. 8996

4897
ROBERT C. KAIN, JR.
750 SOUTHEAST THIRD AVENUE
SUITE 100
FT LAUDERDALE, FL 333161153

PUBLICATION NOTICE

OC000000038189694

Title: Digital information infrastructure and method

Publication No.US-2009-0254572-A1
Publication Date:10/08/2009

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 publically 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 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PTO/SB/122 (11-08)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
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	12/453,124
Filing Date	4/29/2009
First Named Inventor	
Art Unit	
Examiner Name	
Attorney Docket Number	6851-08-cip

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

☑ The address associated with Customer Number: 004897

OR

☐ Firm 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:	6357917
Application Number:	12453124
International Application Number:	
Confirmation Number:	8996
Title of Invention:	Digital information infrastructure and method
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	04897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-08-cip
Receipt Date:	29-OCT-2009
Filing Date:	29-APR-2009
Time Stamp:	16:34:09
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	6851-08-cip-change-address-sb0122_fill.pdf	320699 6da93d4934967b75ccecae1b9fddb26392584808	no	2

Warnings:	
Information:	

Total Files Size (in bytes):	320699

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.

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-08-cip	Application Number 12/453,124
Title: Digital Information Infrastructure and Method	Applicant(s) Ron M. Redlich, et al.	
	Filing Date April 29, 2009	Group Art Unit 2444

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.)

	Oracle - Information Lifecycle Management (ILM) for Business Data- Lilian Hobbs	
	Data Mobility Group - The ILM Puzzle- EMC puts all the piece together- September 18, 2006	
	Life Cycle -White paper10218_0115.txt- Practical Steps Toward Information Lifecycle Management	

EXAMINER DATE CONSIDERED

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-08	Application Number
Title: Information Infrastructure Management Tools with Extractor, Secure Storage, Content Analysis and Classification and Method Therefor	Applicant(s) Ron M. Redlich, et al.	
	Filing Date	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.)

	MIMEsweeper-Content Security for E-mail, Web Browsing & Webmail, November 12, 2001	
	Cisco IDS Host Sensor Product, October 16, 2001	

EXAMINER DATE CONSIDERED

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-08	Application Number
Title: Information Infrastructure Management Tools with Extractor, Secure Storage, Content Analysis and Classification and Method Therefor	Applicant(s) Ron M. Redlich, et al.	
	Filing Date	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

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-08	Application Number
Title: Information Infrastructure Management Tools with Extractor, Secure Storage, Content Analysis and Classification and Method Therefor	Applicant(s) Ron M. Redlich, et al.	
	Filing Date	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner 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.)

	The 1996 book, Applied Cryptography, by Schneier	
	The Uniform Resource Locator article "FOLD OC"	
	Microsoft Word "Learning Microsoft Word 7.0"	

EXAMINER DATE CONSIDERED

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-08	Application Number
Title: Information Infrastructure Management Tools with Extractor, Secure Storage, Content Analysis and Classification and Method Therefor	Applicant(s)	
	Filing Date	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	

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\6851-08-cip-Form-PTO-1449.wpd

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

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

Serial No. 12/453,124

Confirmation No.: 8996 Group Art 2444

Filed: April 29, 2009

For: Digital Information Infrastructure and Method

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

Our Ref.	Reg./Serial No.	Filed/Registered
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
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

-Ingrian i100, Content Security Appliance (2 pages)

-Element-Wise XML Encryption, Hiroshi Maruyama and Takeshi Imamura, IBM Research, Tokyo Research Laboratory, Ap. 19, 2000. (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.

-Cisco IDS Host Sensor Product, October 16, 2001.

-Oracle - Information Lifecycle Management (ILM) for Business Data- Lilian Hobbs.

-Data Mobility Group - The ILM Puzzle- EMC puts all the piece together- September 18, 2006.

-Life Cycle -White paper10218_0115.txt- Practical Steps Toward Information Lifecycle Management.

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.

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. 6,602298 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.5,581682 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.
Reg. No. 30,648
Kain & Associates, Attorneys at Law, P.A.
900 Southeast Third Avenue
Suite 250
Ft. Lauderdale, Florida 33316-1153
Telephone: 954-768-9002
Facsimile: 954-768-0158

G:\RCK\CLIENTS\Redlich\6851-08-cip-IDS.wpd

Electronic Acknowledgement Receipt

EFS ID:	6434191
Application Number:	12453124
International Application Number:	
Confirmation Number:	8996
Title of Invention:	Digital information infrastructure and method
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	04897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-08-cip
Receipt Date:	11-NOV-2009
Filing Date:	29-APR-2009
Time Stamp:	15:11:31
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	Transmittal Letter	6851-08-cip-transmittal-elec-filing.pdf	20516 70d1d1442df3cc350e648613e55496ed8e7db8a9	no	1

Warnings:	
Information:	

2	Information Disclosure Statement (IDS) Filed (SB/08)	6851-08-cip-IDS.pdf	144997 3ee63708bc5fed91e26c49b12cd6c691638b3f66	no	6
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Information Disclosure Statement (IDS) Filed (SB/08)	6851-08-cip-Form-PTO-1449.pdf	131987 527d73c5240a220305b7fa5cdb977d0d2fde347e	no	5
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
4	Information Disclosure Statement (IDS) Filed (SB/08)	Pr-Art-life-cycle-white-paper10218-0115.pdf	37989 1a7aed44676ed1d3684ac464b51130dc8975856c	no	16
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
5	Information Disclosure Statement (IDS) Filed (SB/08)	Pr-Art-Mimesweeper.pdf	630873 52f47c230ff8defe9869c7bce7e32ab36ba291c4	no	12
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
6	Information Disclosure Statement (IDS) Filed (SB/08)	Pr-Art-Cisco-IDS-Host-Sensor-Product.pdf	510120 ed65a17bd55a4fc2da244b25f6ce3bc6b8704cd6	no	10
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
7	Information Disclosure Statement (IDS) Filed (SB/08)	Pr-Art-Ingrian-I100-content-security-appliance.pdf	104559 c579eaca6c5b7cf7ec2c11d154a422ac3f9dddb2	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
8	Information Disclosure Statement (IDS) Filed (SB/08)	Pr-Art-Element-Wise-XML-Encryption.pdf	235982 de9339bb23b3e33873d0a0a6eadc8fe9a64530a8	no	4
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					

9	Information Disclosure Statement (IDS) Filed (SB/08)	Pr-Art-Survivable-Information-Storage-Systems.pdf	548011 7506a4800840f35b7c81d301ea6f300286b64a91	no	8
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
10	Information Disclosure Statement (IDS) Filed (SB/08)	Pr-Art-ZD-Net-Interactive-Week.pdf	67921 c43a742caf404182928e0ae5de735f74377e99df	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
11	Information Disclosure Statement (IDS) Filed (SB/08)	Pr-Art-Mostly-Static-Decentralized-Myers.pdf	2216378 34a54e2d1a37bc53b2fca1c38a825e6e245095c3	no	43
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
12	Information Disclosure Statement (IDS) Filed (SB/08)	Pr-Art-Applied-Cryptography-Schneier.pdf	362813 7fb0d7acb87291c2b63eef7ea7463a0e4a9d4e74	no	5
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
13	Information Disclosure Statement (IDS) Filed (SB/08)	Pr-Art-FOLDOC.pdf	87383 bc7fc6ce20d225d3fec11736fafab8b77329f93e	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
14	Information Disclosure Statement (IDS) Filed (SB/08)	Pr-Art-Learning-Microsoft-Word.pdf	228594 aa7f75035af8df4a88a8e45d2b69a391723c4116	no	6
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
15	Information Disclosure Statement (IDS) Filed (SB/08)	Pr-Art-Canada-2345148-Silanis.pdf	1113678 52f3e78f2267c62b1f79ceb703fa830d01646c99	no	28
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					

16	Information Disclosure Statement (IDS) Filed (SB/08)	Pr-Art-The-ILM-Puzzle-emc.pdf	656183 31a9a9e0fcf378353185559a7284b1719968e035	no	9
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
17	Information Disclosure Statement (IDS) Filed (SB/08)	Pr-Art-oracle-10218-22964.pdf	104747 e5e289ad70cd840c330074650e1cb1fd8f6466da	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
		Total Files Size (in bytes):	7202731		

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.

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

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

Serial No.: 12/453,124 Group Art 2444

Filed: April 29, 2009

Confirmation No.: 8996

For: Digital Information Infrastructure and Method

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 November 11, 2009 in the Patent and Trademark Office.

X Information Disclosure Statement (6 pages)

X Form PTO-1449 (5 pages)

X Please charge any underpayments or credit any overpayments to Deposit Account No. 03-1231. Applicant is a small entity.

Respectfully submitted,

By _____

Robert C. Kain, Jr.
Reg. No. 30,648
Kain & Associates, Attorneys at Law, P.A.
900 S.E. Third Avenue, Suite 250
Ft. Lauderdale, Florida 33316-1153
Telephone: (954) 768-9002
Facsimile: (954) 768-0158

G:\RCK\CLIENTS\Redlich\6851-08-cjp-Transmittal-Elec-Filing.wpd

(19) Canadian Intellectual Property Office
An Agency of Industry Canada

Office de la Propri,t, 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

(22) 24.09.1999

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

(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).

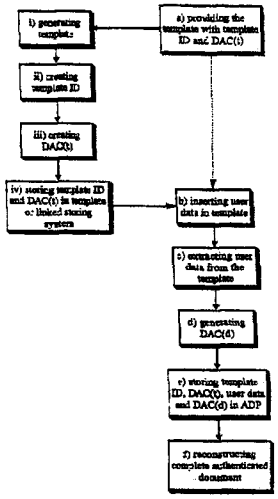
(72)
MILCZAREK, ED (CA).
PETROGIANNIS, TOMMY (CA).
SILVESTER, Joseph (CA).

(74)
ROBIC

(54) PROCEDE D'AUTHENTIFICATION SEPAREE 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.



OPIC
OFFICE DE LA PROPRIÉTÉ INTELLECTUELLE DU CANADA

CIPO
CANADIAN INTELLECTUAL PROPERTY OFFICE

(12)(19)(CA) Demande-Application

(21)(A1) 2,345,148

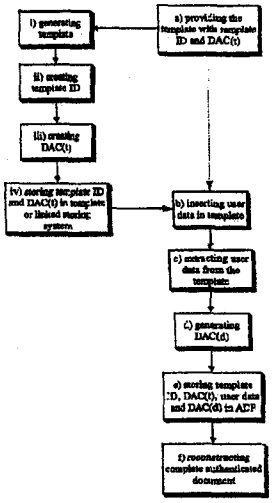
(86) 1999/09/24
(87) 2000/04/06

(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 SEPAREE 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.

PCT WORLD 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). MILCZAREK, Ed; 5135 des Cajeux, 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).

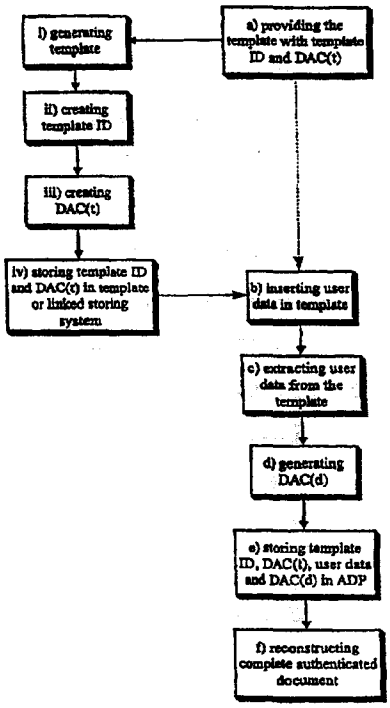
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, 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
With international search report.

(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.



METHOD FOR THE SEPARATE AUTHENTICATION OF A TEMPLATE AND USER DATA

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.

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.

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. Some are particularly limited, such as U.S. patent no. 4,933,969 to

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 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 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 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 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). 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 information and verifies the identity of the signer. In another mechanism,

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 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 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 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 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 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 purchase services on-line.

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 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 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 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 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 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 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.

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;

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.

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;

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;

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.

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;

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);

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;

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 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.

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

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 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 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 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 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 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 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 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;

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);

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;

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.

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.

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:

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;

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.

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

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.

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 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:

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.

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;

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 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.

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;

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);

viii) inserting the user data in the template;

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).

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;

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 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 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;

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);

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;

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.

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.

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 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);

viii) inserting the user data in the template;

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).

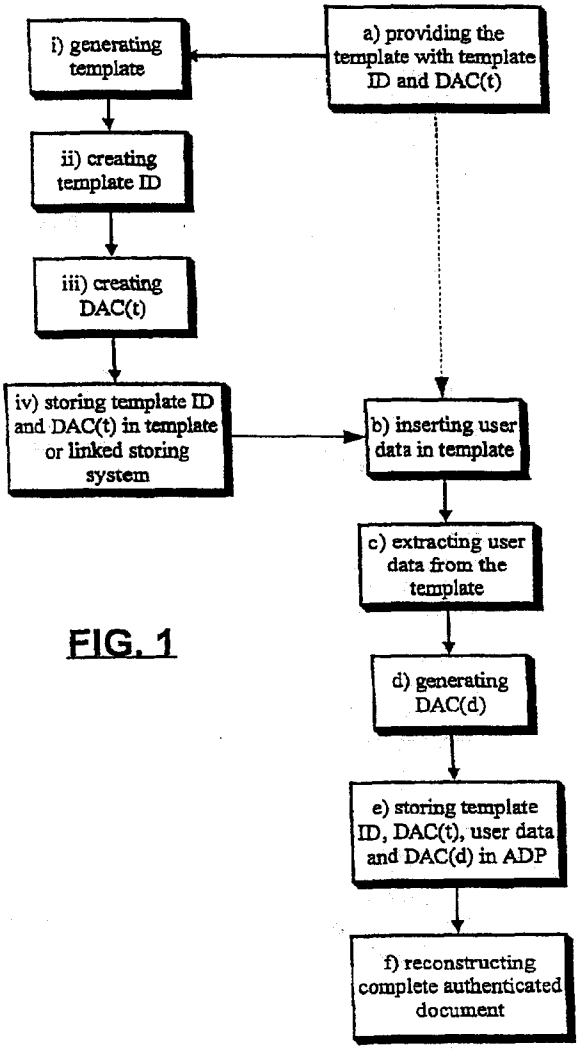

a) providing the template with template ID and DAC(t)
i) generating template
ii) creating template ID
iii) creating DAC(t)
iv) storing template ID and DAC(t) in template or linked storing system
b) inserting user data in template
c) extracting user data from the template
d) generating DAC(d)
e) storing template ID, DAC(t), user data and DAC(d) in ADP
f) reconstructing complete authenticated document

FIG. 1

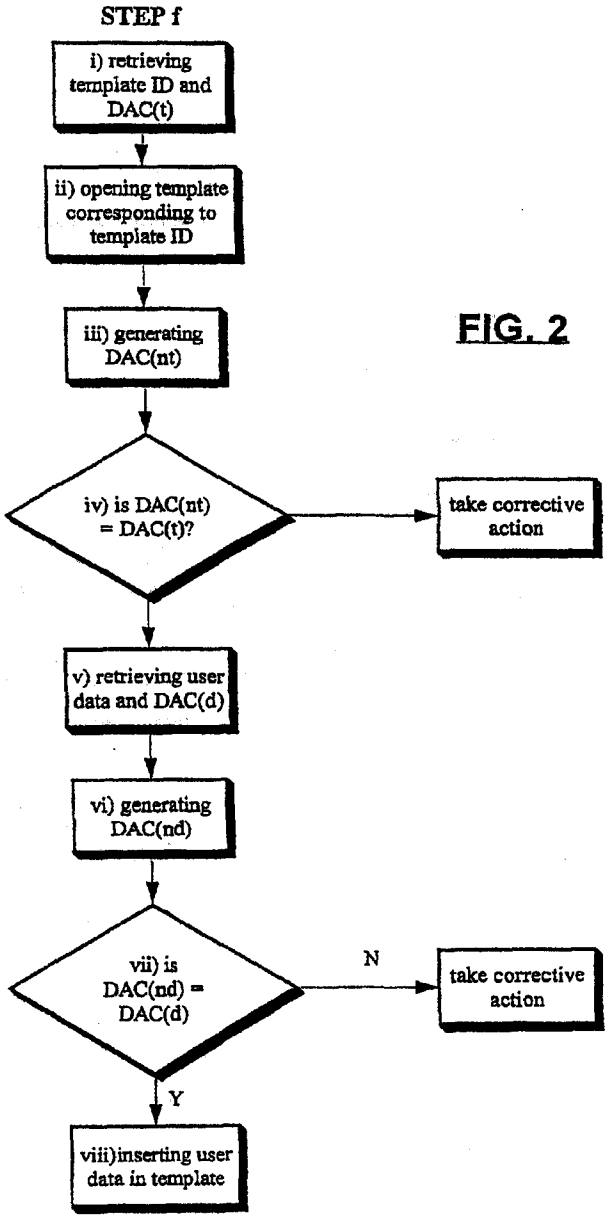

STEP f
i) retrieving template ID and DAC(t)
ii) opening template corresponding to template ID
iii) generating DAC(nt)
iv) is DAC(nt) = DAC(t)?
take corrective action
v) retrieving user data and DAC(d)
vi) generating DAC(nd)
vii) is DAC(nd) = DAC(d)
N
take corrective action
Y
viii)inserting user data in template

FIG. 2

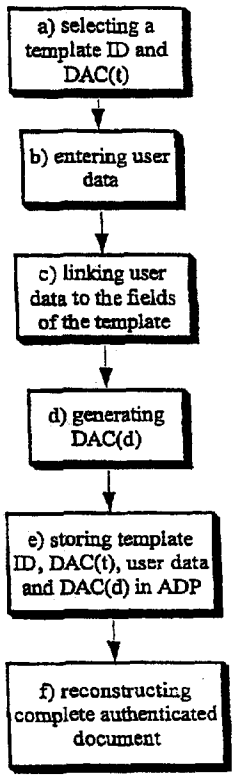

a) selecting a template ID and DAC(t)
b) entering user data
c) linking user data to the fields of the template
d) generating DAC(d)
e) storing template ID, DAC(t), user data and DAC(d) in ADP
f) reconstructing complete authenticated document

FIG. 3

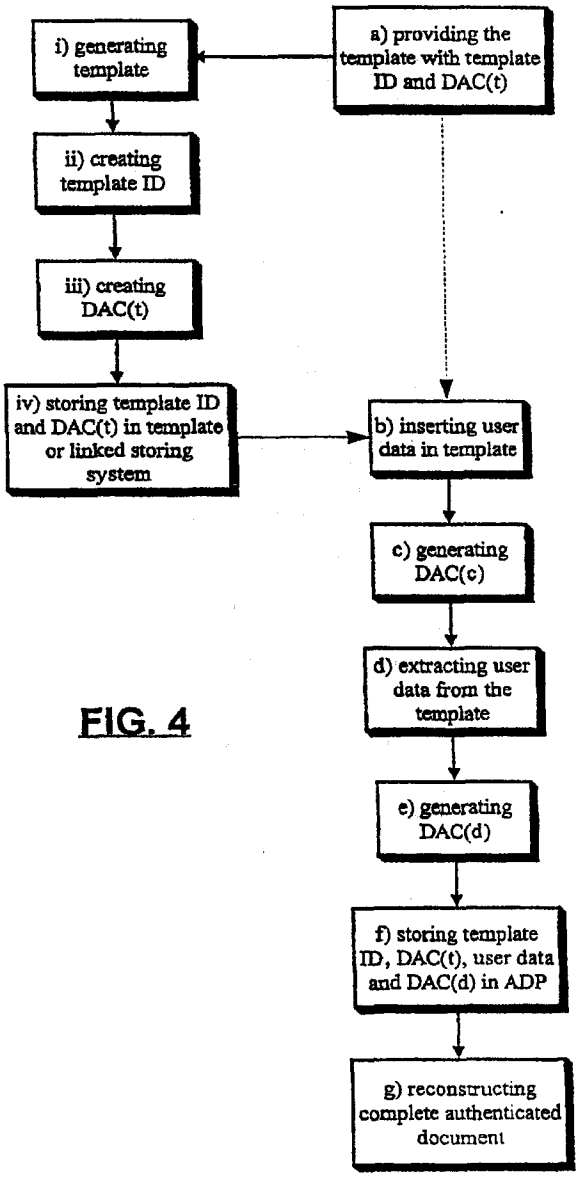

i) generating template
a) providing the template with template ID and DAC(t)
ii) creating template ID
iii) creating DAC(t)
iv) storing template ID and DAC(t) in template or linked storing system
b) inserting user data in template
c) generating DAC(c)
d) extracting user data from the template
e) generating DAC(d)
f) storing template ID, DAC(t), user data and DAC(d) in ADP
g) reconstructing complete authenticated document

FIG. 4

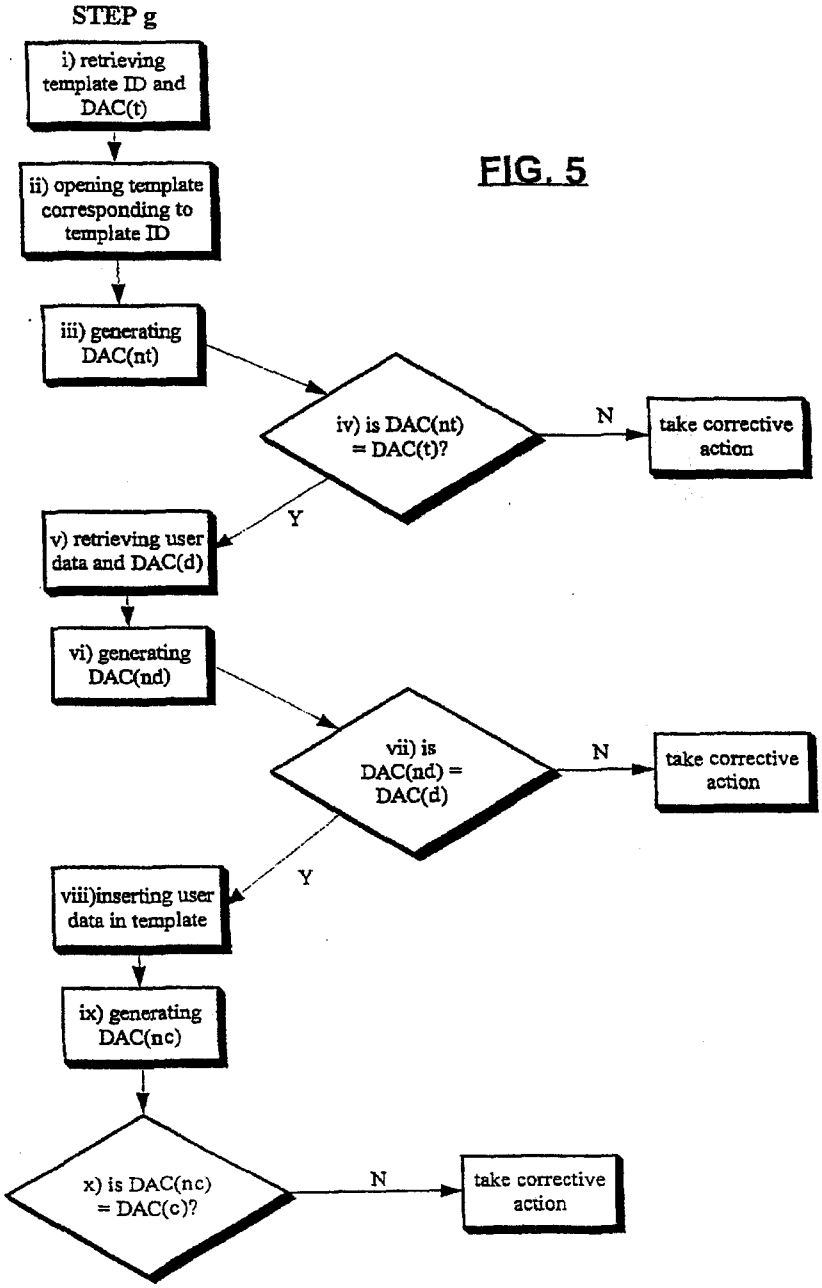

STEP g
i) retrieving template ID and DAC(t)
ii) opening template corresponding to template ID
iii) generating DAC(nt)
iv) is DAC(nt) = DAC(t)?
N
take corrective action
Y
v) retrieving user data and DAC(d)
vi) generating DAC(nd)
vii) is DAC(nd) = DAC(d)
N
take corrective action
Y
viii)inserting user data in template
ix) generating DAC(nc)
x) is DAC(nc) = DAC(c)?
N
take corrective action

FIG. 5

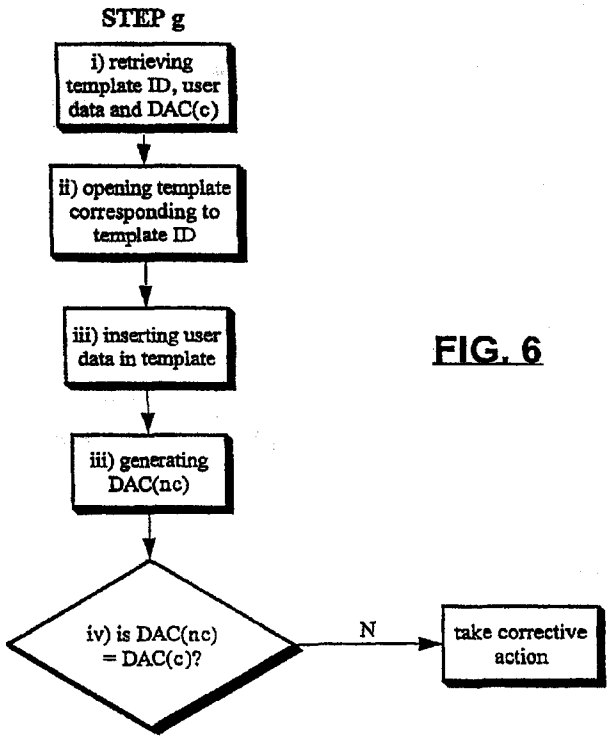

STEP g
i) retrieving template ID, user data and DAC(c)
ii) opening template corresponding to template ID
iii) inserting user data in template
iii) generating DAC(nc)
iv) is DAC(nc) = DAC(c)?
N
take corrective action

FIG. 6

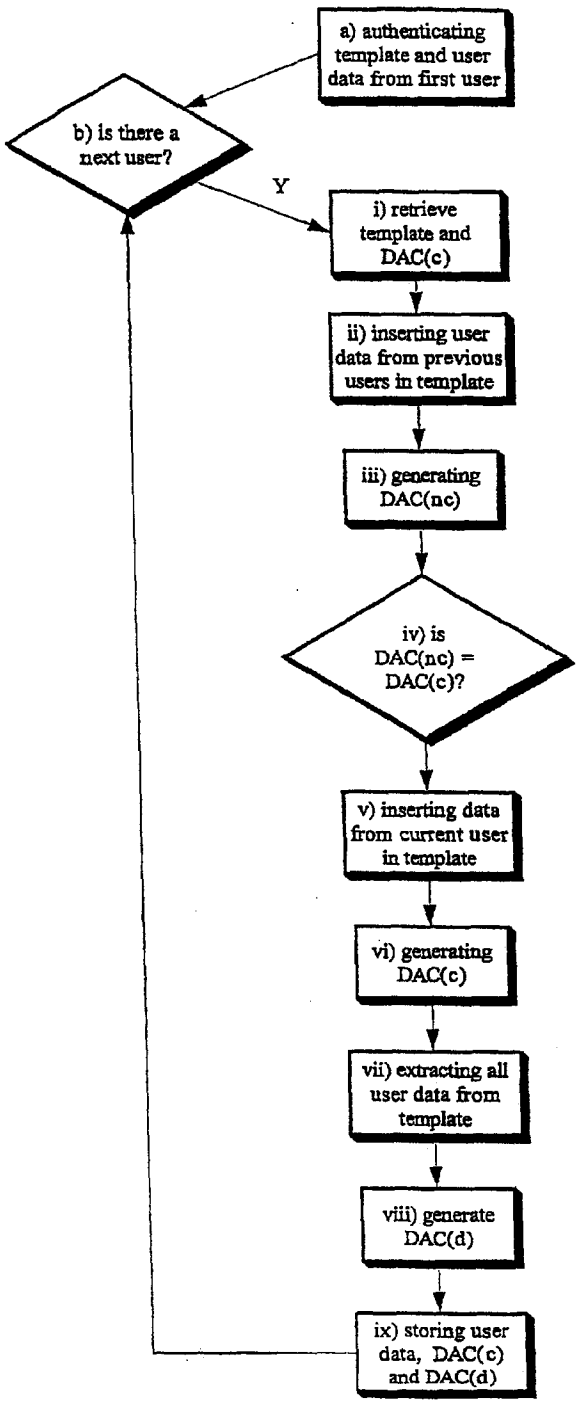

a) authenticating template and user data from first user
b) is there a next user?
Y
i) retrieve template and DAC(c)
ii) inserting user data from previous users in template
iii) generating DAC(nc)
iv) is DAC(nc) = DAC(c)?
v) inserting data from current user in template
vi) generating DAC(c)
vii) extracting all user data from template
viii) generate DAC(d)
ix) storing user data, DAC(c) and DAC(d)

FIG. 7

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.
12/453,124	04/29/2009	Ron M. Redlich	6851-08-cip	8996

4897 7590 11/24/2010

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

EXAMINER	
NAWAZ, ASAD M	
ART UNIT	PAPER NUMBER
2455	

NOTIFICATION DATE	DELIVERY MODE
11/24/2010	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.	Applicant(s)	
	12/453,124	REDLICH ET AL.	
	Examiner	Art Unit	
	ASAD M. NAWAZ	2455	

-- 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 *10 June 2009*.

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) *1-4* 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) *1-4* 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)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/11/09*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to the application submitted 6/10/09. Claims 1-4 are submitted for examination.

Priority

2. The provisional application relied upon, 60/883522, does not disclose or provide adequate support/description of several limitations claimed. Therefore, this application has not been accorded the priority date of the provisional application.

Information Disclosure Statement

3. An international reference, submitted in an IDS filed 11/11/09, was not considered due to the fact it was placed under "US Patents" section. Furthermore, a copy of the reference was not provided.

Specification

4. The abstract of the disclosure is objected to because it contains legal phraseology. Correction is required. See MPEP § 608.01(b).

5. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

6. The lengthy specification is also objected to because it contains narratives and material that in no way corresponds to the inventive subject matter being claimed. Portions of the specification are narratives and philosophical reflections that do not provide any relevant teaching to the subject matter at hand.

7. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

8. The use of several trademarks has been noted in this application. They should be capitalized wherever they appear and be accompanied by the generic terminology.

Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

9. The listing of references in the specification is not a proper information disclosure statement. 37 CFR 1.98(b) requires a list of all patents, publications, or other information submitted for consideration by the Office, and MPEP § 609.04(a) states, "the list may not be incorporated into the specification but must be submitted in a separate paper." Therefore, unless the references have been cited by the examiner on form PTO-892, they have not been considered.

Election/Restrictions

10. The examiner notes that claim 1 contains the term withdrawing. It is not readily clear whether this term is referring to or equivalent to reconstruction, as in claim 3. For the purposes of examination, it is assumed that the process of both limitations is the same. Applicant is advised that if the two terms are not equivalent, the application

would contain distinct patentable subjected matter and thus a restriction requirement would be necessary.

Examiner's Note

11. It is noted that there are several significant limitations recited in the preamble. Such limitations have not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

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 1-4 rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-72 of U.S. Patent No. 7103915. Although the conflicting claims are not identical, they are not patentably distinct from each other because Claims 1-72 of the patent contain every limitation, or an obvious variation, of claims 1-4 of the present Application.

Claims 1-4 rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-73 of U.S. Patent No. 7140044. Although the conflicting claims are not identical, they are not patentably distinct from each other because Claims 1-73 of the patent contain every limitation, or an obvious variation, of claims 1-4 of the present Application.

Claims 1-4 rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-67 of U.S. Patent No. 7146644. Although the conflicting claims are not identical, they are not patentably distinct from each other because Claims 1-67 of the patent contain every limitation, or an obvious variation, of claims 1-4 of the present Application.

Claims 1-4 rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-85 of U.S. Patent No. 7191252. Although the conflicting claims are not identical, they are not patentably distinct from each other because Claims 1-85 of the patent contain every limitation, or an obvious variation, of claims 1-4 of the present Application.

Claims 1-4 rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-143 of U.S. Patent No. 7313825. Although the conflicting claims are not identical, they are not patentably distinct from each other because Claims 1-143 of the patent contain every limitation, or an obvious variation, of claims 1-4 of the present Application.

Claims 1-4 rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-90 of U.S. Patent No. 7322047. Although the conflicting claims are not identical, they are not patentably distinct from each other because Claims 1-90 of the patent contain every limitation, or an obvious variation, of claims 1-4 of the present Application.

Claims 1-4 rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-27 of U.S. Patent No. 7349987. Although

the conflicting claims are not identical, they are not patentably distinct from each other because Claims 1-27 of the patent contain every limitation, or an obvious variation, of claims 1-4 of the present Application.

Claims 1-4 rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-72 of U.S. Patent No. 7546334. Although the conflicting claims are not identical, they are not patentably distinct from each other because Claims 1-72 of the patent contain every limitation, or an obvious variation, of claims 1-4 of the present Application.

Claims 1-4 rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-54 of U.S. Patent No. 7552482. Although the conflicting claims are not identical, they are not patentably distinct from each other because Claims 1-54 of the patent contain every limitation, or an obvious variation, of claims 1-4 of the present Application.

Claims 1-4 rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-45 of U.S. Patent No. 7669051. Although the conflicting claims are not identical, they are not patentably distinct from each other because Claims 1-45 of the patent contain every limitation, or an obvious variation, of claims 1-4 of the present Application.

Claims 1-4 rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-145 of U.S. Patent No. 7721344. Although the conflicting claims are not identical, they are not patentably distinct from

each other because Claims 1-145 of the patent contain every limitation, or an obvious variation, of claims 1-4 of the present Application.

Claims 1-4 rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-45 of U.S. Patent No. 7721345. Although the conflicting claims are not identical, they are not patentably distinct from each other because Claims 1-45 of the patent contain every limitation, or an obvious variation, of claims 1-4 of the present Application.

Claims 1-4 are provisionally rejected under 35 U.S.C. 101 as claiming the same invention as that of claims 1-20 of copending Application No. 11/829,207. This is a provisional double patenting rejection since the conflicting claims have not in fact been patented.

Claims 1-4 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-108 of copending Application No. 10998363. Although the conflicting claims are not identical, they are not patentably distinct from each other because Claims 1-108 of the copending application contain every limitation, or an obvious variation, of claims 1-4 of the present Application. This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claims 1-4 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-45 of copending Application No. 11465388. Although the conflicting claims are not identical, they are not patentably distinct from each other because Claims 1-45 of the copending application contain

every limitation, or an obvious variation, of claims 1-4 of the present Application. This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claims 1-4 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-44 of copending Application No. 11682941. Although the conflicting claims are not identical, they are not patentably distinct from each other because Claims 1-44 of the copending application contain every limitation, or an obvious variation, of claims 1-4 of the present Application. This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claims 1-4 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-28 of copending Application No. 12403850. Although the conflicting claims are not identical, they are not patentably distinct from each other because Claims 1-28 of the copending application contain every limitation, or an obvious variation, of claims 1-4 of the present Application. This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Objections

12. Claims 2-4 are objected to because of the following informalities: Claim 3 recites “there by”. It should be amended to read "thereby'. Claims 2 and 4 refer back to claims 1 and 3. However, they recite "A method" and "A distributed computer system". They

should recite "The method" and "The distributed computer system". Appropriate correction is required.

Claim Rejections - 35 USC § 112

13. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

14. Claims 1-4 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

15. Claims 1-4 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically claim 1 recites “in the presence of said respective access controls applied”. It is unclear what the term presence is referring to because the term “applied" already indicates the existence of access controls.

16. Claims 1-4 are rejected because the claim “scarcity designated data”. However, there is no definition for the term. Rather, it is a relative term at best which renders the claim indefinite. The term "scarcity designated data" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one

of ordinary skill in the art would not be reasonably apprised of the scope of the invention. In fact, the instant specification specifically states that this cannot be measured (see 1482).

17. Claims 1-4 are rejected because they contain the phrase “designated data in *respective* select content data stores". However, it is unclear whether the term respect applies to the security and scarcity data or to each item with the two values. Appropriate corrections are required.

18. Claims 3 and 4 contain "means for" language. However, the claims do not properly invoke 35 USC 112, 6th paragraph. They fail one or more of the three pronged test.

Claim Rejections - 35 USC § 103

19. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

20. Claims 1-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fahlman et al (US Patent No. 5,960,080) hereinafter referred to as Fahlman in view of Hoffberg (US Publication No. 2008/0087756).

As to claim 1. Fahlman teaches a method of organizing and processing data in a distributed computing system having select: content represented by one or more predetermined words, characters, images, data elements or data objects, said distributed computing system having a plurality of select content data stores for

respective ones of a plurality of security designated data and scarcity designated data, each with respective access controls thereat, said plurality of select content data stores operatively coupled over a communications network, the method of organizing and processing data comprising: extracting and storing said security designated data and said scarcity designated data in respective select content data stores (col 5, lines 14-19);

withdrawing some or all of said security designated data and said scarcity designated data in said respective select content data stores only in the presence of said respective access controls applied to said select content data stores (col 3, lines 31-43 and col 4, lines 38-46).

However, Fahlman does not explicitly disclose the use of a server cloud environment. Hoffberg teaches a similar environment including cloud based computing (0524). It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the teachings of Hoffberg into those of Fahlman to make the system more efficient. By allowing the computing environment to be a cloud, the devices contained within the environment can communicate without the need for additional security clearances/credentials.

As to claim 2, Falhman and Hoffberg teach a method of organizing and processing data as claimed in claim 1 including applying a monetization algorithm to said security designated data and said scarcity designated data based upon non-secure availability of said security designated data and said scarcity designated data and

generating and assigning either a financial value to said security designated data and said scarcity designated data or generating and assigning a risk-release value to said security designated data and said scarcity designated data (Fahlman col 4, lines 47-59 and Hoffberg 0136-0138, 0150-0159, 0565-0566).

As to claim 3, Fahlman teaches a distributed computer system for organizing and processing data having select content represented by one or more predetermined words, characters, images, data elements or data objects, said distributed computing system having a plurality of select content data stores for respective ones of a plurality of security designated data and scarcity designated data, each with respective access controls thereat, said plurality of select content data stores operatively coupled over a communications network, comprising:

means for identifying plurality of select content data stores for respective ones of a plurality of security designated data and scarcity designated data, a processor activating at least one of said select content data stores there by permitting access to said select content data stores and respective security designated data and scarcity designated data based upon an application of one or more of said access controls thereat (col 5, lines 14-19);

said processor having means for applying a reconstruction data process employing said respective access control to combine one or more of said security designated data and scarcity designated data (col 3, lines 39-43 and col 4, lines 38-46).

However, Fahlman does not explicitly disclose the use of a server cloud environment. Hoffberg teaches a similar environment including cloud based computing (0524). It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the teachings of Hoffberg into those of Fahlman to make the system more efficient. By allowing the computing environment to be a cloud, the devices contained within the environment can communicate without the need for additional security clearances/credentials.

As to claim 4, Fahlman and Hoffberg teach a distributed computer system for organizing and processing data as claimed in claim 3 including means for applying a monetization algorithm to said security designated data and said scarcity designated data based upon non-secure availability of said security designated data and said scarcity designated data and means for generating and assigning either a financial value to said security designated data and said scarcity designated data or generating and assigning a risk-release value to said security designated data and said scarcity designated data (Fahlman col 4, lines 47-59 and Hoffberg 0136-0138, 0150-0159, 0565-0566).

Conclusion

21. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ASAD M. NAWAZ whose telephone number is (571)272-3988. The examiner can normally be reached on M-R 6-3:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on (571)272-4006. 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.

Asad M Nawaz
Primary Examiner
Art Unit 2455

/Asad M Nawaz/
Primary Examiner, Art Unit 2455

Notice of References Cited	Application/Control No. 12/453,124	Applicant(s)/Patent Under Reexamination REDLICH ET AL.	
	Examiner ASAD M. NAWAZ	Art Unit 2455	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2007/0087756	04-2007	Hoffberg, Steven M.	455/450
*	B	US-5,960,080	09-1999	Fahlman et al.	380/252
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	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.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	458	server near2 cloud	US-PGPUB; USPAT	OR	ON	2010/11/07 18:05
L2	2118	monetiz$4 or assign$4 near2 (dollar or financial or monet$4) near2 (value or amount)	US-PGPUB; USPAT	OR	ON	2010/11/07 18:06
L3	8	1 and 2	US-PGPUB; USPAT	OR	ON	2010/11/07 18:06
L4	59291	cloud	US-PGPUB; USPAT	OR	ON	2010/11/07 18:10
L5	8	3 and 2	US-PGPUB; USPAT	OR	ON	2010/11/07 18:10
L6	130	4 and 2	US-PGPUB; USPAT	OR	ON	2010/11/07 18:10
L7	33	4 same (store or memory or db or database) and 2	US-PGPUB; USPAT	OR	ON	2010/11/07 18:21
L8	197	redlich.in.	US-PGPUB; USPAT	OR	ON	2010/11/07 18:26
L9	31	7 not L8	US-PGPUB; USPAT	OR	ON	2010/11/07 18:26
L10	1	(monetiz$4 or assign$4 near2 (dollar or financial or monet$4) near2 (value or amount)) near8 (sensativ$4 or secure) near3 (data or text or information)	US-PGPUB; USPAT	OR	ON	2010/11/07 18:34

L11	4	(monetiz$4 or assign$4 near2 (dollar or financial or monet$4) near2 (value or amount)) near8 (sensitiv$4 or secure) near3 (data or text or information)	US-PGPUB; USPAT	OR	ON	2010/11/07 18:34
L12	4	(monetiz$4 or assign$4 near2 (dollar or financial or monet$4) near2 (value or amount)) with (sensitiv$4 or secure) near3 (data or text or information)	US-PGPUB; USPAT	OR	ON	2010/11/07 18:36
L13	0	12 and 4	US-PGPUB; USPAT	OR	ON	2010/11/07 18:36
L14	2	12/453124 and monetiz $4	US-PGPUB; USPAT	OR	ON	2010/11/07 18:36
L15	65654	server near2 farm or cloud	US-PGPUB; USPAT	OR	ON	2010/11/07 18:39
L16	0	15 and 12	US-PGPUB; USPAT	OR	ON	2010/11/07 18:40
L17	130	15 and 6	US-PGPUB; USPAT	OR	ON	2010/11/07 18:40
L18	12	(monetiz$4 or assign$4 near2 (dollar or financial or monet$4) near2 (value or amount)) same (sensitiv$4 or secure) near3 (data or text or information)	US-PGPUB; USPAT	OR	ON	2010/11/07 18:40
L19	31	(monetiz$4 or assign$4 near2 (dollar or financial or monet$4) near2 (value or amount)) same3 (sensitiv$4 or secure) near3 (data or text or information)	US-PGPUB; USPAT	OR	ON	2010/11/07 18:40

L20	5	19 and 15	US-PGPUB; USPAT	OR	ON	2010/11/07 18:41
L21	34	(("7103915") or ("7140044") or ("7146644") or ("6925454") or ("6874139") or ("20050288939") or ("6192472") or ("6148342") or ("6094483") or ("6055544") or ("5996011") or ("5905980") or ("5832212") or ("5485474") or ("5960080") or ("6602298") or ("6487538") or ("6771290") or ("20020116641") or ("20040054630") or ("5933498") or ("6078907") or ("6598161") or ("5036315") or ("5532950") or ("6301668") or ("6714977") or ("20020073313") or ("5581682") or ("6389542") or ("6073165") or ("6253203") or ("6044375") or ("6662189")).PN.	US-PGPUB; USPAT	OR	OFF	2010/11/07 18:50
L22	0	21 and 2	US-PGPUB; USPAT	OR	ON	2010/11/07 18:58

L23	74	(monetiz$4 or (determin $4 or ascertain$4 or calculat$4 or assign$4) near2 (sale or resale or market or money or dollar or financial or monet$4) near2 (value or amount)) same3 (sensitiv $4 or secure) near3 (data or text or information)	US-PGPUB; USPAT	OR	ON	2010/11/07 19:02
L24	9	23 and 15	US-PGPUB; USPAT	OR	ON	2010/11/07 19:03
L25	19	(monetiz$4 or (determin $4 or ascertain$4 or calculat$4 or assign$4) near2 (sale or resale or market or money or dollar or financial or monet$4) near2 (value or amount)) same (sensitiv $4 or secure) near3 (data or text or information)	US-PGPUB; USPAT	OR	ON	2010/11/07 19:10
L26	19	(monetiz$4 or (determin $4 or ascertain$4 or calculat$4 or assign$4) near2 (sale or resale or market or money or dollar or financial or monet$4) near2 (value or amount)) same (sensitiv $4 or secure or scrubbed or redacted) near3 (data or text or information)	US-PGPUB; USPAT	OR	ON	2010/11/07 19:11
L27	2	26 and 15	US-PGPUB; USPAT	OR	ON	2010/11/07 19:11
L28	2	26 and 4	US-PGPUB; USPAT	OR	ON	2010/11/07 19:11
L29	126	(monetiz$4 and cloud)	US-PGPUB; USPAT	OR	ON	2010/11/07 19:18

L30	2	29 and 8	US-PGPUB; USPAT	OR	ON	2010/11/07 19:18
L31	6	(monetiz$4 same cloud)	US-PGPUB; USPAT	OR	ON	2010/11/07 19:18
L32	96341	"709".clas.	US-PGPUB; USPAT	OR	ON	2010/11/07 19:19
L33	100023	"707".clas.	US-PGPUB; USPAT	OR	ON	2010/11/07 19:19
L34	87300	"705".clas.	US-PGPUB; USPAT	OR	ON	2010/11/07 19:19
L35	53474	"713".clas.	US-PGPUB; USPAT	OR	ON	2010/11/07 19:19
L36	306233	32 or 33 or 34 or 35	US-PGPUB; USPAT	OR	ON	2010/11/07 19:20

EAST Search History (Interference)

<This search history is empty>

11/7/10 7:24:06 PM
C:\Documents and Settings\anawaz\My Documents\EAST\Workspaces\12453124.wsp

11/11/09

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-08-cip	Application Number 12/453,124
Title: Digital Information Infrastructure and Method	Applicant(s) Ron M. Redlich, et al.	
	Filing Date April 29, 2009	Group Art Unit ~~2444~~ 2455

Ex. Nawaz

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.)

	Oracle - Information Lifecycle Management (ILM) for Business Data- Lilian Hobbs	
	Data Mobility Group - The ILM Puzzle- EMC puts all the piece together- September 18, 2006	
	Life Cycle -White paper10218_0115.txt- Practical Steps Toward Information Lifecycle Management	

EXAMINER DATE CONSIDERED

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.N./

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-08	Application Number
Title: Information Infrastructure Management Tools with Extractor, Secure Storage, Content Analysis and Classification and Method Therefor	Applicant(s) Ron M. Redlich, et al.	
	Filing Date	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.)

	MIMEsweeper-Content Security for E-mail, Web Browsing & Webmail, November 12, 2001	
	Cisco IDS Host Sensor Product, October 16, 2001	

EXAMINER DATE CONSIDERED

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.N./

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-08	Application Number
Title: Information Infrastructure Management Tools with Extractor, Secure Storage, Content Analysis and Classification and Method Therefor	Applicant(s) Ron M. Redlich, et al.	
	Filing Date	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. /A.N./

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-08	Application Number
Title: Information Infrastructure Management Tools with Extractor, Secure Storage, Content Analysis and Classification and Method Therefor	Applicant(s) Ron M. Redlich, et al.	
	Filing Date	Group Art Unit

U.S. PATENT DOCUMENTS

Examiner 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.)

	The 1996 book, Applied Cryptography, by Schneier	
	The Uniform Resource Locator article "FOLD OC"	
	Microsoft Word "Learning Microsoft Word 7.0"	

EXAMINER DATE CONSIDERED

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.N./

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-08	Application Number
Title: Information Infrastructure Management Tools with Extractor, Secure Storage, Content Analysis and Classification and Method Therefor	Applicant(s)	
	Filing Date	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	

FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation YES NO

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

EXAMINER /Asad Nawaz/ DATE CONSIDERED 11/07/2010

G:\RCK\CLIENTS\Redlich\6851-08-cip-Form-PTO-1449.wpd

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.N./

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12453124	REDLICH ET AL.
	Examiner	**Art Unit**
	ASAD M NAWAZ	2455

✓	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	11/07/2010								
	1	✓								
	2	✓								
	3	✓								
	4	✓								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12453124	REDLICH ET AL.
	Examiner	Art Unit
	ASAD M NAWAZ	2455

SEARCHED

Class	Subclass	Date	Examiner
709	ALL	11/7/10	AMN
707	ALL	11/7/10	AMN
713	ALL	11/7/10	AMN
705	ALL	11/7/10	AMN

SEARCH NOTES

Search Notes	Date	Examiner
East Search (USPAT; USPGPUB)	11/7/10	AMN
In depth Inventor Name Search for ODP	11/7/10	AMN

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

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

Serial No. 12/453,124

Examiner A. Nawaz

Confirmation No.: 8996 Group Art 2445

Filed: April 29, 2009

For: Digital Information Infrastructure and Method
for Security Designated Data and with Granular Data Stores (as amended)

AMENDMENT

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

Sir:

This Amendment responds to the Office Action dated November 24, 2010. A request to extend time to respond for three (3) months is enclosed ($555.00 fee). Please charge Deposit Account No. 03-1231 for the $555.00 fee. Applicant is a small entity. Please debit or credit Deposit Account No. 03-1231 for any underpayment or overpayment. This amendment includes:

(a) Transmittal (1 pg., p. 1)

(b) Abstract (1 pg., p. 2)

(c) Title (1 pg., p. 3)

(d) Specification (1 pg, p. 4)

(e) Claims (3 pgs., pp. 5 - 7)

(f) Remarks (7 pgs., pp. 8 - 14)

(e) Request to Extend Time to Respond (1 pg.)

[space left blank]

ABSTRACT

Distributed computer system processes data having select content (SC) represented by one or more predetermined words, characters, etc. The system has a plurality of SC data stores in a server cloud for respective security designated (Sec-D) data and ~~scarcity designated (S-D)~~ granular data, each with respective access controls thereat. The ~~SC~~ data stores are ~~is~~ operatively coupled ~~on~~ over a network. An identification module ~~for identifying~~ identifies SC data and granular data stores for ~~the Sec-D data and S-D data~~ in the server cloud. A processor activates ~~an SC~~ data stores in the server cloud thereby permitting access to the SC data and granular data stores ~~and respective Sec-D data and S-D data~~ based upon an application of ~~one or more of said~~ access controls thereat. The processor has a reconstruction module operating as a data process employing the respective access controls to combine one or more of the Sec-D data and granular ~~S-D~~ data.

Title

Digital Information Infrastructure and Method for Security Designated Data and with Granular Data Stores

SPECIFICATION

[002]The present invention relates to information management data processing modules and computer software system and method enabling protection of confidential information, identification of such information, identification of select content, classification for the same, and security system for the same. Businesses and enterprises use information in many different types of forms and format. Structured information is typically data found in database or spreadsheet formats or stored in self-defining formats wherein the information is managed by a software application. A further example of self-defining format is XML documents in format schematics. Some information is "semi-structured" wherein the information has certain defined fields such as email and the structured data fields from, to, cc, bcc and subject, but the body of the email message is unstructured. Unstructured information includes documents generated by end users with the assistance of applications program such as Microsoft ~~Office~~ OFFICE, word processing programs, image processing programs ~~(Adobe)~~ (ADOBE), files downloaded from the Internet, audio and video files etc. Enterprises focus their attention on mission critical applications and data relative thereto which is often located in structured databases or other structured data formats. However, a large majority of information is contained in unstructured or semi-structured formats. There are significant risks involved in handling and locating confidential information in these information files as well as identifying and handling intellectual property data in those files.

CLAIMS

1. (currently amended) A method of organizing and processing data in a distributed computing system, the data to be processed having select content represented by one or more predetermined words, characters, images, data elements or data objects, said distributed computing system having (a) a plurality of select content data stores in a server cloud for respective ones of a plurality of security designated data and (b) a plurality of granular data stores, ~~scarcity designated data,~~ each said select content data store and granular data store having ~~with~~ respective access controls thereat which restrict access to data in the respective data store, said plurality of ~~select content~~ data stores ~~and~~ in said server cloud being operatively coupled over a communications network, the method of organizing and processing data comprising:

extracting and storing said security designated data ~~and said scarcity designated data~~ in respective select content data stores of said server cloud;

parsing remainder data not extracted from said data to be processed and storing the parsed data as data segments in respective granular data stores;

withdrawing some or all of said security designated data and said ~~scarcity designated data~~ parsed data segments in ~~said~~ respective ~~select content~~ data stores ~~only in the presence~~ upon presentation of said respective access controls applied to said ~~select content~~ data stores in said server cloud.

2. (currently amended) ~~A~~ The method of organizing and processing data as claimed in claim 1 including applying a monetization algorithm to said security designated data ~~and said scarcity designated data~~ based upon non-secure availability of said security designated data ~~and said scarcity designated data~~ and generating and assigning either a financial value to said security designated data

~~and said scarcity designated data~~ or generating and assigning a risk-release value to said security designated data. ~~and said scarcity designated data.~~

3. (currently amended) A distributed computer system for organizing and processing data having, the data to be processed having select content represented by one or more predetermined words, characters, images, data elements or data objects, said distributed computing system having (a) a plurality of select content data stores in a server cloud for respective ones of a plurality of security designated data and (b) a plurality of granular data stores, each said select content data store and granular data store having ~~scarcity designated data, each with~~ respective access controls thereat, said plurality of ~~select content~~ data stores and said server cloud operatively coupled over a communications network, comprising:

means for identifying plurality of select content data stores for respective ones of a plurality of security designated data ~~and scarcity designated data~~ in said server cloud,

an extractor for extracting and storing said security designated data in respective select content data stores of said server cloud;

a processor activating at least one of said select content data stores in ~~a~~ said server cloud ~~there by~~ thereby permitting access to said select content data stores and respective security designated data ~~and scarcity designated data~~ based upon an application of one or more of said access controls thereat;

means for parsing remainder data not extracted from said data to be processed and storing the parsed data as data segments in respective granular data stores;

said processor having means for applying a reconstruction data process employing said respective access controls to combine one or more of said security designated data and ~~scarcity designated~~ remainder data. ~~in said server cloud.~~

4. (currently amended) ~~A~~ The distributed computer system for organizing and processing data as claimed in claim 3 including means for applying a monetization algorithm to said security designated data ~~and said scarcity designated data~~ based upon non-secure availability of said security designated data ~~and said scarcity designated data~~ and means for generating and assigning either a financial value to said security designated data ~~and said scarcity designated data~~ or generating and assigning a risk-release value to said security designated data. ~~and said scarcity designated data.~~

REMARKS

This Amendment responds to the Office Action dated November 24, 2010.

In the Office Action on pages 2-11, paragraphs 1-18, the patent examiner questions the use of certain language in the claim (a rejection or an objection under 35 U.S.C. §112).

In the Office Action on pages 11-14, the patent examiner rejects claims 1-4 as being non-patentable in view of certain prior or pre-existing technology or art disclosed in the following references:

U.S. Patent No. 5,960,080 to Fahlman et al. ("Fahlman '080")

U.S. Patent Publication No. 2007/0087756 to Hoffberg ("Hoffberg '756")

Abstract

The Abstract has been amended as suggested by the Examiner.

Specification

The Examiner objects to the specification as having "narratives." This rejection is improper in that all descriptions, purposes , intentions and alterations of the invention may assist the jury and the judge to understand the important features and components of the present invention after issuance of a patent. Further, the Examiner has not identified the legal basis for the "narrative" objection. The specification has been corrected for trademarks of others. Applicant notes that only references cites on the IDS are considered.

Applicant submits herewith the PCT reference and another IDS.

The Examiner states that he thinks the term "withdrawing" in claim 1 is the same as "reconstruction" in claim 3. Claim 1 recites: "withdrawing some or all of said security designated data and said scarcity designated data in said respective select content data stores only in the presence of said respective access controls applied to said select content data stores in said server

cloud." This "withdrawing" refers to copying or extracting data from the select content data stores. See specification at para. 443, 444, 450, 453, 686 and 2854.

Claim 3 recites "said processor having means for applying a reconstruction data process employing said respective access control to combine one or more of said security designated data and scarcity designated data in said server cloud." The means for reconstructing is discussed throughout the specification and includes a module to extract, copy or withdraw data from the select content data stores. Applicant does not have sufficient information about the Examiner's thought process to answer the Examiner's proposed restriction requirement because the claim 3 reconstruction module has a sub-module for copying or extracting data from the select content data stores.

Double Patenting

The Examiner rejects the claims under the double patenting theory. Applicant will submit a disclaimer near the end of the prosecution of this application. In future Office Actions, please refer to the double patenting rejection in the Office Action dated November 24, 2010.

Claim Objections

The Examiner objects to the claims due to certain informalities. These are corrected in this amendment.

Section 112 Rejections

The Examiner rejects claims 1 - 4 regarding the claim recitation "in the presence of said respective access controls." The Examiner seeks clarification of the term "applied." This term is described later herein.

The Examiner rejects claims 1 - 4 regarding the claim recitation "scarcity designated data." This term is deleted as described later herein.

The Examiner rejects claims 1 - 4 regarding the claim recitation "respective." This is corrected in the amended claims.

The Examiner rejects claims 3 - 4 regarding the "means" claim recitation. The Examiner states "Claims 3 and 4 contain 'means for' language. However, the claims do not properly invoke 35 USC 112, 6th paragraph. They fail one or more of the three pronged test." Office Action dated Nov. 24, 2010, pg. 11. Since the Examiner did not identify the statute nor the rule nor the MPEP, Applicant is uncertain as to the scope and meaning of this rejection. Therefore, Applicant cannot frame a proper response to the rejection.

Notwithstanding the foregoing, Applicant submits that the means plus function ("MPF") clauses in claims 3 and 4 are found in the patent specification and in the drawings.

Claim Amendments

The claims have been re-focused to relate to the processing of data on a granular basis. Support for all the changes to the claims is found in the specification at several locations, the most concise being reproduced below. No new matter is added to this case by these changes to the claims.

> The present inventive process and system enables use of granular data which is which is stored in a known and accessible storage store (in defined storage locations (sec-con store or SC store). The security risk in the present system can be reduced by storing smaller and more granular pieces of data. Further, after splitting granular data from a source document or data stream, the granular pieces of data may be processed using the prior art information dispersal algorithms.

Pub.Pat.Appln. ¶ 2774 (see also ¶ 2775, 2776)

> 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. D-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. 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.

Pub.Pat.Appln. ¶ 3160 - 61

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.

Pub.Pat.Appln. ¶ 3156

Discussion of "remainder data" (data from the "input data" left over after extraction of security sensitive (sec-con) or select content (SC) data) is found throughout the specification. See,

for example, "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." Pub.Pat.Appln. ¶ 3171. See also FIGs. B-1A (common text 104, ¶ 2864 "separates out common text or remainder data 104"), B-1B; and B-3.

Extractor modules and extraction functions are discussed throughout the specification. See, for example Section D.1, ¶ 3070; 2756; 2857 and Section A.20.

Response to Prior Art Rejections

In the Office Action, the Examiner rejects the claims in light of Fahlman '080 and Hoffberg '756.

Fahlman '080 does not show, teach or suggest (a) extraction to different Sec-Con or SC stores, each with a separate access control (which limits further access to the data stored therein) and (b) granular parsing of remainder data and (c) storage of the parsed data in granular data stores. Essentially, Fahlman '080 does not show a granular data store for non-secured data, and multiple security levels for Sec-Con or SC data. In fact, nowhere does Fahlman '080 discuss password or security clearance control.

In Fig. 1, step 111 of Fahlman "automatically" merges sensitive information into non-sensitive information. In FIG. 2, step 217, the Fahlman system again "automatically" merges secured data with un-secured data. Fahlman discusses merging secured data with unsecured data at col. 2, line 22, col. 2, line 34, and col. 2, line 49, and col. 2, line 54 and col. 2, line 40. Fahlman '080 discloses identifying security information and extracting that information and replacing it with place holders. Col. 2, line 37 and col. 3, line 47. "The sanitized message is then transmitted with a low level of security." Col. 3, line 54. The sensitive information is stripped from the original

message and stored in a separate location or together with the sanitized message. Col. 3, line 64. A map showing the location of the security information is also stored with the secured information. Col. 3, line 63. "Then, in step 111, the sensitive terms received from the second path are merged with the sanitized message to create a final confidential message." Col. 4, line 1. The examiner should note that Fahlman does not discuss reconstruction or merger in the presence of any type of security clearance. In contrast, the present invention requires multiple security clearances, each unique to a security level. Fahlman also discusses: "Then, in step 217, the sensitive terms are automatically merged back into the serviced message to create a final message." Col. 5, line 27. No discussion of multi-level security clearance is noted. The same is true regarding merger of security information and non-secured information at col. 6, line 62.

Fahlman does not seem to store granular data or non-secure data in a separate stores apart from Sec-Con or SC secure data. Fahlman (1) identifies secret words, (2) replaces the words with placeholders, then (3) transmits the "sanitized message." Fig. 1, step 107, Fig. 2, step 209, col 2, line 19, col. 2, line 34, col. 2, line 49, col. 3, line 54 (transmission - no storage of non-secure data), col. 4, line 64 (transmission - no separate storage). Fahlman does discuss storing the sanitized message, that is, the non-secure data and the placeholders, but not separate storage of granular data. Col. 3, line 63, col. 4, line 47, col. 5, line 1. In the present invention, remainder, non-secret data is stored separately from secret data. Fahlman teaches away from this aspect of the present invention.

Fahlman does not discuss multiple security levels for Sec-con or SC data into multiple storage sites at each security level. Since multiple security levels are not addressed in Fahlman, multiple security clearance codes to obtain "access" to the secured data levels is not discussed. Since Fahlman does not use any type of password or security clearance procedures, there is no presentation of access controls.

There is no motivation nor suggestion to combine Fahlman '080 with Hoffberg '756.

Hoffberg '756 does not discuss nor describe granular extraction and safe storage of non Sec-Con or non-SC data. Hoffberg discusses "A passport containing user-defined information at various security levels is stored in a secure server apparatus, or passport agent, connected to computer network" at ¶ 052 but this is not access controls to Sec-Con or SC data stores and access to granular data stores. Hoffberg '756 does not discuss Sec-Con or SC data stores and granular data stores and therefore simple password control does not disclose multiple storages for multiple types of data, all with multiple access controls thereat.

Accordingly, claims 1 - 4 are patentable over Fahlman '080 and Hoffberg '756. Allowance is requested.

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

fG:\RCK\CLIENTS\Redlich\Patents\6851-08-cip-Amdt-1st-20110516.wpd

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

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

Serial No. 12/453,124

Examiner A. Nawaz
Confirmation No.: 8996 Group Art 2445

Filed: April 29, 2009

For: Digital Information Infrastructure and Method

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.

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

fG:\RCK\CLIENTS\Redlich\6851-08-cip-Req-Time-3mth-20110516.wpd

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

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

Serial No. 12/453,124

Confirmation No.: 8996 Group Art 2444

Filed: April 29, 2009

For: Digital Information Infrastructure and Method

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.

WO 00/75779 A2	PCT	Dec. 14, 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 Kain/_____

Robert C. Kain, Jr.
Reg. No. 30,648
Kain & Associates, Attorneys at Law, P.A.
900 Southeast Third Avenue
Suite 250
Ft. Lauderdale, Florida 33316-1153
Telephone: 954-768-9002
Facsimile: 954-768-0158

G:\RCK\CLIENTS\Redlich\6851-08-cip-1-IDS-wpd.wpd

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-08-cip	Application Number 12/453,124
Title: Digital Information Infrastructure and Method	Applicant(s) Ron M. Redlich, et al.	
	Filing Date April 29, 2009	Group Art Unit 2444

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
	WO 00/75779-A2	12/14/2000	PCT			

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

EXAMINER DATE CONSIDERED

G:\RCK\CLIENTS\Redlich\6851-08-cip-1-Form-PTO-1449.wpd

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 December 2000 (14.12.2000)

PCT

(10) International Publication Number
WO 00/75779 A2

(51) International Patent Classification[7]: G06F 9/46

(21) International Application Number: PCT/US00/15224

(22) International Filing Date: 2 June 2000 (02.06.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/137,568 4 June 1999 (04.06.1999) US

(71) Applicant *(for all designated States except US)*: **IWITNESS, INC.** [US/US]; Suite 2N, 2995 Wilderness Place, Boulder, CO 80301 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LAMBERT, Francis, T.** [US/US]; 1901 Spruce Street, Boulder, CO 80302 (US). **ARCHER, Emory, Scott** [US/US]; 4799 White Rock Circle, #E, Boulder, CO 80301 (US).

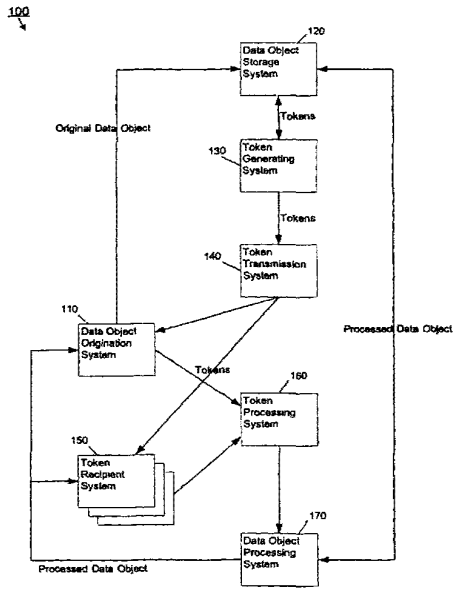
(74) Agents: **SABETT, Randy, V.** et al.; Cooley Godward LLP, One Freedom Square-Reston Town Center, 11951 Freedom Drive, Reston, VA 20190-5601 (US).

(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, 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, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, 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,

[Continued on next page]

(54) Title: TOKEN BASED DATA PROCESSING SYSTEMS AND METHODS



(57) Abstract: A token based data processing system is disclosed that uses data object tokens (DOTs) to manage the associated data objects within the data processing system. The numerous advantages of a token based data processing system stem from the ability to utilize a DOT separate from its associated data object. A data processing system according to the present invention can include a data object origination system, a data object storage system, a token generating system, a token transmission system, one or more token recipient systems, a token processing system, and a data object processing system. The token generating system can generate a DOT that contains metadata corresponding to the information that the token generating system receives regarding the data object, including its attributes, the parameters stored with it, and other information regarding its originating system and its recipient system. After being distributed by a token transmission system, token recipient systems can analyze and process the DOTs in lieu of the associated data objects.

WO 00/75779 A2

IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

TOKEN BASED DATA PROCESSING SYSTEMS AND METHODS

RELATED APPLICATION

The present application claims priority to Provisional Application No. 60/137,568, filed June 4, 1999, which is incorporated herein by reference in its entirety.

BACKGROUND

Field of the Invention

This invention relates to a data processing system containing diverse data objects and to methods for using those data objects. More specifically, the invention relates to a data processing system where the system utilizes data objects called "tokens" to perform processes related to, and upon, other data objects to which the tokens refer.

Description of the Related Art

The advent of electronic data interchange, the growth of electronic communications, the growth of the number of electronic communication users, the growth of the availability of information, and the growth in the size, number and types of data objects has greatly increased the requirements of both data storage and data communication bandwidth. Typical use of these data objects requires processing and transfer of the data object itself, often due to the complexity or sensitivity of the data content of the object, or to the limitations of the data systems used to manipulate the data object. These systems generally require transfer or transmission of the entire data object for a user to be able to edit, preserve, alter, or "own" the data on the person's

local computing system. Examples of these systems can include any that use e-mail attachments, ftp file transfer, and http file transfer.

Unfortunately, a modern data object storage event or a transmission event, such as an electronic document transfer via e-mail, may contain a large volume of data that one entity wishes to transfer to another entity. This type of transfer forces both the sending and receiving parties to expend substantial resources in terms of CPU usage, data storage, and transmission bandwidth at both ends of the transmission. The cost and lost productivity from these types of transmissions will increase as the number and size of these transmissions increase, as is the case in modern data communications.

Additionally, the originator of the transmitted data may wish to keep the transfer of the data secure and private. This requires sending the data using encryption, which requires additional CPU usage. The originator may also wish to guarantee that the transmitted data arrived exactly as sent, which requires that all of the data be sent, verified, and the verification returned to the originating system each time the data is transmitted. These security and authentication technologies must also be present on the receiving system. Prior to the data being released to the transmission network, the originator must have knowledge that the receiving system is capable of reliably authenticating, decrypting, and controlling access to the recipient's copy of the data object.

In many cases, the receiver of the data in this type of transmission is forced to receive all of the transmitted data whenever the originator sends it, regardless of whether or not it is convenient for the receiver at that time. An example of this is a mobile computer user being forced to download a large e-mail attachment over an expensive hotel data line so that they can retrieve all of their e-mail. Another example

is a wireless data transceiver being forced to download unnecessary data when only limited bandwidth is available.

In the case where a data object is transmitted to multiple recipients, the originator is required to transmit the data object multiple times, thereby expending valuable CPU and bandwidth resources in a the concentrated time period of transmission Also, each recipient is required to receive and store its copy of the transmitted object, thereby using bandwidth and data storage resources at each recipient. If the recipients are receiving diverse variations on a data object, the originator is required to create, store, and transmit the separate variations of the data object.

It is also possible that the volume of data in the transmitted data object is too large for the receiving system to efficiently store, or that numerous accumulated objects are too large for the system to efficiently store, and that it would be desirable to have another system with greater storage capacity hold the object and provide authorized access to the object only as needed.

It is also possible that the originator of the data would want to control the access and use of the object by the receiver, or create an audit trail of the receiver's use of the data object. The originator may wish that various receiving parties have access only to portions of the data object specific to the nature of the receiver. The originator or the receiver may desire to provide authentication relating to a data object without transmitting or storing the object itself.

Mechanisms have existed in the past for providing information about stored data objects. For example, a computer file (one type of data object) under the Disk Operating System (DOS) or the Windows operating system has certain flags associated

with it to indicate information about that file. The flags indicate, for example, whether the file is "read only", whether it has been archived, and whether it can be written. The UNIX operating system utilizes a similar approach of storing flags with files. However, the flags in all of these systems are rudimentary, and they are not easily extensible. The flags also tend to be stored as part of the object to which they refer and are therefore cumbersome to process without access to the file itself.

Other types of data objects contain elements that refer to other data objects within the context of the containing object. An example of this could be a filename combined with disk sector locations in a storage directory object, such as a file allocation table. Another example could be a hyperlink with addressing information contained within an HTML object. These object elements act as "pointers" to an object, but do not function outside of the context of the containing object. They also require a process to access the referenced object to perform processes or analysis on the referenced object. They do not act as a "surrogate" for the object, allowing processes to perform functions on an object without accessing the object itself.

Unfortunately, current data network transmission and storage systems fail to provide a robust, extensible, and universally compatible means for those users or systems transmitting and receiving data to efficiently use data objects in such as way as to conserve CPU usage, bandwidth usage, and storage through the use of smaller, more efficient objects containing metadata about the data object that can be processed separately from the data object itself. This smaller, more efficient object can contain metadata for use in access control, use auditing, redactability (or the filtering of content in an object), recipient and sender authentication, workflow logic, data integrity, and

timing of data delivery, among others. Consequently, a need exists for a data processing and transfer system that overcomes the foregoing drawbacks.

SUMMARY OF THE INVENTION

The present invention provides a data processing system that can allow a user to manipulate a data object through the use of one or more separate data objects comprised of metadata about the original data object. The metadata can represent many attributes of a data object, including, but not limited to, information about the content of the data object and the context of its occurrence. It can also represent information about searchable elements in the data object or information on the use history of the object. Some specific examples of metadata can include object identification, access parameters, authentication requirements and values (for both originator and user), encryption methods and keys, access history, integrity checking values, redaction values (or restricting access to certain elements or properties of the original data object), and token validity expiration period. In an embodiment, the DOT can also contain references (such as hyperlinks) to other locations where other metadata values can be found. Systems holding metadata values can also control access to and log use of those metadata values in other locations according to the contents of the token. A data processing system according to the present invention can combine diverse metadata into a discrete and processable data object called a Data Object Token (DOT) that refers to one or more data objects. The DOT includes metadata that provides information about a data object.

In one embodiment, a data object originator can submit a data object to a token based data processing system, which can optionally store the data object and generate

one or more tokens containing metadata of varying complexity referring to the stored data object. The one or more tokens can then be returned to the originator, or sent directly to token recipients, or stored separately in the data object storage system for later use. This Data Object Token, the DOT, can be used by the originator or by token recipients to interact with the data object that is optionally stored on a system storage device such as a central data depository attached to a network, or in another location specified in the DOT according to the protocol used to locate a data object, including a URL, a storage device identifier, or other data object locating protocols. The DOT user can submit the DOT to the token based data processing system to retrieve, view, alter, delete, or otherwise interact with the data object. The token based data processing system can analyze the metadata values contained in the DOT to determine use of the data object, including allowing access, processing authentication values, performing redaction, transmiting the object or portions thereof, destroying the data object, or otherwise manipulating the data object. It can also store and transmit metadata about data object as a smaller, discrete object that can be managed using native and pre-existent file and transmission processes.

One advantage of a token based data processing system is that it allows users of data objects to have access to and control over data objects without being required to expend local storage or bandwidth resources in the process. A DOT can be of very small size and still refer to a much larger data object in a remote location, while providing many capabilities to the local processes that would otherwise require the presence of the data object on the local system. A DOT can be very efficiently transmitted to multiple users, requiring much less storage and bandwidth than multiple transmissions of the referenced data object.

Another advantage is that the user of the DOT can retrieve, download, view, or otherwise process the referenced data object at their convenience by submitting the DOT to the token based data processing system. Another advantage is that the user can receive a DOT that allows them to decide upon the usefulness of, and securely retrieve, the referenced data object without requiring them to download the data object at time of originator transmission to them.

Furthermore, a token based data processing system can contain the authentication values and methods for both the originator and the DOT user that validate access and other rights to the data object. The token based data processing system can validate the DOT as it contains the originator authentication, as well as validate other parameters of the DOT based on the user authentication, before access, processing, or retrieval of the original data object is allowed.

The DOT can also contain data redaction information tailored to the nature of the DOT user. The DOT can provide the system information as to which portions of the data object the user will be allowed access. This relieves the data object storage system from the requirement of having to store and process redaction information for every potential user of the data object.

A further advantage is that the DOT can contain data object routing information for workflow and rules processing of data objects. The process can be more efficient and less bandwidth intensive if a token representing the workflow data object is passed around instead of the object itself.

Another advantage is that the DOT can append data object usage information to itself whenever it is used, and thereby become a self-contained data object usage audit

trail. This usage information could contain user identity and authentication, and time and type of use of use of both the token and the referenced object.

Yet another advantage is that the data object originator can stipulate in the DOT an expiration or starting time for processing of the referenced data object. This allows an originator to control the timing of various aspects of processing the stored data object, as well as avoid the need to provide a local copy of the data object to the DOT user.

Another advantage to using a DOT as a surrogate for a data object is that it avoids exposure of the data object to potential security and privacy problems inherent in the transmission of data over public networks such as the Internet. For example, even if a DOT is sent to the wrong recipient, or "sniffed" from the public network, the referenced object cannot be processed or retrieved since the unauthorized token possessor will not have the correct authentication to access the object.

Another advantage to using the DOT as a surrogate to the referenced data object is that the DOT can contain searchable elements of the original data object, such as keywords or text, and allow searching of the original data object, or a set of data objects, without requiring access to them. This allows searching to be distributed to the token user machine, thus conserving bandwidth and CPU usage at the object storage system.

Another advantage of using a DOT to retrieve an object is that an integrity value, such as a hash digest, of the retrieved data object can be compared to an integrity value in the token user's DOT to determine if the data object was received correctly.

Another advantage of using a DOT approach is that a token generating system can be embedded in an e-mail server, allowing the e-mail system to embed a DOT in

the place of large e-mail attachments. This conserves bandwidth and storage for both the sender and receiver.

Another advantage of DOTs is that they can be used as an electronic payment system due to their high level of security and ability to provide an audit trail. For example, the DOT can represent a portion of a pre-paid monetary amount represented by the referenced data object, such as a bank account. The payment DOT can be submitted to a token processing system that reduces the bank account balance by the amount embedded in the DOT, and then expires the DOT by placing its unique identifier on an expired DOT list. This would allow cashless payment in electronic business transactions, without exposing any sensitive financial information to a public network.

Another advantage of using DOTs is that they decouple the object storage technology from the object access technology, allowing object storage technologies to change without changing the way the stored objects are accessed by the users, and allowing the access objects, or DOTs, to remain valid and functional over long periods of time, even if the storage systems that they access change.

Another advantage of using DOTs is they it allow users to maintain representations of libraries of objects on a local system for off-line browsing, management, and processing.

Additional aspects and embodiments of the present invention will become apparent upon a review of the following detailed description and accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a functional block diagram of an embodiment of the present invention.

Fig. 2 depicts the process flow of a system according to the present invention.

Fig. 3 depicts the basic structure of a data object token.

Fig. 4 is a notational representation of the structure of one embodiment of a data object token.

Fig. 5 is a notational representation of additional elements in the structure of one embodiment of a data object token.

Fig. 6 is a command table for use in an embodiment of the present invention.

Fig. 7 is a flow chart of an embodiment of a token generating system.

Fig. 8 is a flow chart of an embodiment of a token processing system.

Fig. 9 is a flow chart of an embodiment of a token recipient system.

DETAILED DESCRIPTION

Fig. 1 depicts a block diagram of an embodiment of a token based data processing system 100 according to the present invention. Token based data processing system 100 can contain data object origination system 110, data object storage system 120, token generating system 130, token transmission system 140, token recipient system 150, token processing system 160, and data object processing system 170.

Data object origination system 110 can be any device or system that can be utilized to process information and produce data objects, including but not limited to such things as a personal computer, a mainframe computer, or an embedded computing system connected to a network. Data object origination system 110 can further include numerous processes that utilize data objects. For example, data object origination

system 110 could be utilized to create a data object and store that data object in data object storage system 120. Similarly, data object origination system 110 could also be utilized to download and store information, in the form of one or more data objects, from a data network. In particular, data object origination system 110 can utilize and store various data objects including, but not limited to, database files, electronic documents, e-commerce transactions (such as stock trades or merchandise purchases), electronic records (such as medical records or personal histories), multi-part records from document imaging systems, Web sites, sequences of HTTP data, or digitized video and audio data.

Following the creation or reception of one or more data objects in data object origination system 110, the data objects can be stored in data object storage system 120, which can be a local data storage system or a remote data storage system. For example, in the case of a personal computer, a local data object storage system 120 can include a hard drive, or a combination of a floppy disk drive and a floppy disk. Alternatively, a remote version of data object storage system 120 can include storage on a Local Area Network (LAN) or on a Wide Area Network (WAN) using such mechanisms as file servers or digital tape libraries.

In addition to receiving and storing the data objects, data object storage system 120 can expose the data objects to token generating system 130. Token generating system 130 can analyze and process the information about the data object, such as its attributes, the parameters stored with it, and other information regarding its originating system and its recipient system. Token generating system 130 can then generate metadata corresponding to that information, and create a data object called the Data Object Token (DOT) that contains the metadata associated with the data object. Token

generating system 130 can further process the DOT to embed data values that provide or ensure such things as security, privacy, reliability, or efficiency. Numerous means exist for providing these attributes, including encryption, digital signatures, hash digests, other authenticating technologies, compression, or other processing technologies. As one particular example, token generating system 130 can provide authentication, integrity, and non-repudiation information about the data objects using a public key digital signature. Upon successfully verifying the digital signature, the recipient of the digital signature can have the additional assurance of the authenticity of the originator, of the integrity of the data object, and that the data object creation cannot be repudiated.

Once processed, token generating system 130 can further present the DOT to data object storage system 120 and to token transmission system 140 for transmission to one or more token recipient systems 150. Data object storage system 120 or token transmission system 140 can store the DOT or a portion of the DOT for later use, thereby avoiding later reprocessing of the data object.

Token generating system 130 can read the object to be tokenized from data object storage system 120. Token generating system 130 can then determine from a token reference file the types and fields of metadata desired to be embedded in the token. A token reference file can be viewed as a template that contains rules governing the creation or transformation of tokens, including but not limited to encoding of the DOT (e.g. using XML, ASN.1, or comma-separated); required data and metadata fields; organizing structure of metadata fields; and mappings of data types and structures from the source data object to a token. Token generating system 130 can then read the metadata from the object and write it into a file that will become the DOT.

This metadata can include a unique identifier for the object, object location information, object hash digest values, or other metadata fields as required. Token generating system 130 can then determine from the token reference file if it is required to generate metadata from processing the referenced data object's content or metadata fields. Token generating system 130 can then read the content or metadata from the object, process it as required (such as, for example extracting keywords from content text, or reducing images for more efficient searching), and then embed the processed metadata into the token extension fields (see Fig. 3) in the DOT file. The metadata can be written in popular data formats, such as XML or comma delimited fields.

Token generating system 130 can then determine from the token reference file whether token generating system 130 is required to retrieve metadata external to the object, such as the date, a stock price, a digital certificate, encryption keys, other authentication data, or other data as is available to token generating system 130 and required by the token reference file. Token generating system 130 can then embed the externally retrieved data into the appropriate fields in the DOT file. It can also use predetermined time stamp and authentication fields, as well as token extension fields as required. Token generating system 130 can also embed additional metadata into the token file extension fields, such as token validity period, redaction values, or workflow logic to be used when referencing the original data object. Token generating system 130 then can embed its version number in the token file to allow later processing by token processing system 160 and, particularly, to differentiate among different versions of tokens.

Token generating system 130 can then digitally sign the DOT file by methods well known in the art of digital signing, including without limitation, encrypting, with a

private key from a public key infrastructure (PKI) key pair, a combination of a hash digest of the token with a digital certificate, and embedding the digital signature data into the token file. Token generating system 130 can then encrypt the entire token file using well known encryption algorithms, such as triple DES or the RC5 encryption methods.

The DOT file generated by token generating system 130 can then be stored in the data object storage system 120, in the data object generation system 110, or in token generating system 130 itself to await further processing.

Once token generating system 130 creates a DOT, token transmission system 140 can read the DOT from token generating system 130 and determine from a token transmission reference file whether or not the DOT is required to be transmitted to a token recipient system 150, or stored for later use. A token transmission reference file, similar to a token reference file, can contain template rules, such as recipient types, required transmission metadata, and required authentication, that would govern the transmission of DOTs. If the DOT is to be transmitted, the token transmission system 140 can embed information on accessors to the data object in the DOT as required. This information can be used by token processing system 160 to determine the authorization and access rights of the submitted DOT. The token transmission system 140 can embed multiple object accessors values to allow use of the DOT by multiple users or systems. The DOT can then be encrypted in the public key of the transmission destination system, and can then be securely and reliably transmitted to one or more token recipient systems 150 using either a standard communications protocol, such as FTP, e-mail attachment, or HTTP, or by using a proprietary communications protocol.

A token recipient system 150 system can include a system capable of receiving, storing, or processing a DOT. The token transmission system 140 can determine addressing and routing information for the destination token recipient systems 150 from a token transmission reference file, or from the token reference file contained in token generating system 130. In one embodiment, data object origination system 110 can also be a token recipient system. In an embodiment, token transmission system 140 can further verify and log reception of the DOT by one or more token recipient systems 150.

Token recipient system 150 can receive, store, and optionally process or otherwise condition a DOT. Processing on a DOT could include searching on metadata or content from the object embedded in the DOT. This searchable metadata or content could include, for example, text, keywords, or images from the original data object. Other types of processing that could be performed on a DOT by the token recipient system include embedding recipient reception information, such as time stamp and digital signature, appending additional accessors to the referenced object if the recipient system is so authorized, or forwarding the DOT to another token recipient system. The optional processing performed by token recipient system 150 can include other types of analysis and processing of the information contained in the DOT, including its metadata. Since token recipient system 150 can perform its analysis and processing on the metadata contained within the DOT (which is acting as a surrogate for the data object itself), no resources within data object storage system 120 would need to be used.

For example, in one embodiment, token recipient system 150 can contain an e-mail computer application that receives DOTs associated with e-mail messages. In this

case, each message could be a data object. The metadata contained within a particular DOT that is associated with a specific e-mail message can contain information about the e-mail message, including but not limited to such things as the date, time, subject, sender, and, in particular, any attachments associated with the e-mail message. The DOTs can be used by a token recipient system to search for a particular e-mail message or for a group of messages. However, this search could be done solely within the token recipient system using metadata embedded in the DOTs associated with the data objects (i.e. the e-mail messages), not on the messages themselves, which can be stored on a remote data object storage system 120. Also, using this approach, any attachments to the e-mail message would only need to be stored in the data object storage system, not sent to a token recipient system nor stored at the data object origination system.

Furthermore, in one particular embodiment related to e-mail, a token generating system can be embedded in an e-mail server to allow automated storage and tokenization of e-mail, including, without limitation, any of its components such as header, body, or attachments. Token generating system 130 embedded in the e-mail server can read the e-mail objects controlled by the server, generate a DOT for the e-mail object, replace the original e-mail object with the DOT, and store the e-mail object in a more efficient data object storage system location, such as a digital tape library. The e-mail user can then use the DOT from within the e-mail client application to access or process the e-mail data object. Searching for e-mail content within a group of e-mails can be accomplished by searching the search metadata embedded in the DOTs in the e-mail client application, thereby avoiding the CPU and bandwidth costs associated with searching the group of e-mails on the e-mail server or at the data object storage system. This process of substituting DOTs for data objects such as e-mails can

be applied to many types of data objects, including without limitation, scanned or imaged documents, electronic documents, database tables, electronic spreadsheets, web sites, and other types of data objects specified by the user of a token based data object management system.

Upon the completion of a search and a determination that one or more specific e-mail messages, or other type of data objects, need retrieval or processing, token recipient system 150 can submit one or more DOTs to token processing system 160 which can then cause data object storage system 120 to be accessed and the referenced data objects to be processed according to the instructions in the DOT, or transmitted to a data object processing system 170 as requested in the submitted DOT.

After token recipient system 150 submits a DOT to token processing system 160 to retrieve a data object from data object storage system 120, token processing system 160 can interpret the metadata contained in the DOT. Using the metadata, token processing system 160 can submit processing commands to data object processing system 170 according to the metadata contained in the DOT. These commands could include, for example, transmit, redact, alter, or destroy a data object as shown in Fig. 6.

Alternatively, a token recipient system can submit a DOT to a token processing system to retrieve a set of DOTs associated with the submitted DOT. This referenced set of DOTs can reference data objects or other DOTs, or a combination thereof, as required by the system.

Data object processing system 170 can interact with the data object stored in data object storage system 120 according to the commands submitted by token processing system 160. For example and without limitation, in response to a particular

command, data object processing system 170 can transmit, redact, alter, or destroy the data object stored on the data object storage system, according to the authorizations embedded in the submitted DOT, and as interpreted by the token processing system 160, which can pass the commands to the data object storage system 120.

In another embodiment where data object storage system 120 contains data object processing system 170, data object storage system 120 can process the referenced data object according to the instructions embedded in the DOT. For example, if data object storage system 120 is instructed to transmit the object, it can place the object into a data transmission process as is commonly known to the art, or it can encrypt the object using an encryption value submitted with the token, such as the destination system public key, or it can transmit the encrypted object to a system different from the system that submitted the token, or it can transmit the object to multiple systems. Similarly, data object storage system 120 can redact the stored object by recomposing the object prior to transmission, according to redaction rules embedded in the token. An example without limitation of this can be the removal of personal information from a data object for transmission of the data object from within the European Community to a destination outside of the European Community, thereby complying with the European Privacy Act, or other regulations that require redaction of information in transmission or storage.

Data object storage system 120 can additionally alter the data object by changing its retention information, its authorized accessor list, its storage format or location, or even its content if required by the system. Data object storage system 120 can even destroy the data object according to the processing instructions embedded in the submitted token.

Fig. 2 depicts a process flow diagram of an embodiment of the present invention. In data object origination system 210, a data object can be created. Once created, that data object can be transmitted to data object storage system 220. Once received, data object storage system 220 can process the data object so as to enhance the security and reliability of the data object storage process by, for example, performing encryption, compression, hashing, or mirroring, or by digitally signing the data object. For example, the well known DES encryption algorithm can be used to encrypt the data object. In addition, the well known RSA public key digital signature algorithm can be used to digitally sign the data object in data object storage system 220. Following the processing performed on the data object by data object storage system 220, the data object can be stored. The data object storage system can then place the processed object where it will be read by token generating system 230.

Token generating system 230 can generate tokens in standard data formats. For example, token generating system 230 can generate XML-based tokens based on the content of the data objects. To do so, token generating system 230 first reads the stored data object in data object storage system 220. It then analyzes the data object and the associated token reference files. The token reference files can contain instructions and information that can allow the token generating system to determine how the DOT will be constructed from the data object. Once analyzed, token generating system 230 can generate the necessary XML tags to be placed in the DOT for the particular system. In other embodiments, a token generating system can also, for example, generate fixed length fields, comma delimited fields, and other data formats that are commonly used by computer applications. In general, a token generating system can produce any type of DOT that may be needed for a particular data processing system.

In addition, token generating system 230 can encrypt, compress, hash and otherwise process one or more DOTs so as to enhance the security and reliability of the DOTs. Similar to the processing that can be done on the data object itself, the well known DES encryption algorithm can be used to encrypt the DOT. In addition, the well known RSA public key digital signature algorithm can be used to digitally sign the DOT in token generating system 230.

Furthermore, in an embodiment of the present invention, token generating system 230 can embed in the DOT time relevant attributes of the DOT, the data object, or the token recipient system's 250 ability to manipulate it. These time relevant attributes could include, for example, a time stamp of the DOT generation time, expiration of the DOT, the data object, or authentication metadata as determined by the contents of the token reference file. These time relevant attributes could also include "no access until" information that could not allow the token submitting entity to manipulate the data object until a certain time or event.

In an embodiment, once token generating system 230 has generated a DOT, token transmission system 240 can sense the DOT and can cause token generating system 230 to pass the DOT to token transmission system 240. To do so, token transmission system 240 can poll the system holding the DOT and retrieve the DOT in a data "pull" operation once it is available. Token transmission system 240 can then determine the destination for the DOT, followed by determining the methods to be used for the delivery of the DOT, according to mechanisms such as the transmission reference file in the token transmission system, or from the token reference file in the token generating system, or from a workflow logic file. Token transmission system 240 can then transmit DOTs using any well known data transmission technologies,

including, without limitation, the FTP protocol, the HTTP protocol, the SSL protocol, a virtual private network (VPN), or Secure Shell tunneling in the Unix operating system. In another embodiment, a token transmission system can send the DOT as an attachment to an e-mail message. Alternatively, a token transmission system can send a notification to a token recipient system of a token pending transmission to which token recipient system 250 must respond to release or access the token, and a token transmission system 240 can then issue a receipt describing the token delivery event.

After receipt of a DOT from a token transmission system, another token recipient system, or any other means of transmitting a token, such as in an e-mail as an attachment, token recipient system 250 can authenticate the DOT using any authentication techniques that may have been applied by token generating system 230. Once authenticated, token recipient system 250 can store the DOT and subsequently submit the DOT to token processing system 260 for data object manipulation.

In addition to submitting the DOT for data object manipulation, a token recipient system can also add new metadata to the received DOT, or alter the DOT according to the token recipient system's authority to do so as determined by the authorization metadata embedded in the DOT, and optionally transmit that updated DOT to another token recipient system or to the token processing system 260. This can allow metadata within a DOT to accumulate without having to access the associated data object from storage. A data processing system utilizing this type of DOT approach could undergo a change of the native platform and data formats of data object storage system 220 without impacting the capabilities of pre-existing DOTs used to manage and process the data objects within the system, provided the new native platform and data formats remained compatible with the required versions of the DOT structure.

In one embodiment, workflow logic can be embedded within the token or can be captured in an external file. Workflow logic refers to workflow processing rules stored and interpreted both inside and outside of a DOT, and that can affect both the internal operations of the token based data processing system and the overall workflow distribution patterns of tokens and data objects within an organization.

For example, workflow logic could be used by an organization to manage the workflow associated with a particular project. Workflow routing instructions could be embedded in the DOT if it is advantageous for the logic to be contained in the DOT, or the DOT could reference an external workflow logic file that could be dynamically updated. The DOT can reference an object or a set of objects intended to be the subject of a workflow process. This can allow the workflow system to distribute metadata about workflow-related data objects without expending the CPU and bandwidth to distribute the actual data object(s) themselves. The token recipient system 250 itself can execute the workflow logic embedded in the DOT, such as forwarding a DOT automatically to another token recipient system if the referenced data object is not accessed within a certain period of time, or other similar workflow logic.

Upon receiving the DOT from token recipient system 250, token processing system 260 can perform on the DOT any type of processing that might be necessary. For example, the DOT can be decrypted, uncompressed, or otherwise processed to restore it to its original form in response to security and reliability processing performed by the token generating system. The type of processing required can be determined by token processing system 260 by reading the metadata embedded in the DOT, such as the version number, or other metadata indicating how the DOT has been previously processed.

As another example, token processing system 260 can authenticate the entity submitting the DOT using digital certificates, recipient supplied passwords, biometric measurements, or any combination thereof, according to values contained in the token. Alternatively, the entity originating the DOT can be authenticated using digital certificates, recipient supplied passwords, biometric measurements, or any combination thereof, according to values contained in the token.

In yet another embodiment, token processing system 260 can create and append metadata to the DOT that can describe the use of the DOT and the data object. This metadata can be used create a self-contained audit trail within the token. For example, this self-contained audit trail can be comprised of use metadata and authentication values embedded into the token during a workflow execution by the associated token recipient systems.

Token processing system 260 can, in another embodiment, process metadata that describes the token submitting entity's access rights to the referenced data object. Those access rights can be used by data object processing system 270 to control access to all or portions of the data object. Metadata can also be used to describe the time attributes of a DOT, the referenced data object or the authenticating metadata. Token processing system 260 can interpret this time-based metadata to determine proper usage of the token and the associated data object.

The results of the token processing done by token processing system 260 can be passed as commands to data object processing system 270. Upon receiving one or more of these commands, data object processing system 270 can authenticate the command using any well known authentication technique already described herein. Upon successful authentication, data object processing system 270 can determine what

action needs to be taken to respond to the command. For example, destroying or deleting the referenced object from the object store, or appending the audit trail information embedded in the submitted DOT are actions that can be taken in response to a command.

One frequent action by data object processing system 270 can be the accessing of one or more data objects in data object storage system 220. If data object processing system 270 determines that the proper conditions have been met, including, for example, appropriate authentication information, one or more data objects can then be accessed in data object storage system 220. Once accessed, the requested actions can be performed on the accessed data objects by data object processing system 270 and those actions can also be logged by data object processing system 270. Finally, any results of the processing performed by data object processing system 270 can be passed back to token processing system 260. In another embodiment, data object processing system 270 can transmit one or more data objects to the token submitting entity. Prior to doing so, data object processing system 270 can optionally encrypt, compress, hash, sign, or otherwise process the data object to enhance security and reliability in transmission and delivery.

Figure 3 depicts a DOT 300 in accordance with the present invention. The basic DOT structure consists of a version field 304, token information 308, object accessors 328 , token and referenced object use information 352, and optional token extensions 368.

Version field 304 indicates the version of the data object token protocol to which DOT 300 conforms. The inclusion of version field 304 permits a token processing system to properly parse the DOT.

Token information 308 contains the fields necessary for a token processing system to assess the validity of the DOT and the data object to which the DOT is associated. Data object identifier 312 can contain a unique value or character string that identifies the data object to which it refers. Validity information 316 allows a system to make the determination of whether the DOT is valid. For example, validity information 316 can contain date and time information, such that a validity period can be established. Alternatively, validity information 316 can contain a hash digest of the object and the DOT that can be used for purposes of determining data integrity of a received object or DOT.

Data object and DOT authentication information 320 can contain any type of data that can be used to authenticate the data object or the DOT itself. In an embodiment, data object authentication information can contain a public key from a PKI key pair. In another embodiment, data object authentication information 320 can contain a digital signature. The authentication information can be used to authenticate the system creating the referenced data object, the system generating the DOT, or the system submitting the DOT to a token processing system or token recipient system. Timestamp 324 can provide information to an entity about the time of creation of the token. A data object originator could use the timestamp, for example, to prove that a data object representing a transaction was created at a specific time on a specific date.

The next main component of the DOT is object accessor 328. This can provide information about the entity or entities permitted to access and use the data object referenced by the DOT. In an embodiment, there may be multiple instantiations of object accessor 328 for each permitted accessor of the data object. Each object accessor 328 can contain information about the accessor 332, access rights 336,

authentication requirements 340, accessor authentication information 344, and timestamp 348. In an embodiment, the object accessor metadata can contain a list of workflow destinations upon which workflow distribution processing can be based.

Accessor 332 can contain information that identifies the entity being given rights to access the data object. This entity identifier could identify a system, a process, a class of processes, a specific user, a group of users, a reference to a dynamically alterable accessor list, or the general public. For example, accessor 332 can contain a name, an e-mail address, and a unique identifier. In another embodiment, accessor 332 can contain a digital certificate.

Access rights 336 can provide information to the token processing system regarding the rights that the accessor identified by accessor 332 has to the data object to which the DOT refers. Access rights 336 can include, for example, general rights, such as those used to access, download, modify, or destroy a data object. In addition, access rights 336 can include other, more specific rights that are unique to the particular data processing system. For example, a DOT used in a stock trading system might contain rights particular to a stock trader, such as buy unrestricted, buy limited, sell unrestricted, or sell limited. In another example, access rights can also stipulate authorization of the token recipient system to alter the metadata in the token, or the authorization to append audit trail metadata, as required by the system. Authentication requirements 340 provide information about the type of authentication required to be used by the token user to prove that it is the entity identified by accessor 332. Numerous, well understood, technologies exist to provide authentication in several different formats. For example, a particular data processing system may require something to be known by the token user, such as a password or personal identification

number (PIN). Alternatively, a data processing system may require the user to have an object, such as a smart card or a hardware "dongle". Finally, a data processing system might require physical information from the token user (i.e. a biometric), such as a fingerprint, a retinal scan, or a voice print.

Accessor authentication information 344 provides information about the entity that created the object accessor entry. This can be used to audit the granting of rights to access the referenced data object.

Timestamp 348 can provide information to an entity about the time of creation of the object accessor 328 metadata. A token processing system could use the timestamp, for example, to prove that the authentication information 344 was historically valid at the time of its creation. For example, if a digital certificate is used as authentication information 344, time stamp 348 can be used at a later time to determine if the digital certificate had expired or been revoked at the time of object accessor 328 metadata creation.

The next component of DOT 300 in an embodiment of the present invention, token use information 352, contains information about the use of the DOT and use of the data object to which the DOT refers. Token use information 352 can include information on the type of access requested 356 by the token user. Once authenticated using access authentication information 360, a token processing system can utilize token use information 352 to determine how it should process the object referenced by the DOT. This could include uploading the object to the token submitter, changing data in the object, or destroying the object.

One or more token extensions 368 allow the DOT to provide additional information beyond the standard DOT including, but not limited to, such things as

redaction instructions and audit trail data related to the associated data object. The format of each token extension 368 can consist of extension type 372, extension data 376, and extension authentication information 380. Within token extension 368, extensible metadata can be stored that can then be interpreted by the token recipient system or the token processing system. Some examples of the use of token extension 368 include DOT expiration values for a particular system, searchable content metadata values, workflow logic, additional (system specific) access rights, externally retrieved metadata, and any other fields that may be added by a token recipient system.

Fig. 4 and Fig. 5 provide a description of one embodiment of a DOT that can be associated with a Verified Data Object (VDO), as implemented by iWitness, Inc. of Boulder, Colorado in its electronic records management products. The descriptions in Fig. 4 and Fig. 5 use the well known Abstract Syntax Notation 1 (ASN.1) that is defined in "CCITT Recommendation X.208: Specification of Abstract Syntax Notation One (ASN.1)", published in 1988. The ASN.1 descriptions in Fig. 4 and Fig. 5 depict a Verified Data Object Token (VDOT).

Fig. 4 depicts the basic VDOT structure 410, which includes the two main components of tokenInfo and accessors. The tokenInfo component can provide information specific to the VDO, while the accessors component can provide information about the entities that may access the VDO. As shown in 420, the tokenInfo component can include globally unique object identifier vdo_id, the interval of time during which the token is valid, a digital signature and certificate identifying the creation event, and a timestamp. The vdo_id element can be used to uniquely identify the particular VDO to which the VDOT refers and can contain a randomly generated ASCII character string that had been verified as being unique. In a different

embodiment, the vdo_id could be a consecutive number applied to a particular VDO amongst a large set of other VDOs. The validFrom and validTo components together provide the validity period for the VDOT user to access the particular VDO. In an embodiment, if the UniversalTime value within the data processing system utilizing the VDO is less than the validFrom time or greater than the validTo time, the entity submitting the token in an attempt to access the associated VDO would be denied that access.

The signerInfo component provides the digital signature and information about the signer who applied the digital signature used to verify the VDO. In an embodiment, signerInfo can be the signer information defined in "PKCS #7: Cryptographic Message Syntax Standard: An RSA Laboratories Technical Note", Version 1.5, Revised November 1, 1993, which specifies, amongst other things, the signer's digital certificate, the algorithm used to sign the VDO, and the digital signature itself.

The accessors component within VDOT basic structure 410 specifies a collection of entities along with their access rights and authentication requirements for the specified VDO. As shown in accessor information 430, those entities can be identified in a table consisting of a set of DataObjectTokenAccessor elements, wherein each DataObjectTokenAccessor element can contain a PKCS #6 certificate, the access rights needed to access the VDO, the authentication requirements for the particular VDO, the PKCS #7 signer information, the PKCS #6 certificate of the signer of the VDOT, and a timestamp.

Access rights listing 440 for a particular VDOT can provide information on how a particular entity may use the VDOT in an embodiment of the invention. Only entities identified by the distinguished name and serial number from their enclosed PKCS #6

certificate can make use of the VDOT, including, for example, the ability to retrieve the corresponding VDO. Those entities are limited to their corresponding access rights, which are signed by the entity responsible for their assignment.

Authentication requirements 450 for a particular VDOT provides information on how a particular entity must authenticate itself prior to its use of the VDOT. Any use of the token, whether for VDO retrieval or communication to another entity, may require the using entity to satisfy one or more authentication requirements, such as knowledge of a password, a physical match of biometric data, or an external key. Additionally, each entry in the accessor table can be signed by its creator.

Fig. 5 depicts an ASN.1 description of the token use information 510 element and the token extension 520 element in accordance with an embodiment of the present invention. Token use information 510 can contain request information that indicates how a VDOT user would like to use the corresponding VDO and authentication information that allows the token processing system to determine the validity of the request. Token use information 510 can be included upon initial generation of the VDOT or can be appended at some later time after VDOT creation.

In an embodiment of the invention, one or more instantiations of the optional token extension 520 element can be included in a VDOT. In a VDOT, extType can specify the extension type of this particular extension.

Fig. 6 shows a command table implemented in one embodiment of the present invention that contains commands for performing various operations on a data object. A data object processing system can use the information shown in 610 to execute the commands on the specified data object. Transmit object command 620 can result in a data object being transmitted to the destination specified by the destination argument,

and can include information on authorization, transmission time, recipient requirements, and transport mechanism. Destroy object command 630 can result in the destruction of a data object, and can include information on authorization, destruction time, and disposition rules. Copy object command 640 can result in the copying of a data object from one location to the location specified by the destination argument. Alter object command 650 can result in one or more modifications to the data object, and can include information on the module to perform the operation, a reference to the data object, the actual alteration to be performed on the data object, and any necessary parameters. Redact object command 660 can result in certain information within a data object being removed while the rest of the data remains, and can include the module to perform the redaction, a reference to the data object, the redaction to be performed on the data object, and any necessary parameters. Finally, object encryption command 670 can result in the encryption or digital signing of a data object, and can include the operation to be performed on the data object, the method or algorithm to be used, the key to be used to perform the cryptographic operation, and whether to just perform a hash on the data object for data integrity purposes.

Figure 7 depicts a flow chart of the processing that can occur in a token generating system utilized for workflow processing. In step 704, the token generating system can receive a DOT generation request, which contains request attributes specifying the data object to be analyzed, the token reference file that defines the structure and required contents of the generated DOT, and possibly other control data. In order to ensure the security of the token generating system, and thus the security of the DOT and its future use in other systems, the DOT generation request is validated in step 712 through one or more of the various authentication means available including,

but not limited to, public key digital signatures. Once the DOT generation request is validated, the data object to which it refers is analyzed in step 716 to determine the viability of the request. In particular, as shown in the substeps in 720, the DOT generation request is checked against workflow logic (if any), the data object is then checked against workflow logic carried in the DOT generation request (if any), and finally, the data object is assessed to determine if it contains the necessary data/metadata to fulfill the request according to the token reference file. If the request cannot be fulfilled, a result indicating this can be returned in step 736.

If the authentication and subsequent analysis succeed, the token generation system can proceed to generate the requested DOT in step 724. As shown in substeps 728, all requested metadata that is derived directly from the data object can first be retrieved and attached. Then, all requested metadata that is derived external to the data object (if any) can be attached, possibly including workflow logic defined in the token request file. Finally, any requested DOT access rights can be constructed and attached. The newly formed DOT can then be digitally signed in step 732 by the token generation system, and possibly encrypted and enveloped following the Cryptographic Message Syntax as defined in PKCS #7. As shown in step 736, the DOT can then be returned synchronously to the originator of the DOT request and/or asynchronously transmitted through a token transmission system (as shown in the substeps in 740). Control could then be returned to the token transmission system in step 744.

Figure 8 depicts a flow chart of the processing that can occur in a token processing system utilized for workflow processing. In step 804, the token recipient system can send a processing request. In step 808, the token processing system can receive a processing request, which can contain, as shown in 812, a request DOT and

request attributes specifying one or more operations to be performed on the data object that the DOT references. Before processing, the token processing system can validate the public-key digital signatures on the DOT in step 816, to ensure the authenticity of the DOT and the authenticity of the requestor. Once validated, the token recipient system can open the cryptographic envelope of the DOT in step 816 (if it is encrypted) with the private-key that corresponds to the public-key used in securing the DOT for transmission. This ensures that the token can only be used by the intended token processing system.

Once validated and decrypted, the token processing system can check the token-embedded or external file workflow logic in step 820 and in the substeps shown in 824. The token processing system can then interpret the processing request according to the workflow logic of the token in step 828 in order to cause the data object processing system in 836 to perform the requested operations in step 832, such as fetch data/metadata, update metadata, destroy object, and transmit object/token, all of which can be performed on the data object within the data object processing system.

Results of the data object operation can be validated by the token processing system in step 840 to ensure their authenticity and conformance to the requirements of the request. The results can then be returned in step 844, and in particular, as shown in substeps 848, the results can be returned synchronously to the originator of the processing request and/or asynchronously transmitted as an updated token through a token transmission system. Once the results have been returned, control can return to the token transmission system in step 852.

Figure 9 depicts a flow chart of the processing that can occur in a token recipient system utilized for workflow processing. The token transmission system can

send a DOT in step 904 and token recipient system can receive a DOT from the token transmission system in step 908. Before processing, the token recipient system can validate the public-key digital signatures on the DOT in step 912, to ensure the authenticity of the DOT and the authenticity of the sender. Once validated, the token recipient system can open the cryptographic envelope of the token in step 912 (if it is encrypted) with the private-key that corresponds to the public-key used in securing the token for transmission. This ensures that the token can only be used by the intended token recipient system.

Once validated and decrypted, the token recipient system checks both the token-embedded and external file workflow logic for conflicts in steps 916 and the substeps in 920. If non-critical conflicts are found, resolution may require priority-based assessment or possibly user intervention. The token recipient system can then process the token according to the workflow logic in step 924. As shown in the substeps in 928, processing can include presentation to the user, storage for archival or for later use. At some point, the user of the token recipient system or the system itself can use the received (and possibly stored) token to request one or more operations on the data object to which it refers, as shown in step 932. This processing can be done through the token processing system as shown in step 936.

While the invention has been described in detail, including references to specific embodiments, it will be apparent to one skilled in the art that changes and modifications can be made to the invention without departing from the spirit and scope thereof. Thus, it is intended that the present invention cover the modifications and variations of this invention provided they come within the scope of the appended claims and their equivalents.

What is claimed is:

1. A method of managing one or more data objects within a data processing system using one or more data object tokens, the method comprising the steps of:

generating one or more data objects within a data object origination system;

storing said data objects in a data object storage system;

analyzing said data objects to determine information to be placed in one or more data object tokens;

generating said one or more data object tokens;

transmitting said one or more data object tokens to one or more token recipient systems;

processing said one or more data object tokens; and

processing said one or more data objects based upon said data object tokens.

2. A method as in claim 1, wherein said storing step further comprises storing said data objects in a local storage system.

3. A method as in claim 1, wherein said storing step further comprises storing said data objects in a remote storage system over a network.

4. A method for generating one or more data object tokens associated with a data object, the method comprising:

receiving a token generation request;

validating said token generation request;

analyzing said data object to determine information to be placed in said one or more data object tokens;

populating said data object token with metadata;

creating validation information related to said data object token; and

returning a completed data object token.

5. A method as in claim 4, wherein said validating step further comprises the step of verifying a digital signature using a public key.

6. A method as in claim 4, wherein said analyzing step further comprises the step of determining information to be redacted in said data object.

7. A method as in claim 4, wherein said analyzing step further comprises the step of determining information to be altered in said data object.

8. A method as in claim 4, wherein said populating step further comprises the step of appending one or more optional token extensions.

9. A method for processing one or more data object tokens associated with a data object, the method comprising:

receiving a token processing request;

validating said token processing request;

interpreting said token processing request to determine the operations to be performed on one or more data objects;

commanding said operations to be performed on said one or more data objects by a data object processing system;

validating the results of said operations; and

returning the resulting data object.

10. A method for limiting access by a user to data objects in a data processing system, the method comprising:

storing said data object securely within said data processing system;

creating a data object token corresponding to said data object, said data object containing authentication requirements;

distributing said data object token;

receiving an access request from a data object token user, said request containing data object token user authentication information and access authentication information;

authenticating said access request;

processing the data object to secure it for use by the data object token user; and

transmitting said processed data object to said data object token user.

11. A method as in claim 10, wherein said storing step further comprises performing local encryption on said data object.

12. A method as in claim 10, wherein said storing step further comprises locating said data object behind a firewall.

13. A method as in claim 10, wherein said first validation step further comprises verification of a first public key digital signature, and wherein said second validation step further comprises verification of a second public key digital signature.

14. A method for validating the use of a data object using a data object token in a token based data processing system, the method comprising:

performing a first validation on data object originator authentication information contained within said data object token; and

performing a second validation on data object token user authentication information contained within said data object token.

15. A method as in claim 14, wherein said first validation step further comprises verification of a first public key digital signature, and wherein said second validation step further comprises verification of a second public key digital signature.

16. A method of retrieving a data object in a token-based data processing system, the method comprising the steps of:

receiving a data object token from a token generating system;

storing said data object token;

appending data object token user authentication information;

submitting said data object token to a token processing system; and

receiving said data object.

17. A method as in claim 16, wherein said data object token user information comprises a public key digital signature.

18. A method for distributing analysis and processing activities related to one or more data objects stored in a data object storage system within a token based data processing system, comprising the steps of:

receiving one or more data object tokens in a token recipient system;

storing said data object tokens; and

processing said data object tokens within said token recipient system.

19. A method as in claim 18, wherein said processing step further comprises the steps of:

extracting metadata associated with said one or more data objects from said one or more data object tokens;

performing an analysis on said metadata; and

accessing one or more data objects within said data object storage system based upon said analysis.

20. A method as in claim 18, wherein:

said processing step further comprises a search through data object tokens containing electronic mail header information based on a set of search criteria; and

said accessing step further comprises accessing e-mail messages meeting said search criteria.

21. A token based data processing system that manages one or more data objects within a data processing system using one or more data object tokens, comprising:

a data object origination system for generating one or more data objects;

a data object storage system for storing said one or more data objects;

a token generating system for generating one or more data object tokens;

a token transmission system for transmitting said one or more data object tokens to one or more token recipient systems;

a token processing system for processing said one or more data object tokens; and

a data object processing system for processing said one or more data objects based upon the processing of said one or more data object tokens.

22. A token based data processing system as in claim 21, wherein said data object storage system is contained within said data object origination system.

23. A token based data processing system as in claim 21, wherein said data object storage system is located over a network remotely from said data object origination system.

24. A token based data processing system as in claim 21, wherein said data objects further comprise scanned or imaged documents.

25. A token generating system for generating one or more data object tokens that refer to one or more data objects, comprising:

a means for receiving a token generation request;

a means for validating said token generation request;

a means for analyzing said data object to determine information to be placed in said one or more data object tokens;

a means for populating said data object token with metadata;

a means for creating validation information related to said data object token; and

a means for returning a completed data object token.

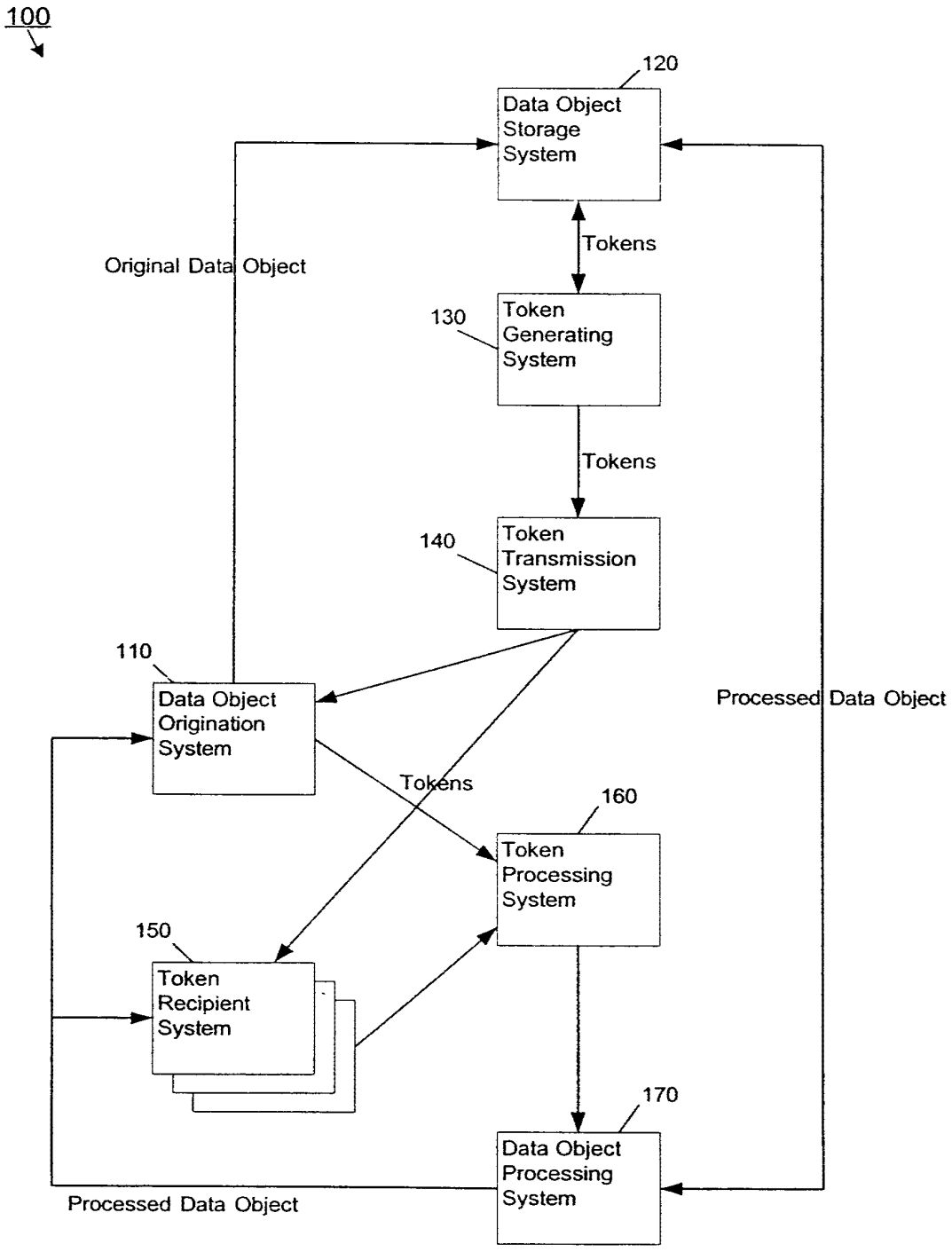

100
120
Data Object Storage System
Tokens
Original Data Object
130
Token Generating System
Tokens
140
Token Transmission System
110
Data Object Origination System
Processed Data Object
Tokens
160
Token Processing System
150
Token Recipient System
170
Data Object Processing System
Processed Data Object

Figure 1

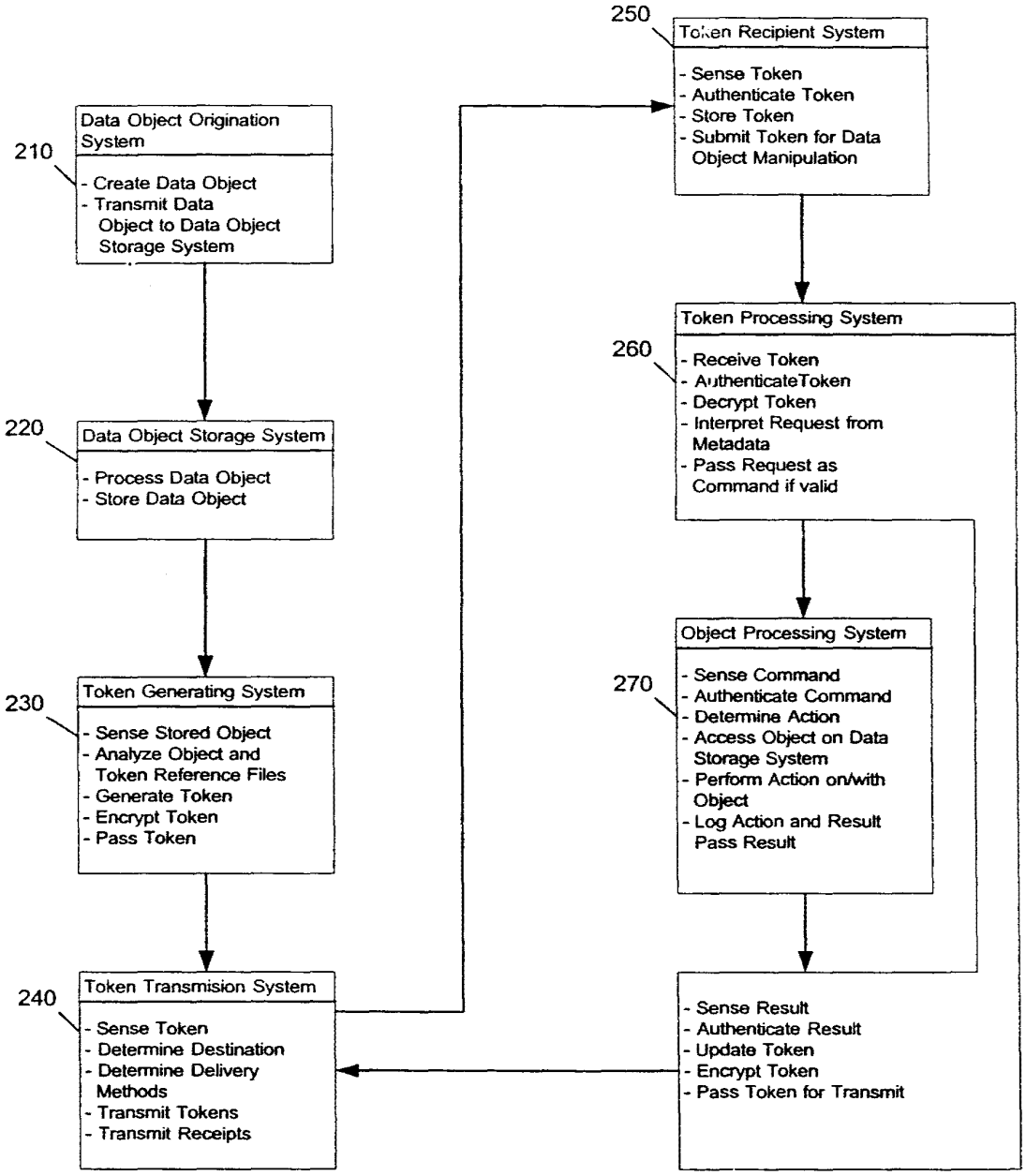

250
Token Recipient System
- Sense Token
- Authenticate Token
- Store Token
- Submit Token for Data Object Manipulation
Data Object Origination System
210
- Create Data Object
- Transmit Data Object to Data Object Storage System
Token Processing System
260
- Receive Token
- AuthenticateToken
- Decrypt Token
- Interpret Request from Metadata
- Pass Request as Command if valid
220
Data Object Storage System
- Process Data Object
- Store Data Object
Object Processing System
270
- Sense Command
- Authenticate Command
- Determine Action
- Access Object on Data Storage System
- Perform Action on/with Object
- Log Action and Result
Pass Result
230
Token Generating System
- Sense Stored Object
- Analyze Object and Token Reference Files
- Generate Token
- Encrypt Token
- Pass Token
240
Token Transmision System
- Sense Token
- Determine Destination
- Determine Delivery Methods
- Transmit Tokens
- Transmit Receipts
- Sense Result
- Authenticate Result
- Update Token
- Encrypt Token
- Pass Token for Transmit

Figure 2

SUBSTITUTE SHEET (RULE 26)

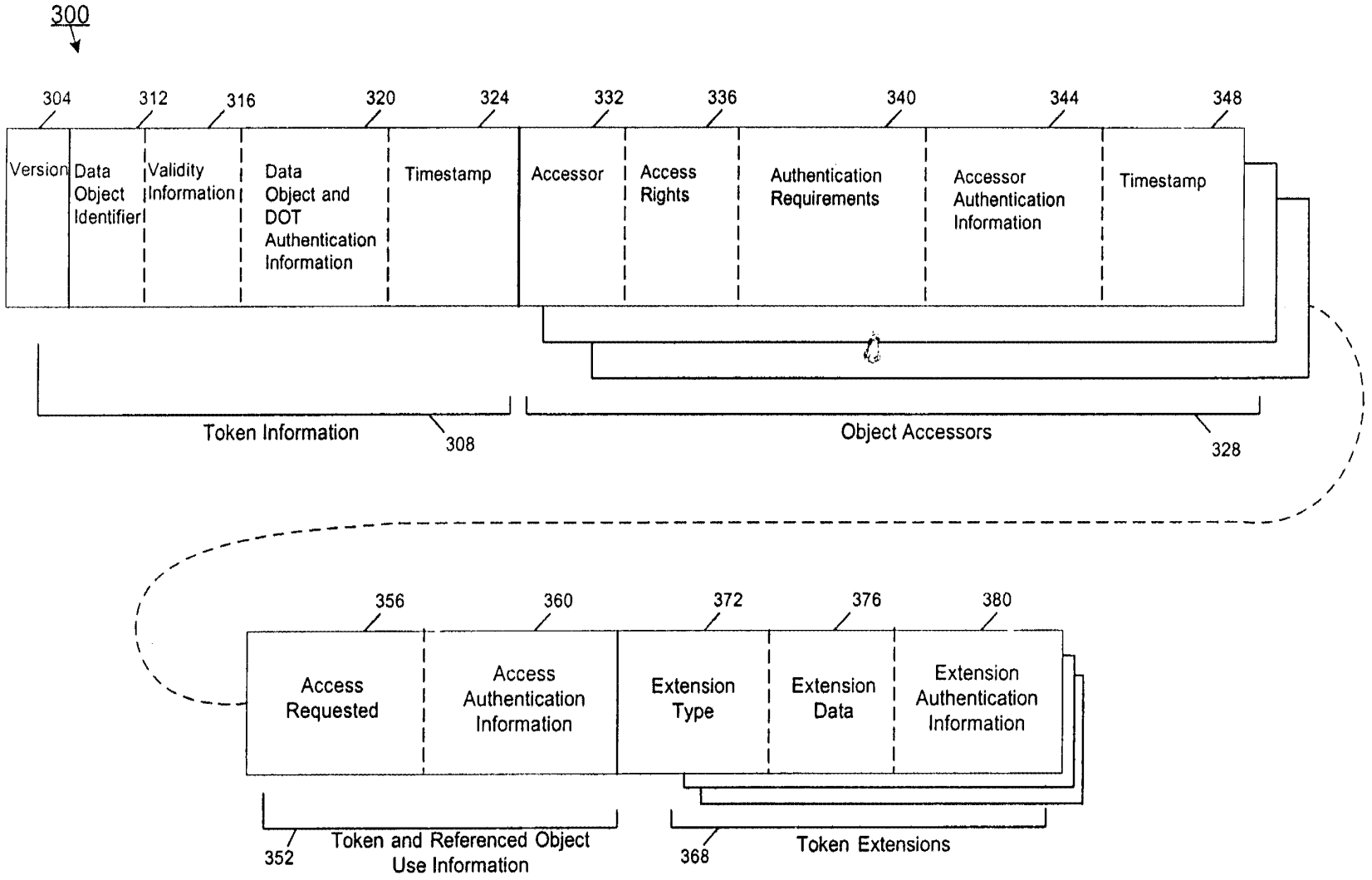


Figure 3

SUBSTITUTE SHEET (RULE 26)

410

```
DataObjectToken::= SEQUENCE {
        version         OCTET STRING,
        tokenInfo       DataObjectTokenInfo,
        accessors       DataObjectTokenAccessors,
        useInfo         DataObjectTokenUseInfo OPTIONAL,
        objectExt       DataObjectTokenExtensions OPTIONAL
        }
```

420

```
DataObjectTokenInfo ::= SEQUENCE {
        vdo_id          OCTET STRING,
        validFrom       UniversalTime,
        validTo         UniversalTime
        extAttributes   InfoExtAttributes,
        signerInfo      PKCS_7_SignerInfo,
                        // sig on previous
attributes
        signerCert      PKCS_6_Certificate,
        timeStamp       VerifiedTimeStamp,
        }

InfoExtAttributes ::= Attributes

Attributes ::= SET OF Attributes
Attribute ::= SEQUENCE {
        key     OCTET STRING,
        value OCTET STRING
        }
```

430

```
DataObjectTokenAccessors ::= SET OF
                        DataObjectTokenAccessor
DataObjectTokenAccessor ::= SEQUENCE {
        accessor                PKCS_6_Certificate,
        accessRights            AccessRights,
        authRequirements        AuthRequirements
        signerInfo              PKCS_7_SignerInfo,
        signerCert              PKCS_6_Certificate
        timestamp               VerifiedTimeStamp,
        }
```

440

```
AccessRights ::= SET OF AccessRight
AccessRight ::= SEQUENCE {
        type ENUMERATED {
                read_whole,
                read_partial,
                update_whole,
                update_partial,
                propagate_access_same,
                propagate_access_limited
                },
        extended UserObject     // extended info
                                   regarding
                                       partials/limited
        }
```

450

```
AuthRequirements ::= SET OF AuthRequirement
AuthRequirement ::= SEQUENCE {
        type ENUMEPATED {
                basic,          // certificate signature
                                   (always at least
                                   this)
                password,
                biometric,
                external_key,
                other
                },
        extended UserObject     // extended info
                                       regarding other
        }
```

Figure 4

510

```
DataObjectTokenUseInfo ::= SEQUENCE {
        accessRequested         Access,
        authentication          UserObject,
        accessorInfo                    PKCS_7_SignerInfo,
        accessorCert                    PKCS_6_Certificate
        }

Access ::= SEQUENCE {
        type ENUMERATED {
                read_whole,
                read_partial,
                update_whole,
                update_partial
                },
        extended UserObject
                }
```

520

```
DataObjectTokenExtensions ::= SET OF DataObjectTokenExtension
DataObjectTokenExtension ::= SEQUENCE {
        extType         OCTET STRING,
        extData         UserObject,
        signerInfos     PKCS_7_SignerInfos,
        signerCerts     PKCS_6_Certificates
        }

PKCS_7_SignerInfos ::= SET OF PKCS_7_SignerInfo
PKCS_6_Certificates ::= SET OF PKCS_6_Certificate
```

Figure 5

SUBSTITUTE SHEET (RULE 26)

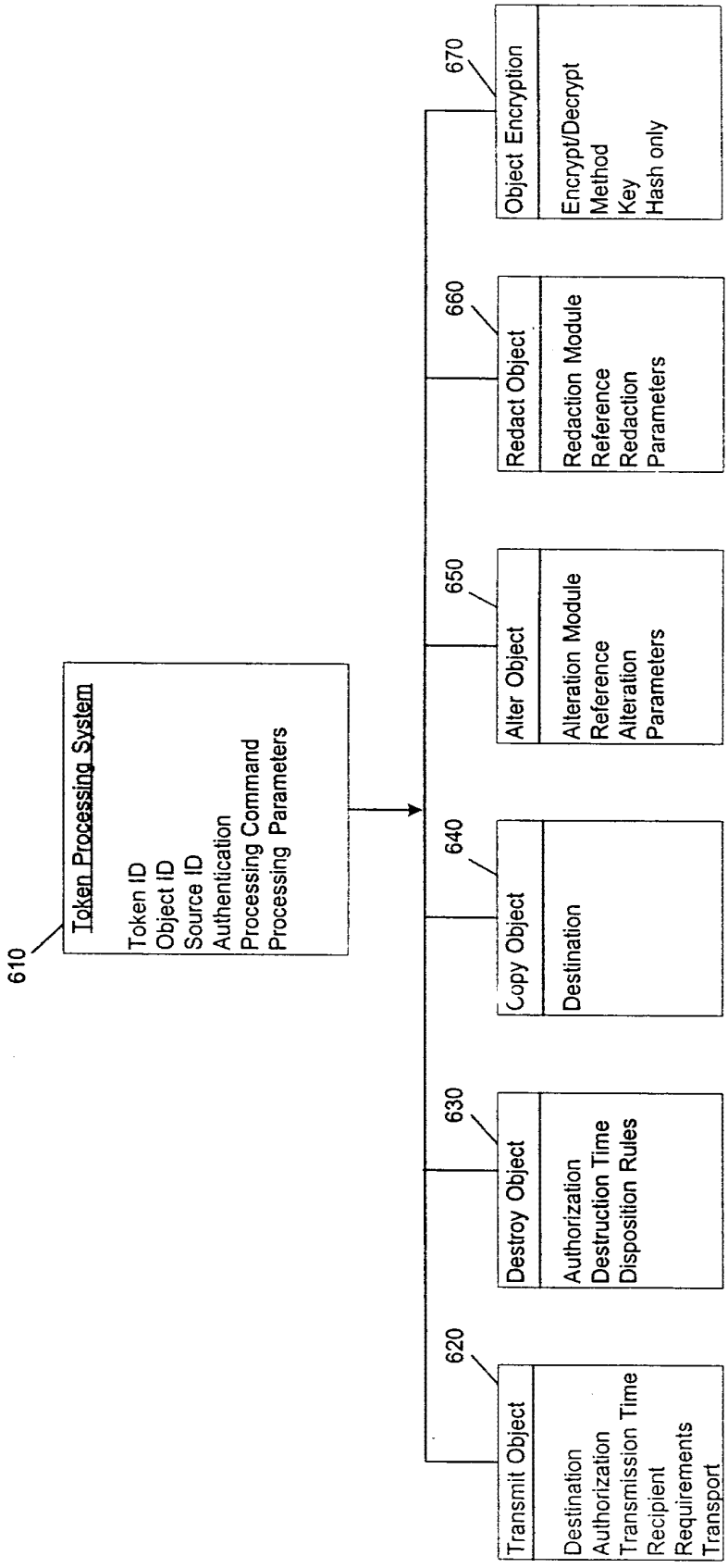


Figure 6

Partial Token Based Data Processing System Command Table

EX. 1002, Page 2314

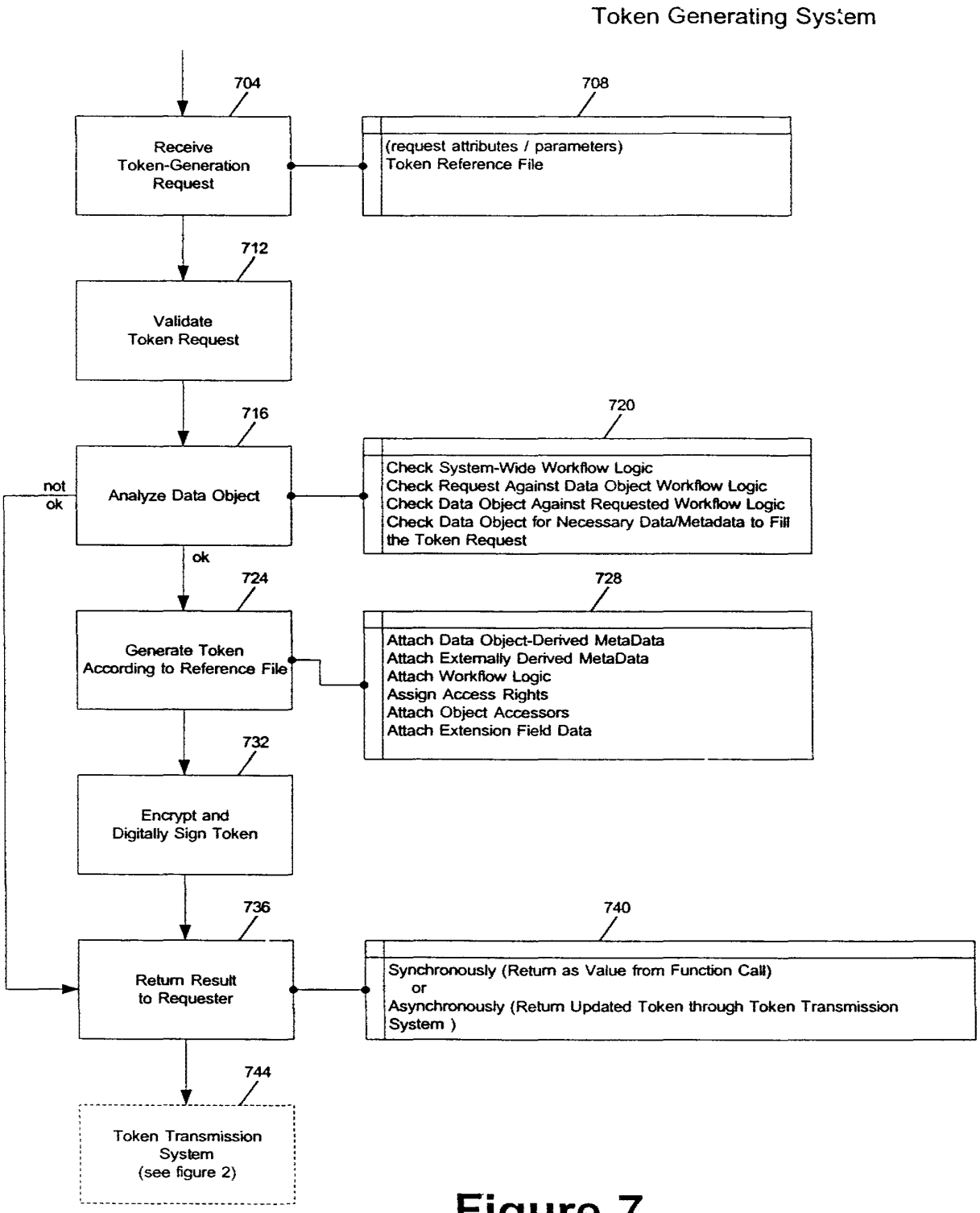

Token Generating System
704
Receive Token-Generation Request
708
(request attributes / parameters)
Token Reference File
712
Validate Token Request
716
Analyze Data Object
not ok
ok
720
Check System-Wide Workflow Logic
Check Request Against Data Object Workflow Logic
Check Data Object Against Requested Workflow Logic
Check Data Object for Necessary Data/Metadata to Fill the Token Request
724
Generate Token According to Reference File
728
Attach Data Object-Derived MetaData
Attach Externally Derived MetaData
Attach Workflow Logic
Assign Access Rights
Attach Object Accessors
Attach Extension Field Data
732
Encrypt and Digitally Sign Token
736
Return Result to Requester
740
Synchronously (Return as Value from Function Call)
or
Asynchronously (Return Updated Token through Token Transmission System)
744
Token Transmission System
(see figure 2)

Figure 7

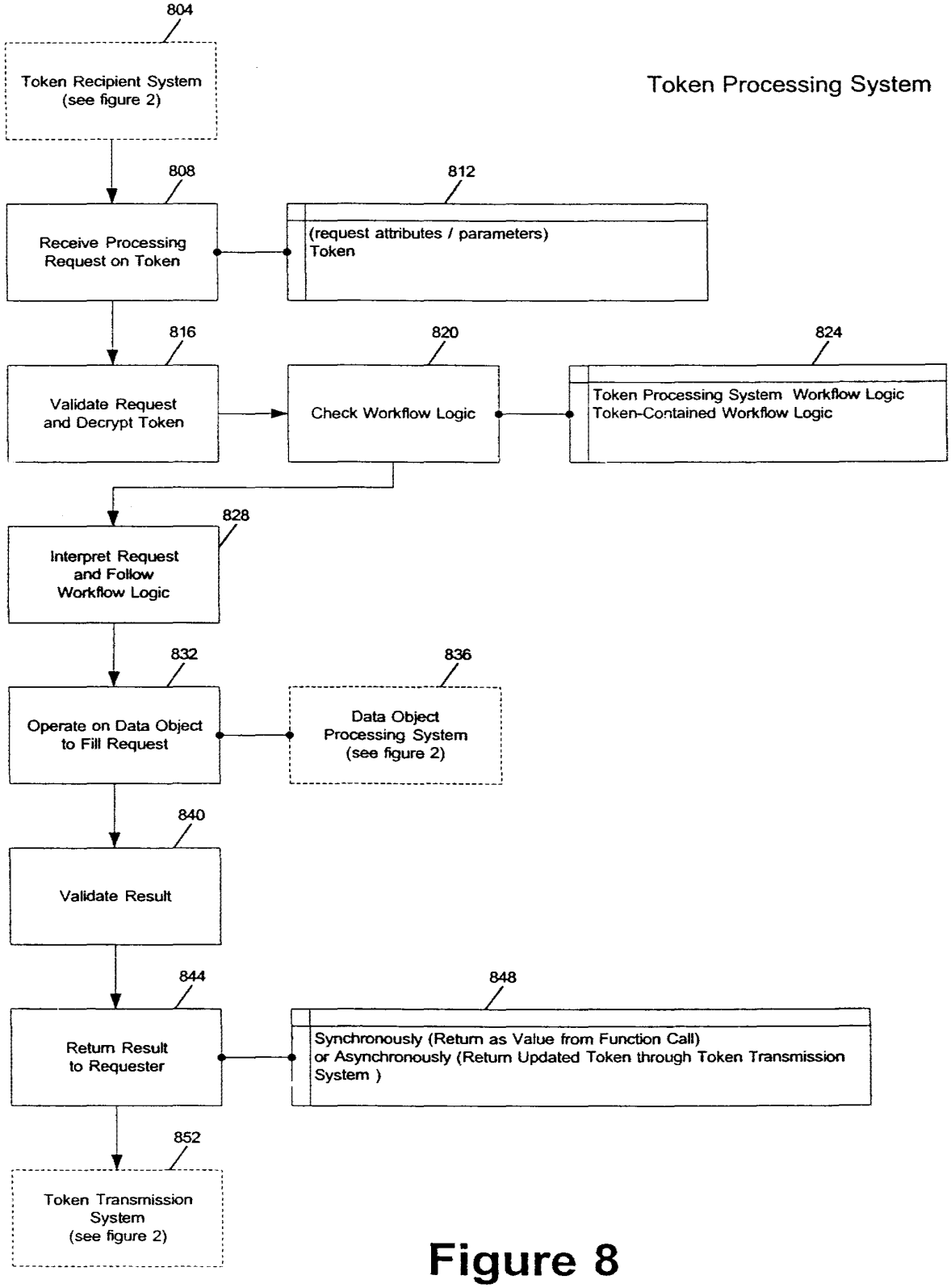

804
Token Recipient System
(see figure 2)
Token Processing System
808
Receive Processing
Request on Token
812
(request attributes / parameters)
Token
816
Validate Request
and Decrypt Token
820
Check Workflow Logic
824
Token Processing System Workflow Logic
Token-Contained Workflow Logic
828
Interpret Request
and Follow
Workflow Logic
832
Operate on Data Object
to Fill Request
836
Data Object
Processing System
(see figure 2)
840
Validate Result
844
Return Result
to Requester
848
Synchronously (Return as Value from Function Call)
or Asynchronously (Return Updated Token through Token Transmission
System)
852
Token Transmission
System
(see figure 2)

Figure 8

9/9

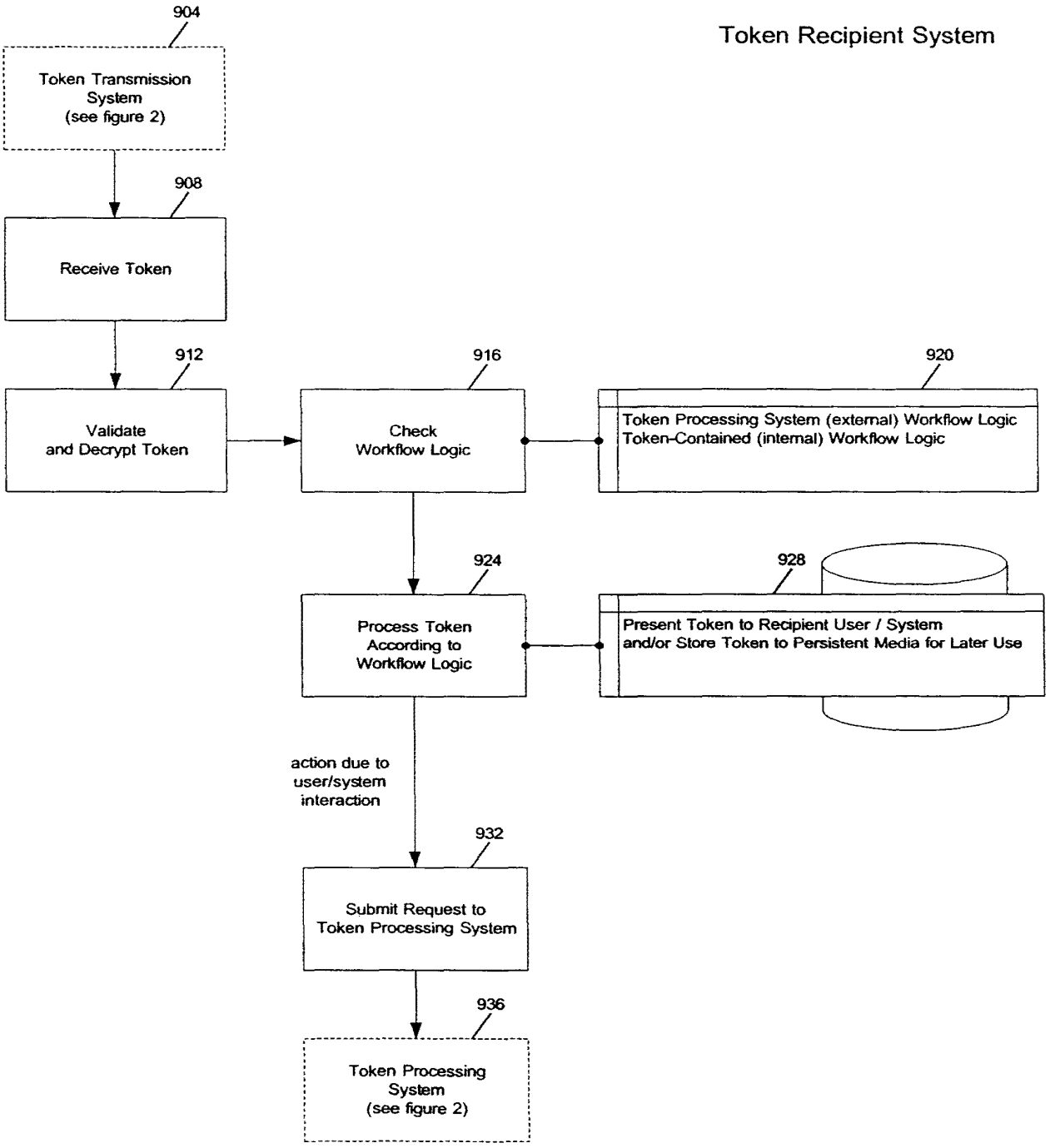

Token Recipient System
904
Token Transmission System (see figure 2)
908
Receive Token
912
Validate and Decrypt Token
916
Check Workflow Logic
920
Token Processing System (external) Workflow Logic
Token-Contained (internal) Workflow Logic
924
Process Token According to Workflow Logic
928
Present Token to Recipient User / System and/or Store Token to Persistent Media for Later Use
action due to user/system interaction
932
Submit Request to Token Processing System
936
Token Processing System (see figure 2)

Figure 9

Electronic Patent Application Fee Transmittal

Application Number:	12453124
Filing Date:	29-Apr-2009
Title of Invention:	Digital information infrastructure and method
First Named Inventor/Applicant Name:	Ron M. Redlich
Filer:	Robert C. Kain
Attorney Docket Number:	6851-08-cip

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:	10127453
Application Number:	12453124
International Application Number:	
Confirmation Number:	8996
Title of Invention:	Digital information infrastructure and method
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	04897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-08-cip
Receipt Date:	19-MAY-2011
Filing Date:	29-APR-2009
Time Stamp:	14:39:54
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$555
RAM confirmation Number	912
Deposit Account	031231
Authorized User	

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 1.21 (Miscellaneous fees and charges)

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	6851-08-cip-Amdt-1st-20110516-trans.pdf	18586 73297e0e761a882248ded97c1158efa9845fd609	no	1
Warnings:					
Information:					
2	Abstract	6851-08-cip-Amdt-1st-20110516-abstr.pdf	15431 09101d4e5672c47f8dfd7b6e56c698b3657e1e88	no	1
Warnings:					
Information:					
3	Abstract	6851-08-cip-Amdt-1st-20110516-title.pdf	13494 63fea8a826e8aa79bd88f1121961777cfbae7f84	no	1
Warnings:					
Information:					
4	Specification	6851-08-cip-Amdt-1st-20110516-spec.pdf	17849 4d5c547850fd47a37a4fb86905557187eff5297d	no	1
Warnings:					
Information:					
5	Claims	6851-08-cip-Amdt-1st-20110516-clms.pdf	20760 aa382bd1449bd6dbe039f81f649284802609a2de	no	3
Warnings:					
Information:					
6	Applicant Arguments/Remarks Made in an Amendment	6851-08-cip-Amdt-1st-20110516-rem.pdf	38259 374459f66bc2bb7341fc847b634b32cbea9d5efb	no	7
Warnings:					
Information:					
7	Extension of Time	6851-08-cip-Req-Time-3mth-20110516.pdf	19610 78f387244df72e27e56735953f81e415eb5727de	no	1
Warnings:					
Information:					
8	Information Disclosure Statement (IDS) Filed (SB/08)	6851-08-cip-Ids-form1449.pdf	59892 8876de31de0ab911541a36259caac2689fafa638	no	3
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					

9	Information Disclosure Statement (IDS) Filed (SB/08)	6851-08-cip-WO2000075779A2.pdf	1933640 7051c47fd086058576395e872c385be7922f0965	no	52
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
10	Fee Worksheet (PTO-875)	fee-info.pdf	29939 c15be79d0366ae2d7ee2b79a1e0c324a62be0e0c	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	2167460		

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.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
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	Filing Date	☐ To be Mailed
12/453,124	04/29/2009	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ 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), (i), 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 $ =		OR	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

AMENDMENT	05/19/2011	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 4	Minus	** 20	= 0	X $26 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $110 =	0	OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)	OR	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	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:
/TONGELINA TUBBS/

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.

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.
12/453,124	04/29/2009	Ron M. Redlich	6851-08-cip	8996

4897 7590 09/19/2011

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

EXAMINER	
NAWAZ, ASAD M	
ART UNIT	PAPER NUMBER
2455	

NOTIFICATION DATE	DELIVERY MODE
09/19/2011	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.	Applicant(s)	
	12/453,124	REDLICH ET AL.	
	Examiner	Art Unit	
	ASAD NAWAZ	2455	

-- 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 *19 May 2011*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ 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

5)☒ Claim(s) *1-4* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☐ Claim(s) _____ is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☒ Claim(s) *1-4* are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ 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).

12)☐ 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

13)☐ 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)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is responsive to the remarks received 5/19/11

Election/Restrictions

Restriction to one of the following inventions is required under 35 U.S.C. 121:

I. Claims 1-2, drawn to withdrawing, classified in class 709, subclass 201.

II. Claim 3-4, drawn to reconstructing, classified in class 709, subclass 230.

The inventions are distinct, each from the other because of the following reasons:

Inventions I and II are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct if they do not overlap in scope and are not obvious variants, and if it is shown that at least one subcombination is separately usable. In the instant case, subcombination I has separate utility such as withdrawing while subcombination II is directed towards reconstraction. See MPEP § 806.05(d).

The examiner has required restriction between subcombinations usable together. Where applicant elects a subcombination and claims thereto are subsequently found allowable, any claim(s) depending from or otherwise requiring all the limitations of the allowable subcombination will be examined for patentability in accordance with 37 CFR 1.104. See MPEP § 821.04(a). Applicant is advised that if any claim presented in a continuation or divisional application is anticipated by, or includes all the limitations of, a claim that is allowable in the present application, such claim may be subject to provisional statutory and/or nonstatutory double patenting rejections over the claims of the instant application.

Restriction for examination purposes as indicated is proper because all these inventions listed in this action are independent or distinct for the reasons given above and there would be a serious search and/or examination burden if restriction were not required because at least the following reason(s) apply:

(a) the inventions have acquired a separate status in the art in view of their different classification;

(b) the inventions have acquired a separate status in the art due to their recognized divergent subject matter;

(c) the inventions require a different field of search (for example, searching different classes/subclasses or electronic resources, or employing different search queries);

(d) the prior art applicable to one invention would not likely be applicable to another invention;

(e) the inventions are likely to raise different non-prior art issues under 35 U.S.C. 101 and/or 35 U.S.C. 112, first paragraph.

.

Applicant is advised that the reply to this requirement to be complete must include (i) an election of a invention to be examined even though the requirement may be traversed (37 CFR 1.143) **and (ii) identification of the claims encompassing the elected invention**.

The election of an invention may be made with or without traverse. To reserve a right to petition, the election must be made with traverse. If the reply does not distinctly

and specifically point out supposed errors in the restriction requirement, the election shall be treated as an election without traverse. Traversal must be presented at the time of election in order to be considered timely. Failure to timely traverse the requirement will result in the loss of right to petition under 37 CFR 1.144. If claims are added after the election, applicant must indicate which of these claims are readable upon the elected invention.

Should applicant traverse on the ground that the inventions are not patentably distinct, applicant should submit evidence or identify such evidence now of record showing the inventions to be obvious variants or clearly admit on the record that this is the case. In either instance, if the examiner finds one of the inventions unpatentable over the prior art, the evidence or admission may be used in a rejection under 35 U.S.C. 103(a) of the other invention.

A telephone call was made to applicant's representative's main line on 9/12/11 to request an oral election to the above restriction requirement, but did not result in an election being made.

Applicant is reminded that upon the cancellation of claims to a non-elected invention, the inventorship must be amended in compliance with 37 CFR 1.48(b) if one or more of the currently named inventors is no longer an inventor of at least one claim remaining in the application. Any amendment of inventorship must be accompanied by a request under 37 CFR 1.48(b) and by the fee required under 37 CFR 1.17(i).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ASAD NAWAZ whose telephone number is (571)272-3988. The examiner can normally be reached on M-R 6-3:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. 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.

Asad M Nawaz
Primary Examiner
Art Unit 2455

/Asad M Nawaz/
Primary Examiner, Art Unit 2455

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12453124	REDLICH ET AL.
	Examiner	**Art Unit**
	ASAD M NAWAZ	2455

✓	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	11/07/2010	09/12/2011							
	1	✓	÷							
	2	✓	÷							
	3	✓	÷							
	4	✓	÷							

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

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

Serial No. 12/453,124

Examiner A. Nawaz

Confirmation No.: 8996

Group Art 2445

Filed: April 29, 2009

For: Digital Information Infrastructure and Method
for Security Designated Data and with Granular Data Stores (as amended)

RESTRICTION RESPONSE

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

This is a response to the Office Action dated October 19, 2011. A request to extend time to respond for three (3) months is enclosed ($635.00 fee). Please charge Deposit Account No. 03-1231 for the $635.00 fee. Applicant is a small entity. Please debit or credit Deposit Account No. 03-1231 for any underpayment or overpayment. Applicant elects claims 3 and 4 (reconstruction). This response includes:

(a) Transmittal (1 pg., p. 1)
(b) Claims (2 pgs., pp. 2 - 3)
(c) Request for Extension of Time (1 pg.)

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

CLAIMS

1. (withdrawn) A method of organizing and processing data in a distributed computing system, the data to be processed having select content represented by one or more predetermined words, characters, images, data elements or data objects, said distributed computing system having (a) a plurality of select content data stores in a server cloud for respective ones of a plurality of security designated data and (b) a plurality of granular data stores, each said select content data store and granular data store having respective access controls thereat which restrict access to data in the respective data store, said plurality of data stores in said server cloud being operatively coupled over a communications network, the method of organizing and processing data comprising:

extracting and storing said security designated data in respective select content data stores of said server cloud;

parsing remainder data not extracted from said data to be processed and storing the parsed data as data segments in respective granular data stores;

withdrawing some or all of said security designated data and said parsed data segments in respective data stores upon presentation of said respective access controls applied to said data stores in said server cloud.

2. (withdrawn) The method of organizing and processing data as claimed in claim 1 including applying a monetization algorithm to said security designated data based upon non-secure availability of said security designated data and generating and assigning either a financial value to said security designated data or generating and assigning a risk-release value to said security designated data.

3. (previously amended) A distributed computer system for organizing and processing data having, the data to be processed having select content represented by one or more predetermined

words, characters, images, data elements or data objects, said distributed computing system having (a) a plurality of select content data stores in a server cloud for respective ones of a plurality of security designated data and (b) a plurality of granular data stores, each said select content data store and granular data store having respective access controls thereat, said plurality of data stores and said server cloud operatively coupled over a communications network, comprising:

means for identifying plurality of select content data stores for respective ones of a plurality of security designated data in said server cloud,

an extractor for extracting and storing said security designated data in respective select content data stores of said server cloud;

a processor activating at least one of said select content data stores in said server cloud thereby permitting access to said select content data stores and respective security designated data based upon an application of one or more of said access controls thereat;

means for parsing remainder data not extracted from said data to be processed and storing the parsed data as data segments in respective granular data stores;

said processor having means for applying a reconstruction data process employing said respective access controls to combine one or more of said security designated data and remainder data.

4. (previously amended) The distributed computer system for organizing and processing data as claimed in claim 3 including means for applying a monetization algorithm to said security designated data based upon non-secure availability of said security designated data and means for generating and assigning either a financial value to said security designated data or generating and assigning a risk-release value to said security designated data.

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

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

Serial No. 12/453,124

Examiner A. Nawaz

Confirmation No.: 8996 Group Art 2445

Filed: April 29, 2009

For: Digital Information Infrastructure and Method

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 $635.00 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.

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

fG:\RCK\CLIENTS\Redlich\6851-08-cip-Req-Time-3mth-20120314.wpd

Electronic Patent Application Fee Transmittal

Application Number:	12453124
Filing Date:	29-Apr-2009
Title of Invention:	Digital information infrastructure and method
First Named Inventor/Applicant Name:	Ron M. Redlich
Filer:	Robert C. Kain
Attorney Docket Number:	6851-08-cip

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	635	635

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**635**

Electronic Acknowledgement Receipt

EFS ID:	12300791
Application Number:	12453124
International Application Number:	
Confirmation Number:	8996
Title of Invention:	Digital information infrastructure and method
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	4897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-08-cip
Receipt Date:	14-MAR-2012
Filing Date:	29-APR-2009
Time Stamp:	12:54:36
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$635
RAM confirmation Number	10631
Deposit Account	031231
Authorized User	

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 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	6851-08-cip-Amdt-2d-20120314-trans.pdf	23469 312d54d8ff45f178d3951d66ba1419fadd6ec59b	no	1
Warnings:					
Information:					
2	Claims	6851-08-cip-Amdt-2d-20120314-clms.pdf	63956 047aea9bf3d810b4f8fc4aea6108934e0dac146d	no	2
Warnings:					
Information:					
3	Extension of Time	6851-08-cip-Req-Time-3mth-20120314.pdf	19889 66852b398377cc5db5ef1a73c86c233cf4ffba5b2	no	1
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	30046 5e82bd60086210ee1a560e181f72b25941445606	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	137360		

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.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
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	Filing Date	☐ To be Mailed
12/453,124	04/29/2009	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ 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), (i), 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 $ =		OR	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

AMENDMENT	03/14/2012	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 4	Minus	** 20	= 0	X $30 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $125 =	0	OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)	OR	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	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:
/CRYSTAL QUEEN/

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: 04/05/2012

RWIMBUSH SALE #00000001 Mailroom Dt: 03/14/2012 031231 12453124
01 FC : 2255 710.00 DA

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.
12/453,124	04/29/2009	Ron M. Redlich	6851-08-cip	8996

4897 7590 08/10/2012

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

EXAMINER	
LAZARO, DAVID R	
ART UNIT	PAPER NUMBER
2455	

NOTIFICATION DATE	DELIVERY MODE
08/10/2012	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.	Applicant(s)	
	12/453,124	REDLICH ET AL.	
	Examiner	Art Unit	
	DAVID LAZARO	2455	

-- 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 *14 March 2012*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ 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

5)☒ Claim(s) *1-4* is/are pending in the application.

5a) Of the above claim(s) *1 and 2* is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *3-4* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *29 April 2009* 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).

12)☐ 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

13)☐ 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)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *5/19/11*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to the election filed 03/14/12.

Election/Restrictions

2. Applicant's election of Claims 3 and 4 in the reply filed on 03/14/12 is acknowledged. Because applicant did not distinctly and specifically point out the supposed errors in the restriction requirement, the election has been treated as an election without traverse (MPEP § 818.03(a)).

Double Patenting

3. 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).

4. Claim 3 is rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 2, 29, 30, 47, 48, 72 and 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 of the following:

5. Claims 1, 2, 29, 30, 47, 48, 72 and 73 of U.S. patent 7,140,044 contain every element of claims 3 of the instant application and thus anticipate the claims of the instant application (see comparison table below). Claims 3 of the instant application therefore are not patently distinct from the earlier patent claims and as such are unpatentable over obvious-type double patenting. A later patent/application claim is not patentably distinct from an earlier claim if the later claim is anticipated by the earlier claim. "*A later patent claim is not patentably distinct from an earlier patent claim if the*

later claim is obvious over, or anticipated by, the earlier claim." In re Longi, 759 F.2d at 896, 225 USPQ at 651.

Claim 3	**US 7,140,044**
the data to be processed having select content represented by one or more predetermined words, characters, images, data elements or data objects	Said data having one or more sensitive words, data objects, characters or icons
(a) a plurality of select content data stores in a server cloud for respective ones of a plurality of security designated data and	A plurality of computers interconnected together…each of said plurality of computers having a memory therein, respective memories designated as a remainder stored and respective extract stores in one or more computers of said plurality
(b) a plurality of granular data stores, each said select content data store and granular data store having respective access controls thereat,	A plurality of computers interconnected together…each of said plurality of computers having a memory therein, respective memories designated as a remainder stored and respective extract stores in one or more computers of said plurality Establishing and managing..security levels Plurality of users having corresponding plurality of security levels each with respective security clearance and respective extract store
said plurality of data stores and said server cloud operatively coupled over a communications network, comprising:	A plurality of computers interconnected together…each of said plurality of computers having a memory therein, respective memories designated as a remainder stored and respective extract stores in one or more computers of said plurality
means for identifying plurality of select content data stores for respective ones of a plurality of security designated data in	each of said plurality of computers having a memory therein, respective memories designated as…respective extract stores

said server cloud,	in one or more computers of said plurality and storing said subsets of extracted data…in said respective extract stores
an extractor for extracting and storing said security designated data in respective select content data stores of said server cloud;	Extracting said security sensitive words…to obtain subsets of remainder data… Storing said subjects of extracted data…in said respected extract stores
a processor activating at least one of said select content data stores in said server cloud thereby permitting access to said select content data stores and respective security designated data based upon an application of one or more of said access controls thereat;	Establishing and managing..security levels Plurality of users having corresponding plurality of security levels each with respective security clearance and respective extract store Permitting reconstruction of…said subset of extract data...in the presence of a predetermined security clearance of said plurality of security levels.
means for parsing remainder data not extracted from said data to be processed and storing the parsed data as data segments in respective granular data stores;	Filtering..to obtain remainder data Storing.. said remainder data in ..said remainder store, respectively
said processor having means for applying a reconstruction data process employing said respective access controls to combine one or more of said security designated data and remainder data.	Establishing and managing..security levels Plurality of users having corresponding plurality of security levels each with respective security clearance and respective extract store Permitting reconstruction of…said subset of extract data and remainder data only in the presence of a predetermined security clearance of said plurality of security levels.

6. The examiner notes the above table can be used as a guide for the remaining double patenting rejection as each US Patent cited below uses similar claim language in relation to data stores/memories for extracted and remainder data, access controls/security levels with respective clearance, parsing/filtering remainder data, and reconstruction data process.

7. Claim 3 is rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-3, 16-18, 31, 43, 55, 63 of U.S. Patent No. 7,103,915. Although the conflicting claims are not identical, they are not patentably distinct from each other because of the following:

8. Claims 1-3, 16-18, 31, 43, 55, 63 of U.S. patent 7,103,915 contain every element of claims 3 of the instant application and thus anticipate the claims of the instant application. Claims 3 of the instant application therefore are not patently distinct from the earlier patent claims and as such are unpatentable over obvious-type double patenting. A later patent/application claim is not patentably distinct from an earlier claim if the later claim is anticipated by the earlier claim. "*A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, or anticipated by, the earlier claim.*" In re Longi, 759 F.2d at 896, 225 USPQ at 651.

9. Claim 3 is rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 15, 33, 47, 65, 79 of U.S. Patent No.

7,322,047. Although the conflicting claims are not identical, they are not patentably distinct from each other because of the following:

10. Claims 1, 15, 33, 47, 65, 79 of U.S. patent 7,322,047 contain every element of claims 3 of the instant application and thus anticipate the claims of the instant application. Claims 3 of the instant application therefore are not patently distinct from the earlier patent claims and as such are unpatentable over obvious-type double patenting. A later patent/application claim is not patentably distinct from an earlier claim if the later claim is anticipated by the earlier claim. "*A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, or anticipated by, the earlier claim.*" In re Longi, 759 F.2d at 896, 225 USPQ at 651.

11. Claim 3 is rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-3, 6, 10-14, 16-18, 21-24, 26 of U.S. Patent No. 7,348,987. Although the conflicting claims are not identical, they are not patentably distinct from each other because of the following:

12. Claims 1-3, 6, 10-14, 16-18, 21-24, 26 of U.S. patent 7,348,987 contain every element of claims 3 of the instant application and thus anticipate the claims of the instant application. Claims 3 of the instant application therefore are not patently distinct from the earlier patent claims and as such are unpatentable over obvious-type double patenting. A later patent/application claim is not patentably distinct from an earlier claim if the later claim is anticipated by the earlier claim. "*A later patent claim is not*

patentably distinct from an earlier patent claim if the later claim is obvious over, or anticipated by, the earlier claim." In re Longi, 759 F.2d at 896, 225 USPQ at 651.

13. Claim 3 is rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-4, 26-29, 51-53 of U.S. Patent No. 7,552,482. Although the conflicting claims are not identical, they are not patentably distinct from each other because of the following:

14. Claims 1-4, 26-29, 51-53 of U.S. patent 7,552,482 contain every element of claims 3 of the instant application and thus anticipate the claims of the instant application. Claims 3 of the instant application therefore are not patently distinct from the earlier patent claims and as such are unpatentable over obvious-type double patenting. A later patent/application claim is not patentably distinct from an earlier claim if the later claim is anticipated by the earlier claim. "*A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, or anticipated by, the earlier claim.*" In re Longi, 759 F.2d at 896, 225 USPQ at 651.

15. Claim 3 is rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 30, 39, 52, 79, 106, 133 of U.S. Patent No. 7,721,344. Although the conflicting claims are not identical, they are not patentably distinct from each other because of the following:

16. Claims 1, 30, 39, 52, 79, 106, 133 of U.S. patent 7,721,344 contain every element of claims 3 of the instant application and thus anticipate the claims of the

instant application. Claims 3 of the instant application therefore are not patently distinct from the earlier patent claims and as such are unpatentable over obvious-type double patenting. A later patent/application claim is not patentably distinct from an earlier claim if the later claim is anticipated by the earlier claim. "*A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, or anticipated by, the earlier claim.*" In re Longi, 759 F.2d at 896, 225 USPQ at 651.

Claim Rejections - 35 USC § 112

17. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

18. Claims 3-4 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

19. The following limitation of claim 3 invokes 35 U.S.C. 112, 6th paragraph:

"*means for identifying plurality of select content data stores for respective ones of a plurality of security designated data in said server cloud*"

20. The specification briefly mentions in the abstract an "identification module", however there is no further discussion of said module and no other particular structures discussed as performing the algorithm for the function of identifying a select data stores. It is not clear how the data stores are being selected and what corresponding structure performs said selection algorithm. As the specifications fails to clearly link the

corresponding structure to the claimed function of this 35 U.S.C. 112, 6th paragraph limitation, the scope of the claim is indefinite.

21. The following limitation of claim 3 invokes 35 U.S.C. 112, 6th paragraph:

"*an extractor for extracting and storing said security designated data in respective select content data stores of said server cloud*"

22. The corresponding structure appears to be found in section D.1, paragraphs 3070-3081. Accordingly this limitation is not at issue.

23. The following limitation of claim 3 invokes 35 U.S.C. 112, 6th paragraph:

"*means for parsing remainder data not extracted from said data to be processed and storing the parsed data as data segments in respective granular data stores"*

24. The corresponding structure and algorithm appears to be found in at least paragraphs 2907 and 3155. Accordingly this limitation is not at issue.

25. The remaining limitations do not invoke 35 U.S.C. 112, 6th paragraph as a structural term, "processor", is coupled with the functional language. Additionally, claim 4 appears to be supported by paragraphs 2254-2258.

Specification

26. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is

requested in correcting any errors of which applicant may become aware in the specification.

Claim Objections

27. Claim 3 objected to because of the following informalities: The first line has the language "…and processing data **having**, the data to be processed having". The bolded 'having' is unclear. Appropriate correction is required.

Information Disclosure Statement

28. The information disclosure statement (IDS) submitted on 5/29/11 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DAVID LAZARO whose telephone number is (571)272-3986. The examiner can normally be reached on 8:30-5:00 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. 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.

/David Lazaro/
Primary Examiner, Art Unit 2455

PTO/SB/42 (10-96)
Sheet 1 of 5

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 6851-08-cip	Application Number 12/453,124
Title: Digital Information Infrastructure and Method	Applicant(s) Ron M. Redlich, et al.	
	Filing Date April 29, 2009	Group Art Unit 2444

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
	WO 00/75779-A2	12/14/2000	PCT			

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

EXAMINER /David Lazaro/ DATE CONSIDERED 07/20/2012

G:\RCK\CLIENTS\Redlich\6851-08-cip-1-Form-PTO-1449.wpd

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DL/

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12453124	REDLICH ET AL.
	Examiner	Art Unit
	ASAD M NAWAZ	2455

SEARCHED			
Class	Subclass	Date	Examiner
709	ALL	11/7/10	AMN
707	ALL	11/7/10	AMN
713	ALL	11/7/10	AMN
705	ALL	11/7/10	AMN
709	225, 229, 246	7/20/2012	DRL
705	50-57	7/20/2012	DRL
726	26-30	7/20/2012	DRL
715	255	7/20/2012	

SEARCH NOTES		
Search Notes	Date	Examiner
East Search (USPAT; USPGPUB)	11/7/10	AMN
In depth Inventor Name Search for ODP	11/7/10	AMN
EAST update	7/20/2012	DRL

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L3	12	(US-7140044-$ or US-7103915-$ or US-7146644-$ or US-7191252-$ or US-7313825-$ or US-7322047-$ or US-7349987-$ or US-7552482-$ or US-7721344-$ or US-7669051-$ or US-7721345-$ or US-7958268-$).did.	USPAT	OR	OFF	2012/07/20 10:06
L4	0	3 and (monetization)	US-PGPUB; USPAT	OR	OFF	2012/07/20 10:06
L5	12	3 and (financial)	US-PGPUB; USPAT	OR	OFF	2012/07/20 10:06
L6	3	3 and (financial).clm.	US-PGPUB; USPAT	OR	OFF	2012/07/20 10:06
L7	38	("redlich, ron" "nemzow, martin").in.	US-PGPUB; USPAT	OR	OFF	2012/07/20 11:05
L8	31	L7 and ((security or sensitive) adj3 data).clm.	US-PGPUB; USPAT	OR	OFF	2012/07/20 11:05
L9	1	(12/453124).APP.	US-PGPUB; USPAT	OR	OFF	2012/07/20 11:06
L10	1	9 and identif$7 with data adj store	US-PGPUB; USPAT	OR	OFF	2012/07/20 11:08
L11	1	9 and identif$7 with (server or memory or storage or store)	US-PGPUB; USPAT	OR	OFF	2012/07/20 11:10
L12	0	9 and designat$3 with (data adj store)	US-PGPUB; USPAT	OR	OFF	2012/07/20 11:16
L13	1	9 and designat$3 with (location)	US-PGPUB; USPAT	OR	OFF	2012/07/20 11:16
L14	1	9 and pars$3 with remainder	US-PGPUB; USPAT	OR	OFF	2012/07/20 11:34
L15	595	extract$3 with (secur$3 or sensitive) with (objects words phrases numbers)	US-PGPUB; USPAT	OR	OFF	2012/07/20 11:51
L16	68	extract$3 with (secur$3 or sensitive) with (objects words phrases numbers) same (document or file)	US-PGPUB; USPAT	OR	OFF	2012/07/20 11:51
L17	32453	((709/225,229,246) or (705/50-57) or (726/26-30) or (715/255)).CCLS.	US-PGPUB; USPAT	OR	OFF	2012/07/20 11:55

L18	27	16 and 17	US-PGPUB; USPAT	OR	OFF	2012/07/20 11:55
S1	38	("redlich, ron" "nemzow, martin").in.	US-PGPUB; USPAT	OR	OFF	2012/06/03 09:46
S3	29	S1 and ((security or sensitive) adj3 data and extract$3 and remainder).clm.	US-PGPUB; USPAT	OR	OFF	2012/06/03 09:47
S4	27	S1 and ((security or sensitive) adj3 data and extract$3 with remainder).clm.	US-PGPUB; USPAT	OR	OFF	2012/06/03 09:48
S5	23	S1 and ((security or sensitive) adj3 data and extract$3 with remainder and reconstruct$3).clm.	US-PGPUB; USPAT	OR	OFF	2012/06/03 09:48

EAST Search History (Interference)

<This search history is empty>

7/20/2012 11:58:10 AM
C:\Users\dlazaro\Documents\EAST\Workspaces\12453124.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12453124	REDLICH ET AL.
	Examiner	Art Unit
	ASAD M NAWAZ	2455

✓	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	11/07/2010	09/12/2011	07/20/2012						
	1	✓	÷	N						
	2	✓	÷	N						
	3	✓	÷	✓						
	4	✓	÷	✓						

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

BIB DATA SHEET

CONFIRMATION NO. 8996

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
12/453,124	04/29/2009	709	2455	6851-08-cip

APPLICANTS

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

**** CONTINUING DATA ***************************

This application is a CIP of 11/746,440 05/09/2007
which claims benefit of 60/883,522 01/05/2007

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
05/15/2009

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /DAVID R LAZARO/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		FL	59	4	2

ADDRESS

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

TITLE

Digital information infrastructure and method

FILING FEE RECEIVED		
3310	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

UNITED STATES PATENT AND TRADEMARK OFFICE
COMMISSIONER FOR PATENTS
P.O.BOX 1450
ALEXANDRIA VA 22313-1451

PRESORTED
FIRST-CLASS MAIL
U.S. POSTAGE PAID
POSTEDIGITAL
NNNNN

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

Courtesy Reminder for
Application Serial No: 12/453,124

Attorney Docket No: 6851-08-cip
Customer Number: 4897
Date of Electronic Notification: 08/10/2012

This is a courtesy reminder that new correspondence is available for this application. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

An email notification regarding the correspondence was sent to the following email address(es) associated with your customer number:

rkain@complexip.com
ekotler@complexip.com

Please verify that these email addresses are correct.

To view your correspondence online or update your email addresses, please visit us anytime at **https://sportal.uspto.gov/secure/myportal/privatepair.** If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov or call 1-866-217-9197.

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

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

Serial No. 12/453,124

Examiner D. Lazaro

Confirmation No.: 8996 Group Art 2455

Filed: April 29, 2009

For: Digital Information Infrastructure and Method
for Security Designated Data and with Granular Data Stores (as amended)

AMENDMENT

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

This is a response to the Office Action dated August 10, 2012. A request to extend time to respond for three (3) months is enclosed ($645.00 fee) in addition to a Terminal Disclaimer ($80.00). Please charge Deposit Account No. 03-1231 for the $725.00 fee. Applicant is a small entity. Please debit or credit Deposit Account No. 03-1231 for any underpayment or overpayment. This response includes:

(a) Transmittal (1 pg., p. 1)
(b) Claims (3 pgs., pp. 2 - 4)
(c) Remarks (10 pgs., pp. 5 - 13)
(d) Request for Extension of Time (1 pg.)
(e) Terminal Disclaimer (3 pgs.)
[space left blank]

CLAIMS

1. (withdrawn) A method of organizing and processing data in a distributed computing system, the data to be processed having select content represented by one or more predetermined words, characters, images, data elements or data objects, said distributed computing system having (a) a plurality of select content data stores in a server cloud for respective ones of a plurality of security designated data and (b) a plurality of granular data stores, each said select content data store and granular data store having respective access controls thereat which restrict access to data in the respective data store, said plurality of data stores in said server cloud being operatively coupled over a communications network, the method of organizing and processing data comprising:

extracting and storing said security designated data in respective select content data stores of said server cloud;

parsing remainder data not extracted from said data to be processed and storing the parsed data as data segments in respective granular data stores;

withdrawing some or all of said security designated data and said parsed data segments in respective data stores upon presentation of said respective access controls applied to said data stores in said server cloud.

2. (withdrawn) The method of organizing and processing data as claimed in claim 1 including applying a monetization algorithm to said security designated data based upon non-secure availability of said security designated data and generating and assigning either a financial value to said security designated data or generating and assigning a risk-release value to said security designated data.

3. (currently amended) A distributed computer system for organizing and processing data, ~~having,~~ the data to be processed having select content represented by one or more predetermined words, characters, images, data elements or data objects, said distributed computing system having (a) a plurality of select content data stores in a server cloud for respective ones of a plurality of security designated data and (b) a plurality of granular data stores, each said select content data store and granular data store having respective access controls thereat, said plurality of data stores and said server cloud operatively coupled over a communications network, comprising:

means for identifying plurality of select content data stores for respective ones of a plurality of security designated data in said server cloud,

an extractor for extracting and storing said security designated data in respective select content data stores of said server cloud;

a processor activating at least one of said select content data stores in said server cloud thereby permitting access to said select content data stores and respective security designated data based upon an application of one or more of said access controls thereat;

means for parsing remainder data not extracted from said data to be processed and storing the parsed data as data segments in respective granular data stores;

said processor having means for applying a reconstruction data process employing said respective access controls to combine one or more of said security designated data and remainder data.

4. (previously amended) The distributed computer system for organizing and processing data as claimed in claim 3 including means for applying a monetization algorithm to said security designated data based upon non-secure availability of said security designated data and means for

generating and assigning either a financial value to said security designated data or generating and assigning a risk-release value to said security designated data.

REMARKS

This is a response to the Office Action dated August 10, 2012. A request for a three (3) month extension of time is enclosed.

In the Office Action on pages 2-9, the Patent Examiner rejects the patent claims 3 and 4 (claims 1 and 2 were sub-divided out by non-election) due to double patenting with respect to several patents. Applicant submits herewith a Terminal Disclaimer.

In the Office Action on pages 9-11, paragraphs 17-27, the Patent Examiner rejects claims 3 and 4 as being non-patentable under Section 112 and requests that the following claim elements be explained: (a) means for identifying select content stores in the server cloud; (b) extractor; and (c) means for parsing remainder data.

Claim 3 has been amended to correct the typographic error.

Part A

The Examiner requested the Applicant provide support for "means for identifying plurality of select content data stores for respective ones of a plurality of security designated data in said server cloud." This identification means is described in the following portions of the specification and is widely discussed in connection with multiple data stores or multiple storage facilities used for select content (SC) or security content (Sec-Con).

As for identifying Select Content data stores ("SC d-stores") in a server cloud, see the following portions of the specification.

para. 2495: - Dispersion

> 1. The location(s) for the remote primary storage of extracted information according to its clearance. 2. The process of securing, distributing, protecting, and anonymizing data by the extraction of identifying components from the source for separate storage or delivery. 3. A method for data storage and delivery where the constituents of the

whole are randomized and/or stored in separate locations requiring a directory or recovery script to restore into initial form. The scattered or diffused storage of critical and important information renders that information valueless without context, nearly impossible to match together correctly, and difficult to locate without a directory. In addition, the scattered or diffuse delivery (often by separate channels and types of delivery methods) of that same data for reconstitution protects the constituents of the whole from useful interception and contextual understanding. Microsoft calls this dissipation.

para. 013:

The select content is represented by one or more predetermined words, characters, images, data elements or data objects. The computing system has a plurality of select content data stores for respective ones of a plurality of enterprise designated categorical filters which include content-based filters, contextual filters and taxonomic classification filters, all operatively coupled over a communications network.

para. 015:

In this manner, security sensitive content is separately stored apart form the select content, which is stored in select content data stores.

para. 581:

It is a significant complication applicable to the architecture of security ecosystem design for the military or for business. DigitalDoors stores selections that are extracted in one, many, or distributed locations. Reconstitution can occur in steps (like defenses-in-depth), up to a predefined sensitivity level, or to full reconstitution. Because of this, starting and ending offsets as defined by the selection process, change as a function of selection priorities and positional precedence. Selections are not independent until DigitalDoors extracts them and creates a recovery file. Selection dispersion creates data independence by virtue of contextual dissociation; this can be further enhanced uniform data stores by creating random chaff. In other words, the position of all selections is a complex simultaneous choreography that depends on the selection and categorization of all prior selections.

para. 0582:

For example, selection priorities and positional precedence becomes important when extracting selections to create directory, recovery, and secured files.

para. 1406:

In addition, this technology retains the ability to call-back information and put the cat back into the bag, so to speak, by applying DigitalDoors reconstitution to minimize the reuse, repurposing, and redistribution of data stores of security-sensitive or privacy privileged personal data.

para. 2764:

Some key operations of the system and process follow. The invention organizes and processes data important to an enterprise operating the distributed computing system. The SC or select content is represented by one or more predetermined words, characters, images, data elements or data objects. The computing system has a plurality of select content data stores 7a-7e for respective ones of a plurality of enterprise designated categorical filters which include content- based filters, contextual filters and taxonomic classification filters, all operatively coupled over a communications network.

para. 2765:

This extracted security sensitive data is stored for the corresponding security level in a respective security sensitive extract store 6a, 6b or 6c. Remainder data is stored in the distributed computer system. Distribution of the data input 1A (FIG. A-3) with respect to said distributed computing system is limited based upon throughput from at least one of the enterprise designated SC filter 45 (e.g., patient privacy or HIPPA filter linked to SC store 76). The controlled release of corresponding extracted security sensitive data from the respective extract TS or S or C stores 6a-6c with the associated security clearances for corresponding security levels is permitted by the system. In this manner, security sensitive content is separately stored apart from the select content, which is stored in select content data stores 7a-7e and 8a.

para. 2778:

Distributed storage stores need less security then a centralized data repository for a number of reasons. First, the distributed storage stores hold only parts of the data and they are of lower interest to an attacker that will need to attack few dispersed stores to get the total content. Second, the stores are scattered and if hidden they call for less security. The need for less security means lower costs; more efficiency and less processing power. Thus dispersal of data to distributed storage stores is inherently "built in", "baked in" security. The split granular data pieces may be sent to distributed storage to be processed in an Information Dispersal Algorithm scheme. Each granular item will be split into n pieces, which will be sent to distributed storage. Reconstructed of a granular item will be enabled by access to M out ofN pieces. A directory/map connects all granular pieces recreate a partial or original document. Using the Information Dispersal Algorithm (IDA) with the present invention may deliver a much higher degree of security. The data stores may be correlated to the sec-con or SC content or maybe otherwise designated.

para. 2779:

A.7 Automatic Dispersal of Data to Remote Storage Locations. The present invention provides a system and method for the automatic dispersal of data to remote storage locations. Examples of these systems and methods are found in sections D.2 through D.14. Any document data stream created by a user may be automatically split

and transported to distributed storage locations. This may take several forms. One form is, when a file is being closed, it will automatically be split and its pieces sent automatically to distributed local or remote storage locations.

para. 2977:

> For select content systems having multiple levels of importance (which may be multiple security levels or multiple levels of SC importance in an organization or related to the organization, for example, primary competitors compared with secondary competitors), a plurality of filters would be created, each filter associated

with a different SC level. Further, multiple SC levels may require, remainder SC document or data stores (unknown data stores) and a plurality of extracted data stores. Multiple levels are similar to the MLS security content (sec-con) system described in section DA to D.9.

para. 3091:

> FIG. D-6 is an exemplary computer network diagram showing various user communities. It should be noted that select content SC data stores may be grouped for different portions of the same enterprise. Therefore, rather than have security groups as discussed herein, the system could provide SC interest groups in an enterprise. An "SC interest group" is the same as a security level group.

The specification describes the "means for identifying plurality of select content data stores

for respective ones of a plurality of security designated data in said server cloud" in section D.4 to

D.9. See para. 3086 below.

para. 3086:

> 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 (or select content) 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.

para. 3091:

> It should be noted that select content SC data stores may be grouped for different portions of the same enterprise. Therefore, rather than have security groups as discussed herein, the system could provide SC interest groups in an enterprise. ... 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 anyone or more of these stores.

Therefore, the specification does support the means for identifying respective data stores for respective select content. "Select Content" is "select content SC which may be of interest or importance to the enterprise." para. 010. "In this manner, security sensitive content is separately stored apart form the select content, which is stored in select content data stores." para. 015. "FIG. A-2 diagrammatically illustrates a basic information life cycle process or system wherein secure content (sec-con) and select content (SC) is separately stored per categorical filters operable by the enterprise." para. 018.

para. 2750:

> The present invention employs an extraction engine which identifies, selects and then extracts the security sensitive content (sec-con) or select content (SC), a classification engine that assists the user (the enterprise's CIO) to classify and organize the content, and a vibrant testing cycle to continually challenge the sec-con store, the sec-con security levels and the quality, breadth, depth and scope of the SC store. The classification engines can be used by the Chief Information Officer ("CIO") to establish information infrastructure policies and re-set the extraction engines to enforce the policies (data acquisition and handling rules) established thereby.
>
> Also, the deconstruction step uses Sec-Con and SC as discussed in para. 2754 and 2755.

Part B

The Examiner questions the support for "an extractor for extracting and storing said security designated data in respective select content data stores of said server cloud." This extractor, and the functions or steps to carry out the extraction is discussed below. As an example, see Section D.1 "Extractor Module." The Examiner should note that the extraction function is widely discussed in the specification. The extraction module is the hardware implementation of these extraction functions.

para. 2756:

The sys-admin may use the info infrastructure with an existing classification system and information policy, ruled-based or may have no pre-existing classification system for his or her documents. The infrastructure process 10 includes a classification generator module 24 which employs an SC extractor, a KE search engine to generate additional supplemental documents (supple docs) which the sys-admin may use the create the hierarchical taxonomic classification system. otherwise, the sys-admin may purchase taxonomic classifications commercially from others. ... Data requests 40 from others are input into access, permission, distribution, reconstruction control module 42. Features and functions for this module are discussed in sections B.7, B.8. e.9-e.14, e.20-e.23 and in the applications D.2 through D.14. The request for data may be an alarm function or may be a data request form another. The info infrastructure then cycles back to source doc 12, editor module 14 and extractor module 15.

para. 2923:

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.

Part C

Support for the "means for parsing remainder data not extracted from said data to be processed and storing the parsed data as data segments in respective granular data stores" is discussed below. See Section AA.4.6.2 Semantic Parsing Rules, para. 1441.

para. 050:

FIG. D-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. Encryption may include data compression and/or expansion or parsing techniques.

para. 120:

The parsing of granular content segments in a documents and/or data stream, can be done manually, automatically, or a combination of both. see also para. 188.

para. 1435:

However, dictionary categorization when combined with semantic parsing rules and pattern matching significantly increases the accuracy and enables full automation.

para. 2907:

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. Parsing is a contextual filter using a content as a marker and a range defines by certain file parameters. 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" (or SC) 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.

As for the "parse" function in the specification, see the following sections.

para. 135:

Incorporated with a trusted OS (for example a certified Trusted Solaris and a TCS guard) DigitaIDoors enables a user to divide a document into granular content segments, tagging and encrypting each of the newly parsed parts according to the classification level of its content (TS, S, C, U) and dispersing the tagged parts to different distributed (TS, S, C, U) storage locations throughout the enterprise. The different segments can also be tagged for users roles. (TS a, TS b, S a, etc.).

para. 1829:

The automated DigitaIDoors metasearch tool takes as source any data stream or document. The DigitalDoors Secure engine automatically parses the source for content recognition and assessment of granular content. This granular content is automatically metatagged for range, sensitivity level, compartmentalization, categories, relevancy, and other multitier overlapping hierarchical factors. The granularized data content becomes the search terms, while these metatags become metafilters for the DigitalDoors knowledge discovery.

para. 1831:

DigitaIDoors Secure is automatically run. The source (which is now the aggregated result from the extant tool processes) is automatically parsed by the DigitaIDoors Secure engine with secondary recognition and assessment of granular content. This granular content is automatically metatagged for range, sensitivity level, compartmentalization, categories, relevancy, and other multitier hierarchical factors.

para. 1922:

When an information data stream (that is, a document, file, message, audio, video, or compound metadata structure) is parsed into its separate components the context is broken. The value of information is contingent on structure, format, encoding, linguistic reference, and other factors. As a result, granularization and dispersion

enables security by similar mechanism to the one-time encryption pad. Although the one-time pad presumes a random seed, DigitalDoors approaches a level of randonmess for each granular content dispersion. Although there are some indications of context (location, language, storage facility, date, etc.), padding occurrence counts and chaff can generate any arbitrary level of statistical randonmess. Basically, all interpretations of the granular content are equally likely, thereby providing no special or usual meaning.

para. 2256:

DigitaIDoors Secure parses and classifies that plaintext document and optionally creates a monetary valuation for the baseline infonnation. Selection and extraction of crown jewels creates a redacted version and optionally creates another monetary valuation. The differences between a monetary valuation of the information at any point in this workflow expresses differing risk and valuation. It is not static.

para. 2831:

A.35 Storage of Separated Data Pieces in One Location. The invention provides a system and method for storing different data extracts in one storage location. The system and method stores extracts of a data stream in different memories within one storage location. There is a major difference between splitting a document or a data stream and placing its parts in one storage location and this invention, which deals with placing extracts of a document or a data stream in one storage location. This invention deals in a situation that a whole data asset was already parsed-and split into a "remainder" and "extracts". What is transferred to one storage location is not all the pieces of a whole document or data assets but partial part of the whole the "extracts." The storage location can be one computer one storage node or other medium that is located in one physical location. To overcome security risks, the extracts in the different memories within the one storage location may contain protective elements which make it very hard to match the different extracted pieces together to create an original data stream.

For the “parse” function, see para. 2907, 2929, 2958, 3155, 3157, 3160, and 3161.

Approval of claims 3 and 4 is respectfully requested.

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

K:\RCK\CLIENTS\Redlich\Patents\6851-08-cip-Amdt-3d-20130206.wpd

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

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

Serial No. 12/453,124

Examiner A. Nawaz

Confirmation No.: 8996 Group Art 2445

Filed: April 29, 2009

For: Digital Information Infrastructure and Method

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 $645.00 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.

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

fK:\RCK\CLIENTS\Redlich\6851-08-cip-Req-Time-3mth-20130206.wpd

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

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

Serial No. 12/453,124

Examiner D. Lazaro

Confirmation No.: 8996 Group Art 2455

Filed: April 29, 2009

For: Digital Information Infrastructure and Method
for Security Designated Data and with Granular Data Stores (as amended)

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. 7,349,987, Serial No. 10/155,192, filed May 23, 2002;
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; and
Serial No. 11/829207, filed September 6, 2007 (the captioned case)

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. 7,349,987, Serial No. 10/155,192, filed May 23, 2002;
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;

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. 7,349,987, Serial No. 10/155,192, filed May 23, 2002;
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; and

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: February 6, 2013

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

K:\RCK\CLIENTS\Redlich\6851-08-cip-Terminal-Disclaim-20130206.wpd

Electronic Patent Application Fee Transmittal

Application Number:	12453124
Filing Date:	29-Apr-2009
Title of Invention:	Digital information infrastructure and method
First Named Inventor/Applicant Name:	Ron M. Redlich
Filer:	Robert C. Kain
Attorney Docket Number:	6851-08-cip

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	645	645

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Statutory or terminal disclaimer	2814	1	80	80
		Total in USD ($)		**725**

Electronic Acknowledgement Receipt

EFS ID:	14897947
Application Number:	12453124
International Application Number:	
Confirmation Number:	8996
Title of Invention:	Digital information infrastructure and method
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	4897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-08-cip
Receipt Date:	07-FEB-2013
Filing Date:	29-APR-2009
Time Stamp:	09:50:17
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	$725
RAM confirmation Number	8297
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	6851-08-cip-Amdt-3d-20130206-trans.pdf	18642 d983b0d3001077ab4e4d70de041ca232ab88fafa	no	1
Warnings:					
Information:					
2	Claims	6851-08-cip-Amdt-3d-20130206-clms.pdf	18982 d1d748eb9016813174d393d0a4607835a9b0768d	no	3
Warnings:					
Information:					
3	Applicant Arguments/Remarks Made in an Amendment	6851-08-cip-Amdt-3d-20130206-rem.pdf	39020 47e8d775f18dcc2437c31b871caea3abfa957669	no	9
Warnings:					
Information:					
4	Extension of Time	6851-08-cip-Req-Time-3mth-20130206.pdf	26921 684b202c85c689cd2be1b4debfbf374f287943f9	no	1
Warnings:					
Information:					
5	Terminal Disclaimer Filed	6851-08-cip-Terminal-Disclaim-20130206.pdf	41506 545629a1c4dfed7d179b0cdb4c27be162c5899a9	no	3
Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	31640 33f6688930e730c3bcd18a03c55d4f80a50b0921	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	176711	

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.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
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	Filing Date	☐ To be Mailed
12/453,124	04/29/2009	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ 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), (i), 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 $ =		OR	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

AMENDMENT 02/07/2013	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 4	Minus	** 20	= 0	X $31 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $125 =	0	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)	OR	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	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:
/DAWN BREWER/

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.

Application Number	Application/Control No.	Applicant(s)/Patent under Reexamination	
	12/453,124	REDLICH ET AL.	

Document Code - DISQ	Internal Document – DO NOT MAIL

TERMINAL DISCLAIMER	☒ APPROVED	☐ DISAPPROVED
Date Filed : 07 FEB 2013	This patent is subject to a Terminal Disclaimer	

Approved/Disapproved by:

JAB

U.S. Patent and Trademark Office

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 02/19/2013

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

EXAMINER
LAZARO, DAVID R

ART UNIT	PAPER NUMBER
2455	

DATE MAILED: 02/19/2013

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/453,124	04/29/2009	Ron M. Redlich	6851-08-CIP	8996

TITLE OF INVENTION: DIGITAL INFORMATION INFRASTRUCTURE AND METHOD

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$885	$300	$0	$1185	05/20/2013

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)

4897 7590 02/19/2013

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

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/453,124	04/29/2009	Ron M. Redlich	6851-08-CIP	8996

TITLE OF INVENTION: DIGITAL INFORMATION INFRASTRUCTURE AND METHOD

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$885	$300	$0	$1185	05/20/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
LAZARO, DAVID R	2455	709-225000

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 _____

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.
12/453,124	04/29/2009	Ron M. Redlich	6851-08-CIP	8996

4897 7590 02/19/2013

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

EXAMINER	
LAZARO, DAVID R	

ART UNIT	PAPER NUMBER
2455	

DATE MAILED: 02/19/2013

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 0 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 0 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.

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.

Notice of Allowability	Application No.	Applicant(s)	
	12/453,124	REDLICH ET AL.	
	Examiner	Art Unit	
	DAVID LAZARO	2455	

-- 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 *the amendment filed 2/7/13*.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are *3 and 4*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .

4. ☐ 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.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ 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)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☒ Examiner's Amendment/Comment
6. ☐ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/David Lazaro/
Primary Examiner, Art Unit 2455

Allowable Subject Matter

1. Claims 3-4 are allowed.

2. The double patenting rejection is withdrawn based on the approved terminal disclaimer filed 02/7/13.

3. The 112 2nd rejection is withdrawn based on the identification of support for 112 6th limitations as identified in the 02/7/13 remarks.

4. The objection is withdrawn based on the amendment to claim 3.

5. This application is in condition for allowance except for the presence of claims directed to an invention non-elected without traverse. Accordingly, claims 1-2 been cancelled.

EXAMINER'S AMENDMENT

6. 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.

The application has been amended as follows:

Claims 1-2 are canceled.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DAVID LAZARO whose telephone number is (571)272-3986. The examiner can normally be reached on 8:30-5:00 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. 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.

/David Lazaro/
Primary Examiner, Art Unit 2455

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12453124	REDLICH ET AL.
	Examiner	Art Unit
	ASAD M NAWAZ	2455

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
709	ALL	11/7/10	AMN
707	ALL	11/7/10	AMN
713	ALL	11/7/10	AMN
705	ALL	11/7/10	AMN
709	225, 229, 246	7/20/2012	DRL
705	50-57	7/20/2012	DRL
726	26-30	7/20/2012	DRL
715	255	7/20/2012	DRL
709	225, 229, 246	2/10/2013	DRL
705	50-57	2/10/2013	DRL
726	26-30	2/10/2013	DRL
715	255	2/10/2013	DRL

SEARCH NOTES		
Search Notes	Date	Examiner
East Search (USPAT; USPGPUB)	11/7/10	AMN
In depth Inventor Name Search for ODP	11/7/10	AMN
EAST update	7/20/2012	DRL
EAST: USPAT, USPGPUB, EPO, JPO, DERWENT, IBM_TDB, FPRS - subject matter and inventor search	2/10/2013	DRL

INTERFERENCE SEARCH			
US Class/ CPC Symbol	**US Subclass / CPC Group**	**Date**	**Examiner**
709	225, 229, 246	2/10/2013	DRL
705	50	2/10/2013	DRL
726	26	2/10/2013	DRL
715	255	2/10/2013	DRL

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	35011	((709/225,229,246) or (705/50-57) or (726/26-30) or (715/255)).CCLS.	US-PGPUB; USPAT	OR	OFF	2013/02/10 15:39
L2	38	("redlich, ron" "nemzow, martin").in.	US-PGPUB; USPAT	OR	OFF	2013/02/10 15:39
L3	74	extract$3 with (secur$3 or sensitive) with (objects words phrases numbers) same (document or file)	US-PGPUB; USPAT	OR	OFF	2013/02/10 15:40
L4	27	1 and 3	US-PGPUB; USPAT	OR	OFF	2013/02/10 15:40
L5	612	reconstruct$3 with remainder	US-PGPUB; USPAT	OR	OFF	2013/02/10 15:41
L6	19	reconstruct$3 with remainder same pars$3	US-PGPUB; USPAT	OR	OFF	2013/02/10 15:41
L7	2059	granular near3 (stor$3)	US-PGPUB; USPAT	OR	OFF	2013/02/10 15:42
L8	34	5 and 7	US-PGPUB; USPAT	OR	OFF	2013/02/10 15:42
L9	4	extract$3 and pars$3 and reconstruct$3 and data and stor$3	FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/02/10 15:43

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L10	35011	((709/225,229,246) or (705/50-57) or (726/26-30) or (715/255)).CCLS.	US-PGPUB; USPAT	OR	OFF	2013/02/10 15:43
L11	35	(extract$3 and pars$3 and reconstruct$3 and data and stor$3).clm.	USPAT; UPAD	OR	OFF	2013/02/10 15:43
L12	6	10 and 11	USPAT; UPAD	OR	OFF	2013/02/10 15:43
L13	61	10 and (granular and access adj control and reconstruct$3)	USPAT; UPAD	OR	OFF	2013/02/10 15:44
L14	0	10 and (granular and access adj control and reconstruct$3).clm.	USPAT; UPAD	OR	OFF	2013/02/10 15:44
L15	5	10 and (access adj control and reconstruct$3).clm.	USPAT; UPAD	OR	OFF	2013/02/10 15:44

2/ 10/ 2013 3:45:18 PM
C:\ Users\ dlazaro\ Documents\ EAST\ Workspaces\ 12453124.wsp

Issue Classification

Application/Control No.	Applicant(s)/Patent Under Reexamination
12453124	REDLICH ET AL.
Examiner	**Art Unit**
DAVID LAZARO	2455

CPC						
Symbol					**Type**	**Version**
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			

CPC Combination Sets							
Symbol				**Type**	**Set**	**Ranking**	**Version**
			/				
			/				

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION										
CLASS	**SUBCLASS**	**CLAIMED**					**NON-CLAIMED**					
709	225	G	0	6	F	15 / 16 (2006.01.01)						
CROSS REFERENCE(S)												
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**											
709	229	246										
705	50											

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	2	
/DAVID LAZARO/ Primary Examiner.Art Unit 2455	02/10/2013	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	3	1A

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12453124	REDLICH ET AL.
	Examiner	**Art Unit**
	DAVID LAZARO	2455

726	26														
715	255														

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	2	
/DAVID LAZARO/ Primary Examiner.Art Unit 2455	02/10/2013	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	3	1A

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12453124	REDLICH ET AL.
	Examiner	**Art Unit**
	DAVID LAZARO	2455

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1														
	2														
1	3														
2	4														

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 2	
/DAVID LAZARO/ Primary Examiner.Art Unit 2455 (Primary Examiner)	02/10/2013 (Date)	O.G. Print Claim(s) 3	O.G. Print Figure 1A

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
12/453,124	04/29/2009	2455	3310	6851-08-CIP	4	2

CONFIRMATION NO. 8996

CORRECTED FILING RECEIPT

4897
ROBERT C. KAIN, JR.
KAIN & ASSOCIATES, ATTORNEYS AT LAW, P.A.
900 SOUTHEAST THIRD AVENUE, SUITE 205
FT LAUDERDALE, FL 33316



Date Mailed: 03/14/2013

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. 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 submit a written request for a Filing Receipt Correction. 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**

Inventor(s)

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

Applicant(s)

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

Power of Attorney:
Robert Kain Jr--30648

Domestic Priority data as claimed by applicant

This application is a CIP of 11/746,440 05/09/2007
which claims benefit of 60/883,522 01/05/2007

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 05/15/2009
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 12/453,124**
Projected Publication Date: Not Applicable
Non-Publication Request: No
Early Publication Request: No
**** SMALL ENTITY ****

Title

DIGITAL INFORMATION INFRASTRUCTURE AND METHOD FOR SECURITY DESIGNATED DATA AND WITH GRANULAR DATA STORES

Preliminary Class

709

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 AssetsControl, 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).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

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.
Kain & Associates, Attorneys at Law, P.A.
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)
03/15/2013	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12453124	04/29/2009	Ron M. Redlich	6851-08-cip	8996

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	$885	$300	$0	$1185	5/20/2013

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 03/15/2013

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:	12453124
Filing Date:	29-Apr-2009
Title of Invention:	DIGITAL INFORMATION INFRASTRUCTURE AND METHOD FOR SECURITY DESIGNATED DATA AND WITH GRANULAR DATA STORES
First Named Inventor/Applicant Name:	Ron M. Redlich
Filer:	Robert C. Kain
Attorney Docket Number:	6851-08-CIP

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	885	885
Publ. Fee- Early, Voluntary, or Normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**1185**

Electronic Acknowledgement Receipt

EFS ID:	15255866
Application Number:	12453124
International Application Number:	
Confirmation Number:	8996
Title of Invention:	DIGITAL INFORMATION INFRASTRUCTURE AND METHOD FOR SECURITY DESIGNATED DATA AND WITH GRANULAR DATA STORES
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	4897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-08-CIP
Receipt Date:	15-MAR-2013
Filing Date:	29-APR-2009
Time Stamp:	15:31:55
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	$1185
RAM confirmation Number	6081
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)	6851-08-cip-issue-fee-trans-031513-ss.pdf	73446 799cb56cec88170c56b0f842df0f4360952f6041	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	31836 cb747e3c4af0ccc5dd542f28f5aa55225e759aeb	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	105282	

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.
12/453,124	04/29/2009	Ron M. Redlich	6851-08-CIP	8996

4897 7590 03/29/2013

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

EXAMINER	
LAZARO, DAVID R	

ART UNIT	PAPER NUMBER
2455	

NOTIFICATION DATE	DELIVERY MODE
03/29/2013	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

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

Application No. : 12453124
Applicant : Redlich
Filing Date : 04/29/2009
Date Mailed : 03/29/2013

NOTICE TO FILE CORRECTED APPLICATION PAPERS

Notice of Allowance Mailed

This application has been accorded an Allowance Date and is being prepared for issuance. The application, however, is incomplete for the reasons below.

Applicant is given 2 month(s) from the mail date of this Notice, or the time remaining from the Notice of Allowance and Fee(s) Due, whichever is longer, within which to respond.

The informalities requiring correction are indicated in the attachment(s). If the informality pertains to the abstract, specification (including claims) or drawings, the informality must be corrected with an amendment in compliance with 37 CFR 1.121 (or, if the application is a reissue application, 37 CFR 1.173). Such an amendment may be filed after payment of the issue fee if limited to correction of informalities noted herein. See Waiver of 37 CFR 1.312 for Documents Required by the Office of Patent Publication, 1280 Off. Gaz. Patent Office 918 (March 23, 2004). In addition, if the informality is not corrected until after payment of the issue fee, for purposes of 35 U.S.C. 154(b)(1)(iv), "all outstanding requirements" will be considered to have been satisfied when the informality has been corrected. A failure to respond within the above-identified time period will result in the application being ABANDONED. **This period for reply is NOT extendable under 37 CFR 1.136(a).**

See attachment(s).

A copy of this notice MUST be returned with the reply. Please address response to "Mail Stop Issue Fee,Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450".

/Carlota Erana/
Publication Branch
Office of Data Management
(571) 272-4200

Application No. 12453124 **Drawings filed: 05/27/2009**

DRAWINGS AND BRIEF DESCRIPTION OF DRAWINGS IN NON-COMPLIANCE WITH 37 CFR 1.84(u)(1)

37 CFR 1.84(u)(1) states, "The different views must be numbered in consecutive Arabic numerals, starting with 1 … Partial views intended to form one complete view, on one or several sheets, must be identified by the same number followed by a capital letter. View numbers must be preceded by the abbreviation 'FIG.' "

Other methods of identification are improper, including Roman numerals (FIG. I, FIG, II, etc.) and alphabetic characters (FIG. A, FIG. B, etc.). Abbreviations and words other than "FIG." ("Illustration, 1" "Diagram 2," "Photo 3," etc.) are improper.

[X] Applicant must submit drawings that number the views using consecutive Arabic numerals.

[X] Applicant must amend the brief description of the drawings on Page(s) **28 to 32** of the specification to show consecutive Arabic numerals.

NOTE: Applicant is advised that the detailed description may voluntarily be amended to identify the drawings by Arabic numerals.

[ ] The drawing is continued onto a second page (or more) without proper labeling under 37 CFR 1.84(u)(1). FIG(s)

[ ] Applicant must submit drawings on which the view numbers are preceded by the abbreviation "FIG."

[ ] Applicant must amend the brief description of the drawings on Page(s) of the specification to show view numbers preceded by the abbreviation "FIG."

NOTE: Applicant is advised that the detailed description may voluntarily be amended to show view numbers preceded by the abbreviation "FIG."

Application No. 12453124

IDENTIFICATION OF SPECIFICATION/DRAWING INCONSISTENCIES

[X] On Page 30 of the specification there is a brief description of FIG. C-13C, but the drawings filed 05/27/2009 do not include a drawing with that designation. Applicant must respond either by supplying the omitted drawing or by amending the specification to remove all references to that drawing.

[ ] The drawings filed include FIG. , but the specification's brief description of the drawings does not describe a drawing with that designation. Applicant must respond either by amending the specification to add a brief description of that drawing or by correcting the drawings to remove the drawing in question.

[ ] Drawings are present in the application and are referred to in the detailed description of the invention, but the specification does not contain a brief description of the drawings as required by 37 CFR 1.74 and 37 CFR 1.77(b)(8).

[ ] Page of the specification refers to FIG. , but no drawing with that designation is described in the brief description of the drawings and no drawing with that designation is present in the application. Applicant must respond either by amending the specification to remove all references to that drawing, or by supplying that drawing and amending the specification to add a brief description of it.

[ ] OTHER:

[ ] COMMENTS:

Application No. 12453124 **Drawings filed: 05/27/2009**

IDENTIFICATION OF DRAWING DEFICIENCIES

- [ ] There is a hole or the image thereof within the illustration. FIG(s)
- [ ] The illustration is penetrated or traversed by a solid or broken line that is not intended to be part of the drawing, such as a dark line caused by a flaw in the copying process. FIG(s)
- [ ] An ink stamp or the image thereof obscures part of the illustration. FIG(s)
- [ ] The drawing is marred by black smudges, obliterations, or fax/copier marks (for example, speckles or dots in a substantial portion of the drawing). FIG(s)
- [ ] Figure numbers are duplicated or missing. FIG(s)
- [ ] Drawing sheet or figure is missing. FIG(s)
- [X] Numbers, letters, or reference characters in the drawing have been crossed out or are illegibly handwritten. FIG(s) a-2
- [ ] The character of the lines, numbers, and letters is poor. FIG(s)
- [ ] The drawing's background shows that the original drawing was made on graph paper or other paper with a pattern or decoration. FIG(s)
- [ ] The FIG. number label is placed in a location that causes the drawing to be read upside down. FIG(s)
- [ ] Data, a reference number, or part of the drawing is truncated or missing, or a lead line has no reference number. FIG(s)
- [ ] The drawing and/or the FIG. label contain(s) foreign language. FIG(s)
- [ ] This utility application contains a photograph of a view that is capable of being illustrated as a line drawing. FIG(s)
- [ ] A petition under 37 CFR 1.84(a)(2) to accept color drawings has been granted, but the brief description of the drawings in the specification does not contain (or has not been amended to contain) the paragraph required by 37 CFR 1.84(a)(2)(iii).
- [ ] This reissue application contains amended drawings that are not labeled as "Amended" as required by 37 CFR 1.173(b)(3). FIG(s)
- [ ] OTHER:
- [X] COMMENTS:
Fig. A-2 reference no. '7d', please verify if there is a letter missing in the word "Compete".

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

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

Serial No. 12/453,124

Examiner D. Lazaro

Confirmation No.: 8996 Group Art 2455

Filed: April 29, 2009

For: Digital Information Infrastructure and Method
for Security Designated Data and with Granular Data Stores (as amended)

NOTICE OF FILING MARKED DRAWINGS SHOWING CORRECTIONS

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

Pursuant to 37 C.F.R. sec. 1.85, Applicant hereby submits a marked version of the drawings showing corrections. No new matter is added to these drawings.

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

K:\RCK\CLIENTS\Redlich\Patents\6851-08-cip-Sub-Spec-Notice-File-Marked-Dwgs-20130430.wpd

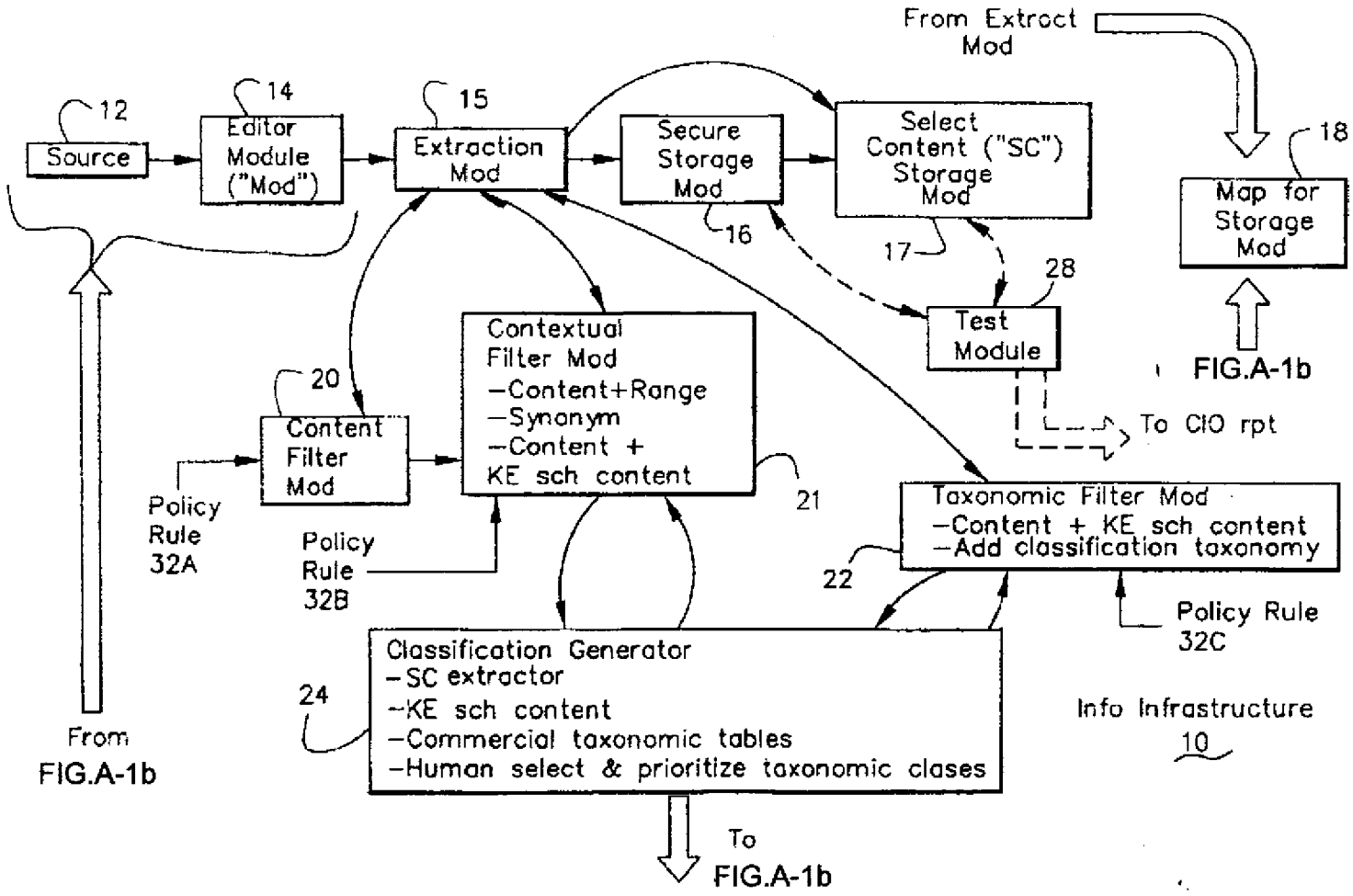

From Extract Mod
12
Source
14
Editor Module ("Mod")
15
Extraction Mod
Secure Storage Mod
16
Select Content ("SC") Storage Mod
17
18
Map for Storage Mod
28
Test Module
FIG.A-1b
To CIO rpt
20
Content Filter Mod
Contextual Filter Mod
-Content+Range
-Synonym
-Content + KE sch content
21
Policy Rule 32A
Policy Rule 32B
Taxonomic Filter Mod
-Content + KE sch content
-Add classification taxonomy
22
Policy Rule 32C
Classification Generator
-SC extractor
-KE sch content
-Commercial taxonomic tables
-Human select & prioritize taxonomic clases
24
Info Infrastructure
10
From FIG.A-1b
To FIG.A-1b

FIG.A-1a

1a

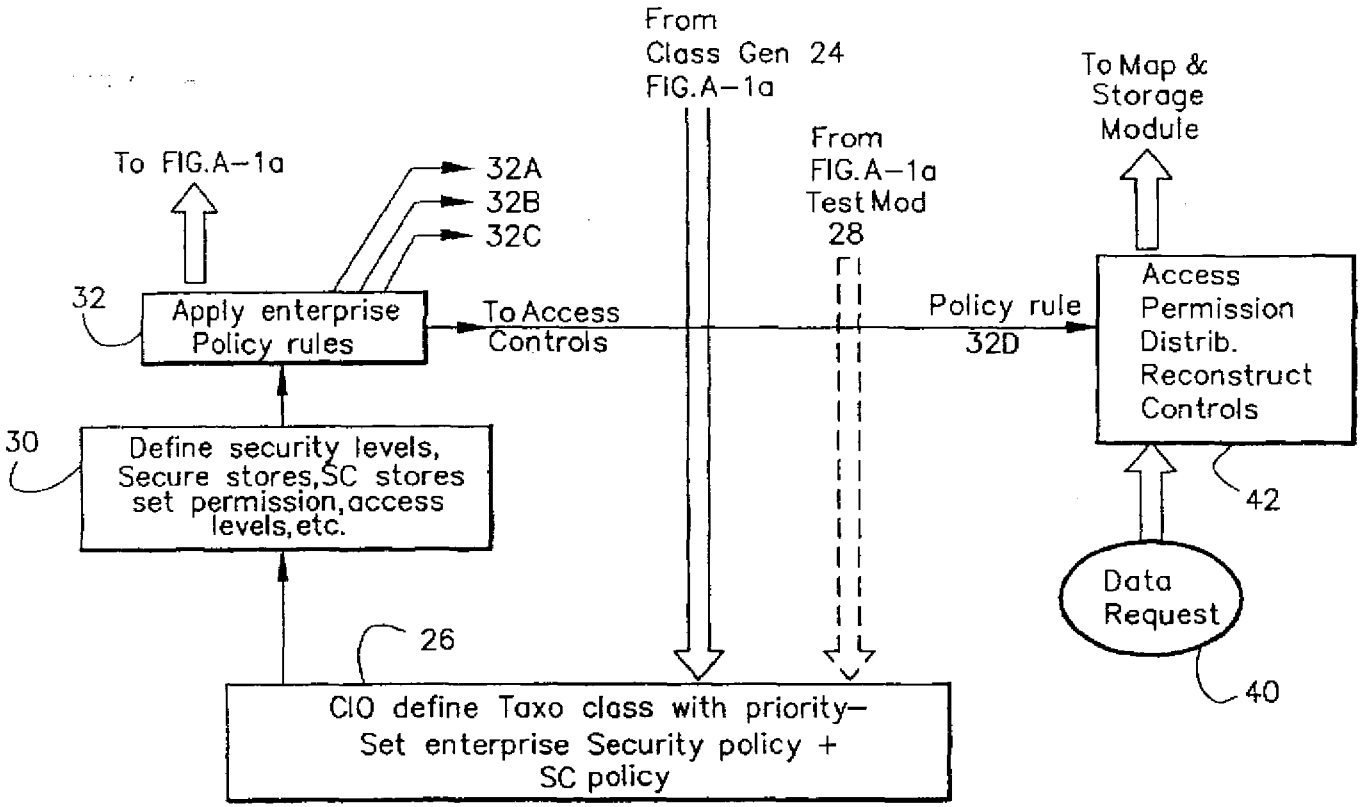


FIG. A-1b

Fig 16

FIG A-1b

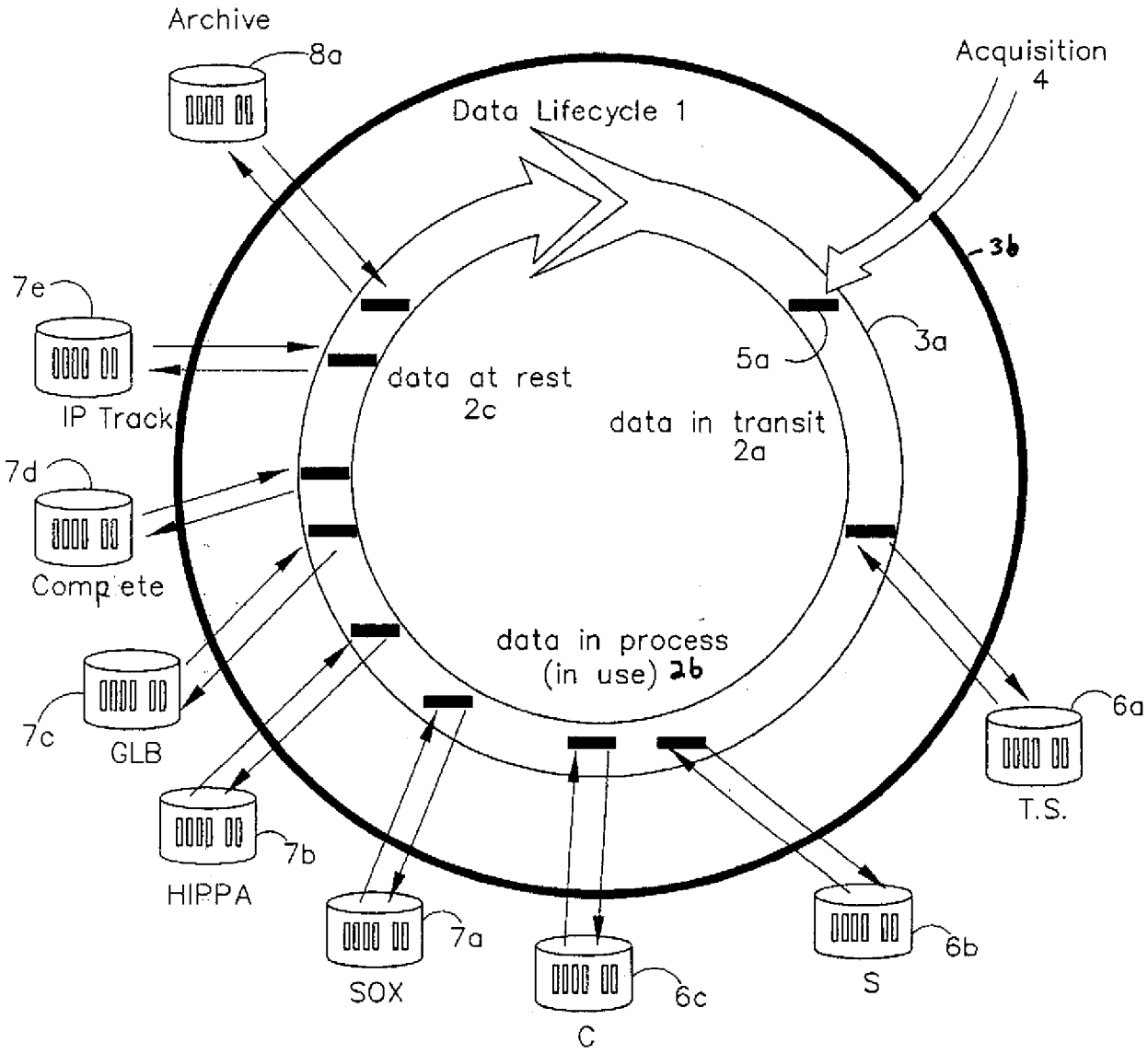

Archive
8a
Acquisition
4
Data Lifecycle 1
3b
7e
IP Track
data at rest
2c
5a
3a
data in transit
2a
7d
Comp ete
data in process
(in use) 2b
7c
GLB
6a
T.S.
7b
HIPPA
7a
SOX
6c
C
6b
S

FIG. ~~A~~ 2

2

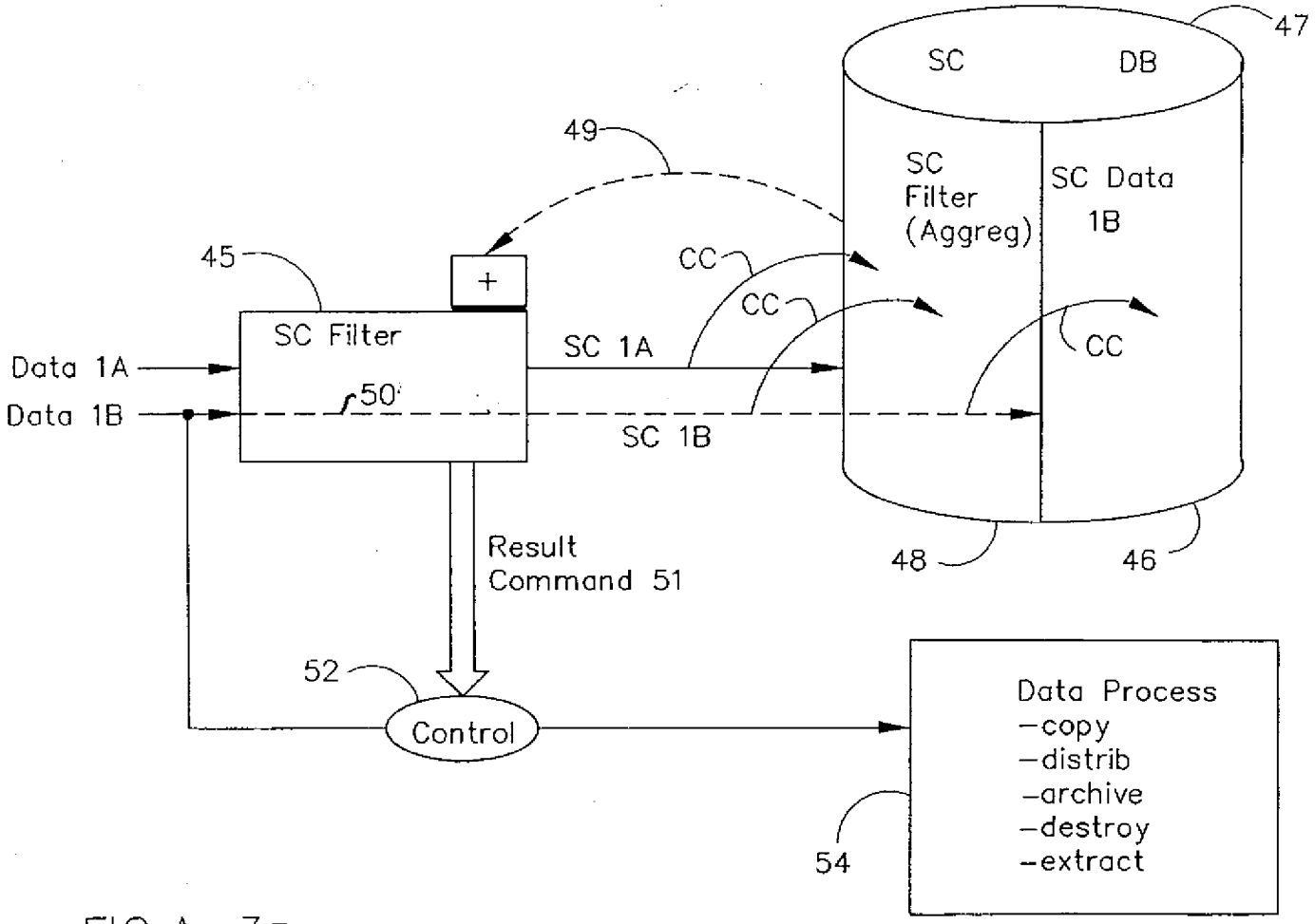

47
SC
DB
49
SC
Filter
(Aggreg)
SC Data
1B
45
+
CC
CC
CC
SC Filter
Data 1A
Data 1B
50
SC 1A
SC 1B
Result
Command 51
48
46
52
Control
Data Process
-copy
-distrib
-archive
-destroy
-extract
54

FIG. ~~A 3~~
3

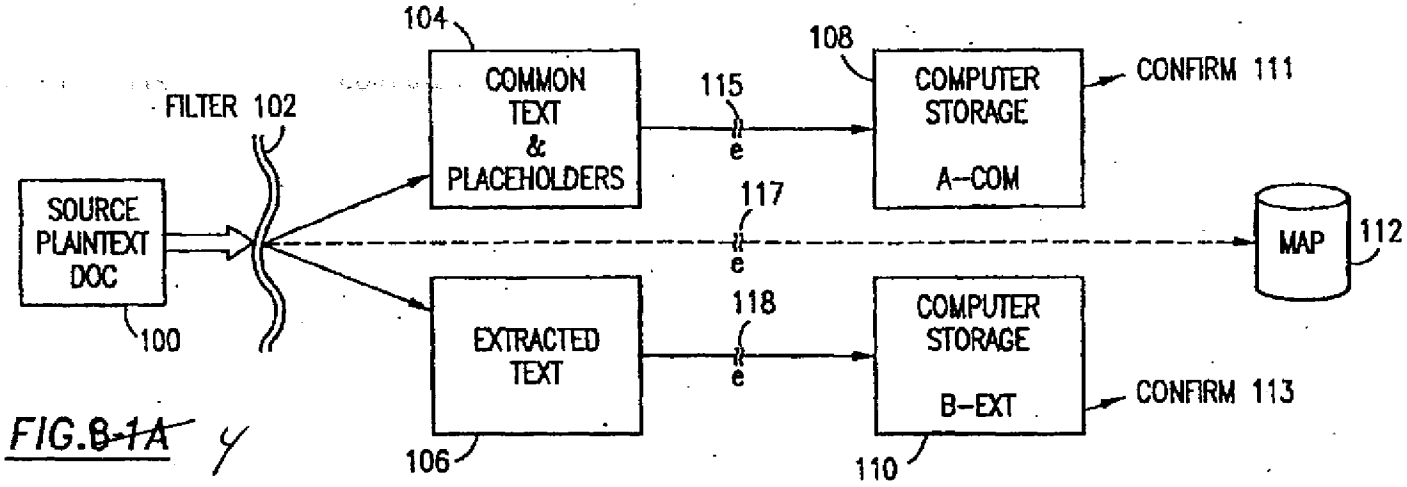


FIG. B-1A

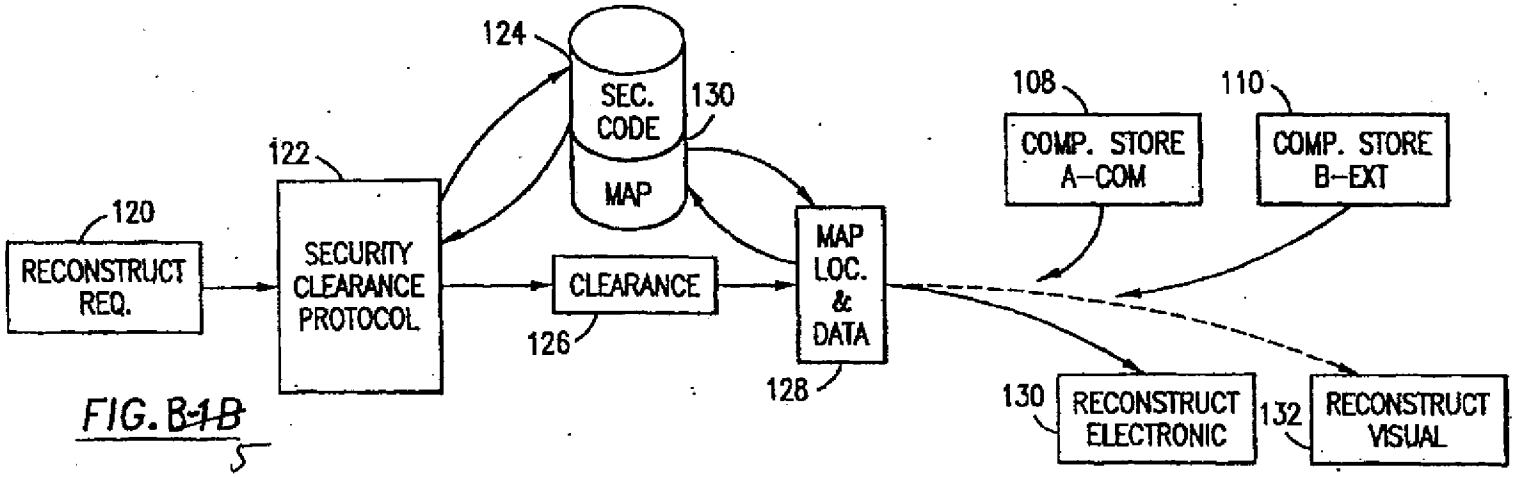


FIG. B-1B

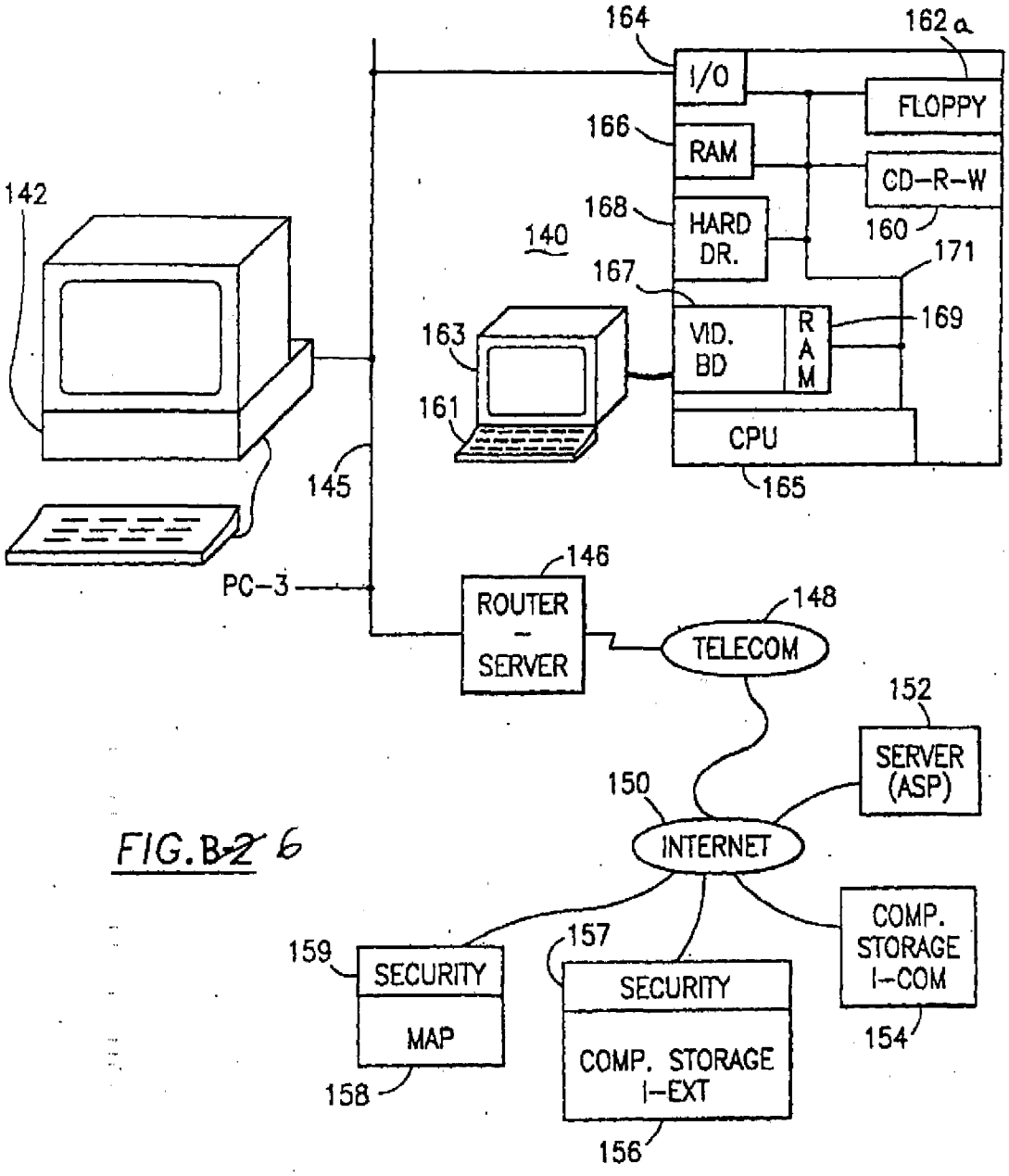

164
162a
I/O
FLOPPY
166
RAM
CD-R-W
142
168
HARD DR.
160
140
171
167
VID. BD
R A M
169
163
161
CPU
165
145
PC-3
146
ROUTER - SERVER
148
TELECOM
152
SERVER (ASP)
150
INTERNET
159
SECURITY
MAP
158
157
SECURITY
COMP. STORAGE I-EXT
156
COMP. STORAGE I-COM
154

FIG. B-2 6

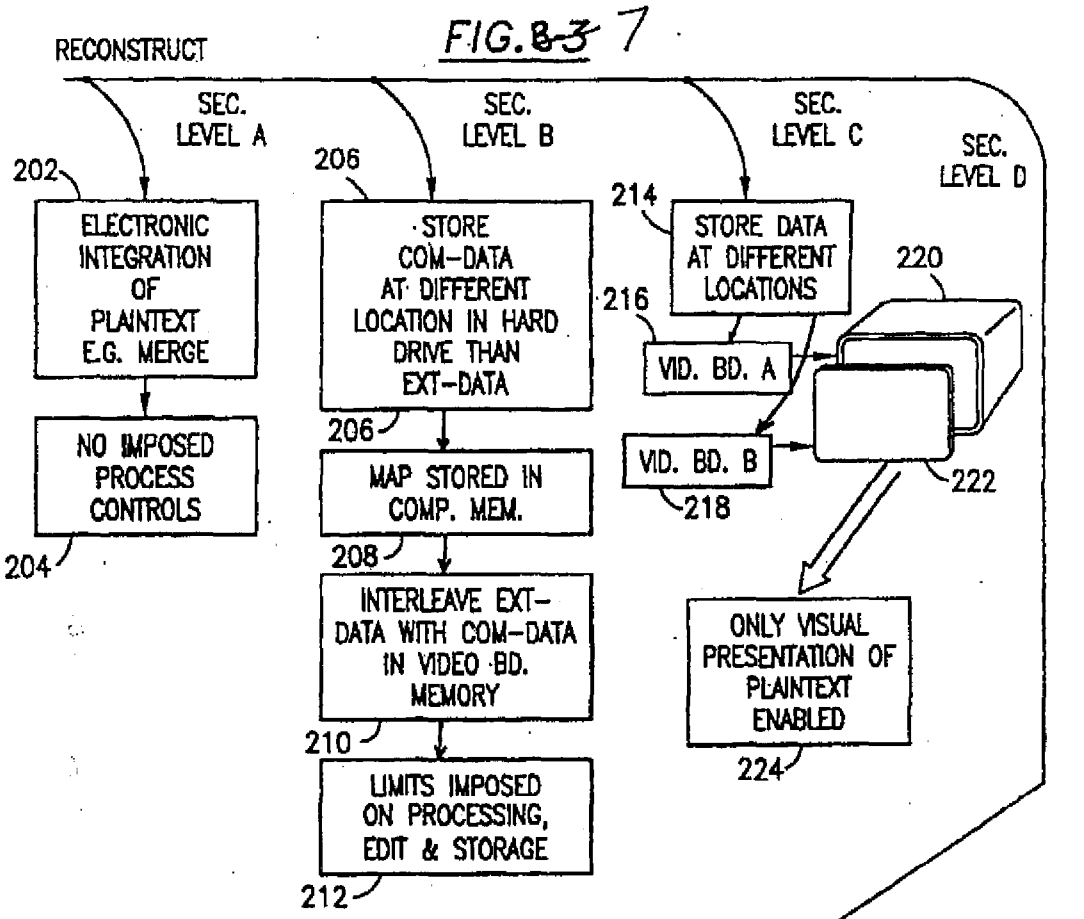


FIG. B-3 7

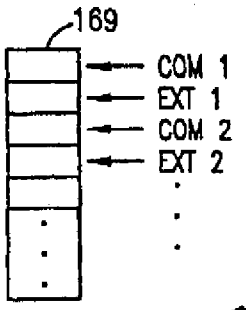
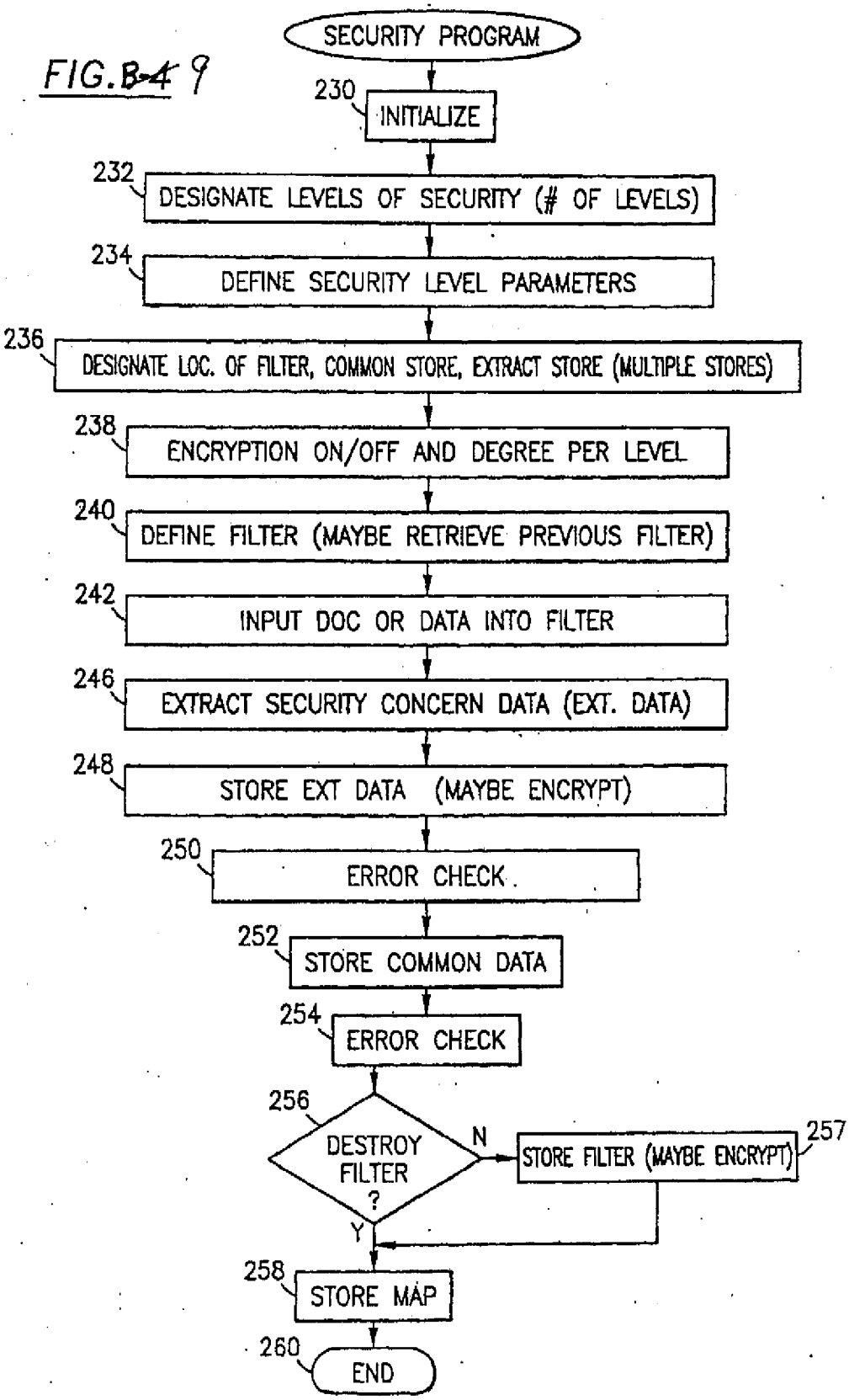


FIG. B-3A 8

FIG. B-4 9


SECURITY PROGRAM
230
INITIALIZE
232
DESIGNATE LEVELS OF SECURITY (# OF LEVELS)
234
DEFINE SECURITY LEVEL PARAMETERS
236
DESIGNATE LOC. OF FILTER, COMMON STORE, EXTRACT STORE (MULTIPLE STORES)
238
ENCRYPTION ON/OFF AND DEGREE PER LEVEL
240
DEFINE FILTER (MAYBE RETRIEVE PREVIOUS FILTER)
242
INPUT DOC OR DATA INTO FILTER
246
EXTRACT SECURITY CONCERN DATA (EXT. DATA)
248
STORE EXT DATA (MAYBE ENCRYPT)
250
ERROR CHECK
252
STORE COMMON DATA
254
ERROR CHECK
256
DESTROY FILTER ?
N
257
STORE FILTER (MAYBE ENCRYPT)
Y
258
STORE MAP
260
END

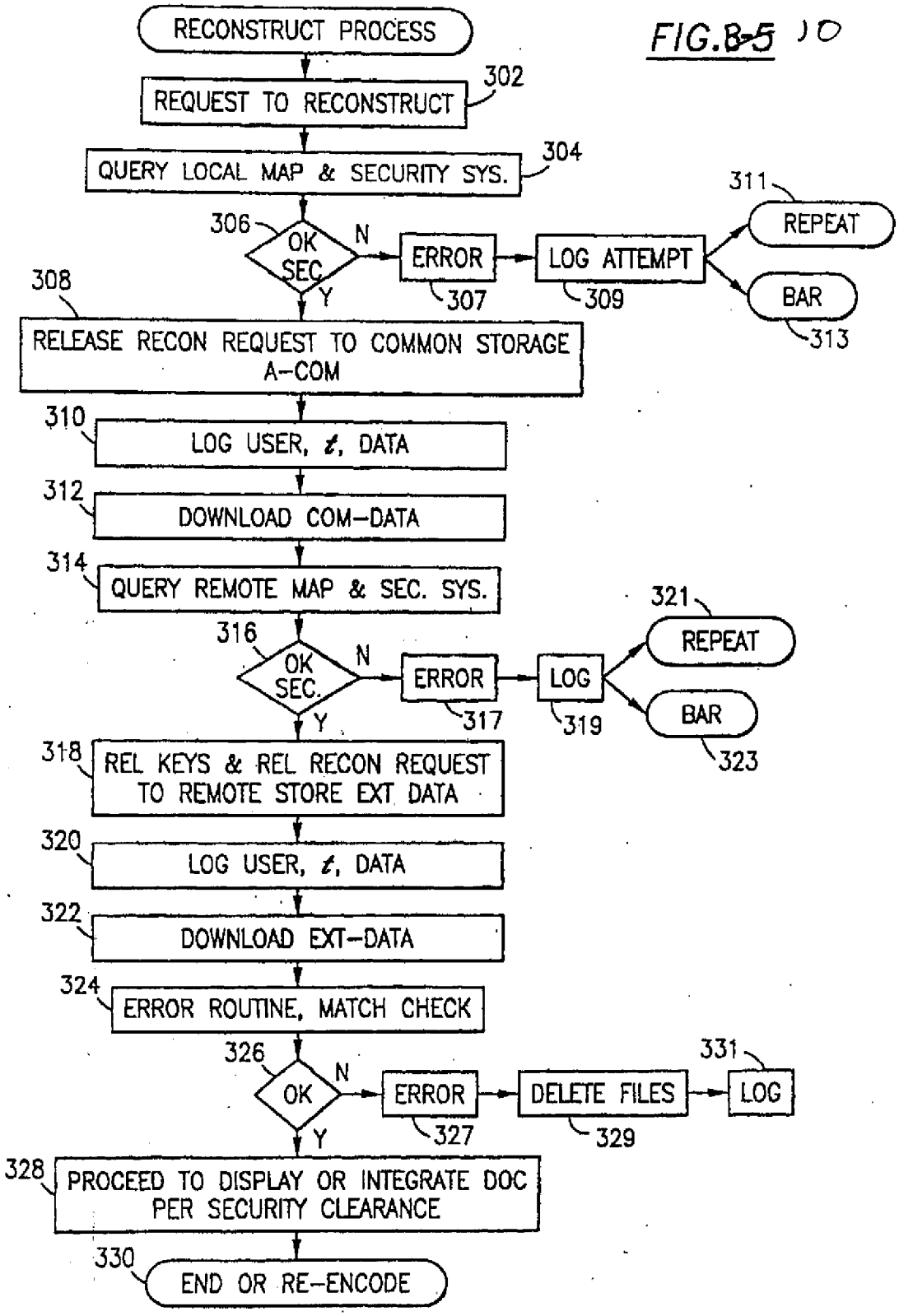

RECONSTRUCT PROCESS
REQUEST TO RECONSTRUCT
302
QUERY LOCAL MAP & SECURITY SYS.
304
306
OK SEC.
N
Y
ERROR
307
LOG ATTEMPT
309
311
REPEAT
BAR
313
308
RELEASE RECON REQUEST TO COMMON STORAGE A-COM
310
LOG USER, t, DATA
312
DOWNLOAD COM-DATA
314
QUERY REMOTE MAP & SEC. SYS.
316
OK SEC.
N
Y
ERROR
317
LOG
319
321
REPEAT
BAR
323
318
REL KEYS & REL RECON REQUEST TO REMOTE STORE EXT DATA
320
LOG USER, t, DATA
322
DOWNLOAD EXT-DATA
324
ERROR ROUTINE, MATCH CHECK
326
OK
N
Y
ERROR
327
DELETE FILES
329
331
LOG
328
PROCEED TO DISPLAY OR INTEGRATE DOC PER SECURITY CLEARANCE
330
END OR RE-ENCODE

FIG. 3-5 10

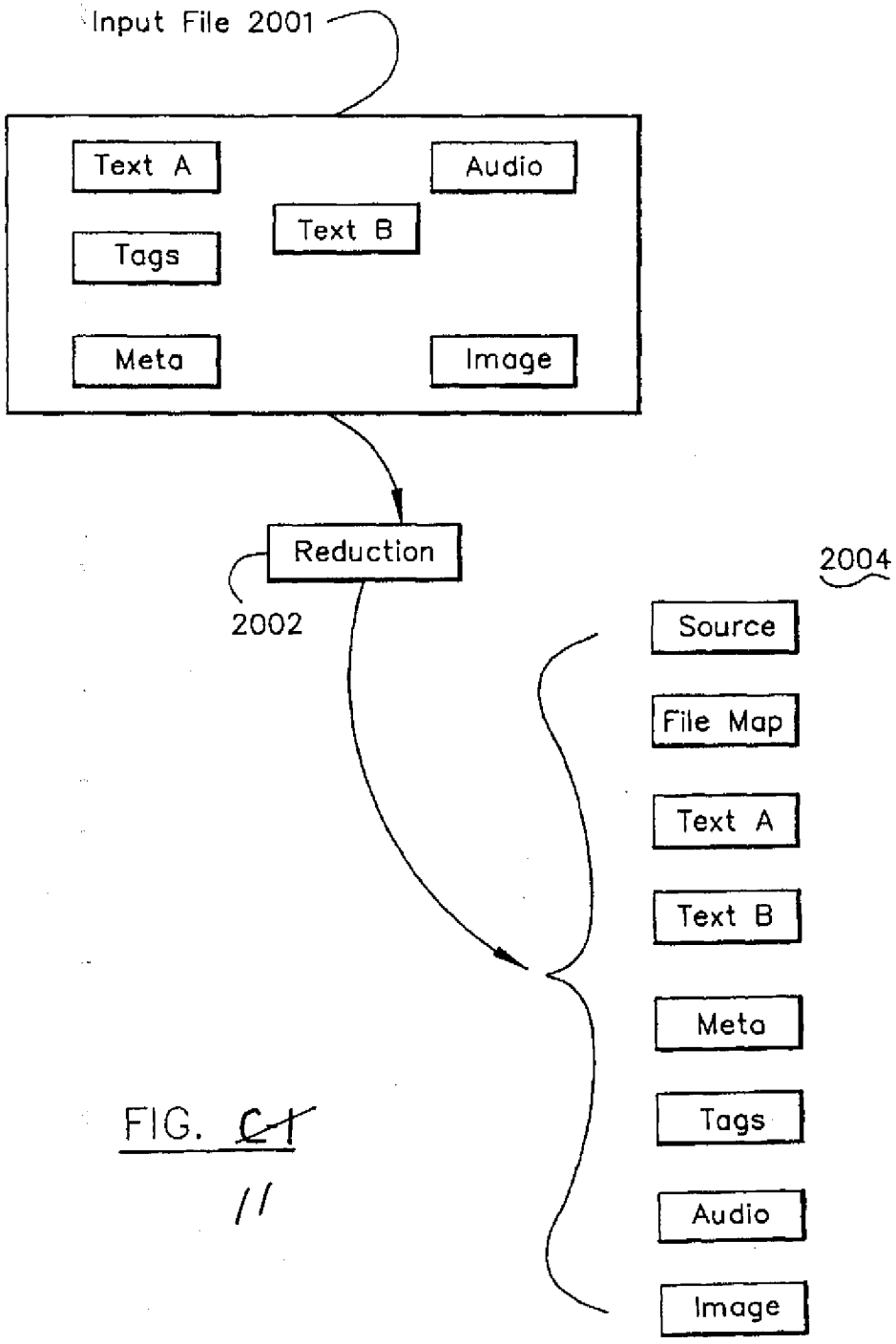

Input File 2001
Text A
Audio
Text B
Tags
Meta
Image
Reduction
2002
2004
Source
File Map
Text A
Text B
Meta
Tags
Audio
Image

FIG. 2A

11

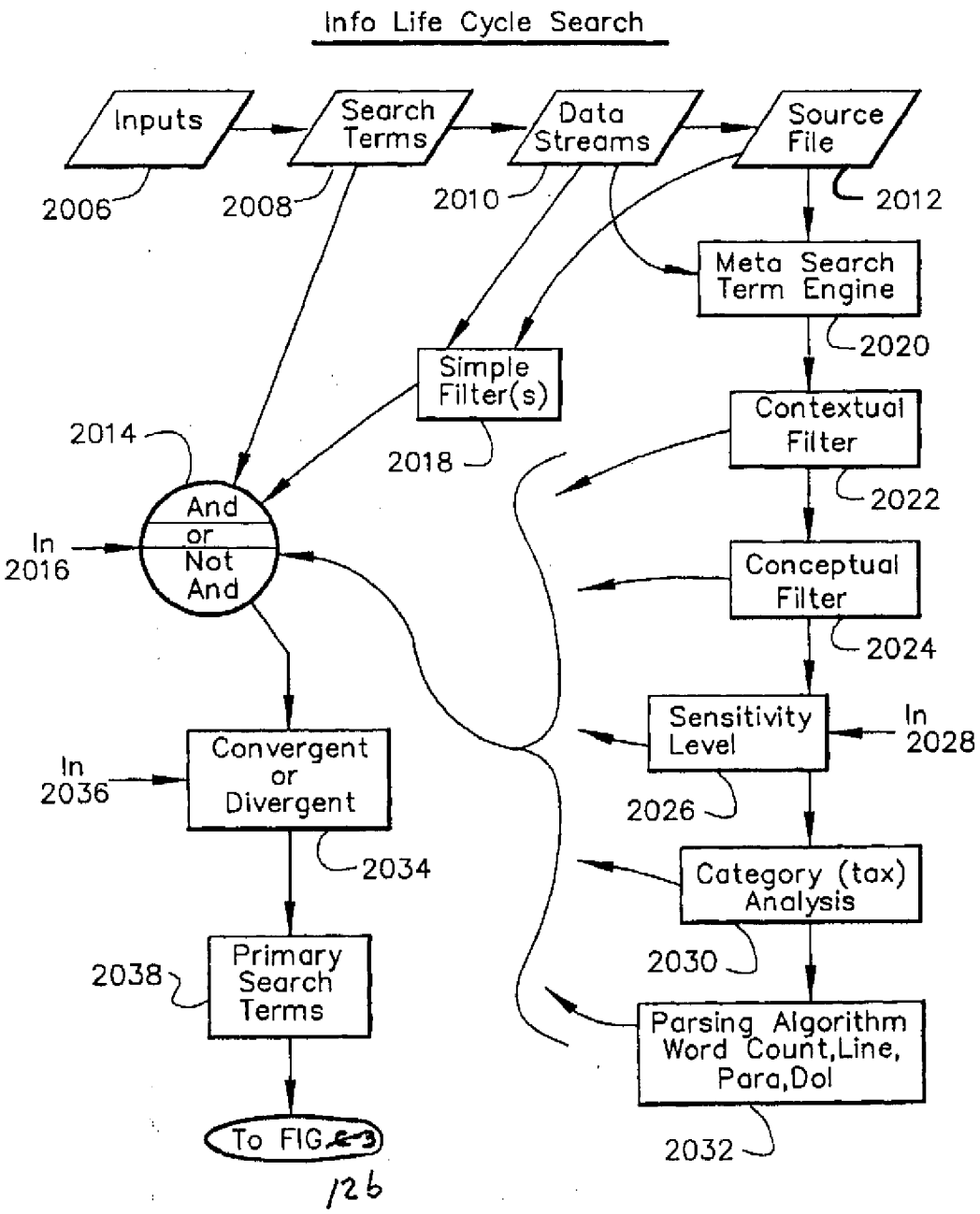

Info Life Cycle Search
Inputs
Search Terms
Data Streams
Source File
2006
2008
2010
2012
Meta Search Term Engine
2020
Simple Filter(s)
2018
Contextual Filter
2022
2014
And
or
Not
And
In
2016
Conceptual Filter
2024
Sensitivity Level
In
2028
2026
In
2036
Convergent or Divergent
2034
Category (tax) Analysis
2030
2038
Primary Search Terms
Parsing Algorithm Word Count,Line, Para,Dol
2032
To FIG 3
126

FIG. 2

129

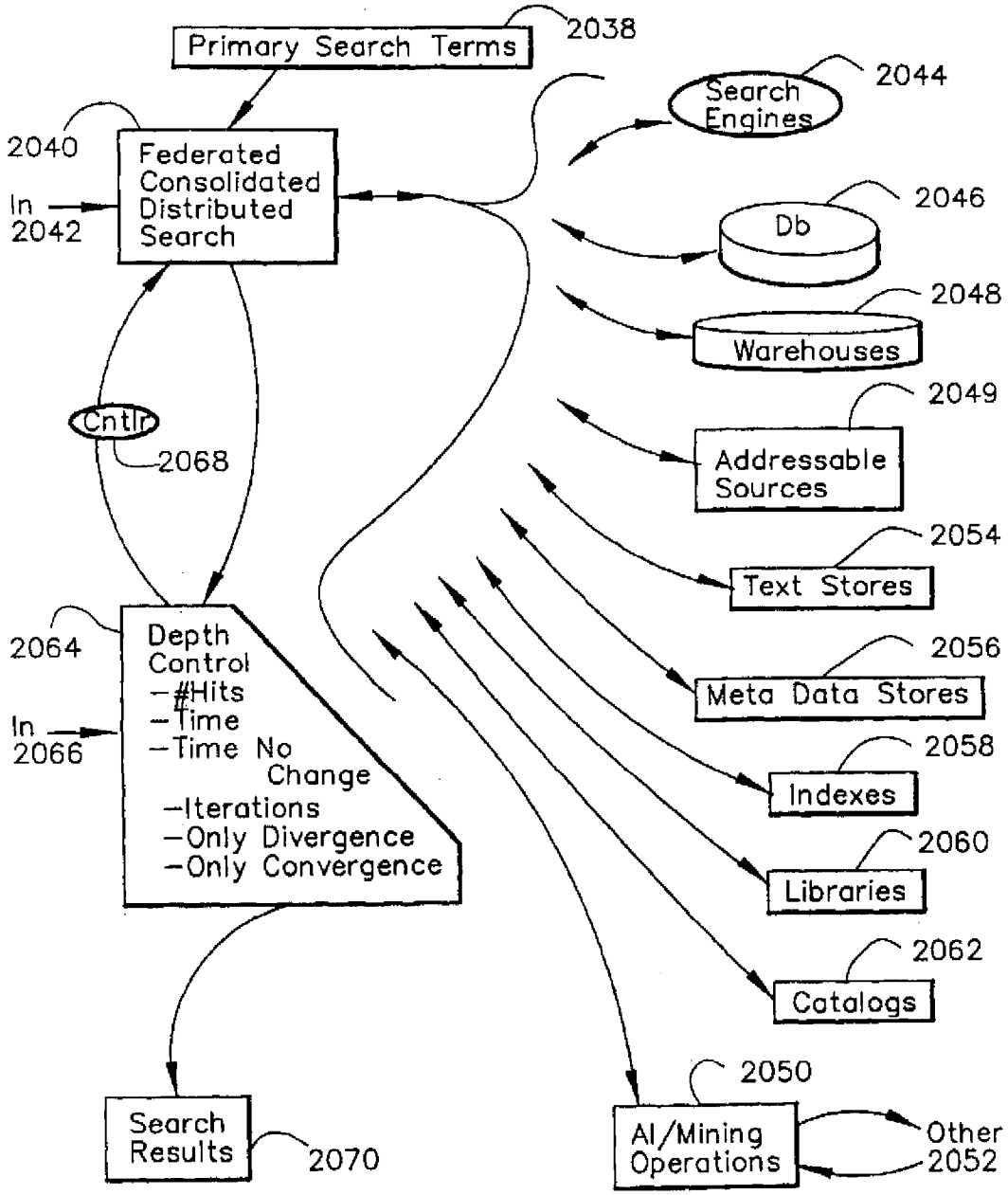

Primary Search Terms
2038
2040
In
2042
Federated
Consolidated
Distributed
Search
Search
Engines
2044
Db
2046
Warehouses
2048
Addressable
Sources
2049
Text Stores
2054
Meta Data Stores
2056
Indexes
2058
Libraries
2060
Catalogs
2062
Cntlr
2068
2064
In
2066
Depth
Control
-#Hits
-Time
-Time No
Change
-Iterations
-Only Divergence
-Only Convergence
Search
Results
2070
2050
AI/Mining
Operations
Other
2052

FIG. ~~C-3~~ 126

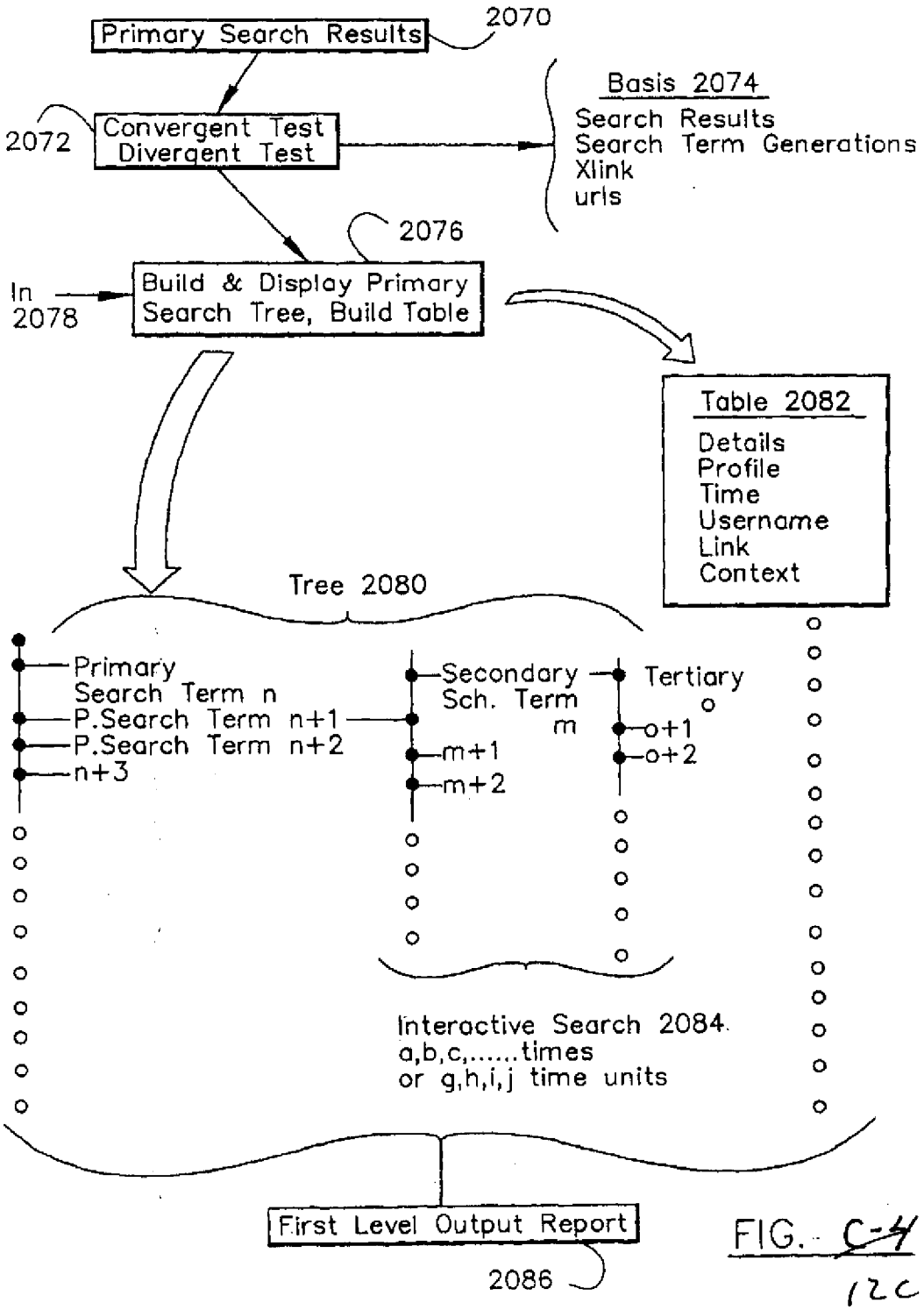

Primary Search Results
2070
Basis 2074
Search Results
Search Term Generations
Xlink
urls
2072
Convergent Test
Divergent Test
2076
In
2078
Build & Display Primary
Search Tree, Build Table
Table 2082
Details
Profile
Time
Username
Link
Context
Tree 2080
Primary
Search Term n
P.Search Term n+1
P.Search Term n+2
n+3
Secondary
Sch. Term
m
m+1
m+2
Tertiary
o
o+1
o+2
Interactive Search 2084
a,b,c,.....times
or g,h,i,j time units
First Level Output Report
2086

FIG. C-4

12C

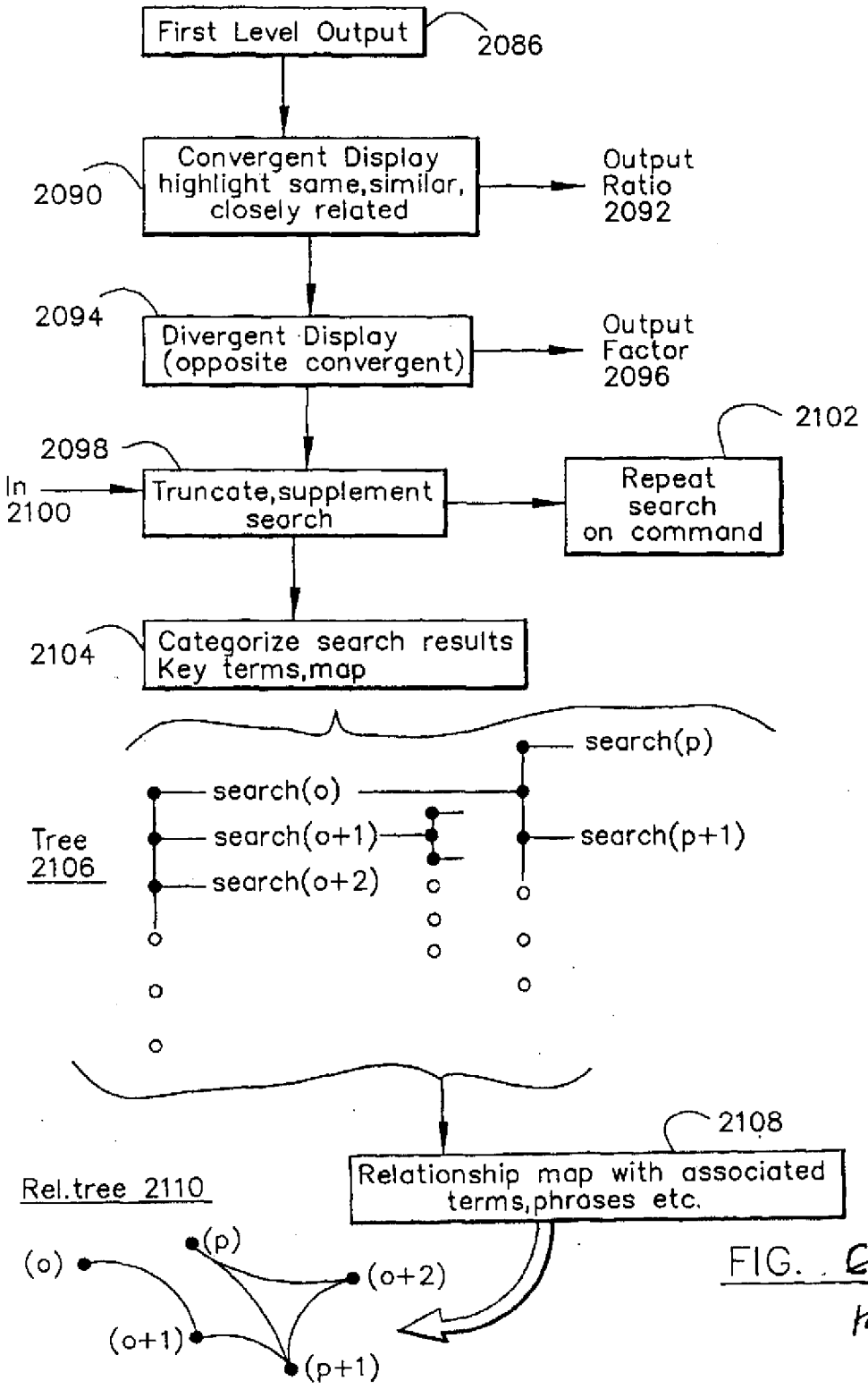

First Level Output
2086
Convergent Display highlight same,similar, closely related
2090
Output Ratio 2092
2094
Divergent Display (opposite convergent)
Output Factor 2096
2098
In 2100
Truncate,supplement search
2102
Repeat search on command
2104
Categorize search results Key terms,map
Tree 2106
search(o)
search(o+1)
search(o+2)
search(p)
search(p+1)
2108
Relationship map with associated terms,phrases etc.
Rel.tree 2110
(o)
(p)
(o+2)
(o+1)
(p+1)

FIG. 5

12d

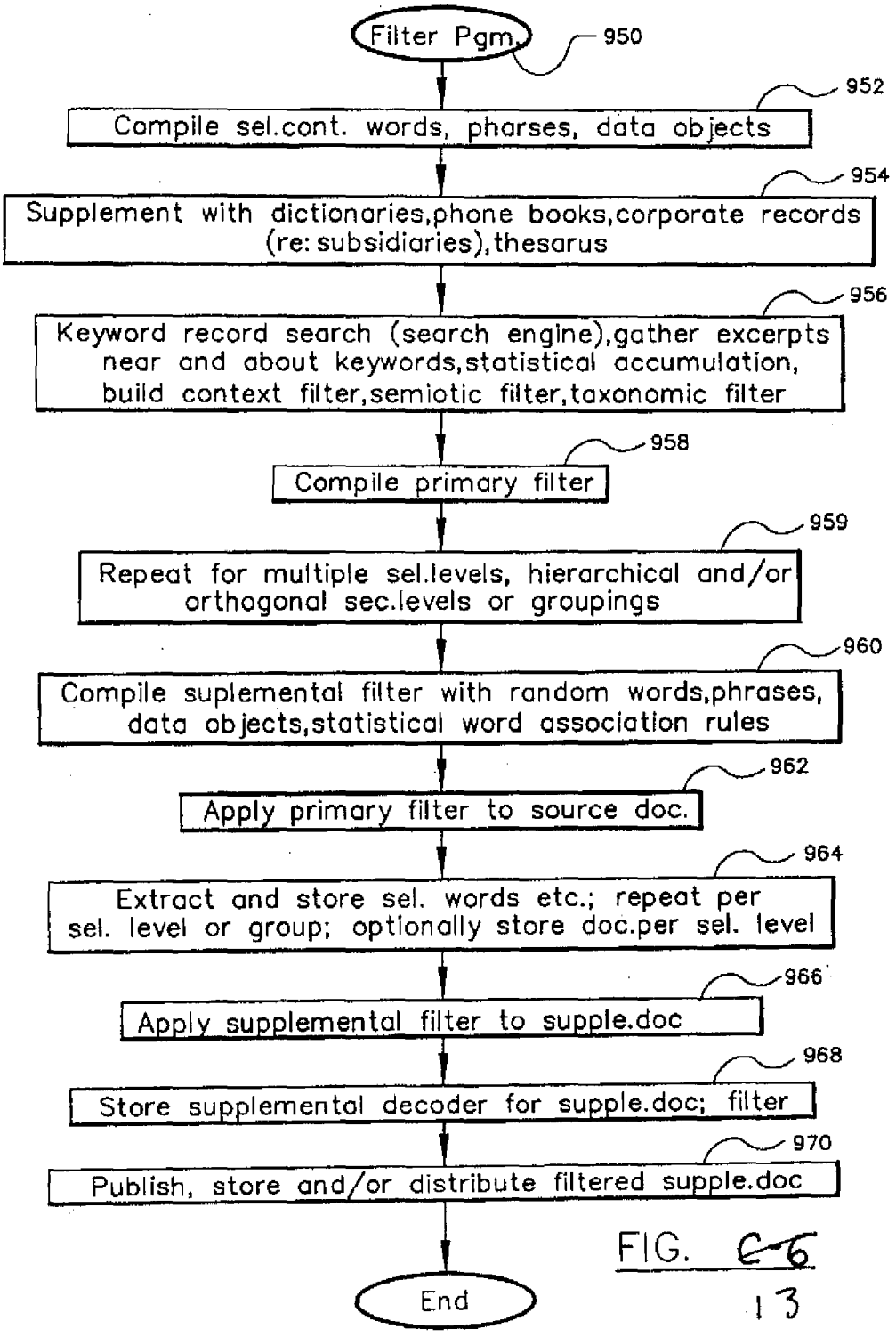

Filter Pgm.
950
952
Compile sel.cont. words, pharses, data objects
954
Supplement with dictionaries,phone books,corporate records (re: subsidiaries),thesarus
956
Keyword record search (search engine),gather excerpts near and about keywords,statistical accumulation, build context filter,semiotic filter,taxonomic filter
958
Compile primary filter
959
Repeat for multiple sel.levels, hierarchical and/or orthogonal sec.levels or groupings
960
Compile suplemental filter with random words,phrases, data objects,statistical word association rules
962
Apply primary filter to source doc.
964
Extract and store sel. words etc.; repeat per sel. level or group; optionally store doc.per sel. level
966
Apply supplemental filter to supple.doc
968
Store supplemental decoder for supple.doc; filter
970
Publish, store and/or distribute filtered supple.doc
End

FIG. ~~6~~ 13

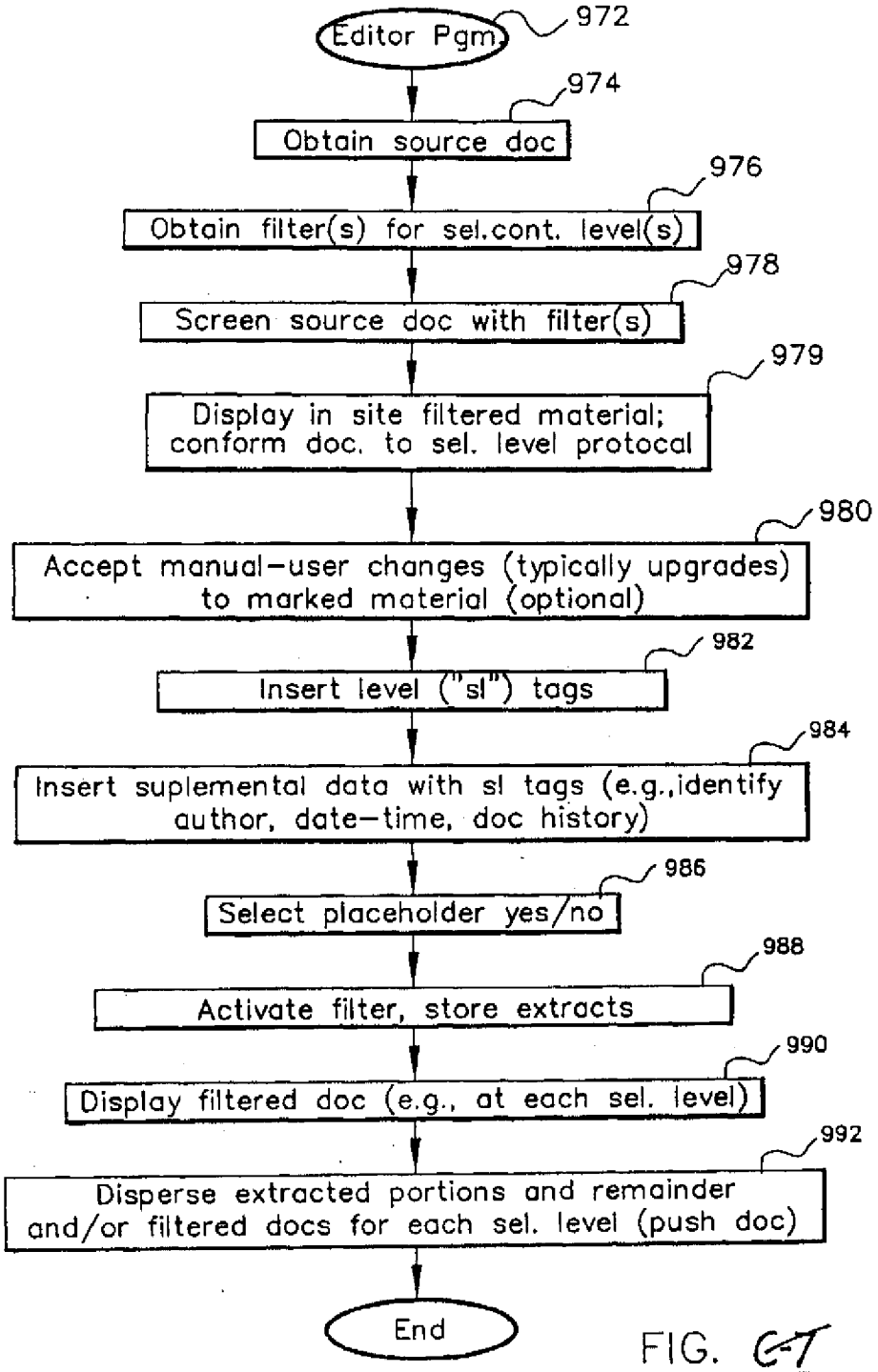

Editor Pgm
972
Obtain source doc
974
Obtain filter(s) for sel.cont. level(s)
976
Screen source doc with filter(s)
978
Display in site filtered material; conform doc. to sel. level protocal
979
Accept manual-user changes (typically upgrades) to marked material (optional)
980
Insert level ("sl") tags
982
Insert suplemental data with sl tags (e.g.,identify author, date-time, doc history)
984
Select placeholder yes/no
986
Activate filter, store extracts
988
Display filtered doc (e.g., at each sel. level)
990
Disperse extracted portions and remainder and/or filtered docs for each sel. level (push doc)
992
End

FIG. 6-7

14

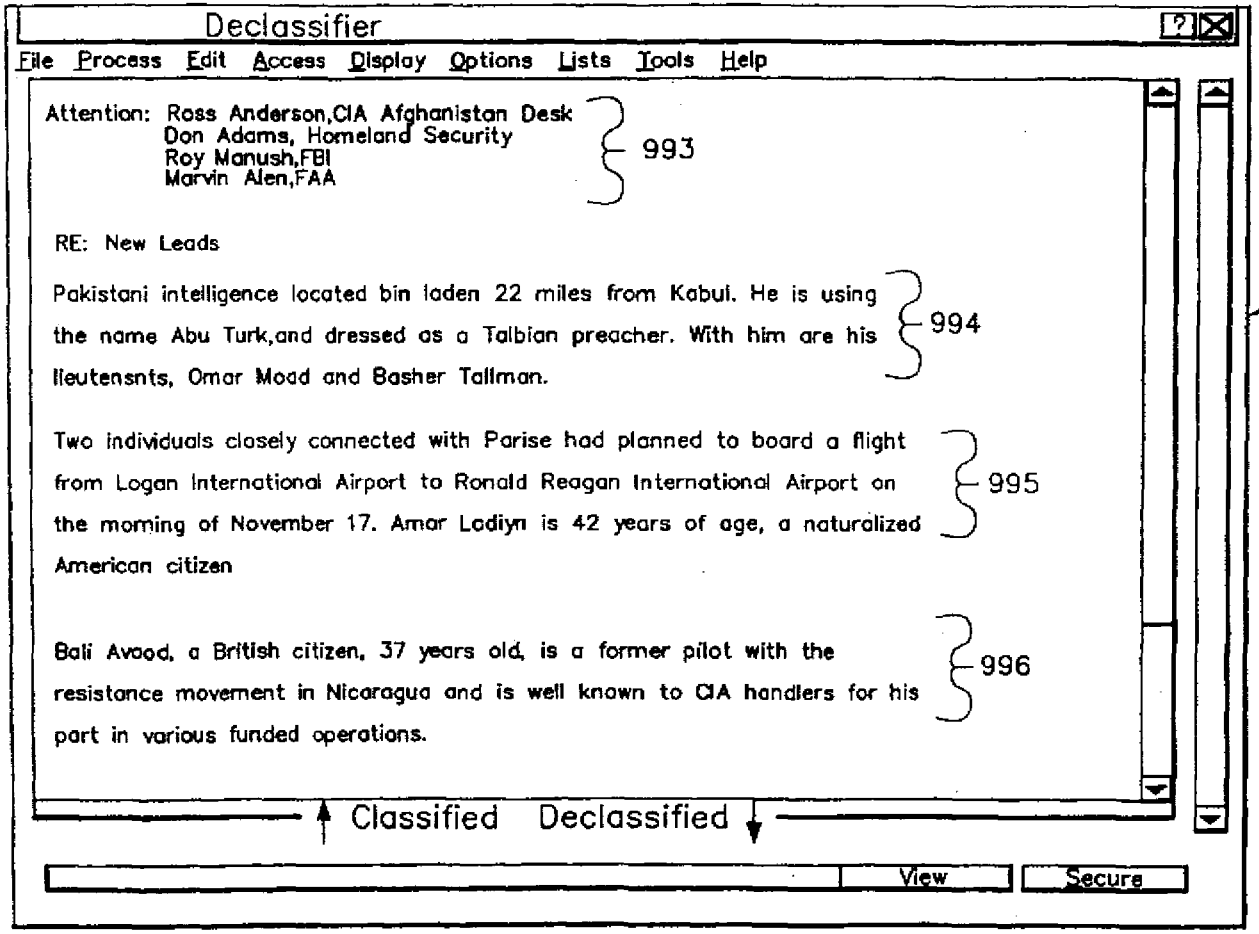

Declassifier
File Process Edit Access Display Options Lists Tools Help
Attention: Ross Anderson,CIA Afghanistan Desk
Don Adams, Homeland Security
Roy Manush,FBI
Marvin Alen,FAA
993
RE: New Leads
Pakistani intelligence located bin laden 22 miles from Kabul. He is using the name Abu Turk,and dressed as a Talbian preacher. With him are his lleutensnts, Omar Mood and Basher Tallman.
994
Two individuals closely connected with Parise had planned to board a flight from Logan International Airport to Ronald Reagan International Airport on the morning of November 17. Amar Lodiyn is 42 years of age, a naturalized American citizen
995
Bali Avood, a British citizen, 37 years old, is a former pilot with the resistance movement in Nicaragua and is well known to CIA handlers for his part in various funded operations.
996
Classified
Declassified
View
Secure
991

FIG. ~~C-8A~~ 15

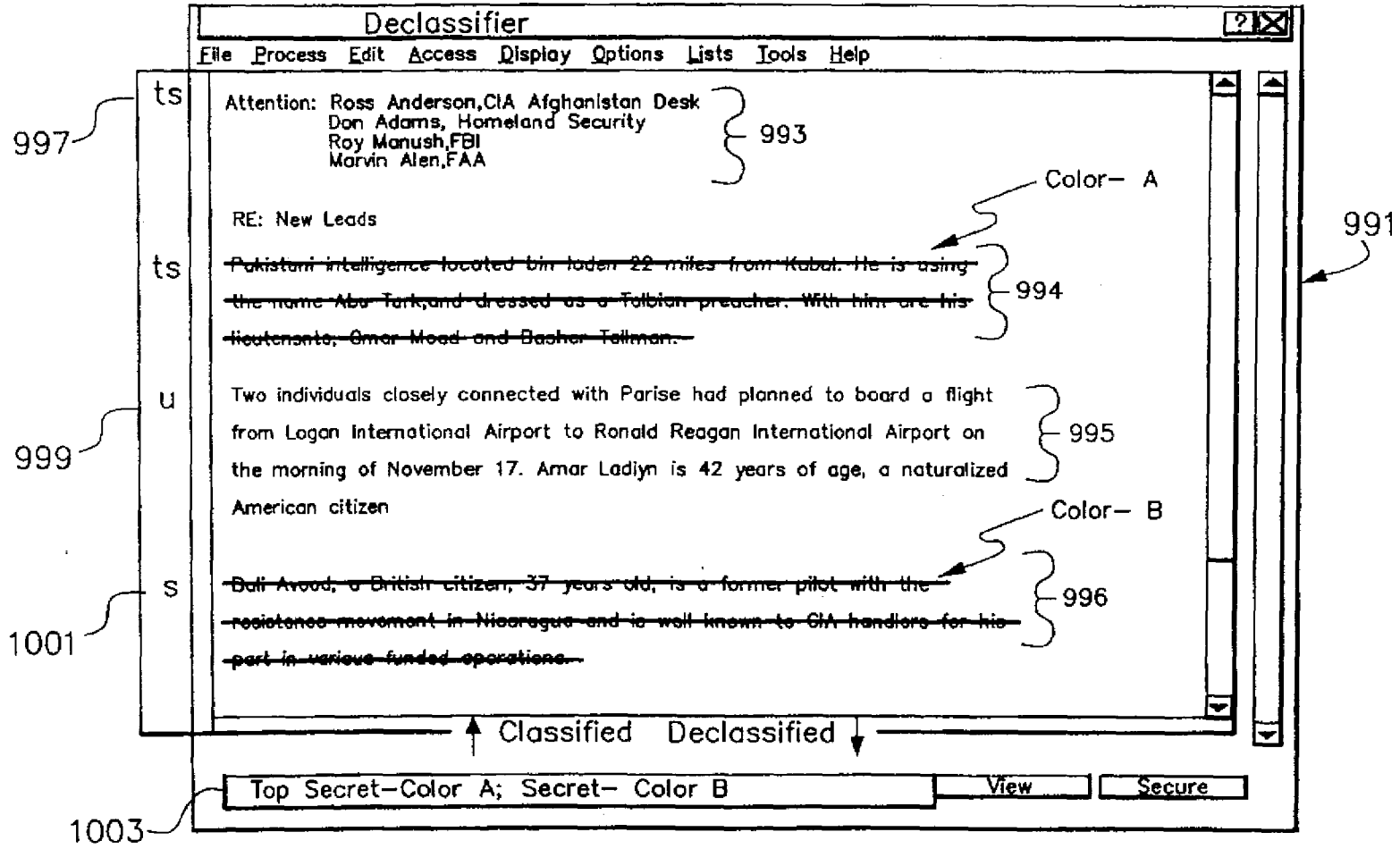

Declassifier
File Process Edit Access Display Options Lists Tools Help
ts
997
Attention: Ross Anderson,CIA Afghanistan Desk
Don Adams, Homeland Security
Roy Manush,FBI
Marvin Alen,FAA
993
Color– A
RE: New Leads
991
ts
Pakistani intelligence located bin laden 22 miles from Kabul. He is using the name Abu Tark,and dressed as a Talbian preacher. With him are his lieutenants, Omar Moad and Bashar Tallman.
994
u
999
Two individuals closely connected with Parise had planned to board a flight from Logan International Airport to Ronald Reagan International Airport on the morning of November 17. Amar Ladiyn is 42 years of age, a naturalized American citizen
995
Color– B
s
1001
Bali Avood, a British citizen, 37 years old, is a former pilot with the resistance movement in Nicaragua and is well known to CIA handlers for his part in various funded operations.
996
Classified Declassified
1003
Top Secret–Color A; Secret– Color B
View
Secure

FIG. ~~C-8B~~ 16

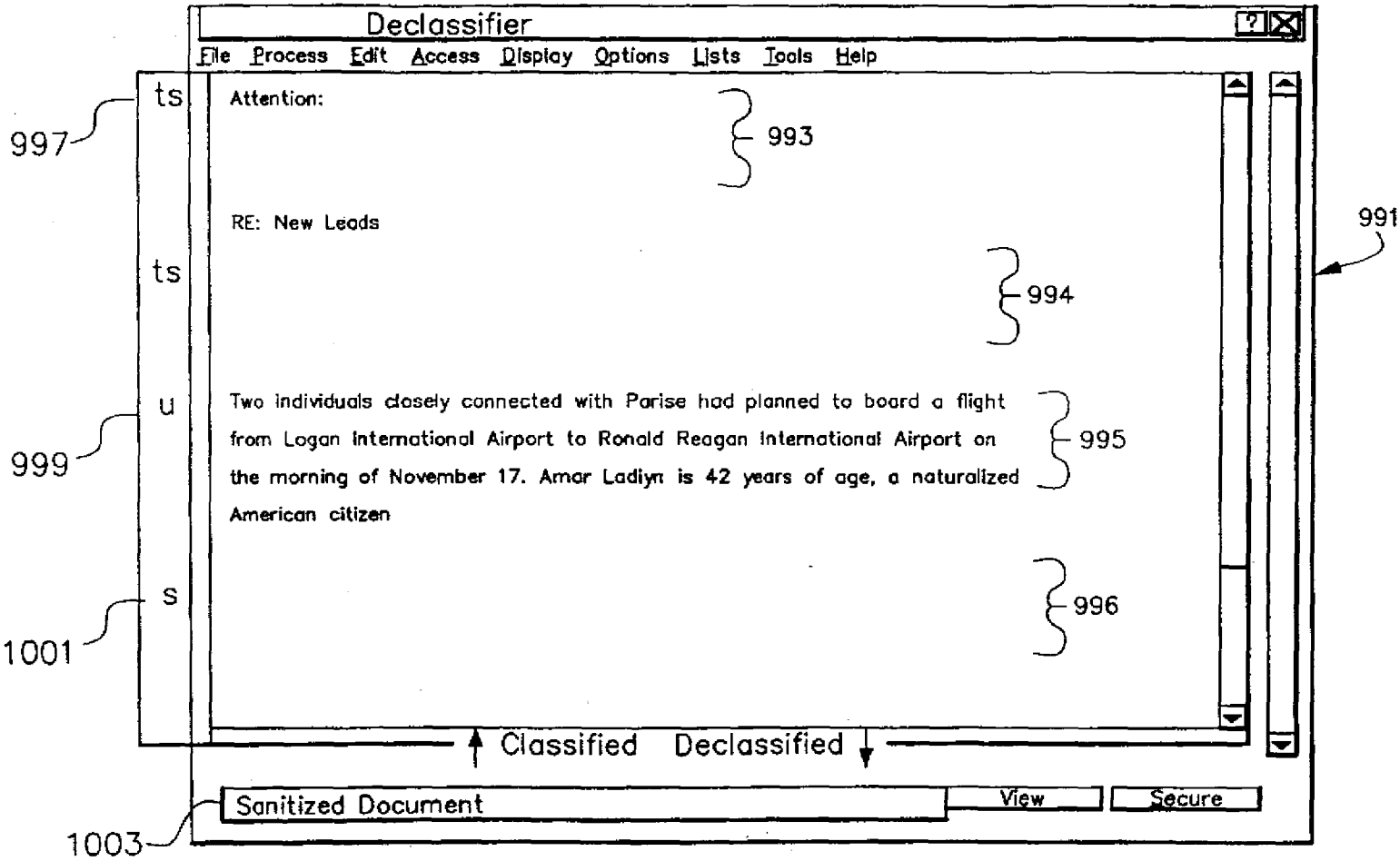

Declassifier
File Process Edit Access Display Options Lists Tools Help
ts
997
Attention:
993
RE: New Leads
991
ts
994
u
999
Two individuals closely connected with Parise had planned to board a flight from Logan International Airport to Ronald Reagan International Airport on the morning of November 17. Amar Ladiyn is 42 years of age, a naturalized American citizen
995
s
1001
996
Classified Declassified
Sanitized Document
View
Secure
1003

FIG. ~~C-8C~~ 17

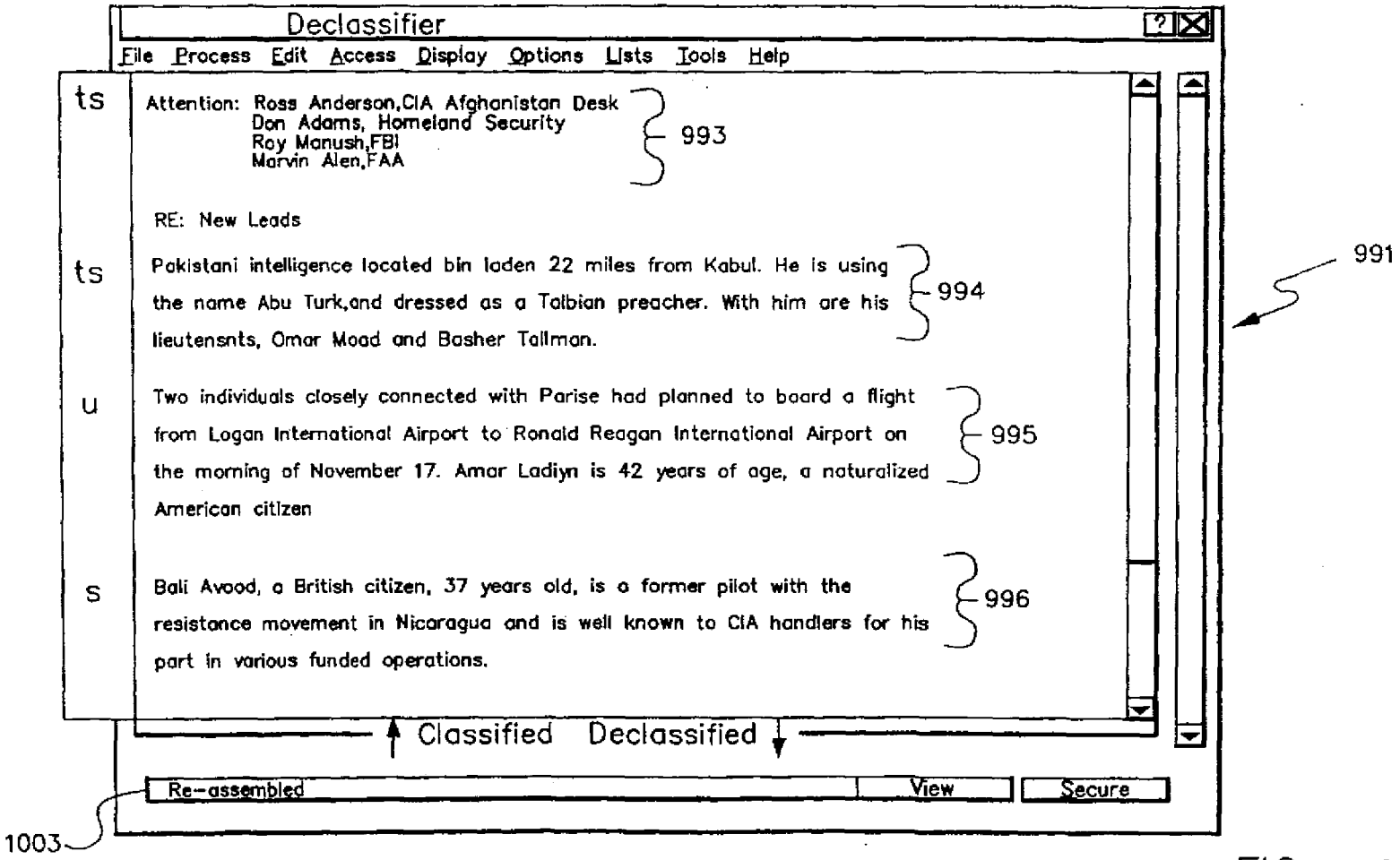

Declassifier
File Process Edit Access Display Options Lists Tools Help
ts
Attention: Ross Anderson,CIA Afghanistan Desk
Don Adams, Homeland Security
Roy Manush,FBI
Marvin Alen,FAA
993
RE: New Leads
ts
Pakistani intelligence located bin laden 22 miles from Kabul. He is using the name Abu Turk,and dressed as a Talbian preacher. With him are his lieutensnts, Omar Moad and Basher Tallman.
994
991
u
Two individuals closely connected with Parise had planned to board a flight from Logan International Airport to Ronald Reagan International Airport on the morning of November 17. Amar Ladiyn is 42 years of age, a naturalized American citizen
995
s
Bali Avood, a British citizen, 37 years old, is a former pilot with the resistance movement in Nicaragua and is well known to CIA handlers for his part in various funded operations.
996
Classified Declassified
Re-assembled
View
Secure
1003

FIG. ~~8D~~ 8

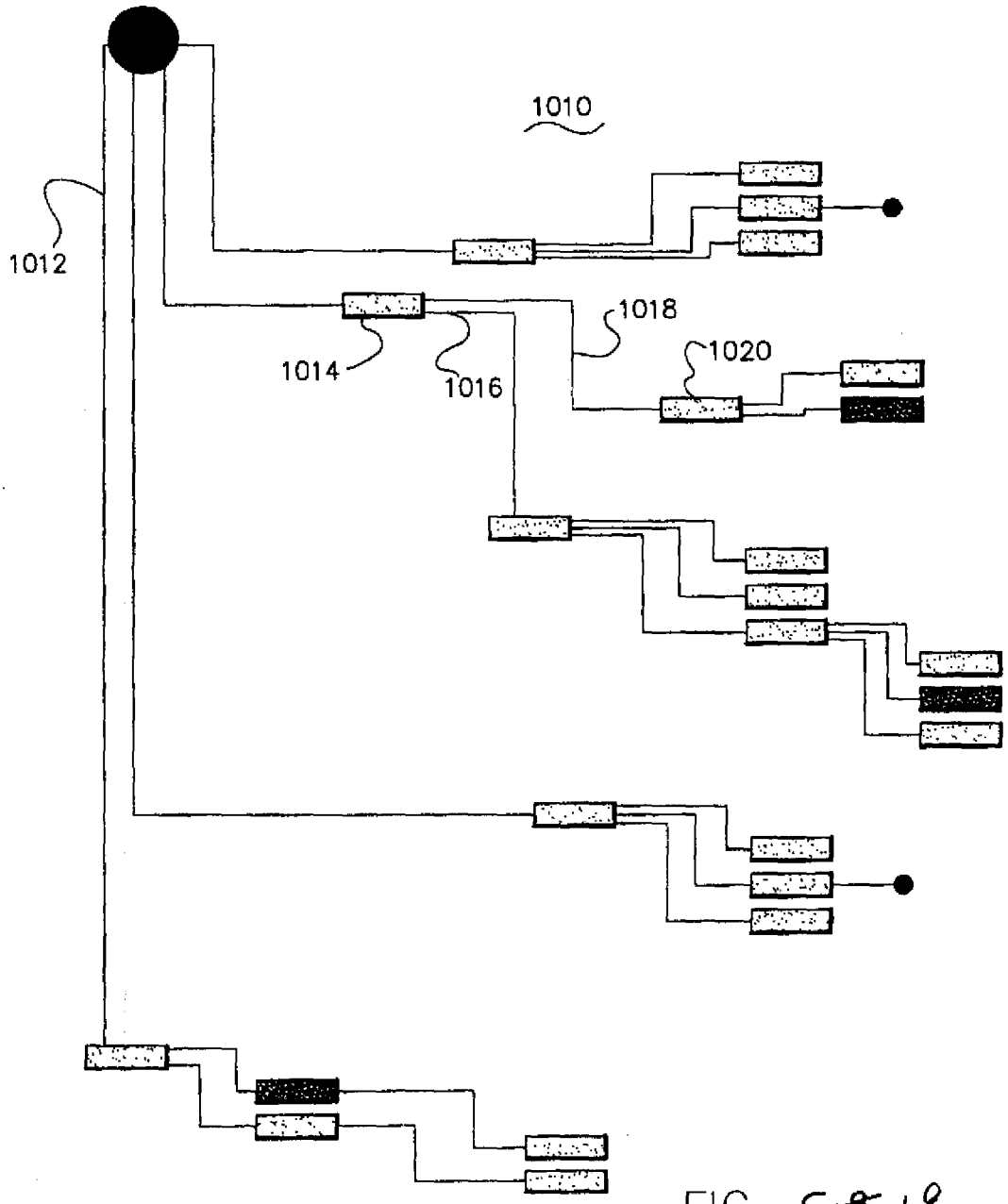


FIG. 19

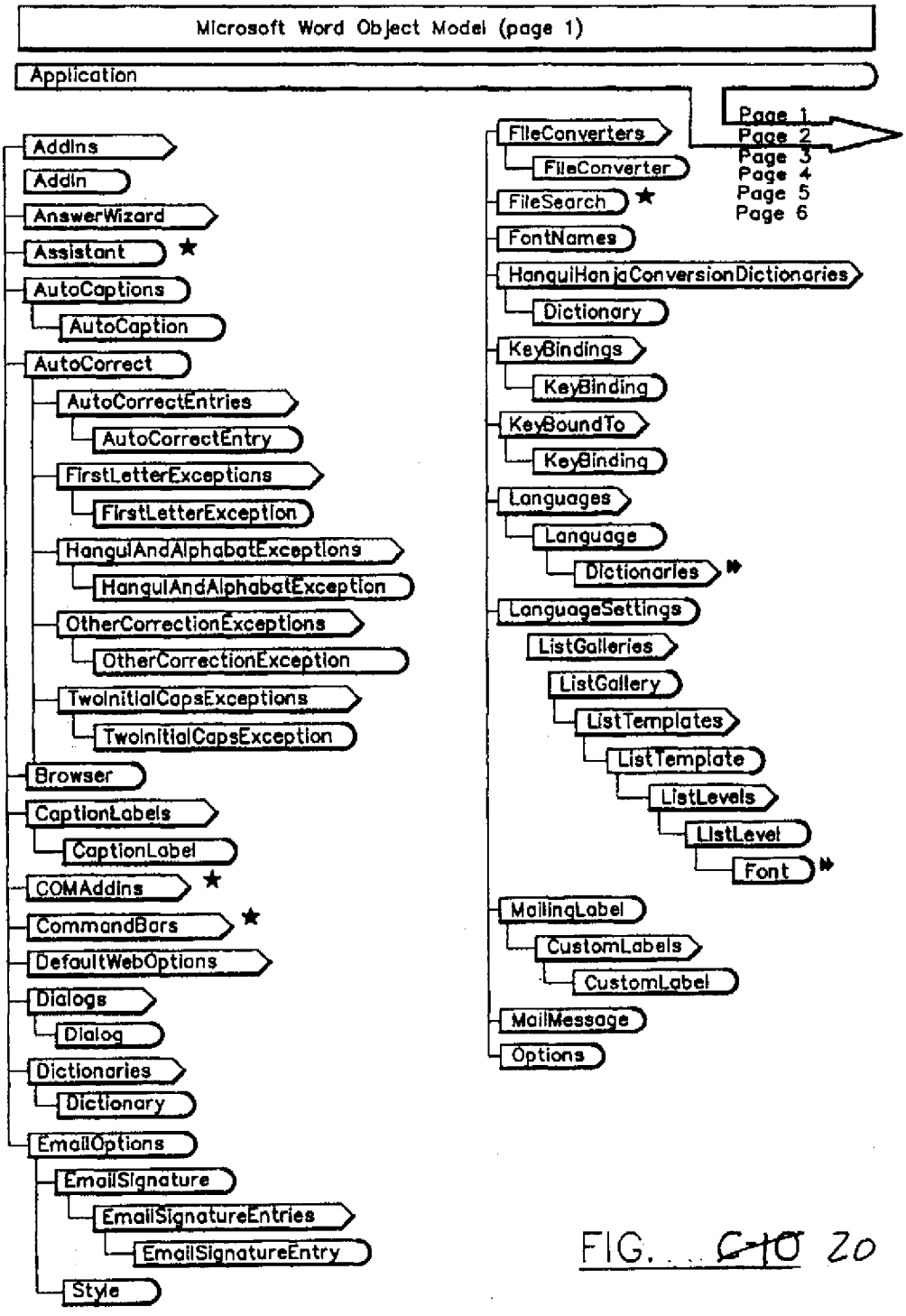

Microsoft Word Object Model (page 1)
Application
Page 1
Page 2
Page 3
Page 4
Page 5
Page 6
AddIns
AddIn
AnswerWizard
Assistant
AutoCaptions
AutoCaption
AutoCorrect
AutoCorrectEntries
AutoCorrectEntry
FirstLetterExceptions
FirstLetterException
HangulAndAlphabatExceptions
HangulAndAlphabatException
OtherCorrectionExceptions
OtherCorrectionException
TwoInitialCapsExceptions
TwoInitialCapsException
Browser
CaptionLabels
CaptionLabel
COMAddIns
CommandBars
DefaultWebOptions
Dialogs
Dialog
Dictionaries
Dictionary
EmailOptions
EmailSignature
EmailSignatureEntries
EmailSignatureEntry
Style
FileConverters
FileConverter
FileSearch
FontNames
HangulHanjaConversionDictionaries
Dictionary
KeyBindings
KeyBinding
KeyBoundTo
KeyBinding
Languages
Language
Dictionaries
LanguageSettings
ListGalleries
ListGallery
ListTemplates
ListTemplate
ListLevels
ListLevel
Font
MailingLabel
CustomLabels
CustomLabel
MailMessage
Options

FIG. ~~6~~ 20

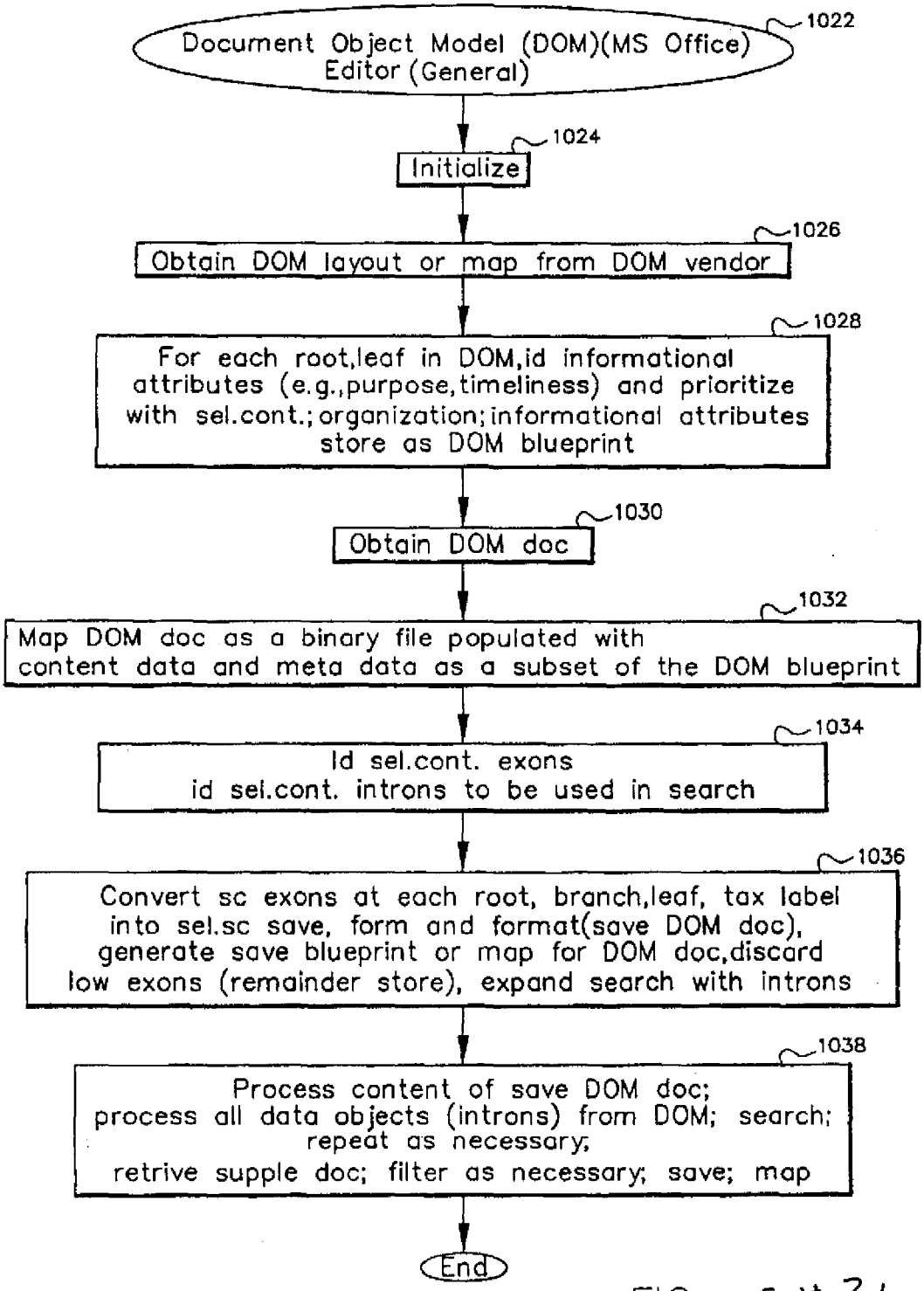
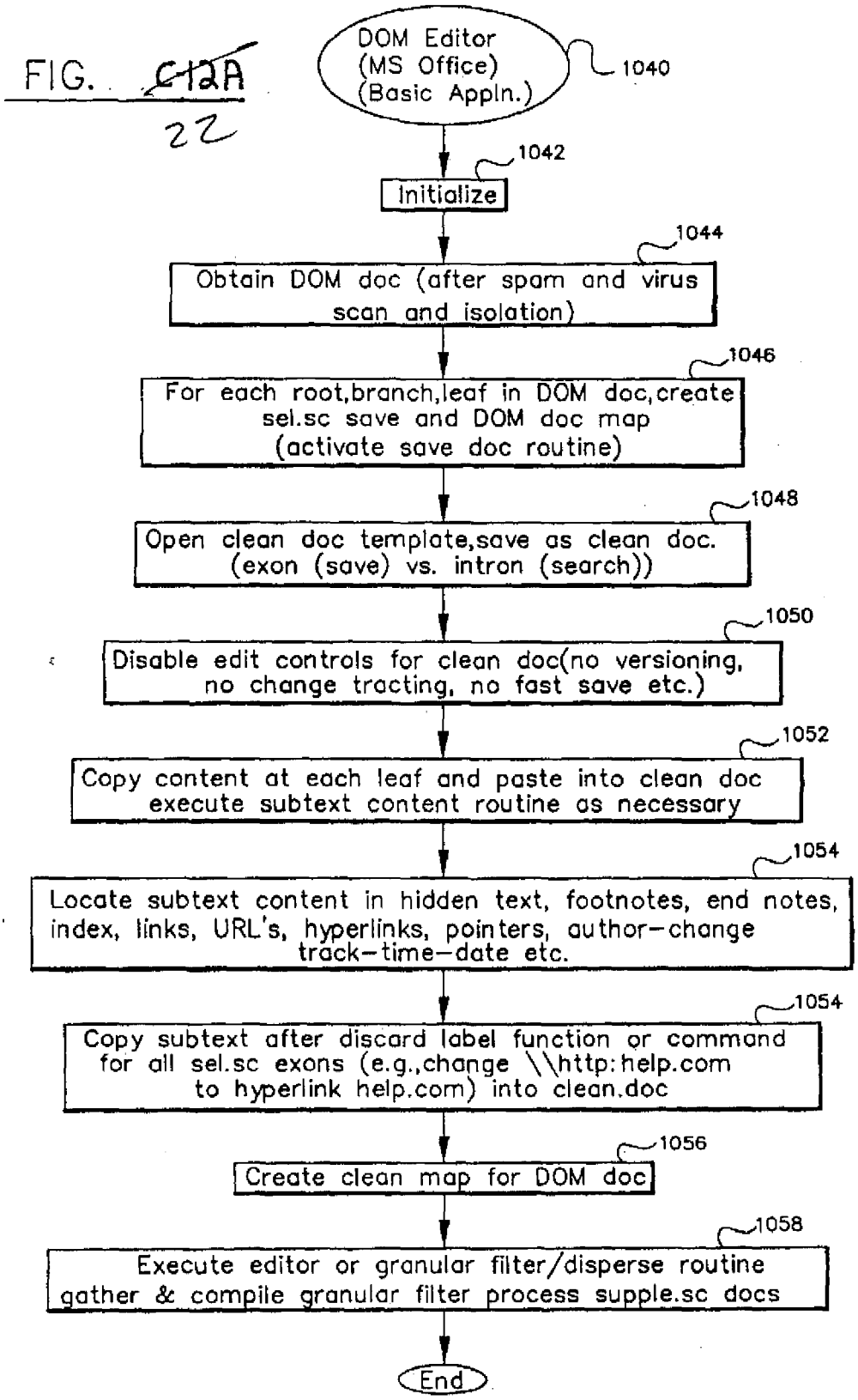

Document Object Model (DOM)(MS Office) Editor (General)
1022
Initialize
1024
Obtain DOM layout or map from DOM vendor
1026
For each root,leaf in DOM,id informational attributes (e.g.,purpose,timeliness) and prioritize with sel.cont.; organization; informational attributes store as DOM blueprint
1028
Obtain DOM doc
1030
Map DOM doc as a binary file populated with content data and meta data as a subset of the DOM blueprint
1032
Id sel.cont. exons
id sel.cont. introns to be used in search
1034
Convert sc exons at each root, branch,leaf, tax label into sel.sc save, form and format(save DOM doc), generate save blueprint or map for DOM doc,discard low exons (remainder store), expand search with introns
1036
Process content of save DOM doc;
process all data objects (introns) from DOM; search; repeat as necessary;
retrive supple doc; filter as necessary; save; map
1038
End

FIG. ~~11~~ 21

FIG. ~~C12A~~ 22


DOM Editor
(MS Office)
(Basic Appln.)
1040
1042
Initialize
1044
Obtain DOM doc (after spam and virus scan and isolation)
1046
For each root,branch,leaf in DOM doc,create sel.sc save and DOM doc map (activate save doc routine)
1048
Open clean doc template,save as clean doc. (exon (save) vs. intron (search))
1050
Disable edit controls for clean doc(no versioning, no change tracting, no fast save etc.)
1052
Copy content at each leaf and paste into clean doc execute subtext content routine as necessary
1054
Locate subtext content in hidden text, footnotes, end notes, index, links, URL's, hyperlinks, pointers, author-change track-time-date etc.
1054
Copy subtext after discard label function or command for all sel.sc exons (e.g.,change \\http:help.com to hyperlink help.com) into clean.doc
1056
Create clean map for DOM doc
1058
Execute editor or granular filter/disperse routine gather & compile granular filter process supple.sc docs
End

23

FIG. ~~C-12B~~ -- Table 1: Categorical Identifiers For Personal Identity

name
address(es) and variants
telephone number(s) and variants
username
biometrics
gene typing
photograph
date of birth
age
marital status
gender
sexual orientation
sexual proclivities
disabilities
tattoos
scars
visible or functional injuries
age/age range
hair color
eye color
race profile
educational history
employment history
home price
ethnicity
personal interests
personal descriptive information (e.g., SWHM 38, Professional)
physical stigmata
skill set
credit history
credit reports (formal NCR, etc.)
social security number
patient ID or other location- or process-specific
user assignment
insurance number
credit card numbers
birthplace
heritage
health history
political party
political beliefs
association(s)
frequent flyer/buyer club info
remittance advice
investigation evidence
court evidence
EDI/EDIFACT records
applications
personal web sites
Chain of trust forms
Chain of custody forms
skill set
religion
personal interests
travel log
number of siblings
business partners
business name
profession
account numbers (banking, services, suppliers)
service providers (physicians, insurers, hospitals, clinics, etc.)
X-rays
surveillance
dental charts
medical records
account balances
account transfer or transaction amounts
income range
neighborhood/city/region/country
license (driver, occupational, professional)
vehicle registration (license, tag, plate, etc.)
vehicle identification
vehicle make, type, model, color, year
date of life events
incident reports (legal, criminal, health services, news)
accident reports (auto, OSHA, EPA, EEOC, etc.)
criminal convictions
court records
abuse records
divorce proceedings
bankruptcy records
organization registrations
Corporation officers and registrations
tax records (chattel, land, local, state, Federal, and special use taxes)
property ownership
permit applications
donor lists
news reports
family history
family relationships
family health history
legal documents
consent forms
newsgroup postings

24

FIG. ~~C-12C~~ -- Table 2: Ranked Identity Category

name	disabilities
address	tattoos
telephone	scars
username	injuries
biometrics	age range
gene typing	hair color
photograph	eye color
date of birth	race profile
age	education
marital status	employment
sex	personal interests
sexual orientation	
sexual proclivities	

25

FIG. ~~C-12D~~ -- Table 3: Categorical Identifiers for Manufacturing Business

- Manufacturing
  - product brand names
  - product generic name
  - drawings
  - tools (brand names and generic names)
    - hand tools
    - software
    - machines
  - software, computer programs, etc.
  - Research and Development
    - competitors products, competitor names, patent numbers, patent titles, project names, project personnel
- Sales
  - personnel
  - competitors
  - sales data
    - quantity
    - geographic distribution
  - customers
    - names, addresses, contacts
  - sales projections
- Financial
  - chart of accounts
  - ledgers
  - financial statements
  - tax returns
- Human Resources
  - see categorical identifiers for personal identity

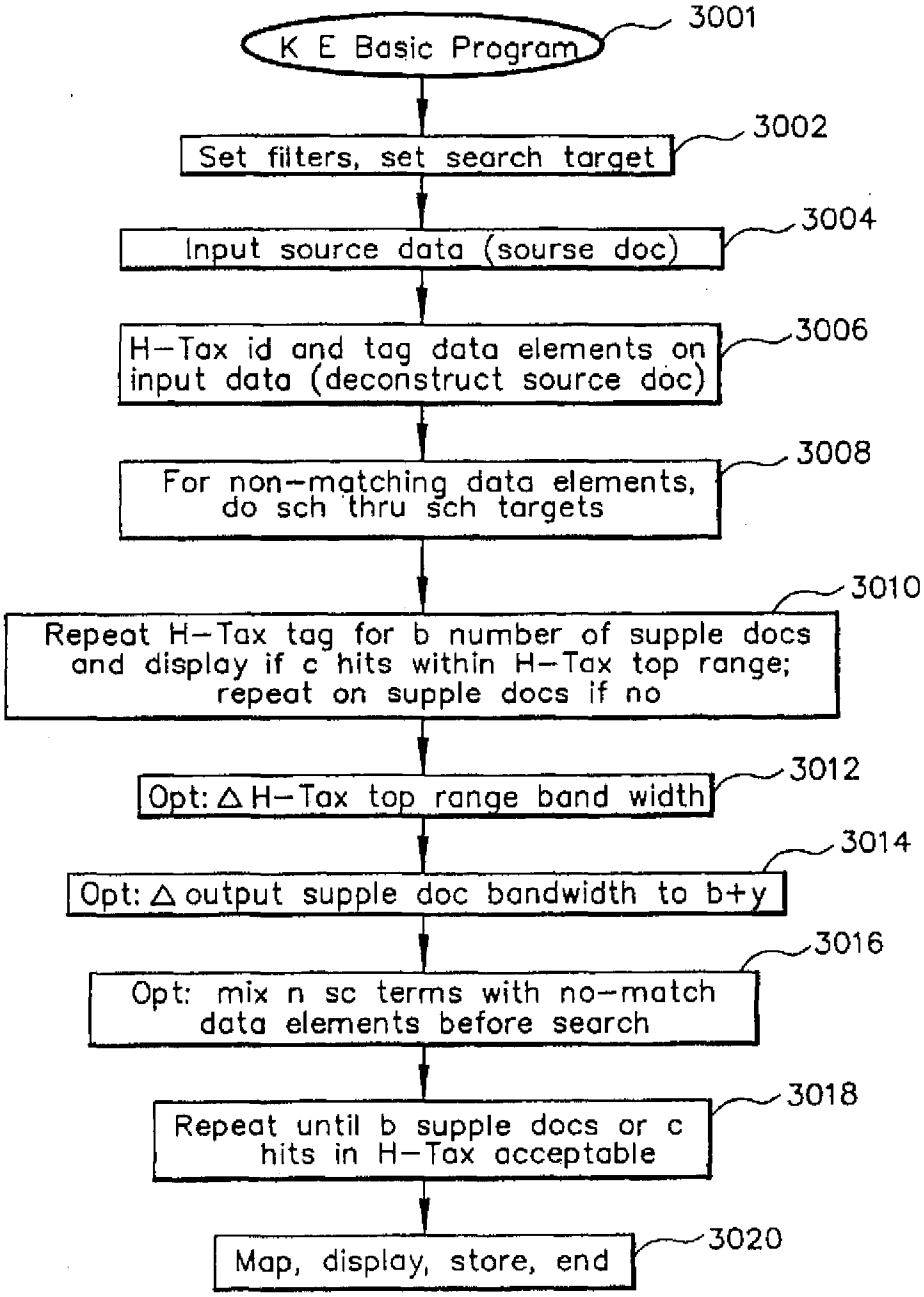

K E Basic Program
3001
Set filters, set search target
3002
Input source data (sourse doc)
3004
H–Tax id and tag data elements on input data (deconstruct source doc)
3006
For non–matching data elements, do sch thru sch targets
3008
Repeat H–Tax tag for b number of supple docs and display if c hits within H–Tax top range; repeat on supple docs if no
3010
Opt: Δ H–Tax top range band width
3012
Opt: Δ output supple doc bandwidth to b+y
3014
Opt: mix n sc terms with no–match data elements before search
3016
Repeat until b supple docs or c hits in H–Tax acceptable
3018
Map, display, store, end
3020

FIG. ~~C-13~~ 26

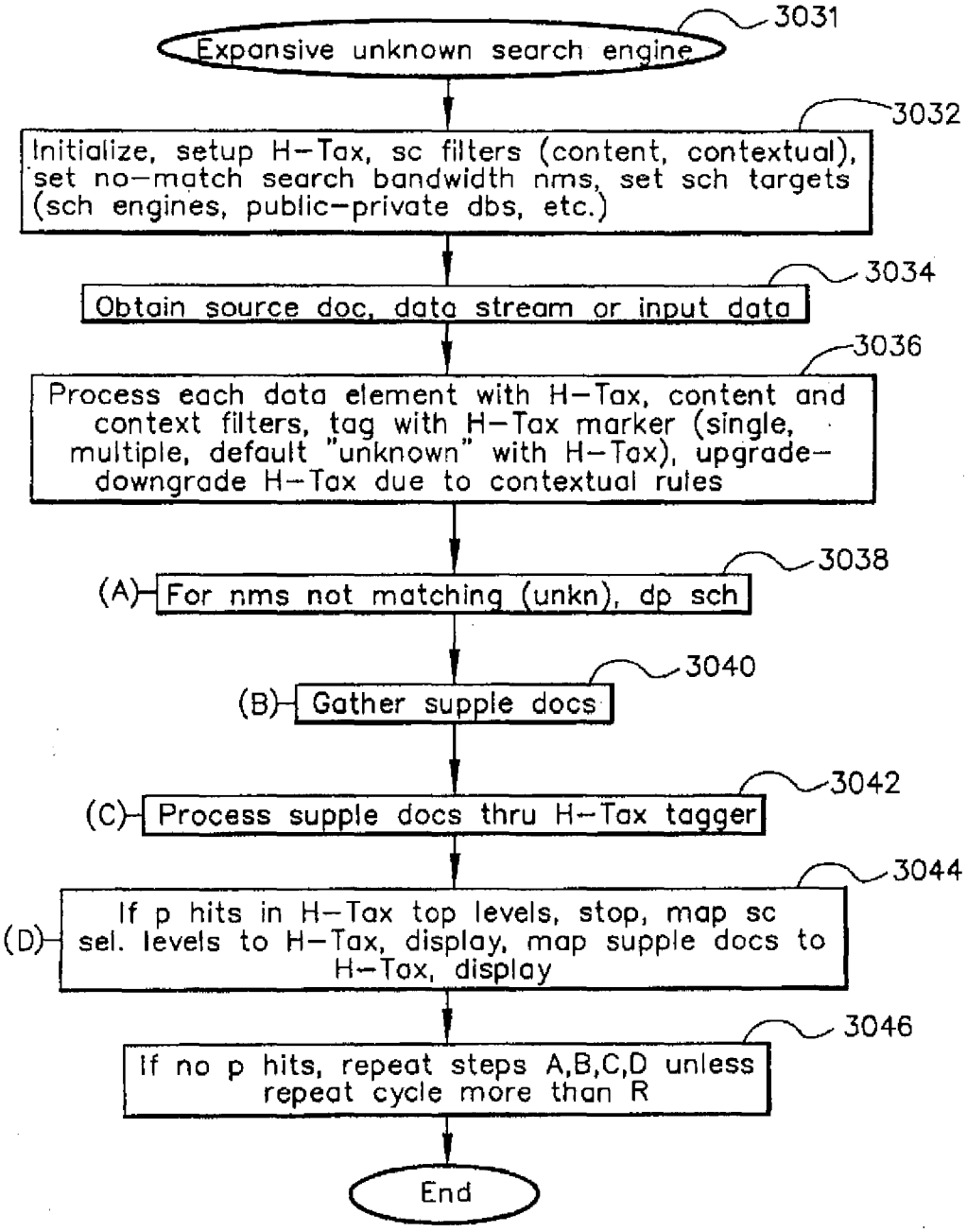

3031
Expansive unknown search engine
3032
Initialize, setup H-Tax, sc filters (content, contextual), set no-match search bandwidth nms, set sch targets (sch engines, public-private dbs, etc.)
3034
Obtain source doc, data stream or input data
3036
Process each data element with H-Tax, content and context filters, tag with H-Tax marker (single, multiple, default "unknown" with H-Tax), upgrade-downgrade H-Tax due to contextual rules
3038
(A) For nms not matching (unkn), dp sch
3040
(B) Gather supple docs
3042
(C) Process supple docs thru H-Tax tagger
3044
(D) If p hits in H-Tax top levels, stop, map sc sel. levels to H-Tax, display, map supple docs to H-Tax, display
3046
If no p hits, repeat steps A,B,C,D unless repeat cycle more than R
End

FIG. 14

27

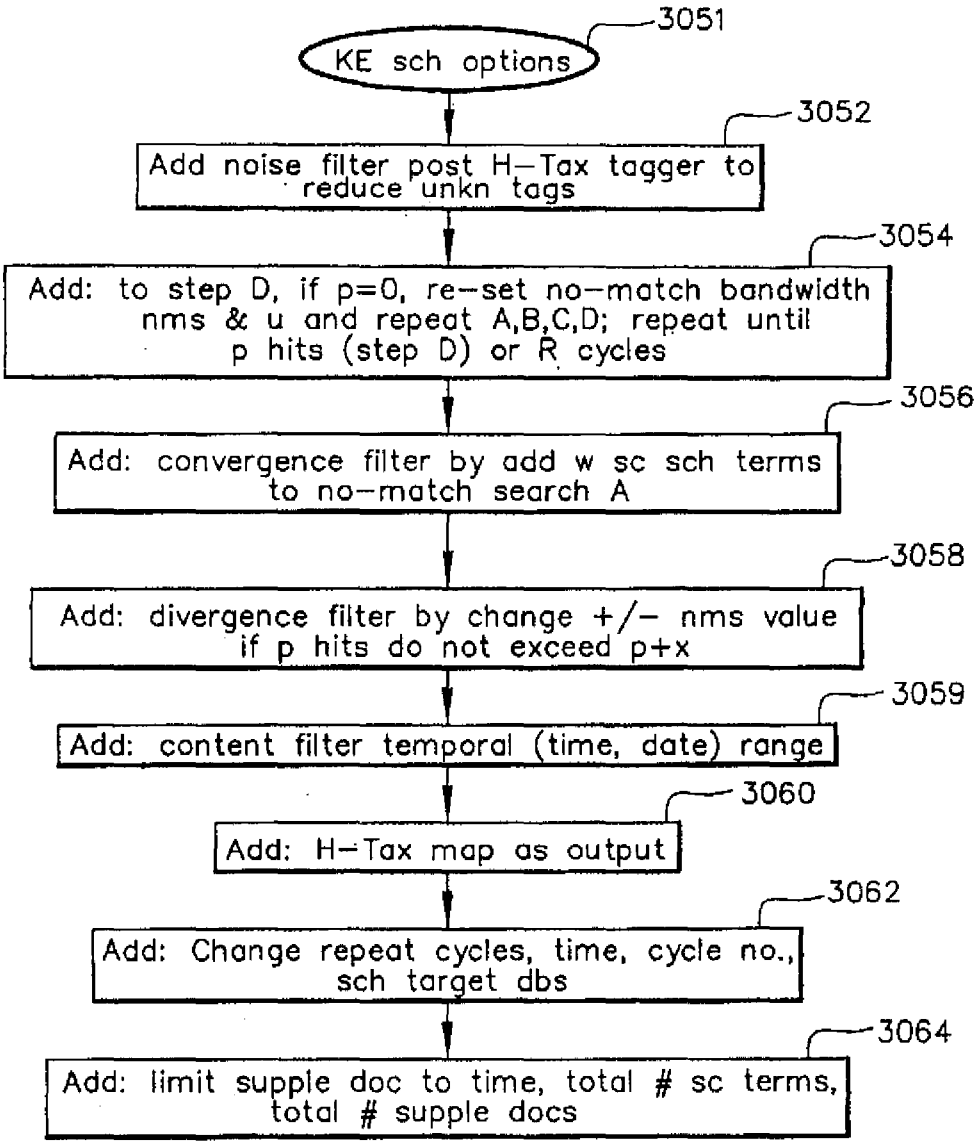

3051
KE sch options
3052
Add noise filter post H–Tax tagger to reduce unkn tags
3054
Add: to step D, if p=0, re–set no–match bandwidth nms & u and repeat A,B,C,D; repeat until p hits (step D) or R cycles
3056
Add: convergence filter by add w sc sch terms to no–match search A
3058
Add: divergence filter by change +/– nms value if p hits do not exceed p+x
3059
Add: content filter temporal (time, date) range
3060
Add: H–Tax map as output
3062
Add: Change repeat cycles, time, cycle no., sch target dbs
3064
Add: limit supple doc to time, total # sc terms, total # supple docs

FIG. 15

28

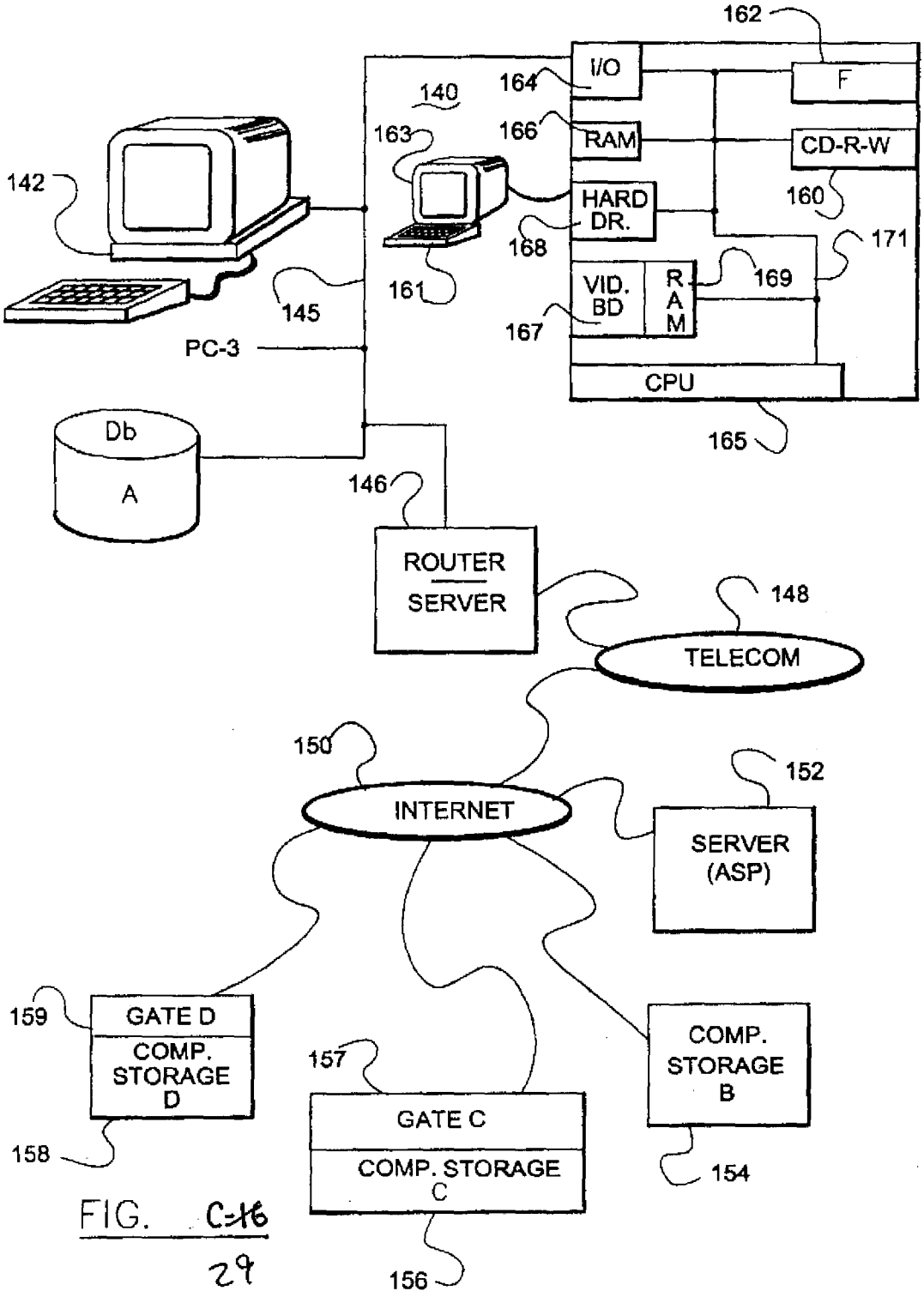

162
I/O
164
F
140
163
166
RAM
CD-R-W
142
HARD DR.
160
168
171
VID. BD
R A M
169
161
145
167
PC-3
CPU
165
Db
A
146
ROUTER SERVER
148
TELECOM
150
152
INTERNET
SERVER (ASP)
159
GATE D
COMP. STORAGE D
157
COMP. STORAGE B
GATE C
COMP. STORAGE C
158
154
156

FIG. C-16

29

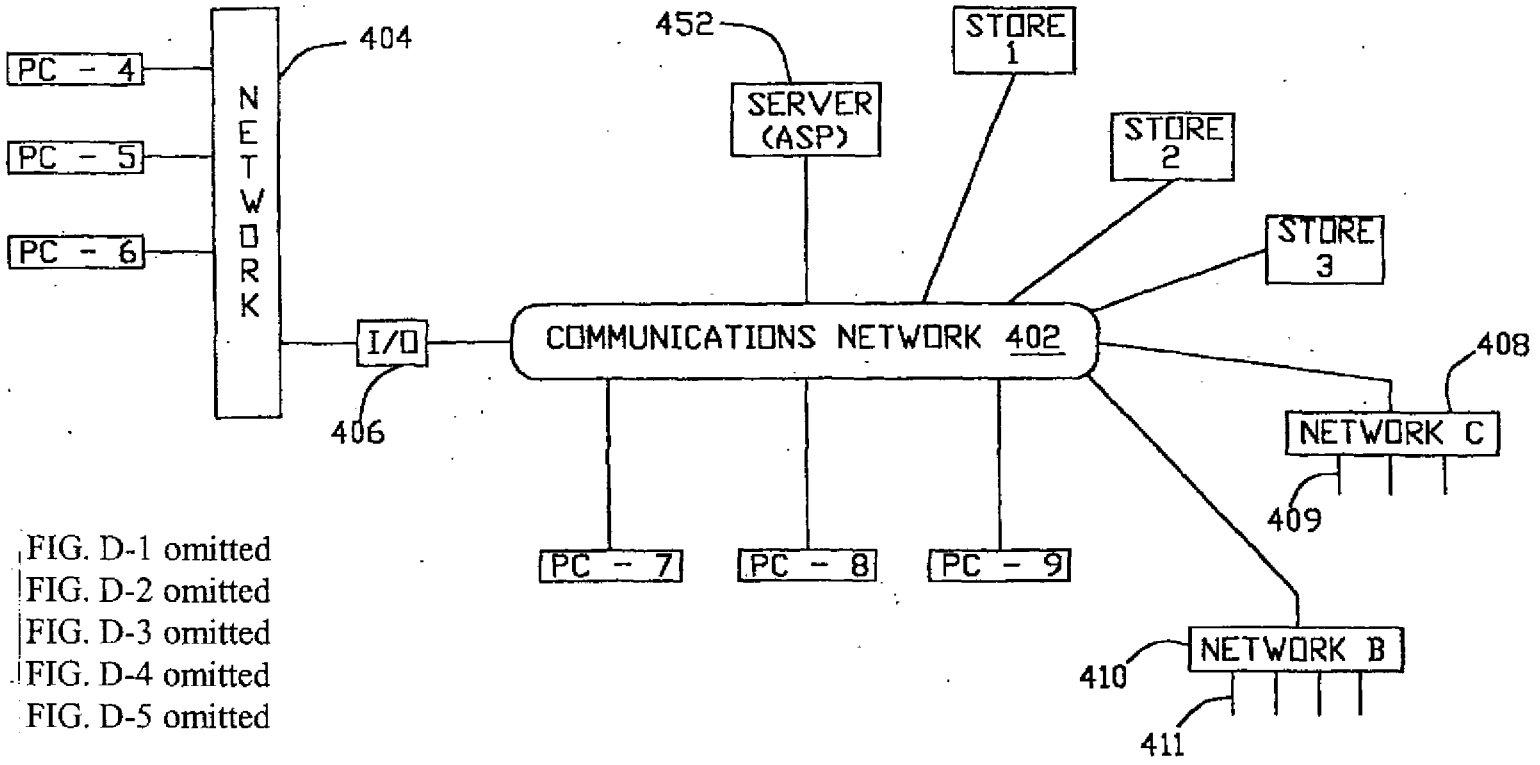
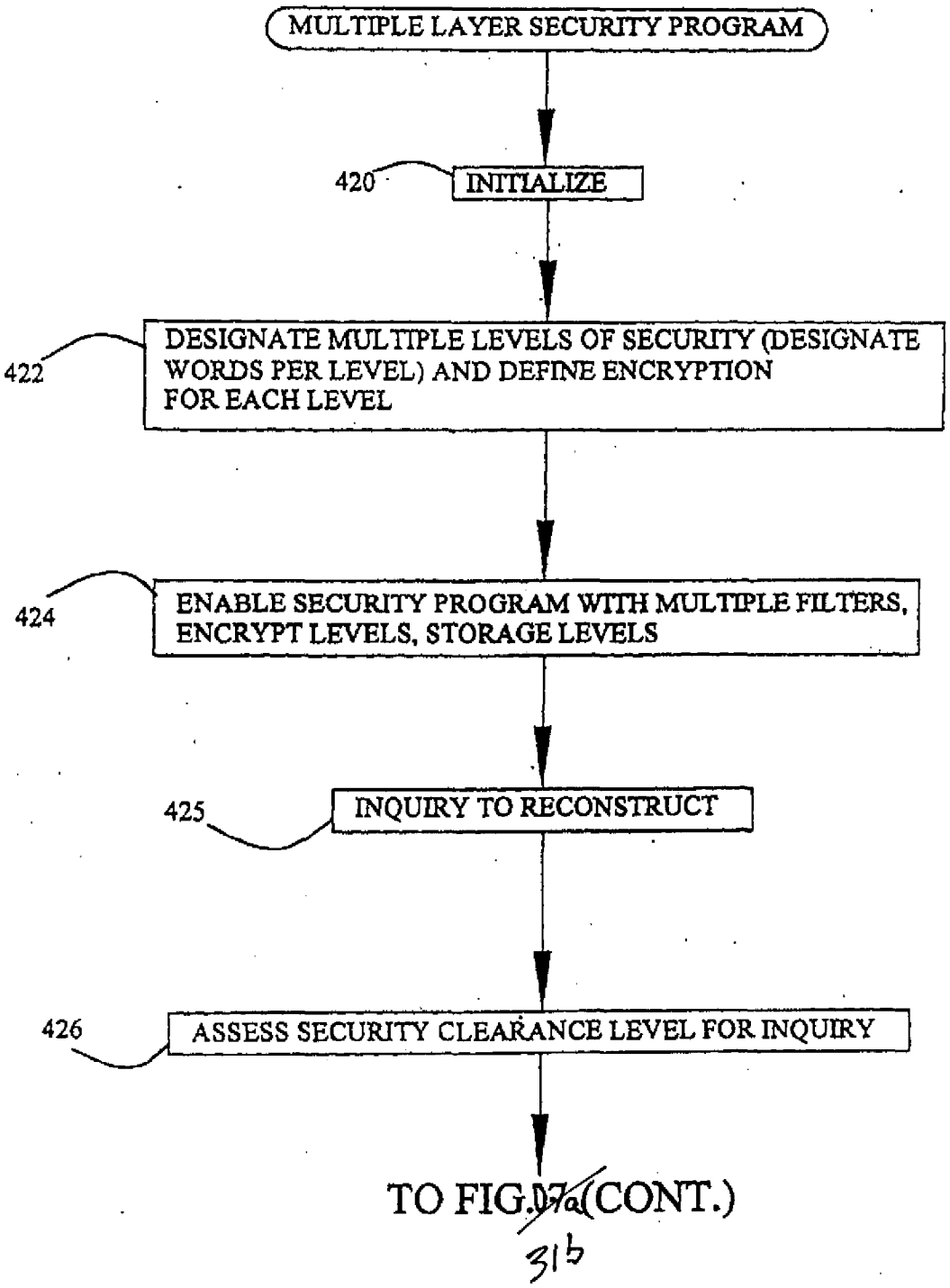


FIG. D-1 omitted
FIG. D-2 omitted
FIG. D-3 omitted
FIG. D-4 omitted
FIG. D-5 omitted

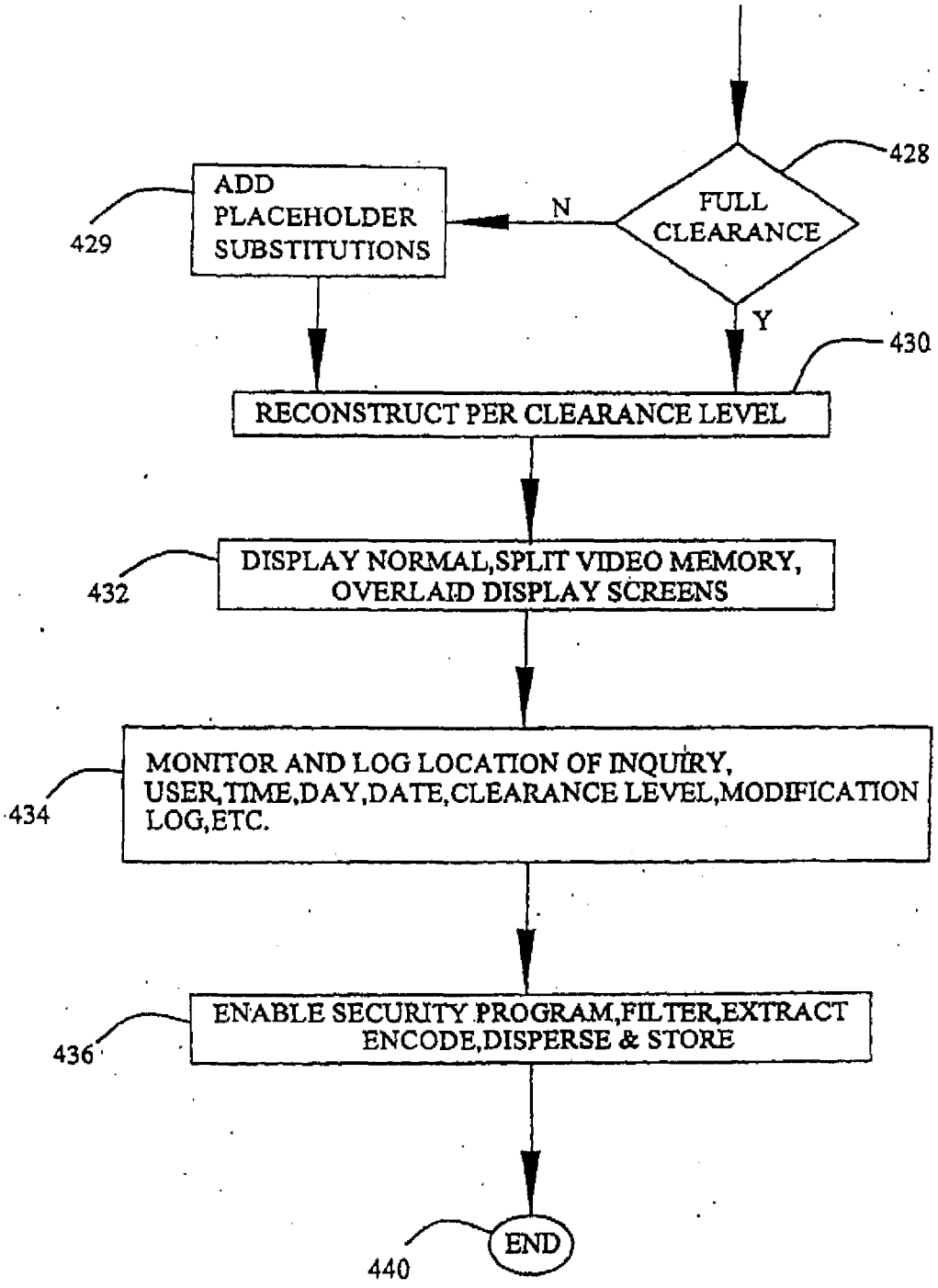
FIG. ~~D-6~~ 30

FIG. ~~D-7a~~ 31a



31b

FIG. 3a (CONT.) 3b



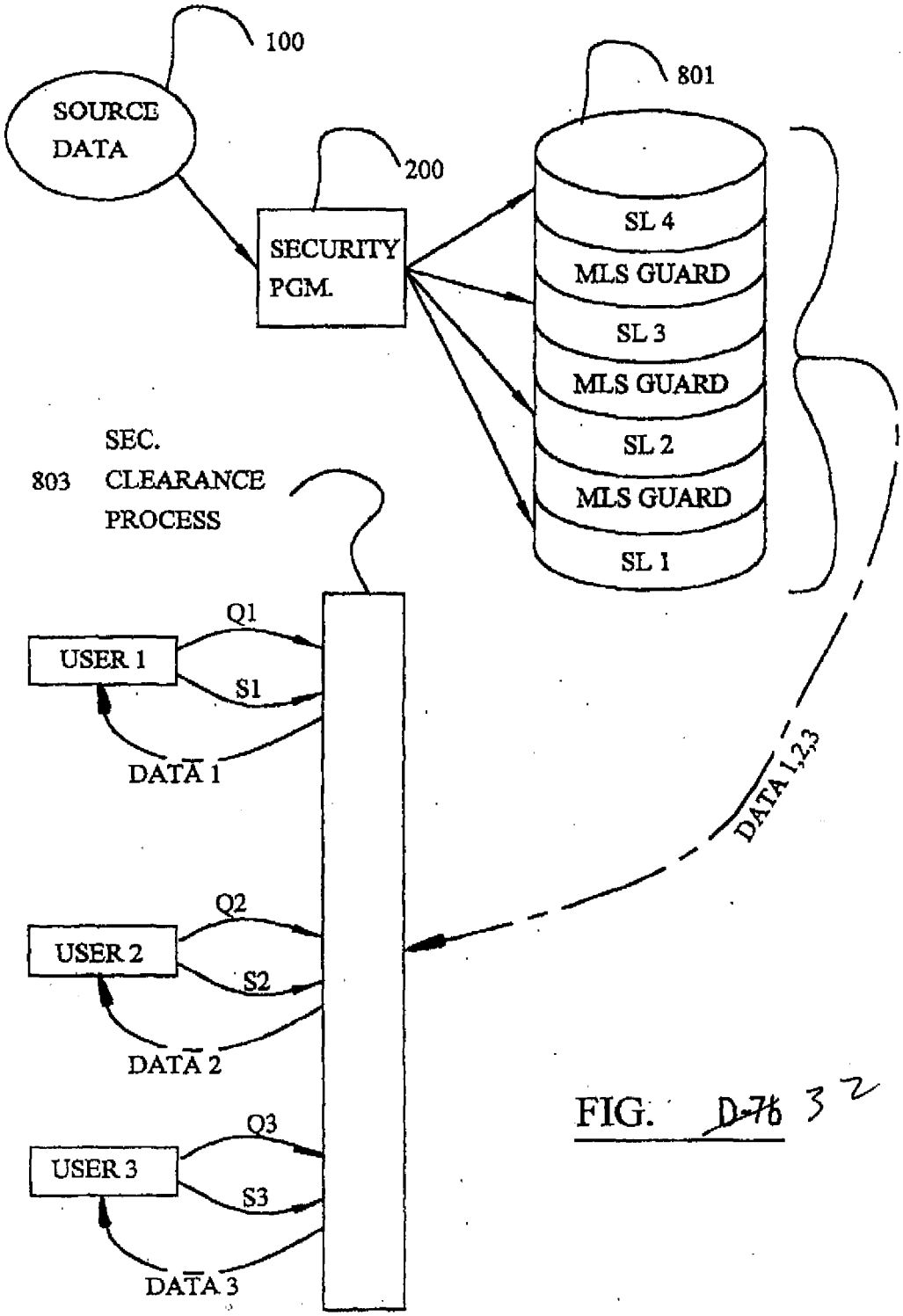
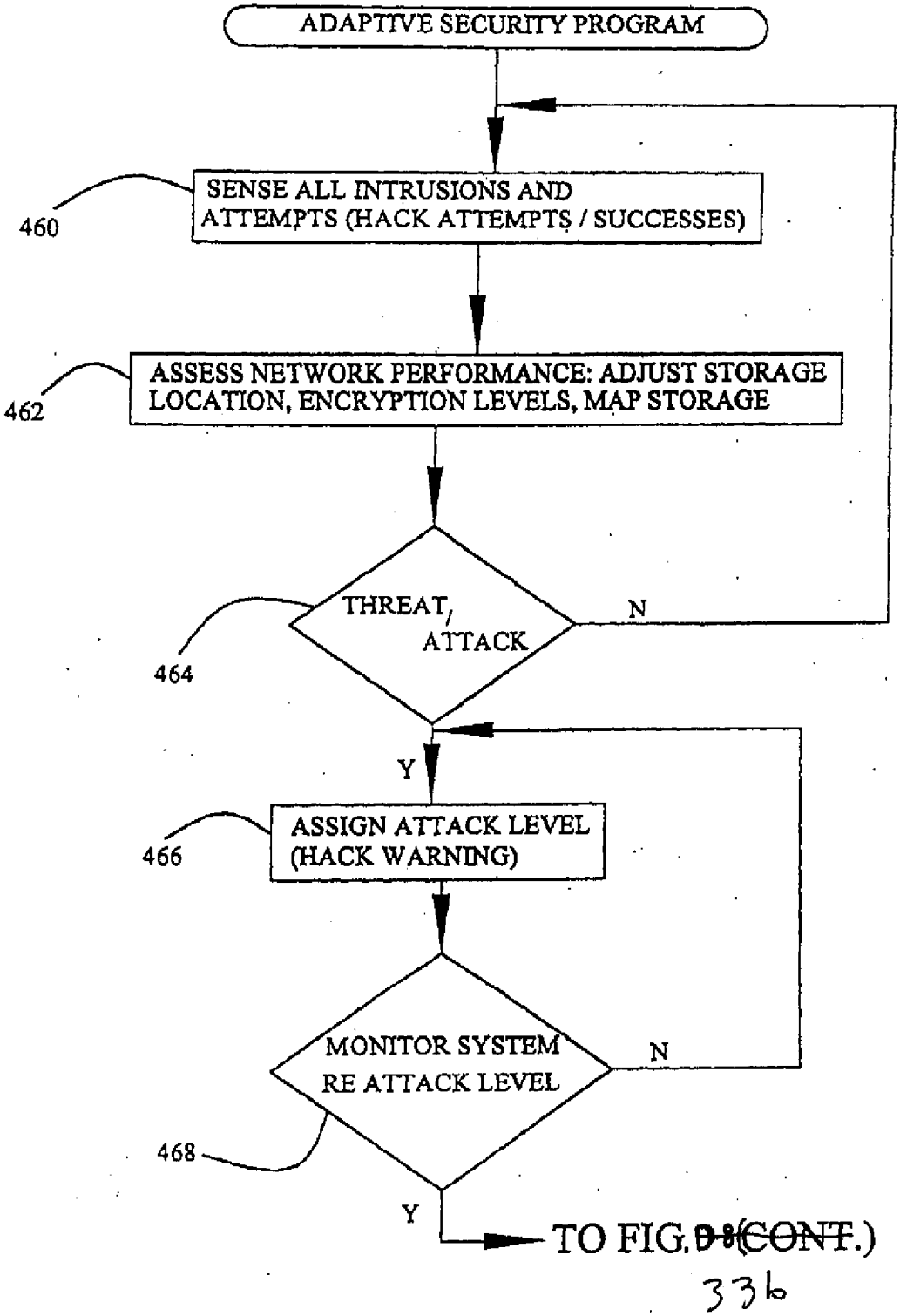

100
SOURCE DATA
200
SECURITY PGM.
801
SL 4
MLS GUARD
SL 3
MLS GUARD
SL 2
MLS GUARD
SL 1
803
SEC. CLEARANCE PROCESS
Q1
USER 1
S1
DATA 1
Q2
USER 2
S2
DATA 2
Q3
USER 3
S3
DATA 3
DATA 1,2,3

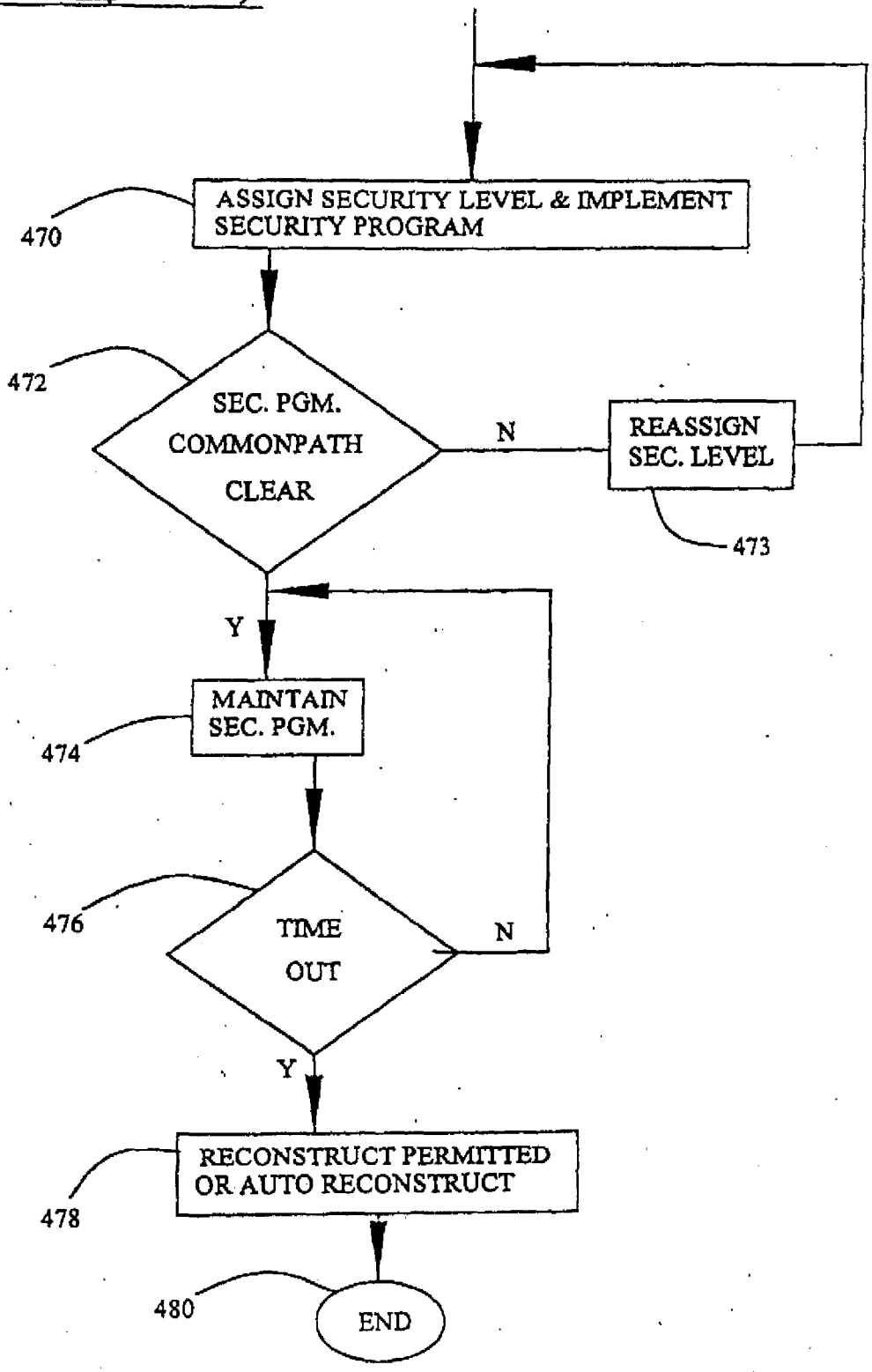
FIG. ~~D-76~~ 3 2

FIG. ~~D8~~ 33a


ADAPTIVE SECURITY PROGRAM
460
SENSE ALL INTRUSIONS AND ATTEMPTS (HACK ATTEMPTS / SUCCESSES)
462
ASSESS NETWORK PERFORMANCE: ADJUST STORAGE LOCATION, ENCRYPTION LEVELS, MAP STORAGE
464
THREAT, ATTACK
N
Y
466
ASSIGN ATTACK LEVEL (HACK WARNING)
MONITOR SYSTEM RE ATTACK LEVEL
N
468
Y
TO FIG. ~~D8~~ (CONT.)
336

33b

FIG. ~~D-8~~ (CONT.)



3C

FIG. ~~D-8A~~

Standard Automatic Defenses Matrix Table

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

35

FIG. ~~D-8B~~ Optional Automatic Defenses Matrix Table

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

36

FIG. ~~D-8C~~

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

37

FIG. ~~D-8D~~

Normal Work Mode Table

	Extraction Level 1	Level 2	Level 3	Level 4	Storage Web	Offline	Remote	Removable	Local
social security	X						X		
credit card	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 cap			X					X	
currency				X					X
postal code				X					X
address				X					X
location				X					X
date				X					X

38

FIG. ~~D-8E~~

Threat Mode Table

	Extraction Level 1	Level 2	Level 3	Level 4	Storage Web	Offline	Remote	Removable	Local
social security	X							X	
credit card	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

39

FIG. ~~D-8F~~

Attack Mode Table

	Extraction Level 1	Level 2	Level 3	Level 4	Storage Web	Offline	Remote	Removable
social security	X					X		
credit card	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	

40

FIG. ~~D-9~~

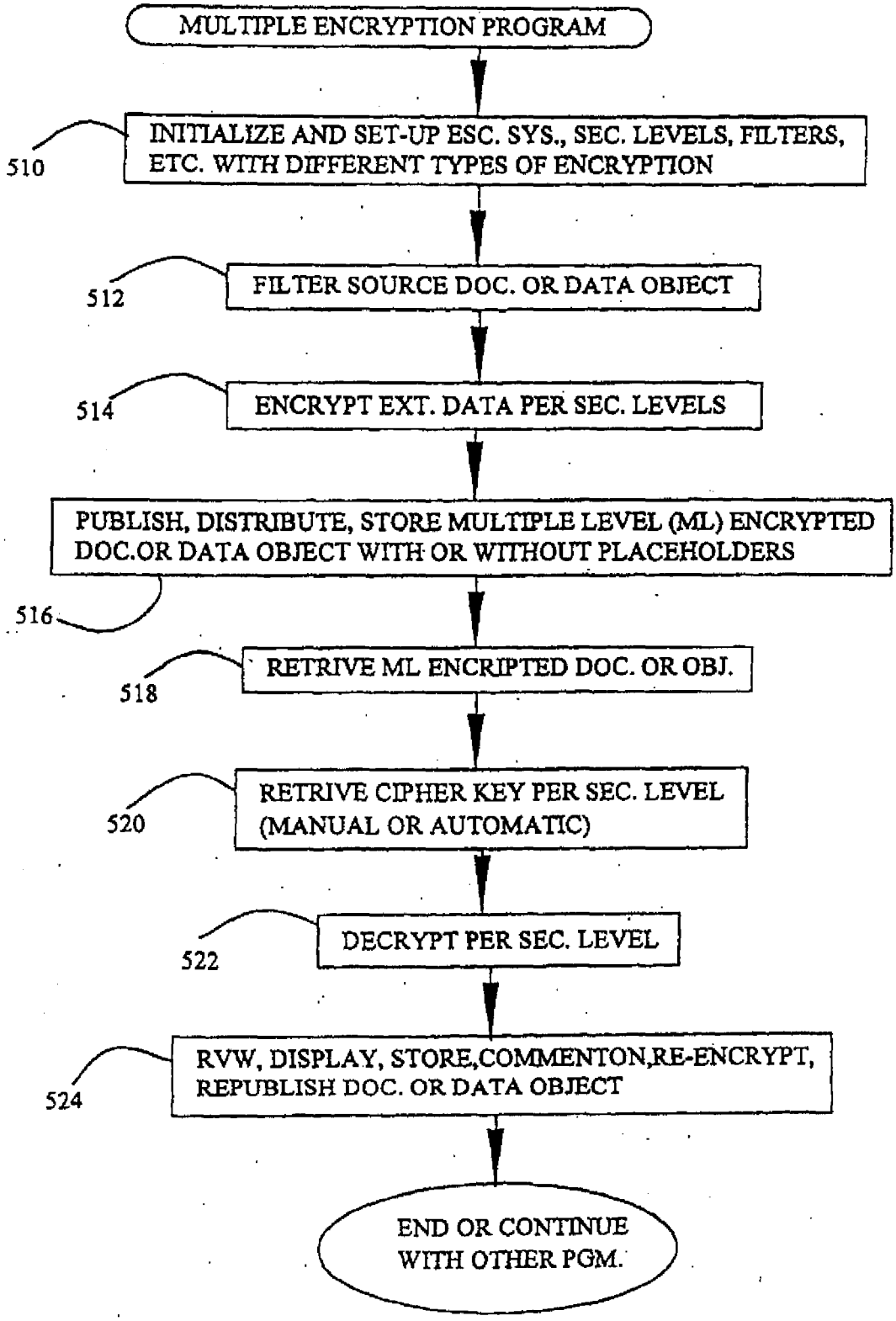

MULTIPLE ENCRYPTION PROGRAM
510
INITIALIZE AND SET-UP ESC. SYS., SEC. LEVELS, FILTERS, ETC. WITH DIFFERENT TYPES OF ENCRYPTION
512
FILTER SOURCE DOC. OR DATA OBJECT
514
ENCRYPT EXT. DATA PER SEC. LEVELS
PUBLISH, DISTRIBUTE, STORE MULTIPLE LEVEL (ML) ENCRYPTED DOC.OR DATA OBJECT WITH OR WITHOUT PLACEHOLDERS
516
518
RETRIVE ML ENCRIPTED DOC. OR OBJ.
520
RETRIVE CIPHER KEY PER SEC. LEVEL (MANUAL OR AUTOMATIC)
522
DECRYPT PER SEC. LEVEL
524
RVW, DISPLAY, STORE,COMMENTON,RE-ENCRYPT, REPUBLISH DOC. OR DATA OBJECT
END OR CONTINUE WITH OTHER PGM.

FIG. 41 D-10

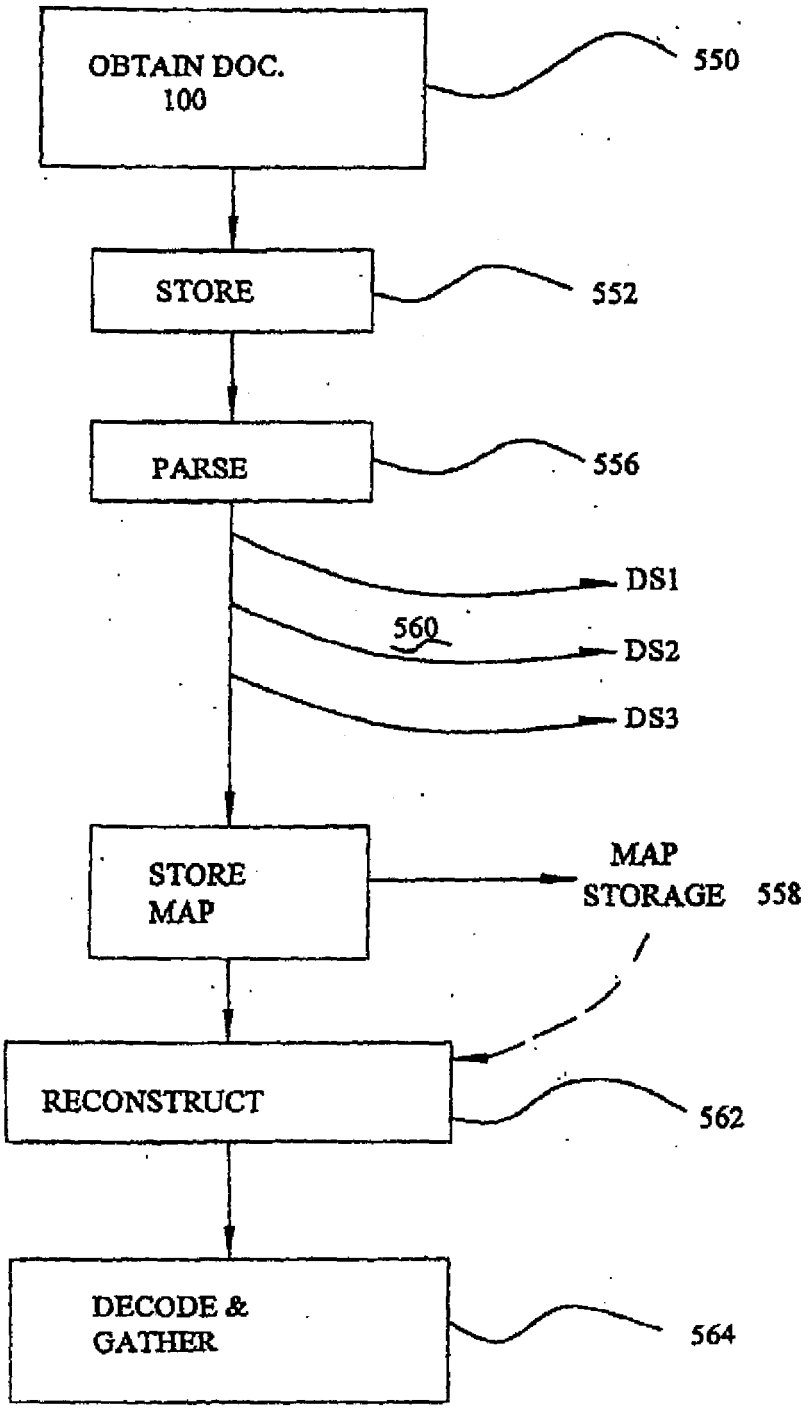

OBTAIN DOC. 100
550
STORE
552
PARSE
556
DS1
560
DS2
DS3
STORE MAP
MAP STORAGE 558
RECONSTRUCT
562
DECODE & GATHER
564

FIG. D-11A

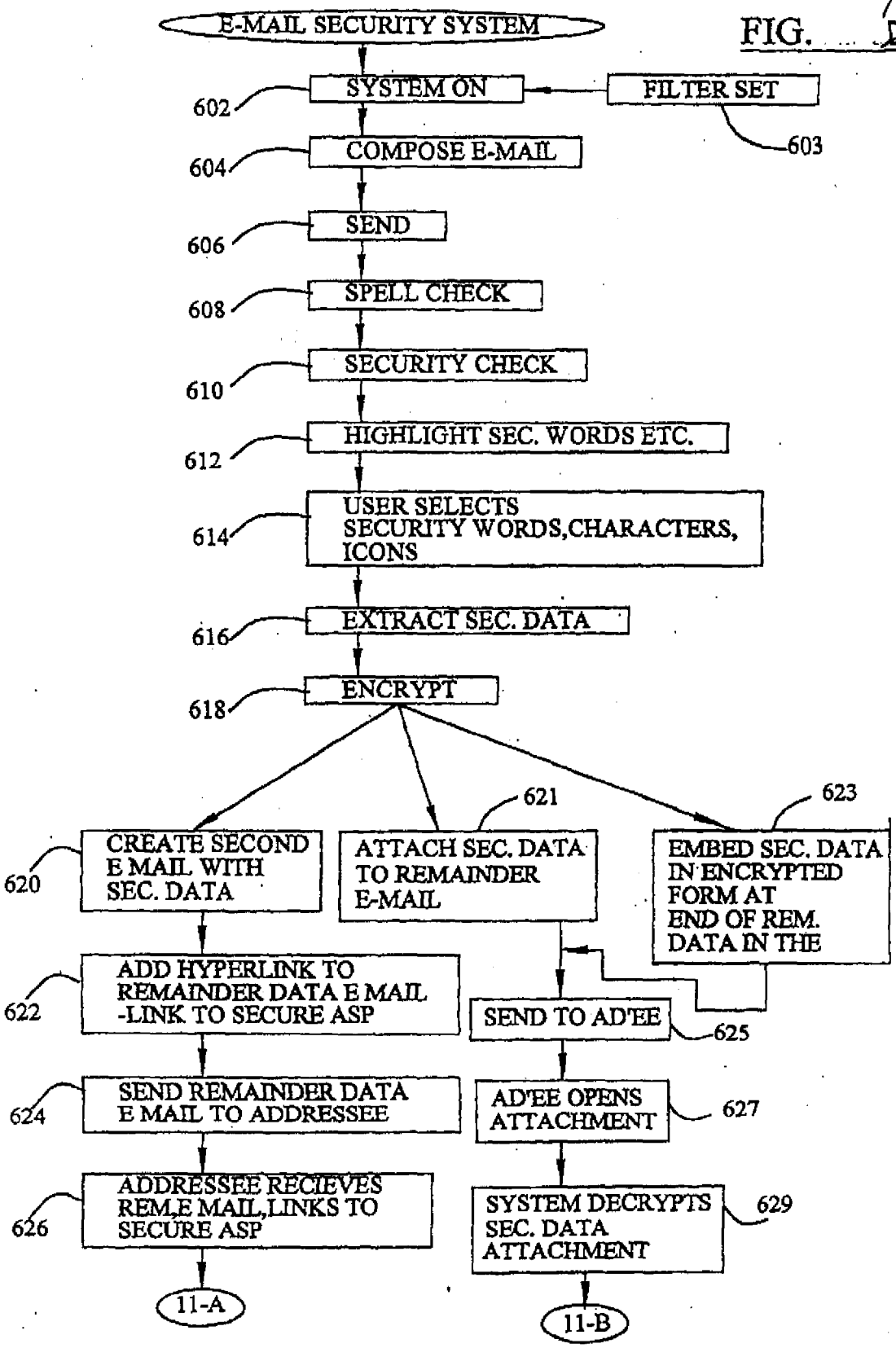

E-MAIL SECURITY SYSTEM
SYSTEM ON
FILTER SET
602
603
COMPOSE E-MAIL
604
SEND
606
SPELL CHECK
608
SECURITY CHECK
610
HIGHLIGHT SEC. WORDS ETC.
612
USER SELECTS SECURITY WORDS,CHARACTERS, ICONS
614
EXTRACT SEC. DATA
616
ENCRYPT
618
CREATE SECOND E MAIL WITH SEC. DATA
620
ATTACH SEC. DATA TO REMAINDER E-MAIL
621
EMBED SEC. DATA IN ENCRYPTED FORM AT END OF REM. DATA IN THE
623
ADD HYPERLINK TO REMAINDER DATA E MAIL -LINK TO SECURE ASP
622
SEND TO AD'EE
625
SEND REMAINDER DATA E MAIL TO ADDRESSEE
624
AD'EE OPENS ATTACHMENT
627
ADDRESSEE RECIEVES REM,E MAIL,LINKS TO SECURE ASP
626
SYSTEM DECRYPTS SEC. DATA ATTACHMENT
629
11-A
11-B

FIG. D-11B

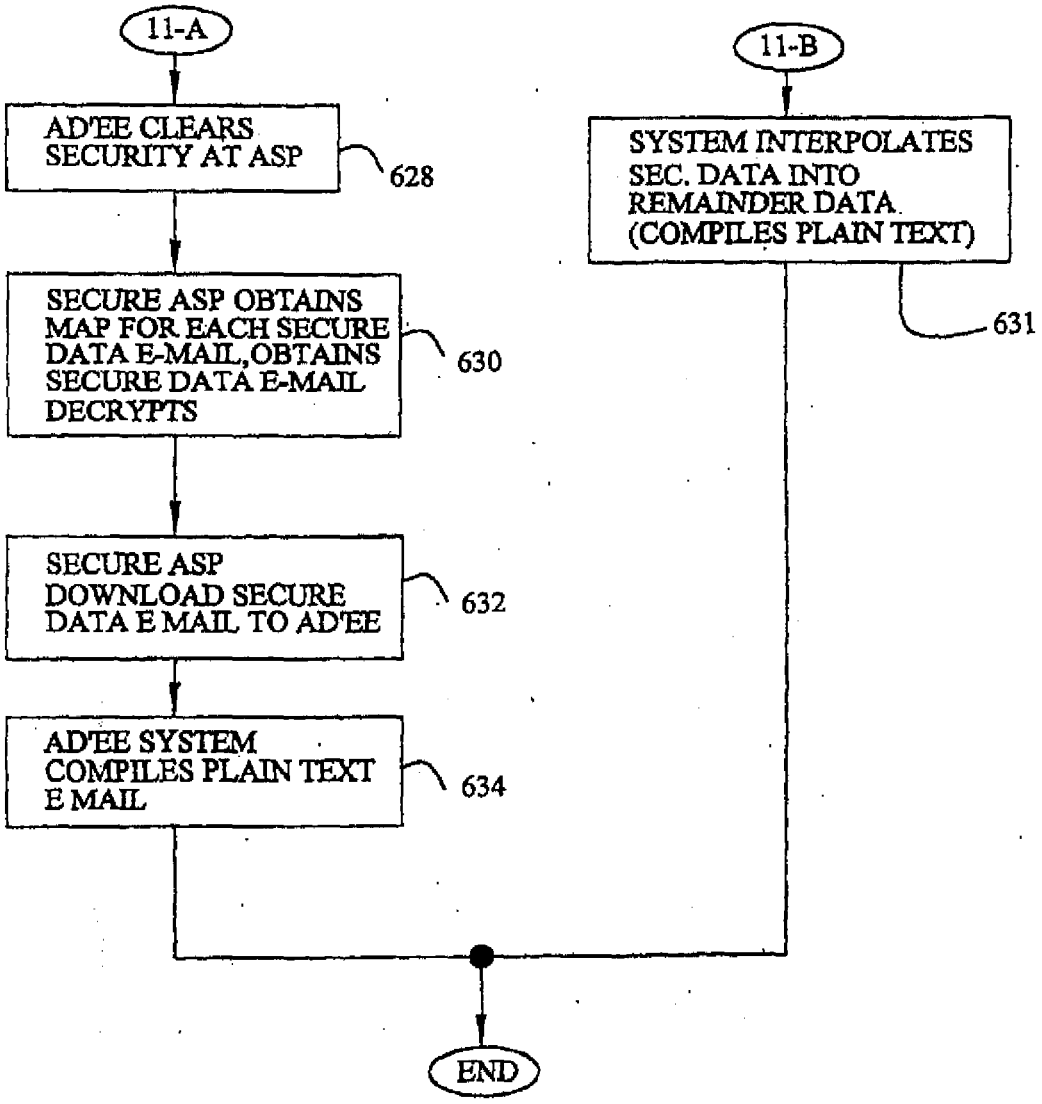
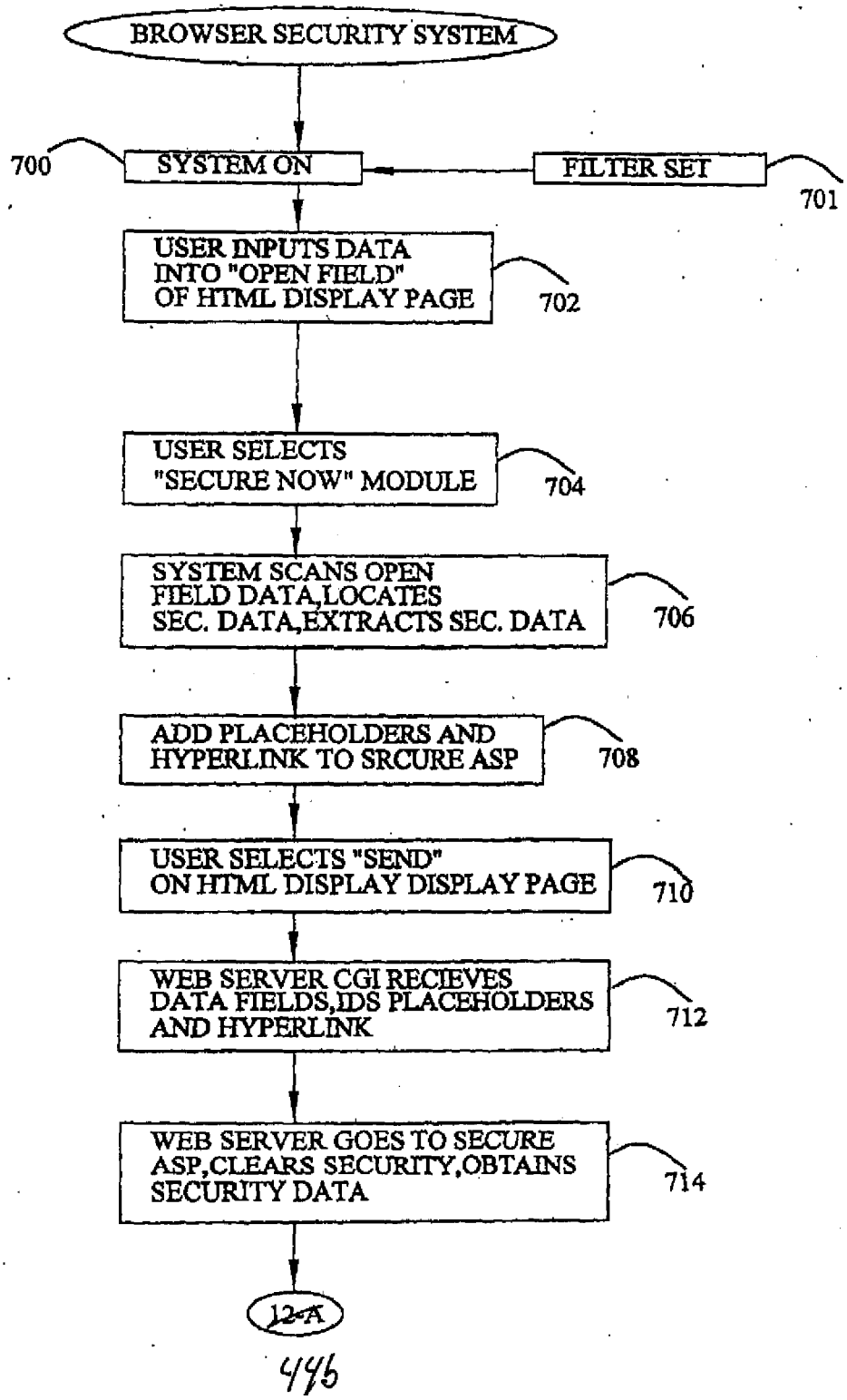

11-A
AD'EE CLEARS SECURITY AT ASP
628
SECURE ASP OBTAINS MAP FOR EACH SECURE DATA E-MAIL, OBTAINS SECURE DATA E-MAIL DECRYPTS
630
SECURE ASP DOWNLOAD SECURE DATA E MAIL TO AD'EE
632
AD'EE SYSTEM COMPILES PLAIN TEXT E MAIL
634
11-B
SYSTEM INTERPOLATES SEC. DATA INTO REMAINDER DATA. (COMPILES PLAIN TEXT)
631
END

FIG. 44a


BROWSER SECURITY SYSTEM
700
SYSTEM ON
FILTER SET
701
USER INPUTS DATA INTO "OPEN FIELD" OF HTML DISPLAY PAGE
702
USER SELECTS "SECURE NOW" MODULE
704
SYSTEM SCANS OPEN FIELD DATA,LOCATES SEC. DATA,EXTRACTS SEC. DATA
706
ADD PLACEHOLDERS AND HYPERLINK TO SRCURE ASP
708
USER SELECTS "SEND" ON HTML DISPLAY DISPLAY PAGE
710
WEB SERVER CGI RECIEVES DATA FIELDS,IDS PLACEHOLDERS AND HYPERLINK
712
WEB SERVER GOES TO SECURE ASP,CLEARS SECURITY,OBTAINS SECURITY DATA
714
12A

44b

FIG. 12B

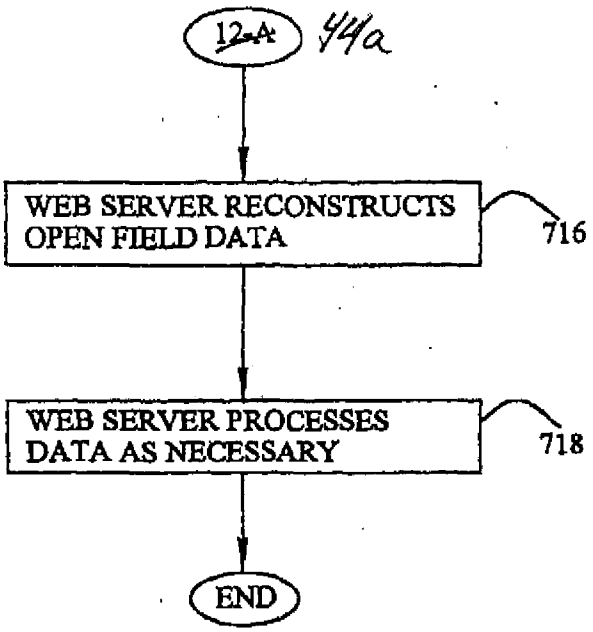
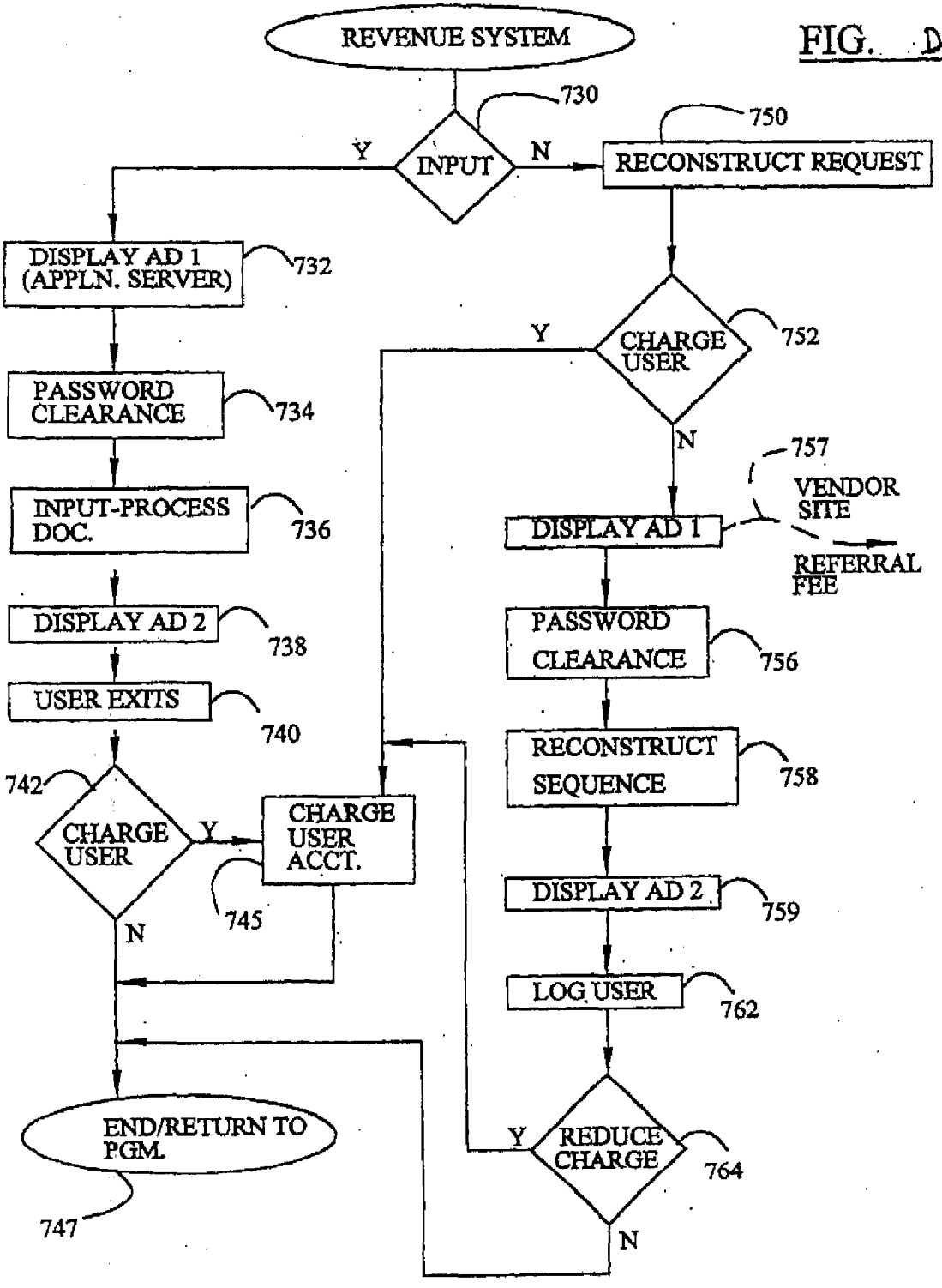

12A
WEB SERVER RECONSTRUCTS OPEN FIELD DATA
716
WEB SERVER PROCESSES DATA AS NECESSARY
718
END

FIG. D-13


REVENUE SYSTEM
730
INPUT
Y
N
750
RECONSTRUCT REQUEST
DISPLAY AD 1 (APPLN. SERVER)
732
PASSWORD CLEARANCE
734
INPUT-PROCESS DOC.
736
DISPLAY AD 2
738
USER EXITS
740
742
CHARGE USER
Y
CHARGE USER ACCT.
745
N
747
END/RETURN TO PGM
Y
CHARGE USER
752
N
757
VENDOR SITE
DISPLAY AD 1
REFERRAL FEE
PASSWORD CLEARANCE
756
RECONSTRUCT SEQUENCE
758
DISPLAY AD 2
759
LOG USER
762
Y
REDUCE CHARGE
764
N

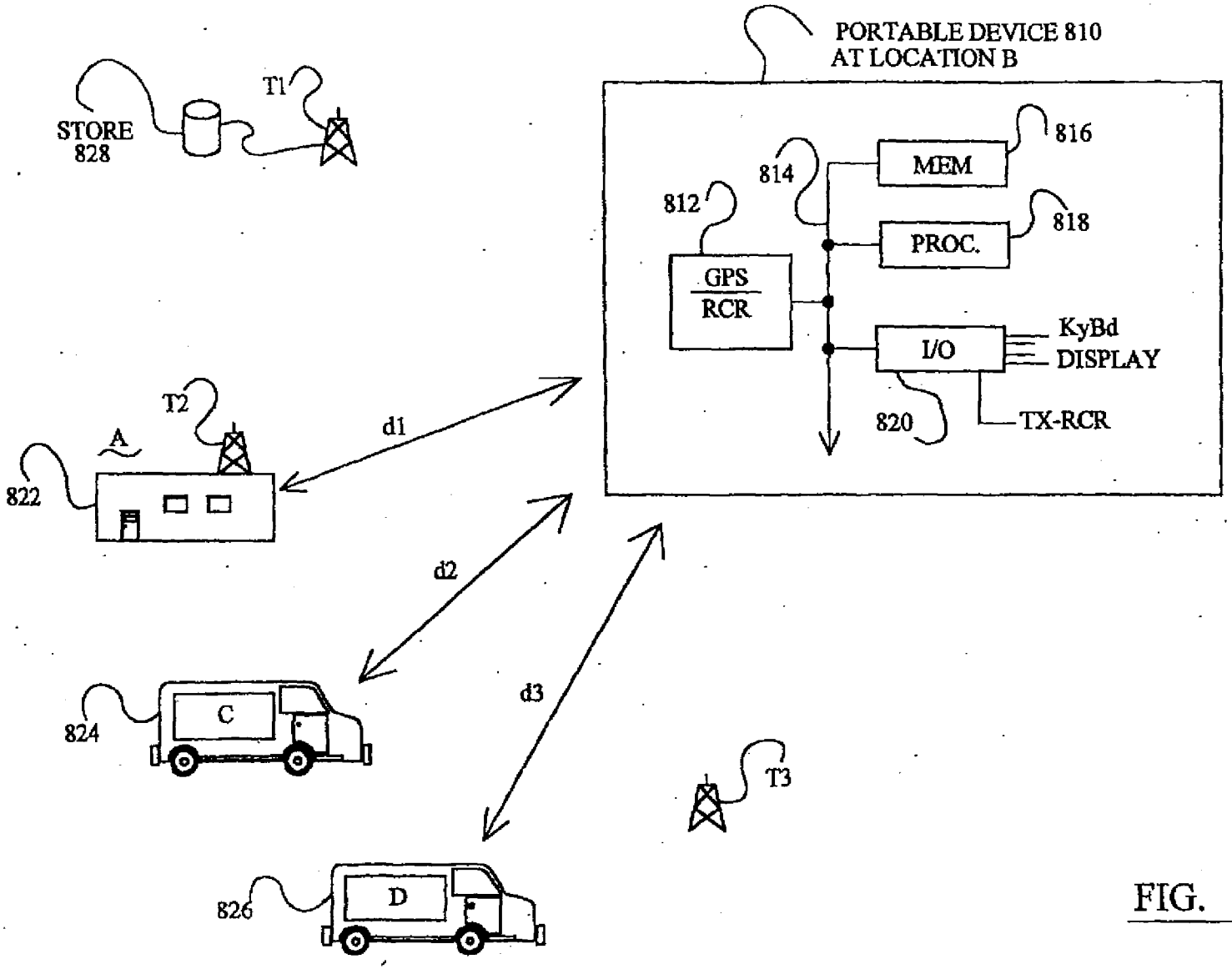
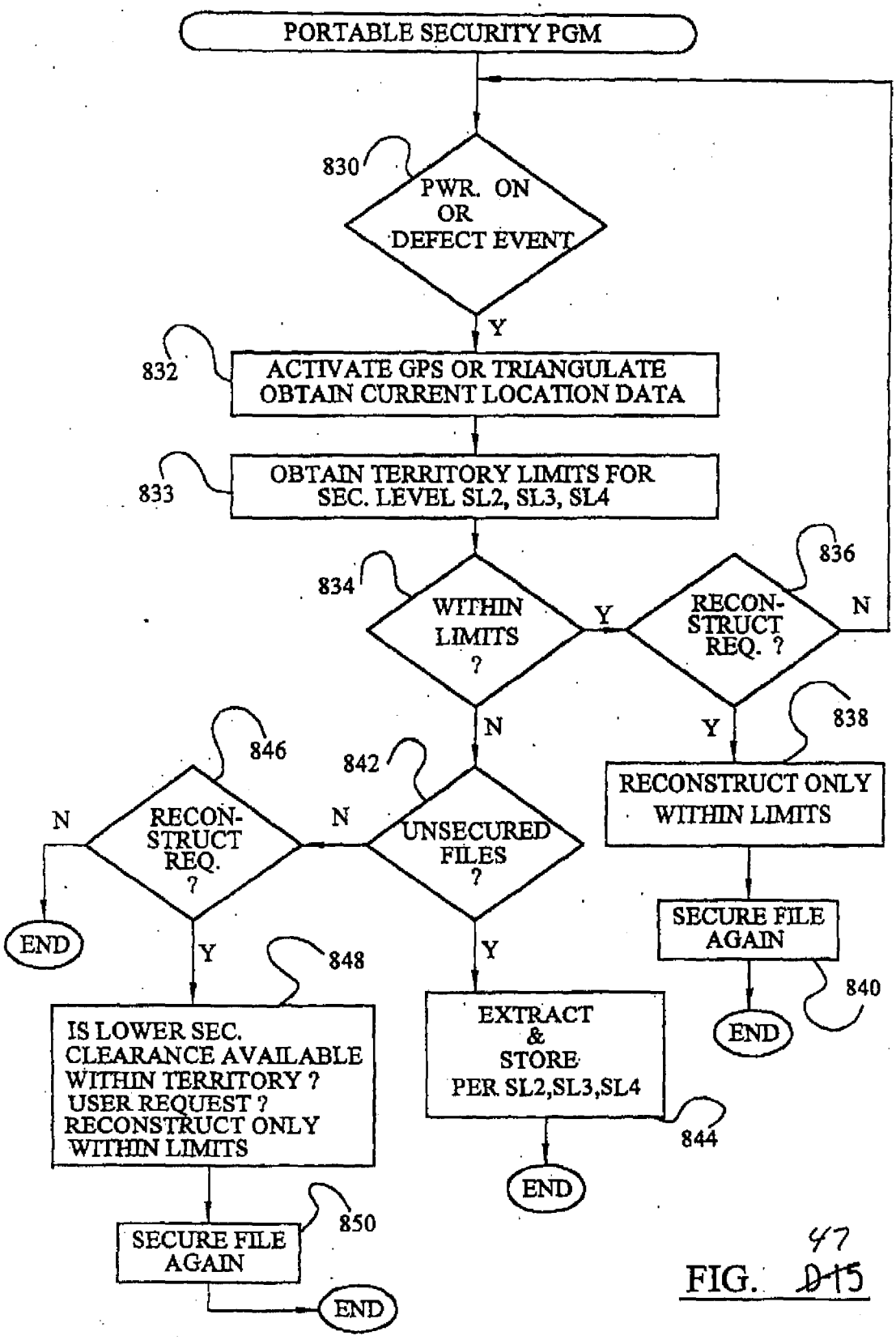

PORTABLE DEVICE 810
AT LOCATION B
STORE
828
T1
816
MEM
814
812
818
PROC.
GPS
RCR
KyBd
DISPLAY
I/O
820
TX-RCR
T2
A
822
d1
d2
d3
C
824
T3
D
826

FIG. 6


PORTABLE SECURITY PGM
830
PWR. ON OR DEFECT EVENT
Y
832
ACTIVATE GPS OR TRIANGULATE OBTAIN CURRENT LOCATION DATA
833
OBTAIN TERRITORY LIMITS FOR SEC. LEVEL SL2, SL3, SL4
834
WITHIN LIMITS ?
Y
836
RECON-STRUCT REQ. ?
N
Y
838
RECONSTRUCT ONLY WITHIN LIMITS
SECURE FILE AGAIN
840
END
N
842
UNSECURED FILES ?
N
846
RECON-STRUCT REQ. ?
N
END
Y
848
IS LOWER SEC. CLEARANCE AVAILABLE WITHIN TERRITORY ? USER REQUEST ? RECONSTRUCT ONLY WITHIN LIMITS
SECURE FILE AGAIN
850
END
Y
EXTRACT & STORE PER SL2,SL3,SL4
844
END

47

FIG. 15

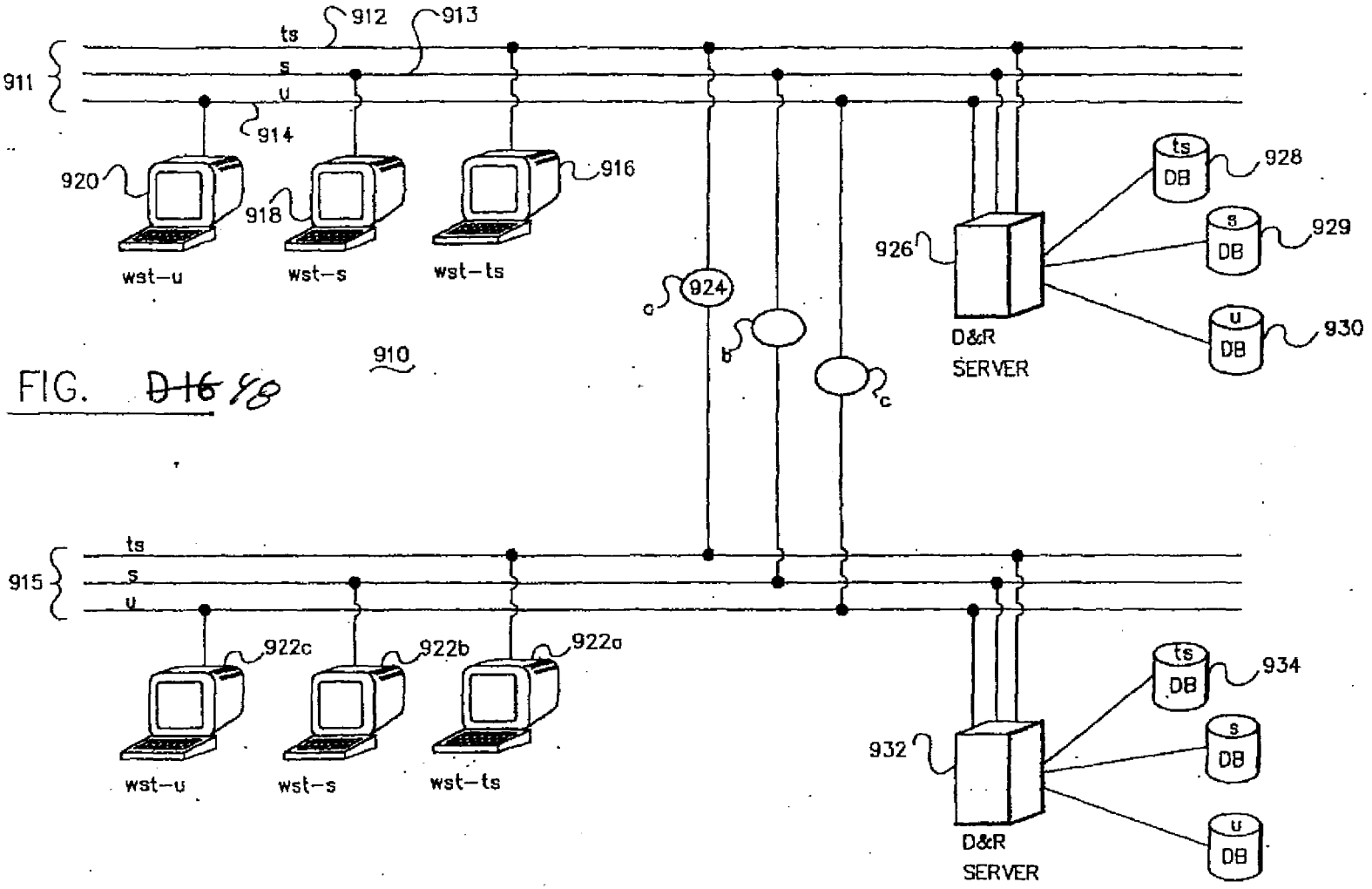

911
ts
s
u
912
913
914
920
918
916
wst–u
wst–s
wst–ts
924
c
b
a
926
D&R
SERVER
ts
DB
928
s
DB
929
u
DB
930
910
915
ts
s
u
922c
922b
922a
wst–u
wst–s
wst–ts
932
D&R
SERVER
ts
DB
934
s
DB
u
DB

FIG. ~~D16~~ 8

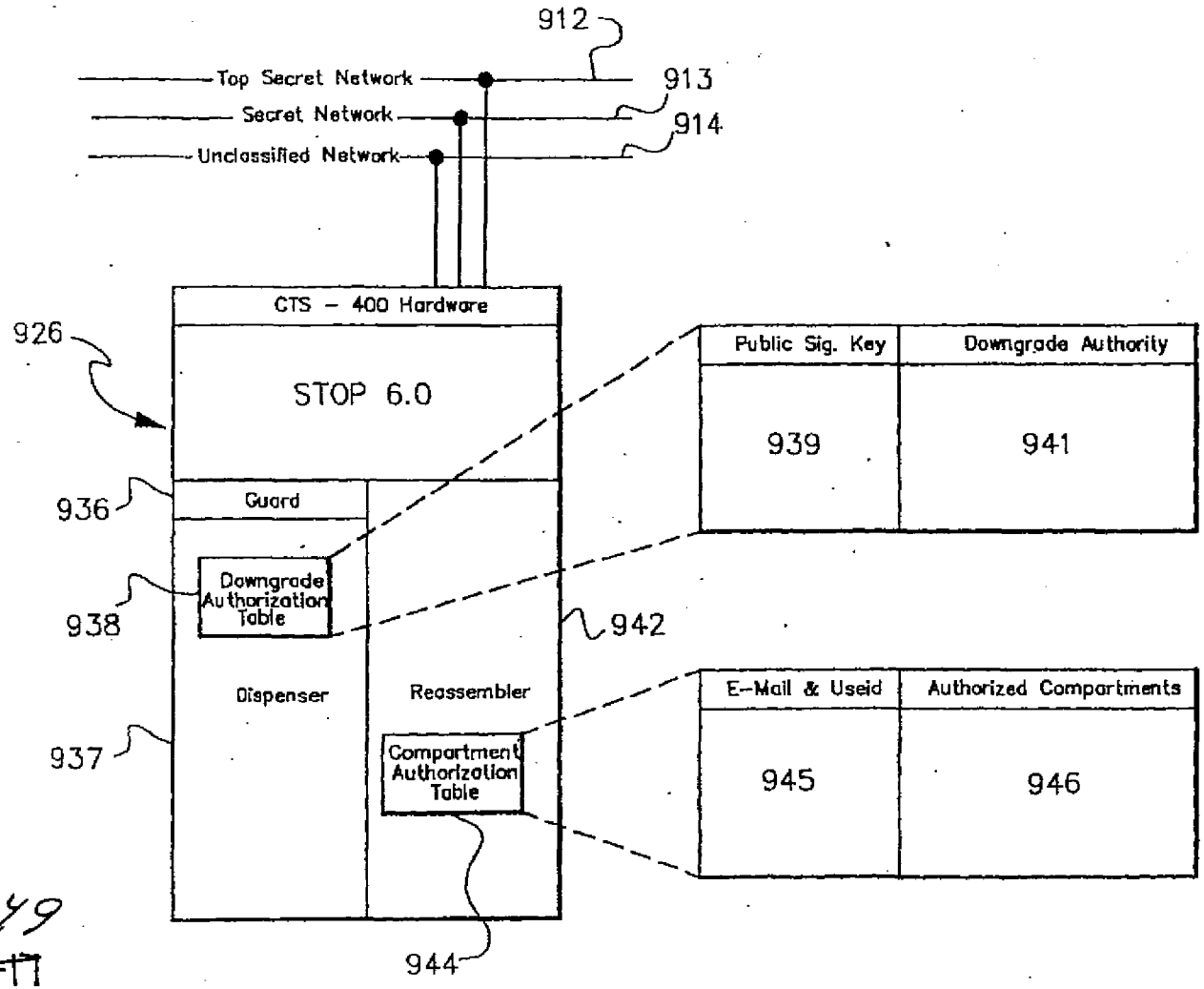

912
Top Secret Network
913
Secret Network
914
Unclassified Network
CTS – 400 Hardware
926
STOP 6.0
936
Guard
938
Downgrade Authorization Table
942
Dispenser
Reassembler
937
Compartment Authorization Table
944
Public Sig. Key
Downgrade Authority
939
941
E-Mail & Useid
Authorized Compartments
945
946

FIG. 49

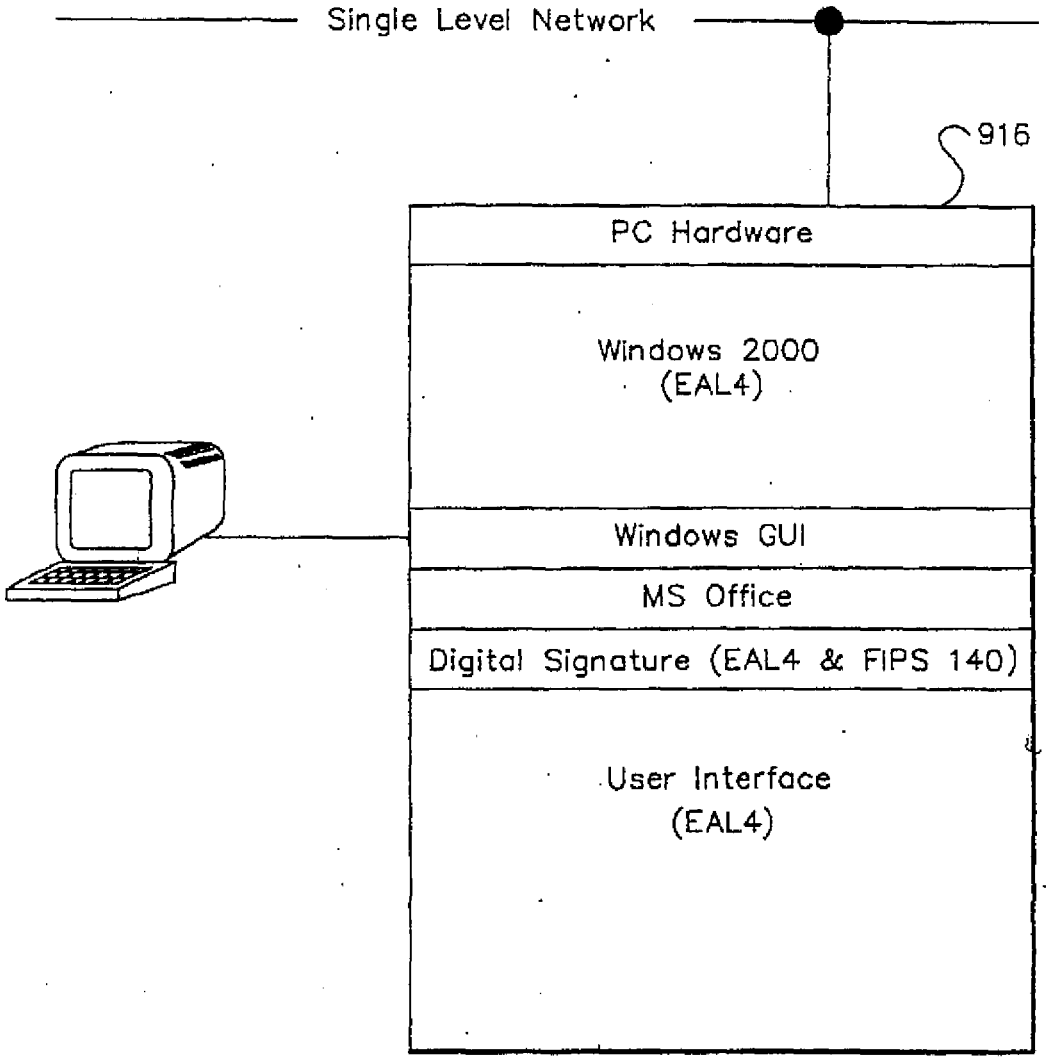

Single Level Network
916
PC Hardware
Windows 2000
(EAL4)
Windows GUI
MS Office
Digital Signature (EAL4 & FIPS 140)
User Interface
(EAL4)

FIG. ~~D-18~~ # 50

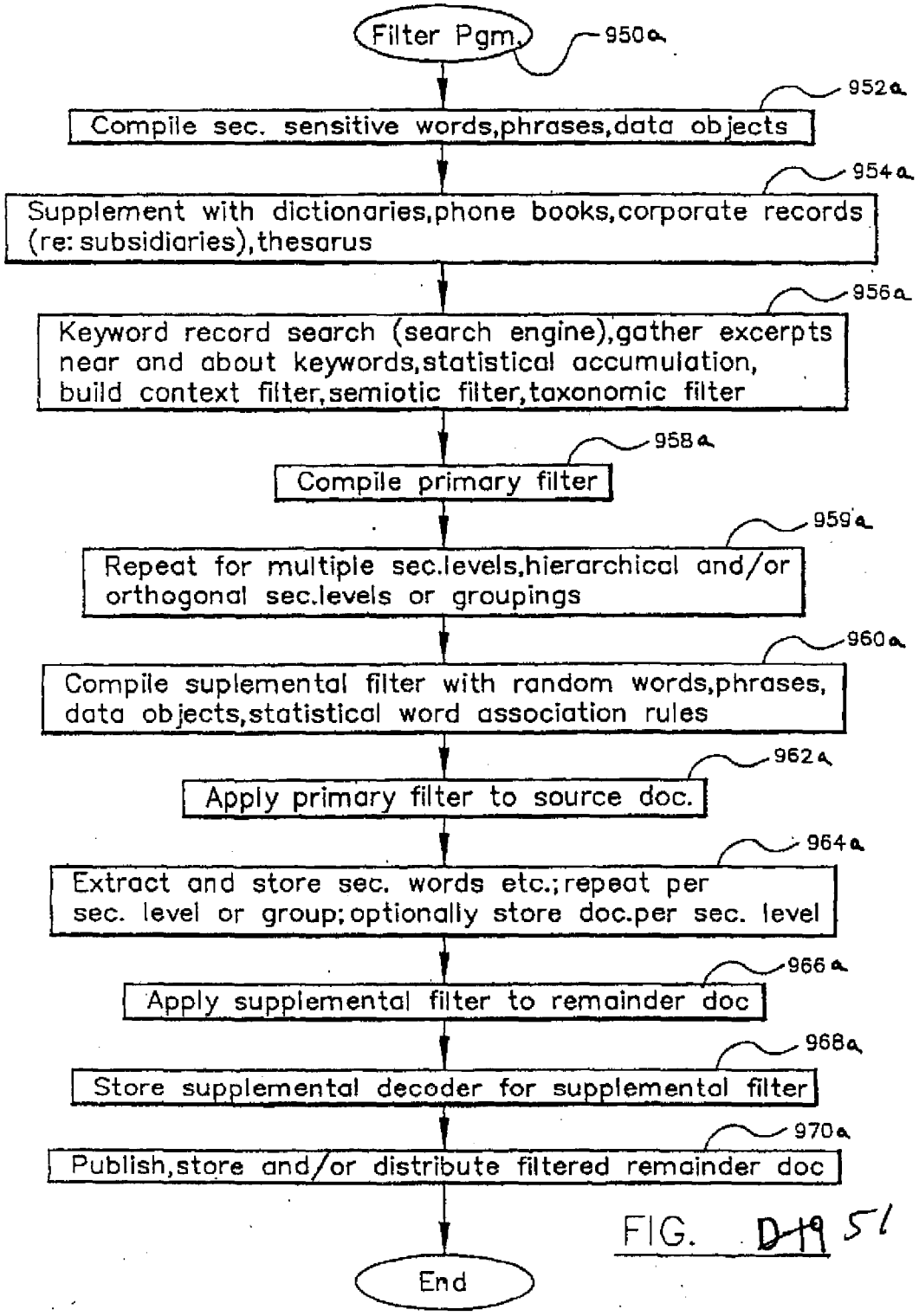

Filter Pgm.
950a
952a
Compile sec. sensitive words,phrases,data objects
954a
Supplement with dictionaries,phone books,corporate records (re: subsidiaries),thesarus
956a
Keyword record search (search engine),gather excerpts near and about keywords,statistical accumulation, build context filter,semiotic filter,taxonomic filter
958a
Compile primary filter
959a
Repeat for multiple sec.levels,hierarchical and/or orthogonal sec.levels or groupings
960a
Compile suplemental filter with random words,phrases, data objects,statistical word association rules
962a
Apply primary filter to source doc.
964a
Extract and store sec. words etc.;repeat per sec. level or group;optionally store doc.per sec. level
966a
Apply supplemental filter to remainder doc
968a
Store supplemental decoder for supplemental filter
970a
Publish,store and/or distribute filtered remainder doc
End

FIG. D-19 51

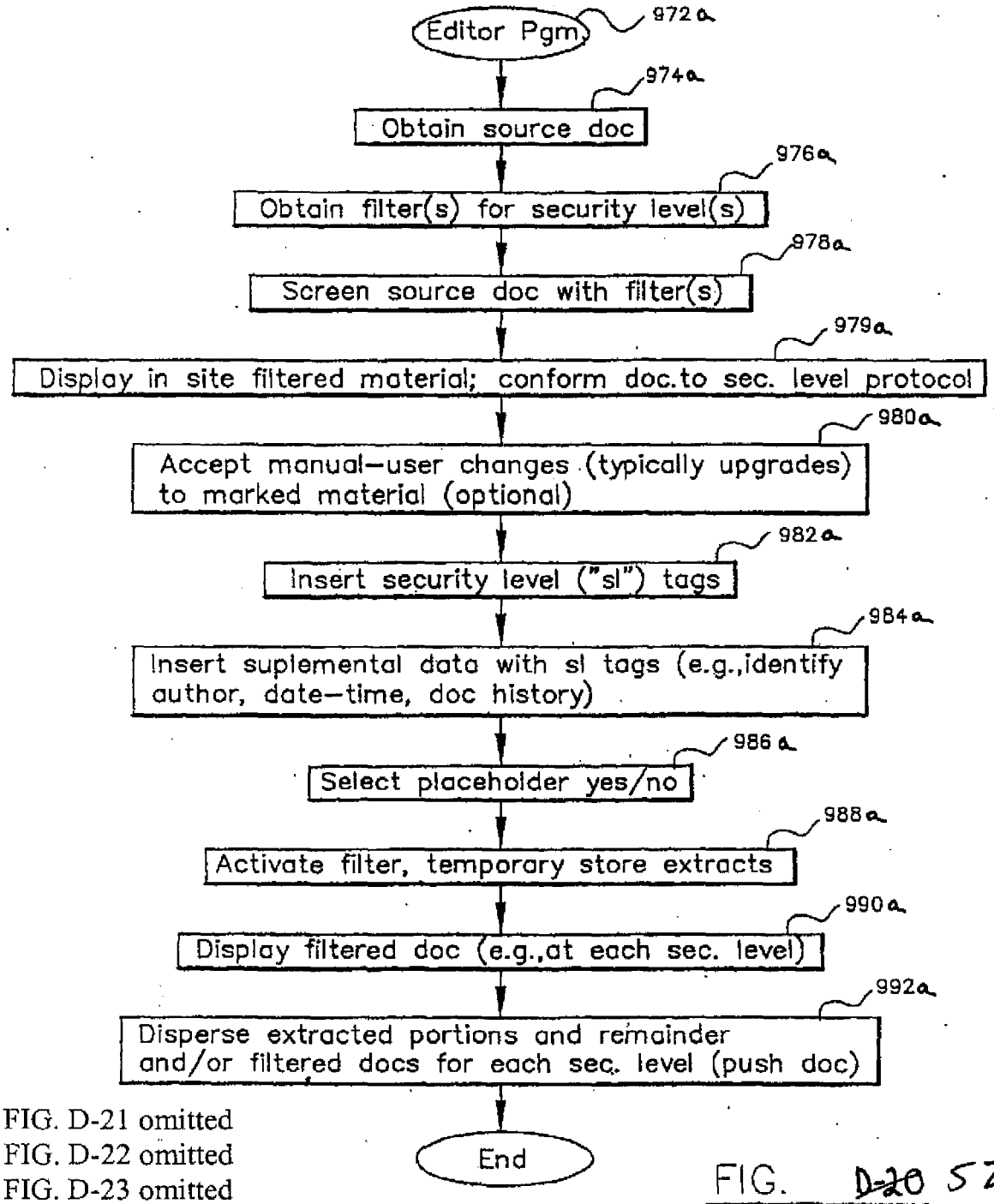


FIG. D-21 omitted
FIG. D-22 omitted
FIG. D-23 omitted

FIG. D-20 52

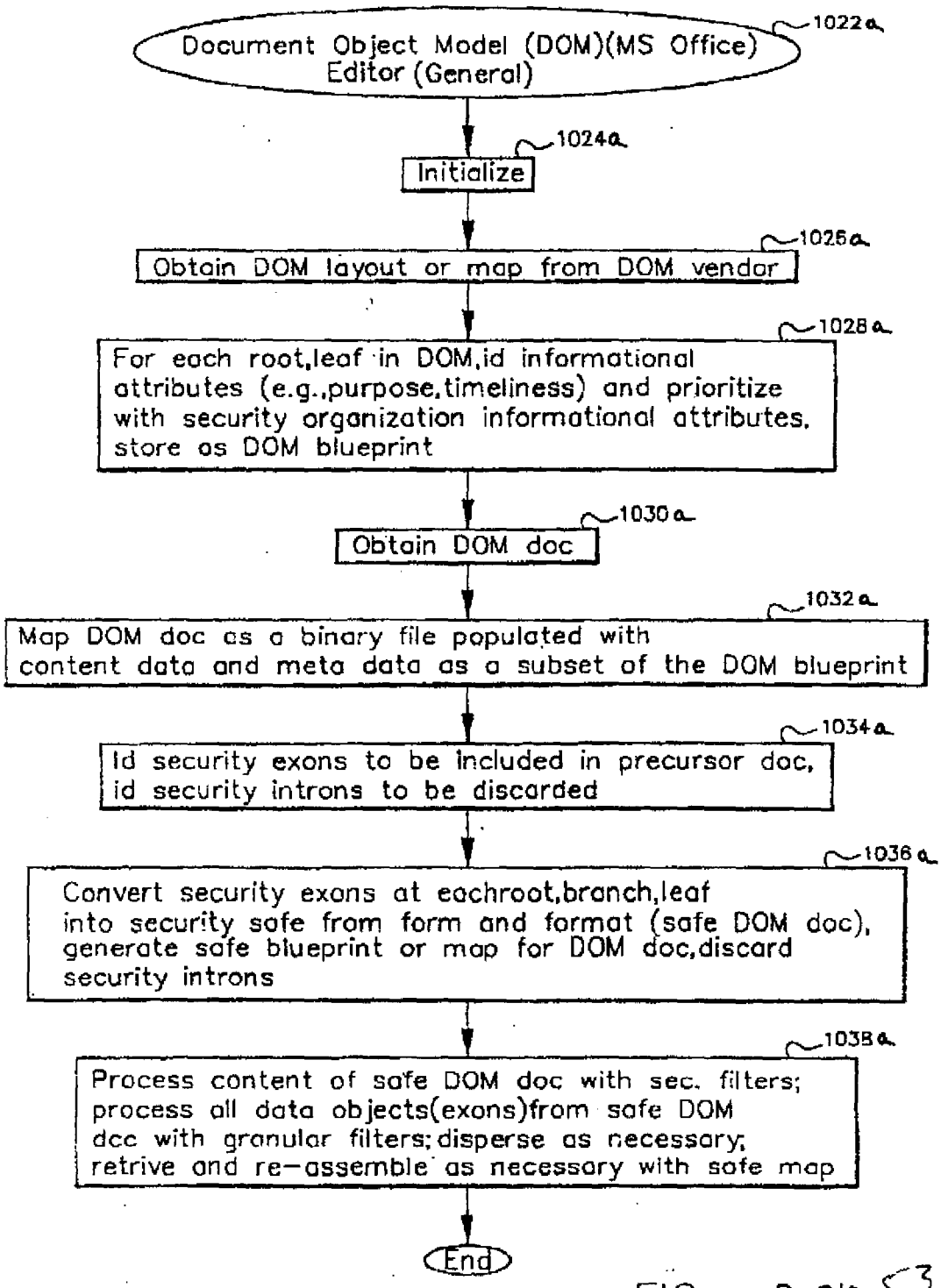
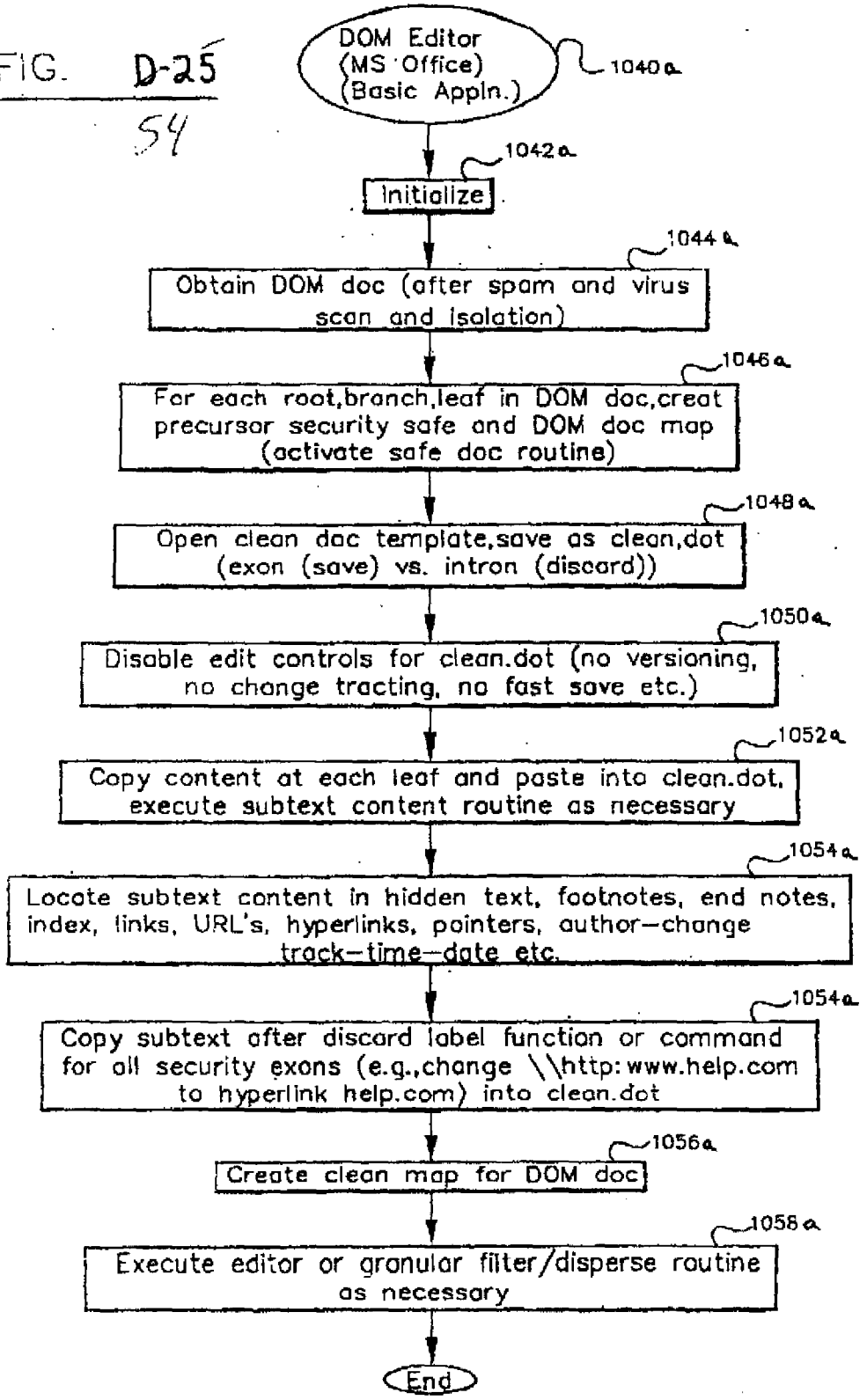

Document Object Model (DOM)(MS Office) Editor (General)
1022a
Initialize
1024a
Obtain DOM layout or map from DOM vendor
1026a
For each root,leaf in DOM,id informational attributes (e.g.,purpose,timeliness) and prioritize with security organization informational attributes, store as DOM blueprint
1028a
Obtain DOM doc
1030a
Map DOM doc as a binary file populated with content data and meta data as a subset of the DOM blueprint
1032a
Id security exons to be included in precursor doc, id security introns to be discarded
1034a
Convert security exons at eachroot,branch,leaf into security safe from form and format (safe DOM doc), generate safe blueprint or map for DOM doc,discard security introns
1036a
Process content of safe DOM doc with sec. filters; process all data objects(exons)from safe DOM doc with granular filters; disperse as necessary; retrive and re-assemble as necessary with safe map
1038a
End

FIG. D-24 53

FIG. D-25

54


DOM Editor
(MS Office)
(Basic Appln.)
1040a
1042a
Initialize
1044a
Obtain DOM doc (after spam and virus scan and isolation)
1046a
For each root,branch,leaf in DOM doc,creat precursor security safe and DOM doc map (activate safe doc routine)
1048a
Open clean doc template,save as clean,dot (exon (save) vs. intron (discard))
1050a
Disable edit controls for clean.dot (no versioning, no change tracting, no fast save etc.)
1052a
Copy content at each leaf and paste into clean.dot, execute subtext content routine as necessary
1054a
Locate subtext content in hidden text, footnotes, end notes, index, links, URL's, hyperlinks, pointers, author–change track–time–date etc.
1054a
Copy subtext after discard label function or command for all security exons (e.g.,change \\http:www.help.com to hyperlink help.com) into clean.dot
1056a
Create clean map for DOM doc
1058a
Execute editor or granular filter/disperse routine as necessary
End

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

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

Serial No. 12/453,124

Examiner D. Lazaro

Confirmation No.: 8996 Group Art 2455

Filed: April 29, 2009

For: Digital Information Infrastructure and Method
for Security Designated Data and with Granular Data Stores (as amended)

NOTICE OF FILING CORRECTED DRAWINGS

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

Pursuant to 37 C.F.R. sec. 1.85, Applicant hereby submits a clean version of the corrected drawings. A marked version of the drawings, showing all corrections, is filed separately.

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

K:\RCK\CLIENTS\Redlich\Patents\6851-08-cip-Sub-Spec-Notice-File-Corr-Dwgs-20130430.wpd

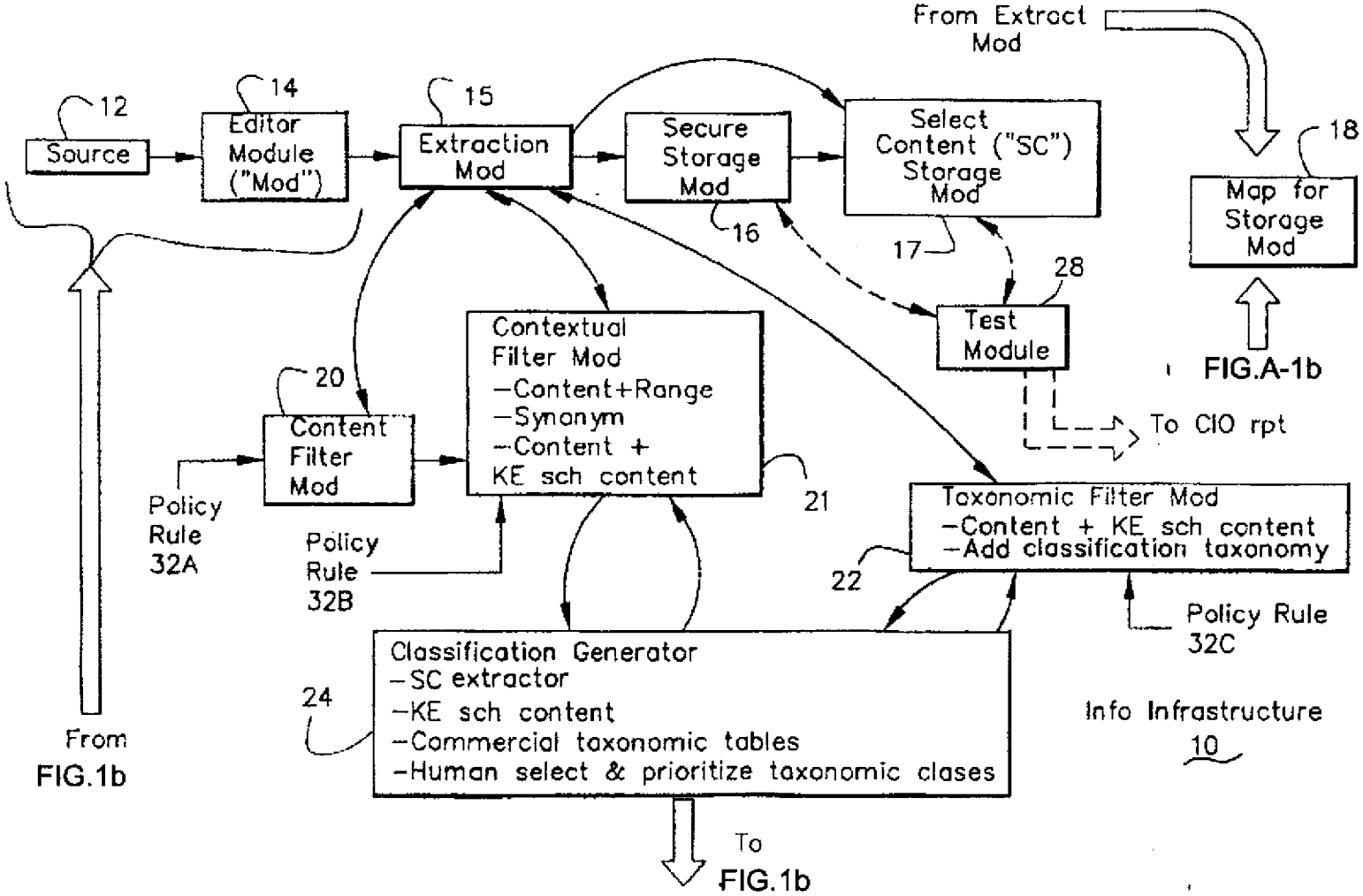

From Extract Mod
12
Source
14
Editor Module ("Mod")
15
Extraction Mod
Secure Storage Mod
16
Select Content ("SC") Storage Mod
17
18
Map for Storage Mod
28
Test Module
FIG.A-1b
To CIO rpt
20
Content Filter Mod
Contextual Filter Mod
–Content+Range
–Synonym
–Content + KE sch content
21
Policy Rule 32A
Policy Rule 32B
Taxonomic Filter Mod
–Content + KE sch content
–Add classification taxonomy
22
Policy Rule 32C
Classification Generator
–SC extractor
–KE sch content
–Commercial taxonomic tables
–Human select & prioritize taxonomic clases
24
Info Infrastructure
10
From FIG.1b
To FIG.1b

FIG.1a

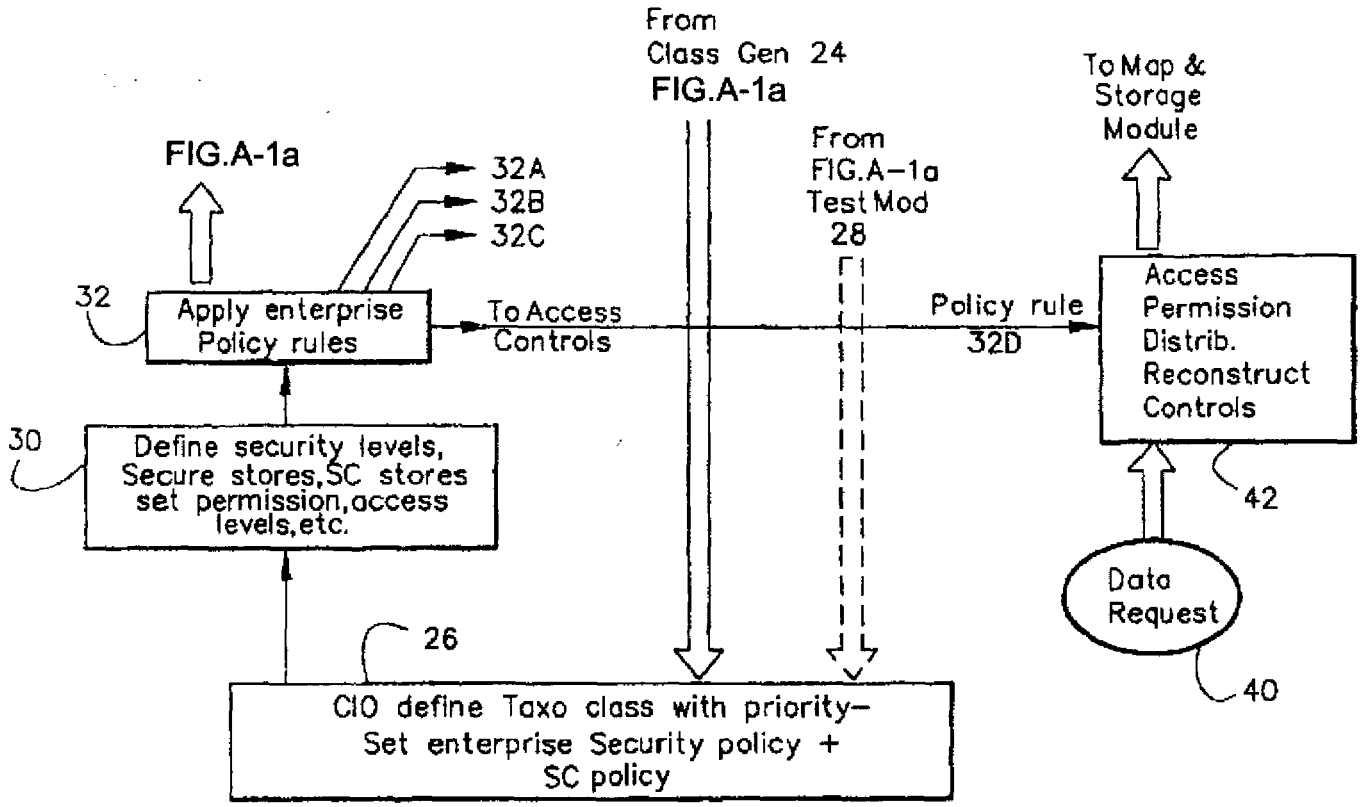

From
Class Gen 24
FIG.A-1a
To Map &
Storage
Module
FIG.A-1a
From
FIG.A-1a
Test Mod
28
32A
32B
32C
32
Apply enterprise
Policy rules
To Access
Controls
Policy rule
32D
Access
Permission
Distrib.
Reconstruct
Controls
30
Define security levels,
Secure stores,SC stores
set permission,access
levels,etc.
42
Data
Request
40
26
CIO define Taxo class with priority–
Set enterprise Security policy +
SC policy

FIG.1b

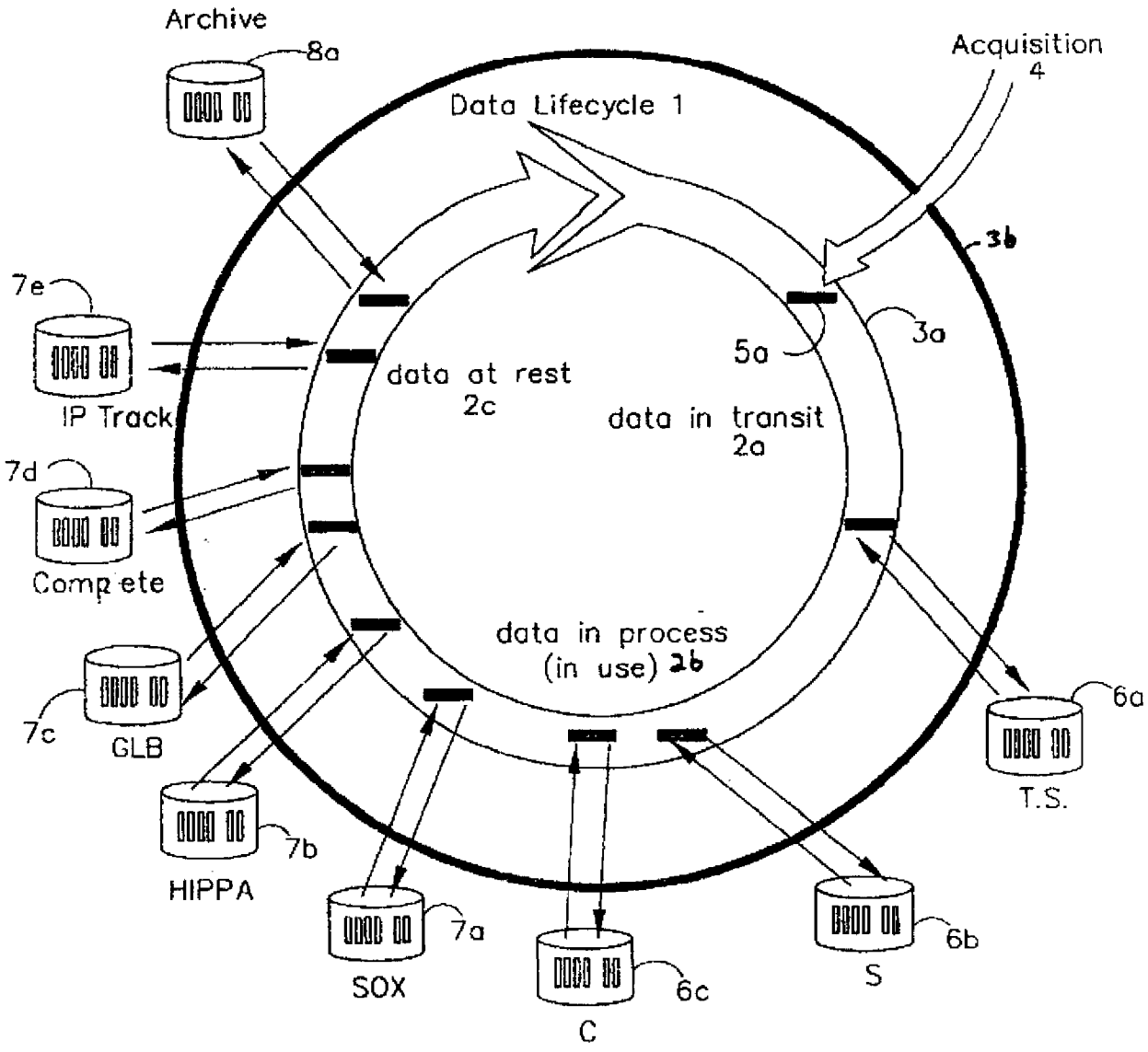

Archive
8a
Acquisition
4
Data Lifecycle 1
3b
7e
IP Track
data at rest
2c
5a
3a
data in transit
2a
7d
Comp ete
data in process
(in use) 2b
7c
GLB
6a
T.S.
7b
HIPPA
7a
SOX
6c
C
6b
S

FIG.2

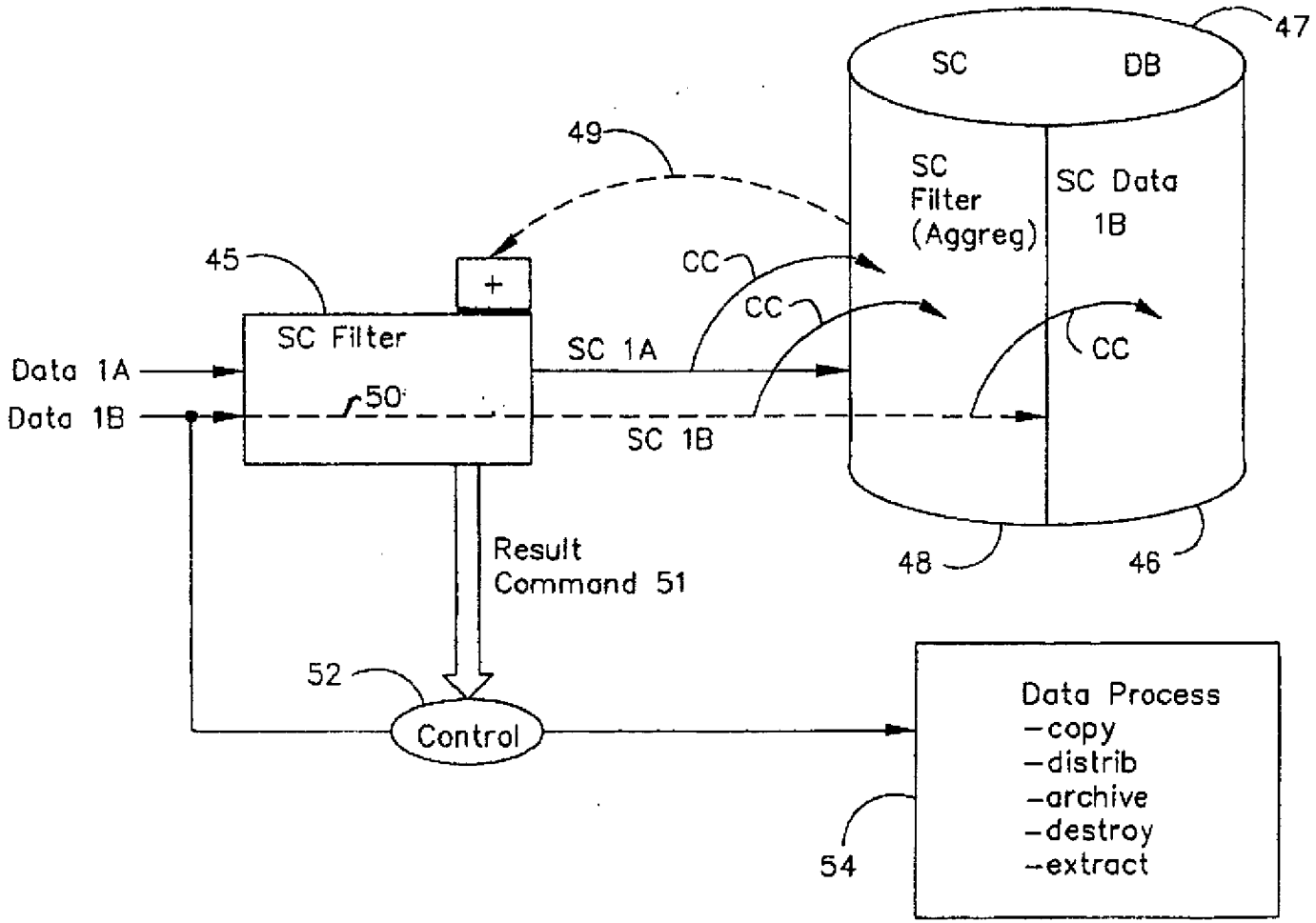

47
SC
DB
49
SC
Filter
(Aggreg)
SC Data
1B
45
+
CC
CC
CC
SC Filter
SC 1A
Data 1A
Data 1B
50
SC 1B
Result
Command 51
48
46
52
Control
Data Process
-copy
-distrib
-archive
-destroy
-extract
54

FIG.3

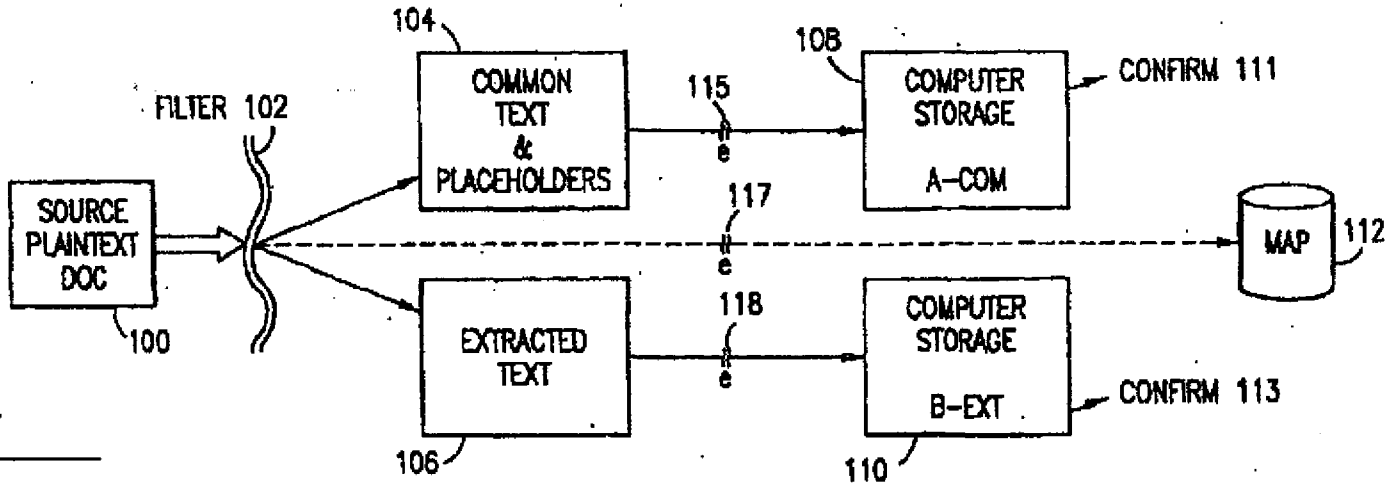

104
COMMON TEXT & PLACEHOLDERS
108
COMPUTER STORAGE A-COM
CONFIRM 111
FILTER 102
115
SOURCE PLAINTEXT DOC
100
117
MAP
112
EXTRACTED TEXT
118
COMPUTER STORAGE B-EXT
CONFIRM 113
106
110

FIG.4

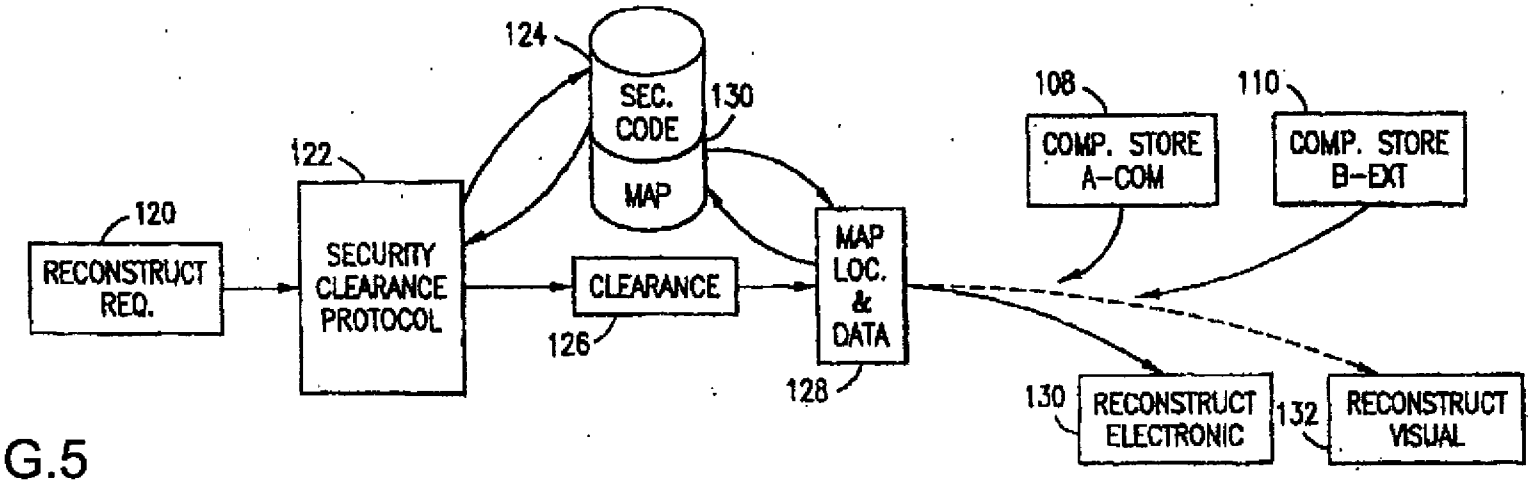

124
SEC. CODE
130
MAP
122
120
RECONSTRUCT REQ.
SECURITY CLEARANCE PROTOCOL
CLEARANCE
126
MAP LOC. & DATA
128
108
COMP. STORE A-COM
110
COMP. STORE B-EXT
130
RECONSTRUCT ELECTRONIC
132
RECONSTRUCT VISUAL

FIG.5

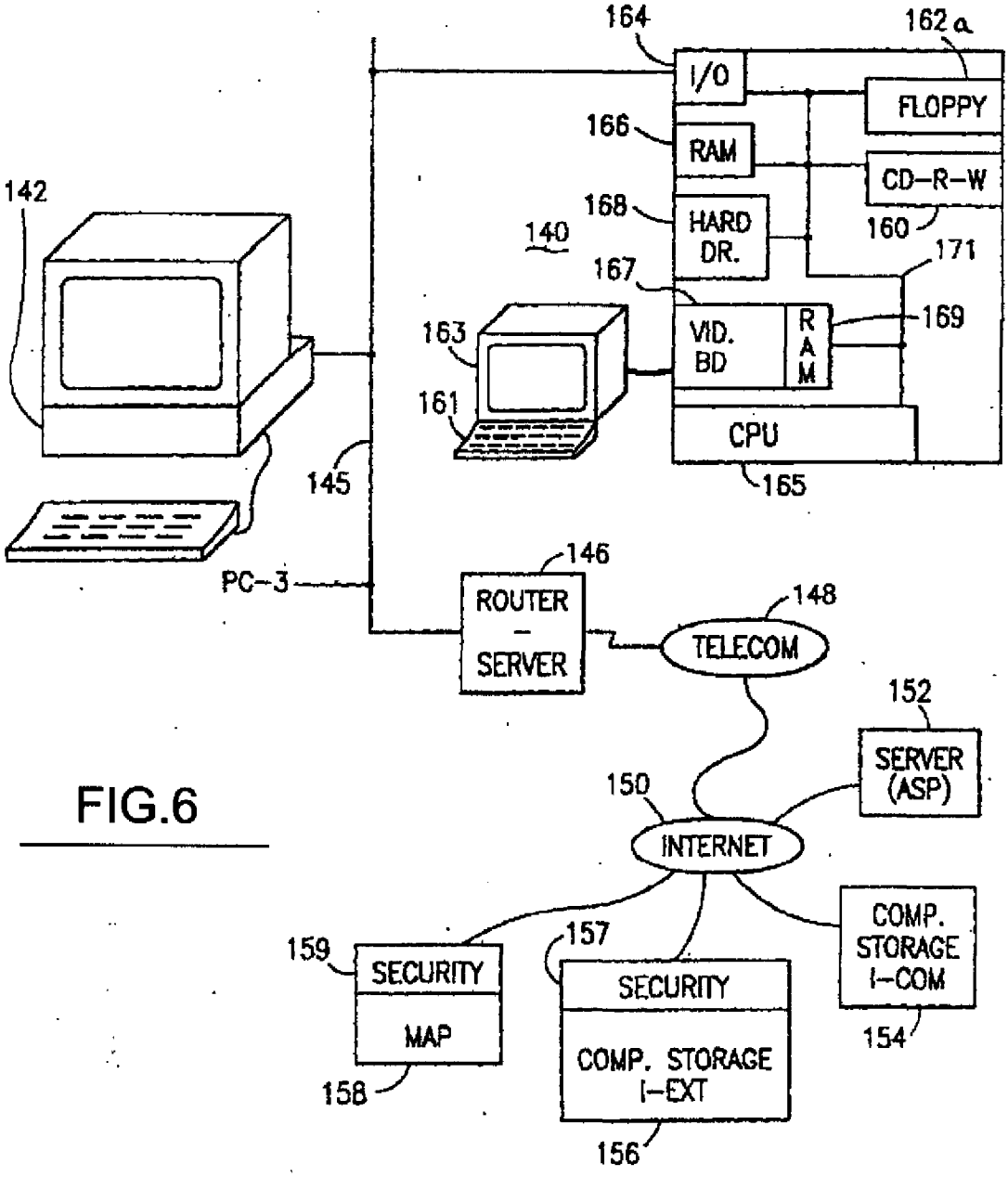
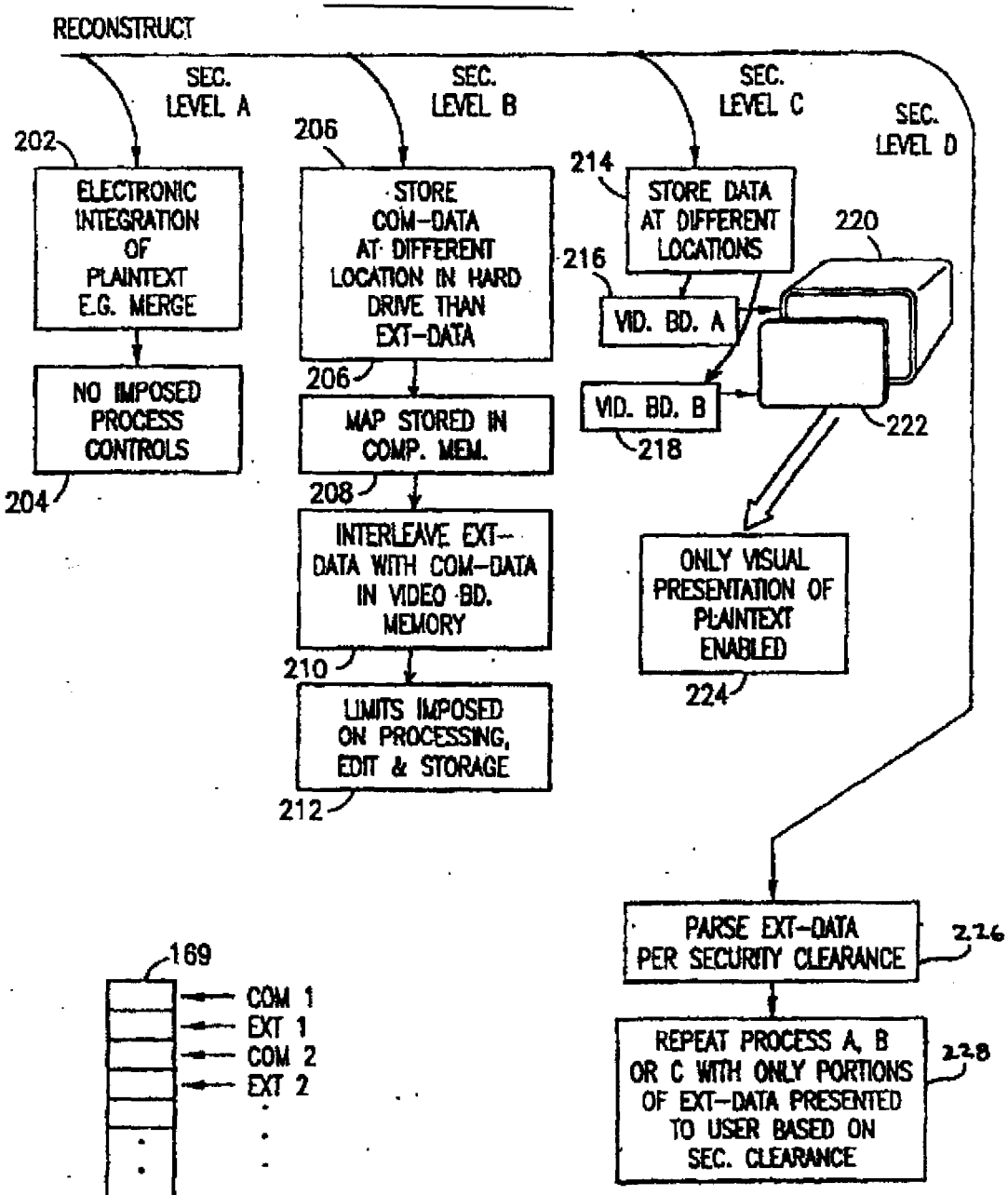

164
162a
I/O
FLOPPY
166
RAM
CD-R-W
142
168
HARD DR.
160
140
171
167
VID. BD
RAM
169
163
161
CPU
165
145
146
PC-3
ROUTER - SERVER
148
TELECOM
152
SERVER (ASP)
150
INTERNET
COMP. STORAGE I-COM
154
159
SECURITY
MAP
158
157
SECURITY
COMP. STORAGE I-EXT
156

FIG.6

FIG.7


RECONSTRUCT
SEC. LEVEL A
SEC. LEVEL B
SEC. LEVEL C
SEC. LEVEL D
202
ELECTRONIC INTEGRATION OF PLAINTEXT E.G. MERGE
NO IMPOSED PROCESS CONTROLS
204
206
STORE COM-DATA AT DIFFERENT LOCATION IN HARD DRIVE THAN EXT-DATA
206
MAP STORED IN COMP. MEM.
208
INTERLEAVE EXT-DATA WITH COM-DATA IN VIDEO BD. MEMORY
210
LIMITS IMPOSED ON PROCESSING, EDIT & STORAGE
212
214
STORE DATA AT DIFFERENT LOCATIONS
216
VID. BD. A
VID. BD. B
218
220
222
ONLY VISUAL PRESENTATION OF PLAINTEXT ENABLED
224
PARSE EXT-DATA PER SECURITY CLEARANCE
226
REPEAT PROCESS A, B OR C WITH ONLY PORTIONS OF EXT-DATA PRESENTED TO USER BASED ON SEC. CLEARANCE
228

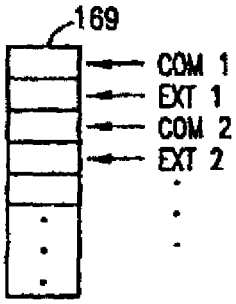

169
COM 1
EXT 1
COM 2
EXT 2

FIG.8

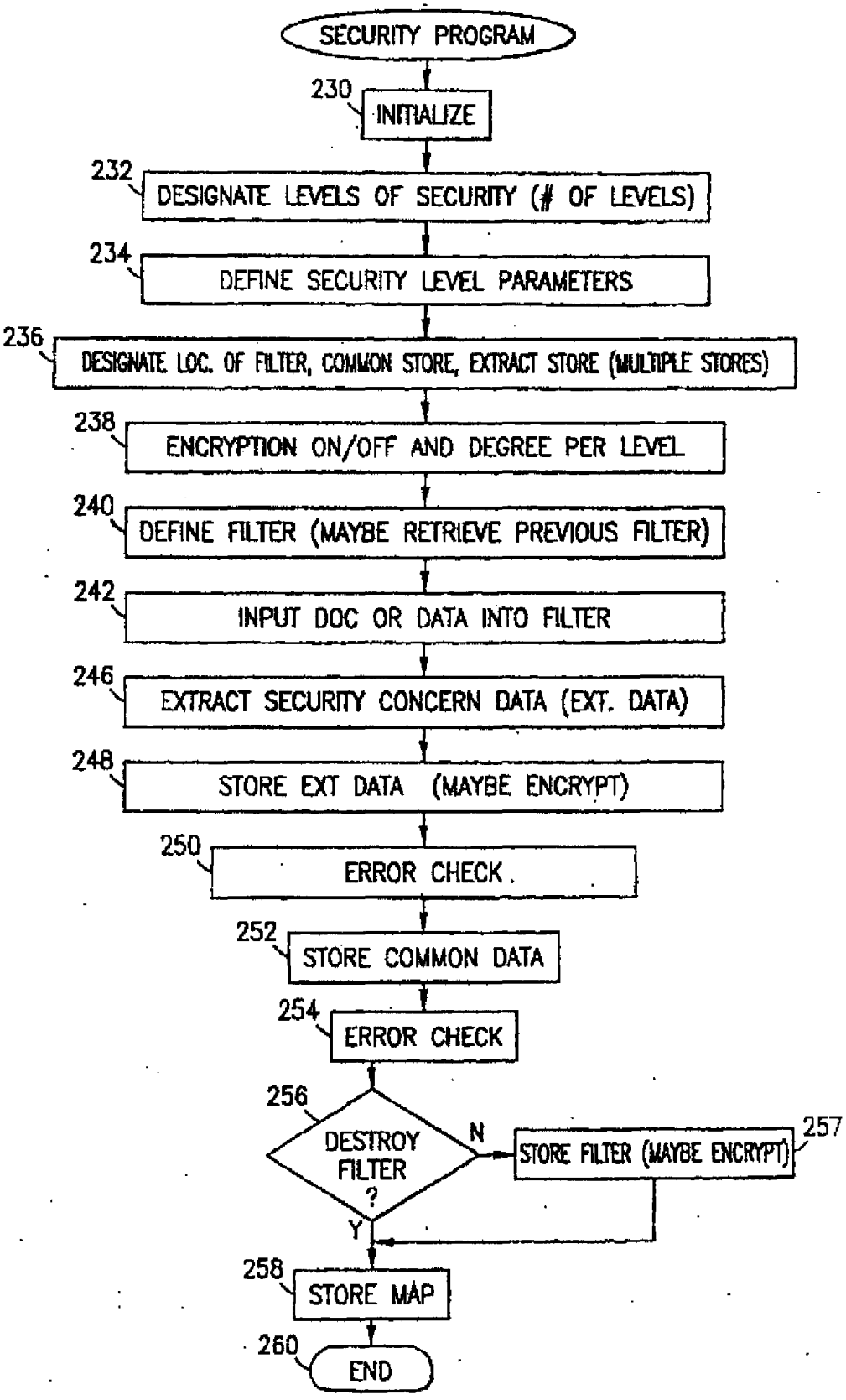
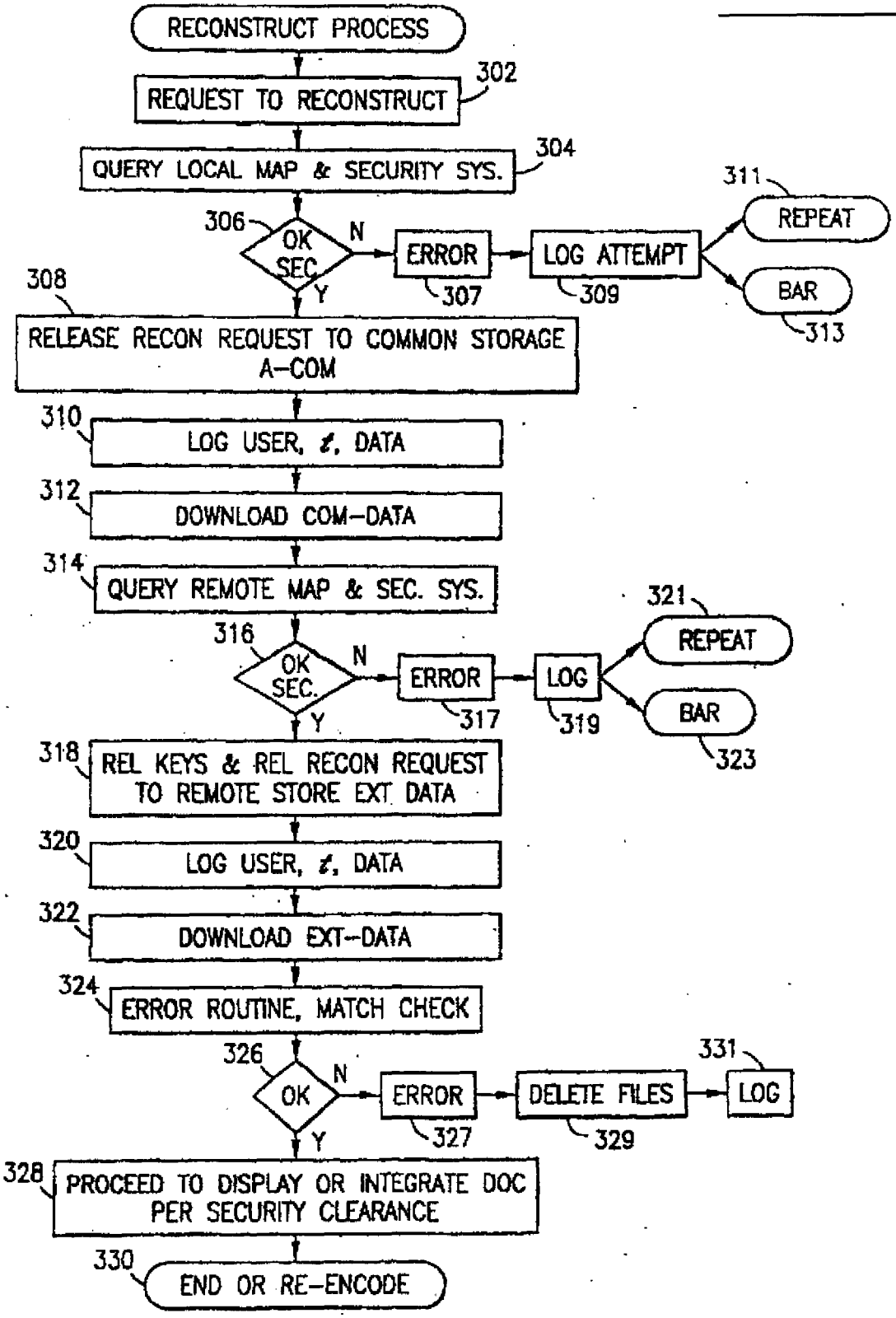

SECURITY PROGRAM
230
INITIALIZE
232
DESIGNATE LEVELS OF SECURITY (# OF LEVELS)
234
DEFINE SECURITY LEVEL PARAMETERS
236
DESIGNATE LOC. OF FILTER, COMMON STORE, EXTRACT STORE (MULTIPLE STORES)
238
ENCRYPTION ON/OFF AND DEGREE PER LEVEL
240
DEFINE FILTER (MAYBE RETRIEVE PREVIOUS FILTER)
242
INPUT DOC OR DATA INTO FILTER
246
EXTRACT SECURITY CONCERN DATA (EXT. DATA)
248
STORE EXT DATA (MAYBE ENCRYPT)
250
ERROR CHECK.
252
STORE COMMON DATA
254
ERROR CHECK
256
DESTROY FILTER ?
N
257
STORE FILTER (MAYBE ENCRYPT)
Y
258
STORE MAP
260
END

FIG.9

FIG.10


RECONSTRUCT PROCESS
REQUEST TO RECONSTRUCT
302
QUERY LOCAL MAP & SECURITY SYS.
304
306
OK SEC.
N
Y
ERROR
307
LOG ATTEMPT
309
311
REPEAT
BAR
313
308
RELEASE RECON REQUEST TO COMMON STORAGE A-COM
310
LOG USER, ℓ, DATA
312
DOWNLOAD COM-DATA
314
QUERY REMOTE MAP & SEC. SYS.
316
OK SEC.
N
Y
ERROR
317
LOG
319
321
REPEAT
BAR
323
318
REL KEYS & REL RECON REQUEST TO REMOTE STORE EXT DATA
320
LOG USER, ℓ, DATA
322
DOWNLOAD EXT-DATA
324
ERROR ROUTINE, MATCH CHECK
326
OK
N
Y
ERROR
327
DELETE FILES
329
331
LOG
328
PROCEED TO DISPLAY OR INTEGRATE DOC PER SECURITY CLEARANCE
330
END OR RE-ENCODE

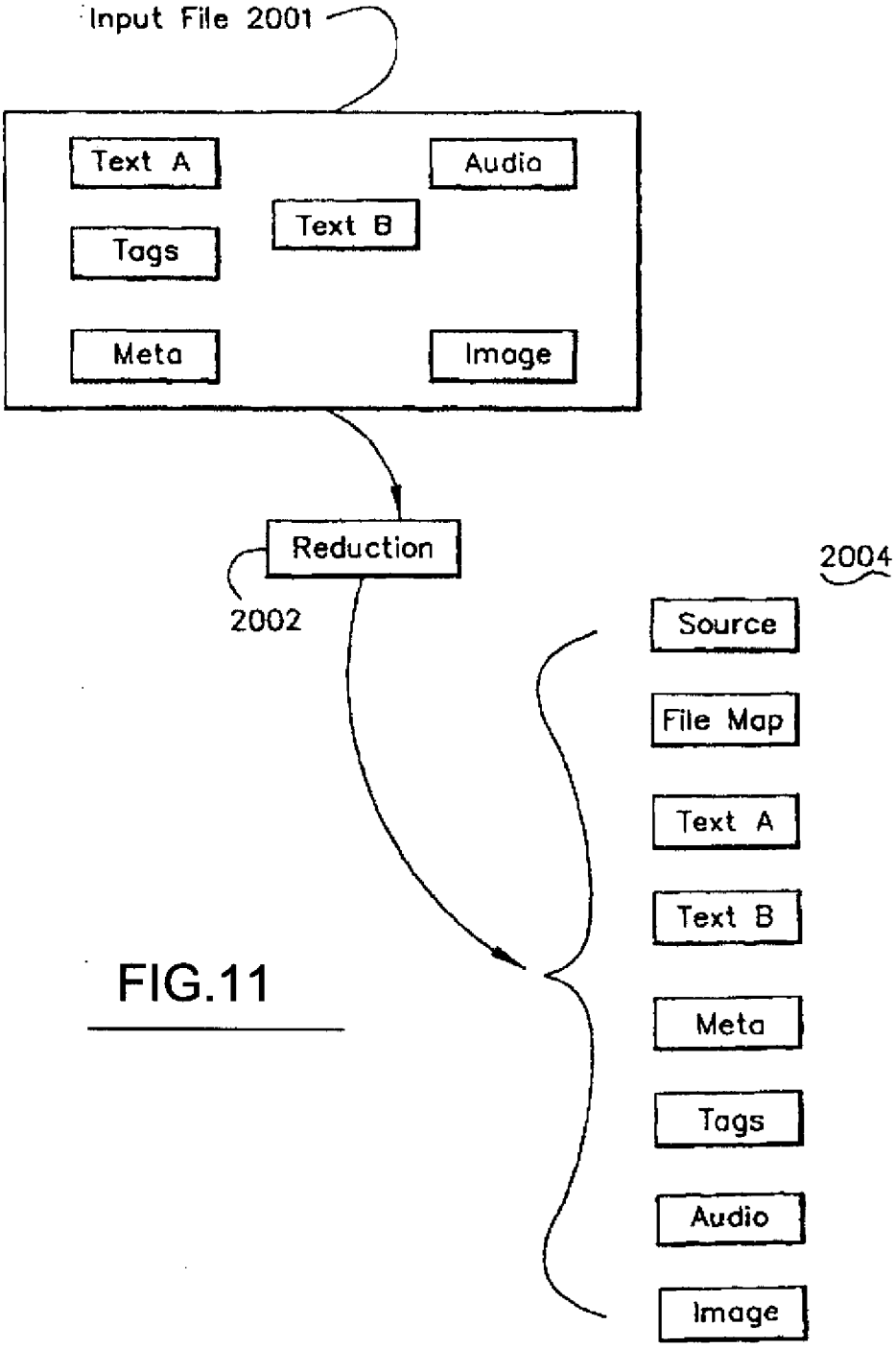

Input File 2001
Text A
Audio
Text B
Tags
Meta
Image
Reduction
2002
2004
Source
File Map
Text A
Text B
Meta
Tags
Audio
Image

FIG.11

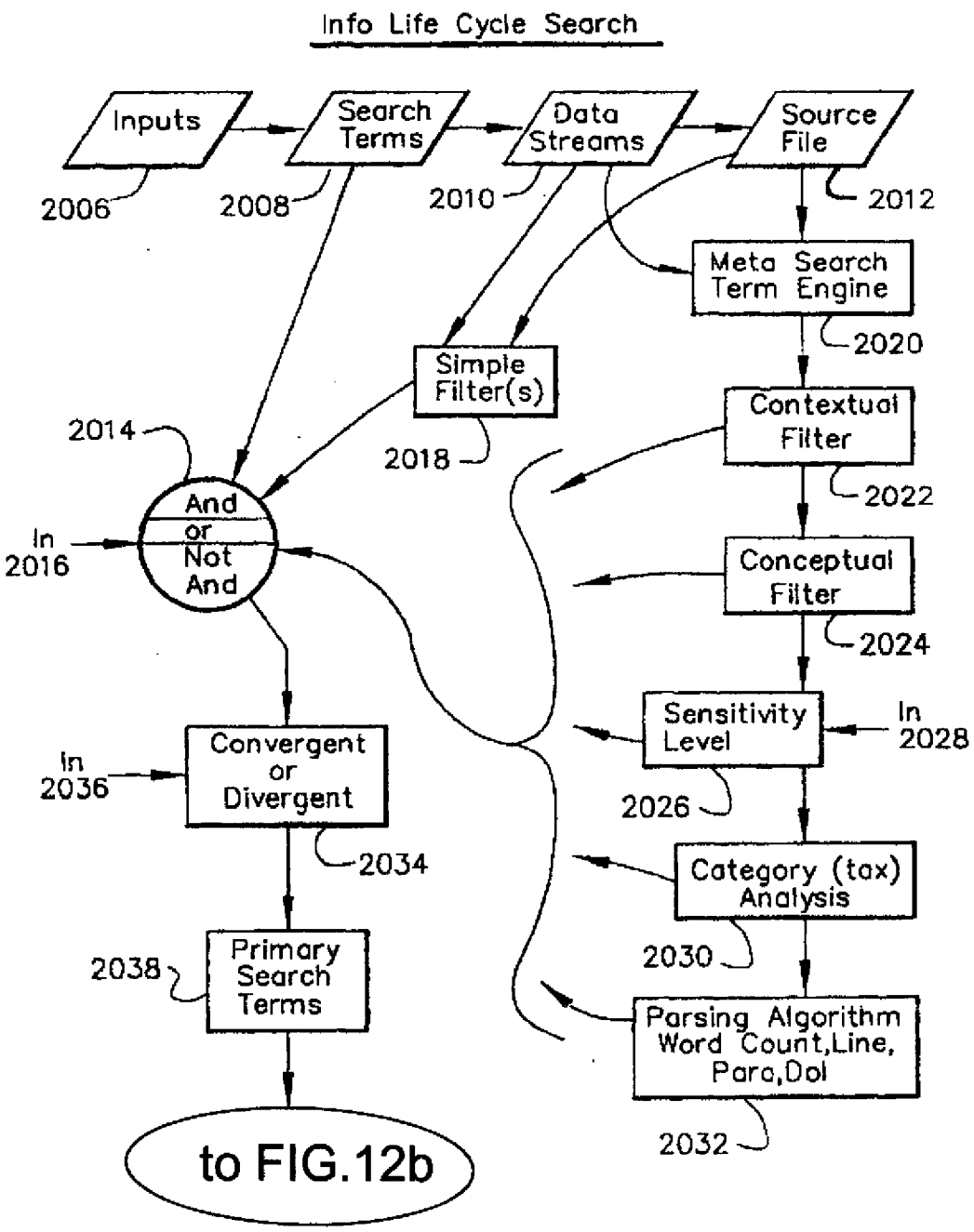

Info Life Cycle Search
Inputs
Search Terms
Data Streams
Source File
2006
2008
2010
2012
Meta Search Term Engine
2020
Simple Filter(s)
2018
Contextual Filter
2022
2014
And
or
Not
And
In
2016
Conceptual Filter
2024
Sensitivity Level
In
2028
2026
Convergent or Divergent
In
2036
2034
Category (tax) Analysis
2030
Primary Search Terms
2038
Parsing Algorithm Word Count,Line, Para,Dol
2032
to FIG.12b

FIG.12a

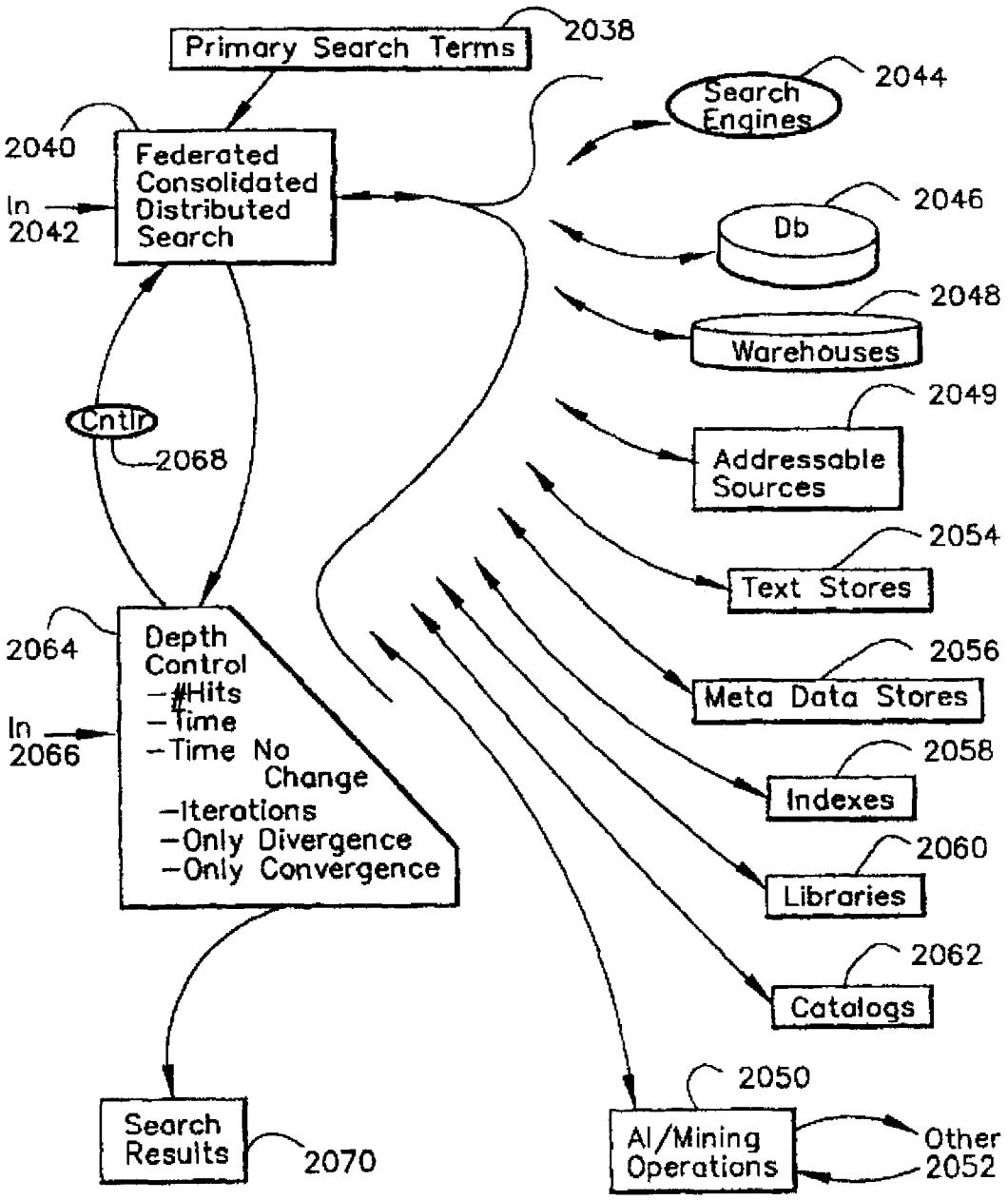

Primary Search Terms
2038
2040
Federated Consolidated Distributed Search
In 2042
Search Engines
2044
Db
2046
Warehouses
2048
Addressable Sources
2049
Text Stores
2054
Meta Data Stores
2056
Indexes
2058
Libraries
2060
Catalogs
2062
Cntlr
2068
2064
Depth Control
-#Hits
-Time
-Time No Change
-Iterations
-Only Divergence
-Only Convergence
In 2066
Search Results
2070
AI/Mining Operations
2050
Other
2052

FIG.12b

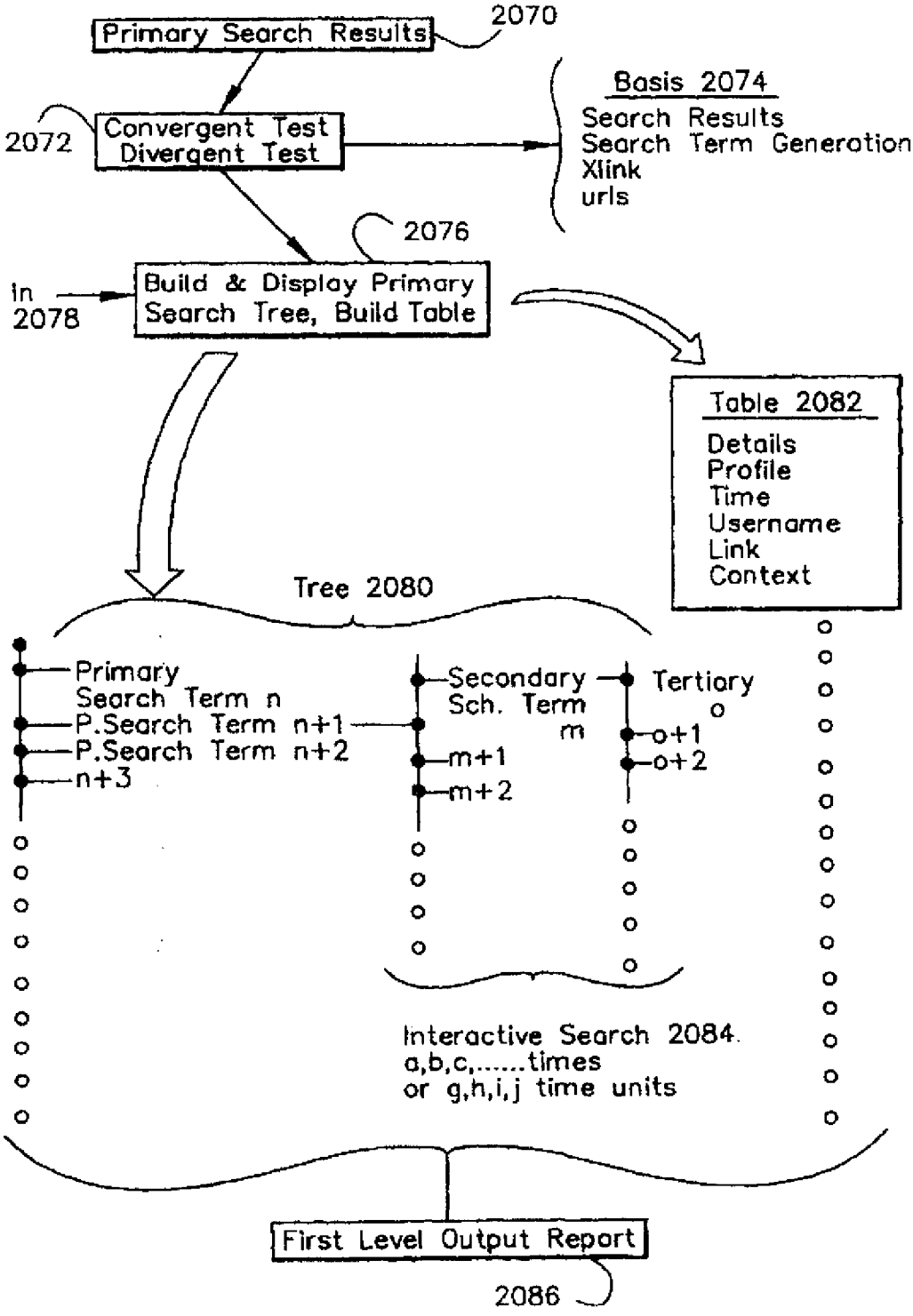

Primary Search Results
2070
Basis 2074
Search Results
Search Term Generations
Xlink
urls
2072
Convergent Test
Divergent Test
2076
In 2078
Build & Display Primary Search Tree, Build Table
Table 2082
Details
Profile
Time
Username
Link
Context
Tree 2080
Primary Search Term n
P.Search Term n+1
P.Search Term n+2
n+3
Secondary Sch. Term m
m+1
m+2
Tertiory o
o+1
o+2
Interactive Search 2084
a,b,c,.....times
or g,h,i,j time units
First Level Output Report
2086

FIG.12c

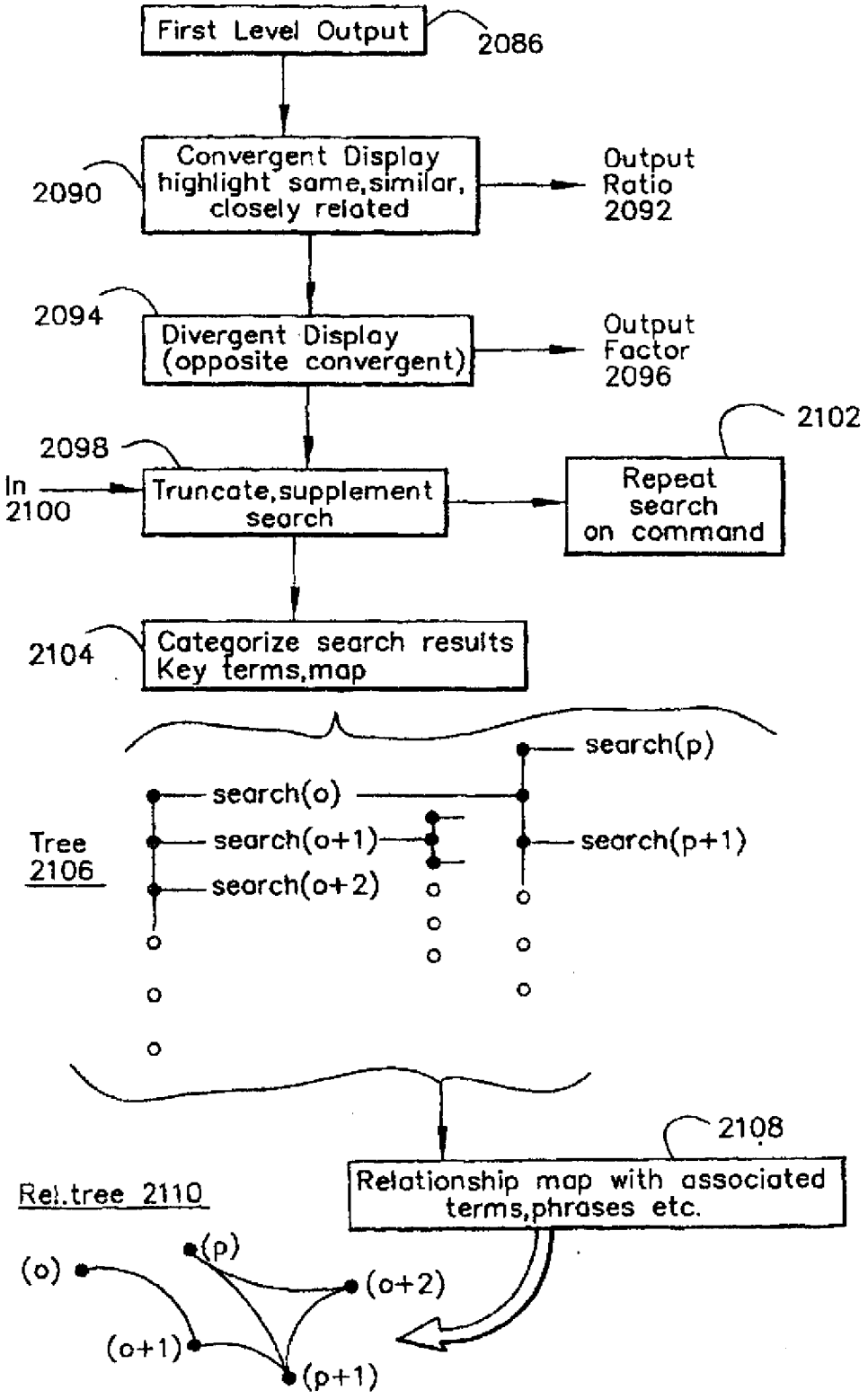

First Level Output
2086
Convergent Display highlight same,similar, closely related
2090
Output Ratio 2092
2094
Divergent Display (opposite convergent)
Output Factor 2096
2102
2098
In 2100
Truncate,supplement search
Repeat search on command
2104
Categorize search results Key terms,map
search(p)
search(o)
search(o+1)
search(o+2)
search(p+1)
Tree 2106
2108
Relationship map with associated terms,phrases etc.
Rel.tree 2110
(p)
(o)
(o+2)
(o+1)
(p+1)

FIG.12d

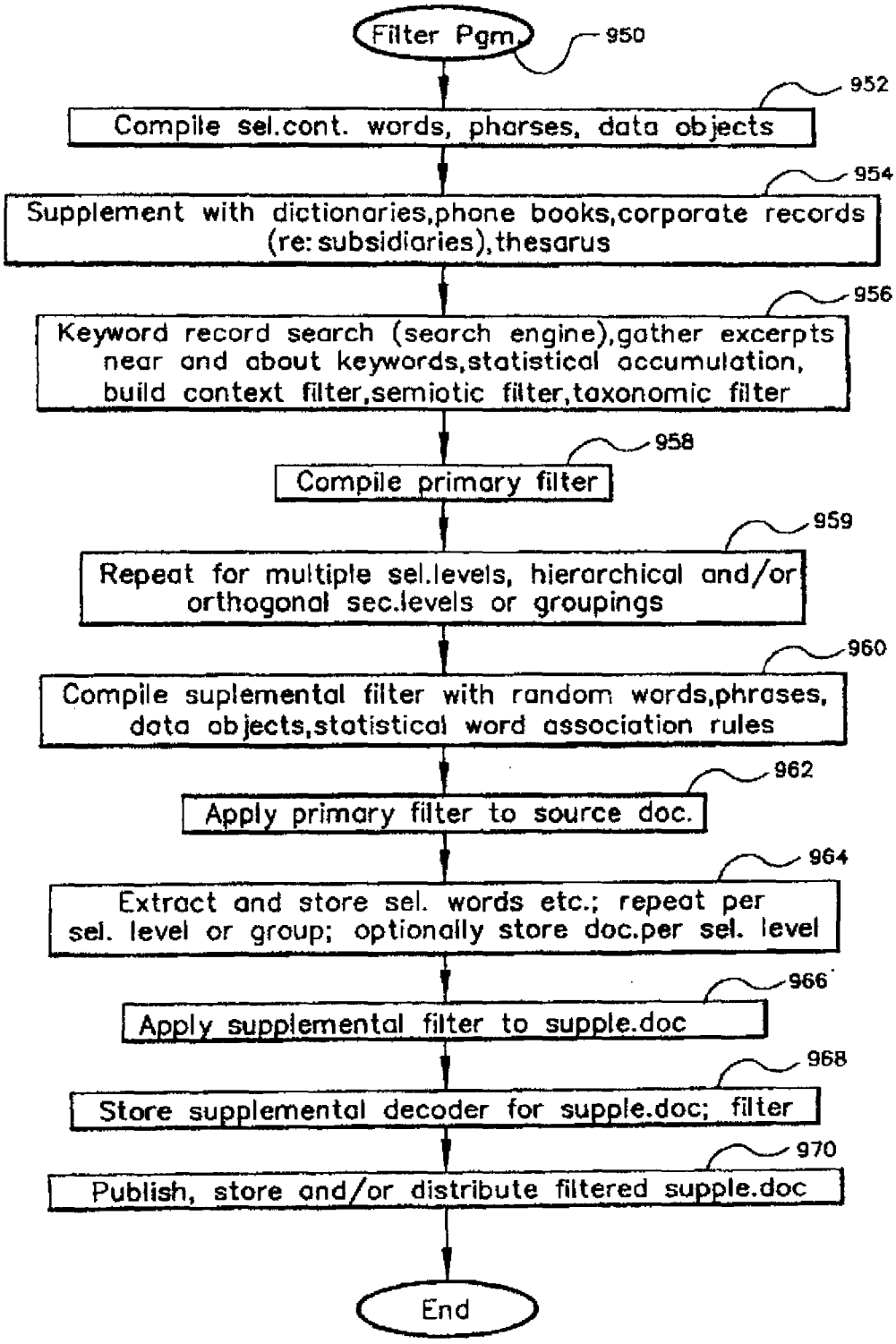

Filter Pgm
950
Compile sel.cont. words, pharses, data objects
952
Supplement with dictionaries,phone books,corporate records (re: subsidiaries),thesarus
954
Keyword record search (search engine),gather excerpts near and about keywords,statistical accumulation, build context filter,semiotic filter,taxonomic filter
956
Compile primary filter
958
Repeat for multiple sel.levels, hierarchical and/or orthogonal sec.levels or groupings
959
Compile suplemental filter with random words,phrases, data objects,statistical word association rules
960
Apply primary filter to source doc.
962
Extract and store sel. words etc.; repeat per sel. level or group; optionally store doc.per sel. level
964
Apply supplemental filter to supple.doc
966
Store supplemental decoder for supple.doc; filter
968
Publish, store and/or distribute filtered supple.doc
970
End

FIG.13

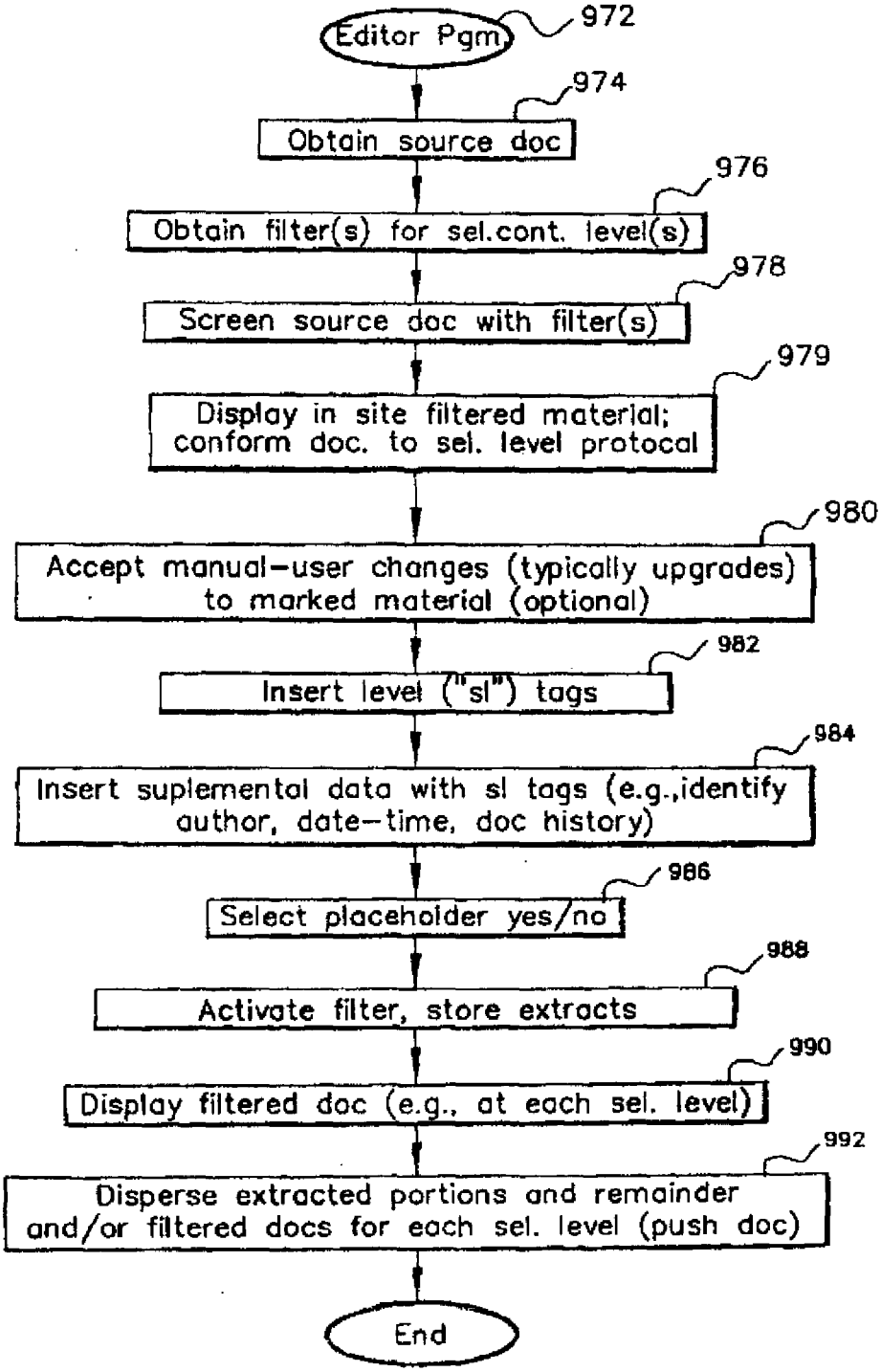

Editor Pgm
972
Obtain source doc
974
Obtain filter(s) for sel.cont. level(s)
976
Screen source doc with filter(s)
978
Display in site filtered material; conform doc. to sel. level protocal
979
Accept manual-user changes (typically upgrades) to marked material (optional)
980
Insert level ("sl") tags
982
Insert suplemental data with sl tags (e.g.,identify author, date-time, doc history)
984
Select placeholder yes/no
986
Activate filter, store extracts
988
Display filtered doc (e.g., at each sel. level)
990
Disperse extracted portions and remainder and/or filtered docs for each sel. level (push doc)
992
End

FIG.14

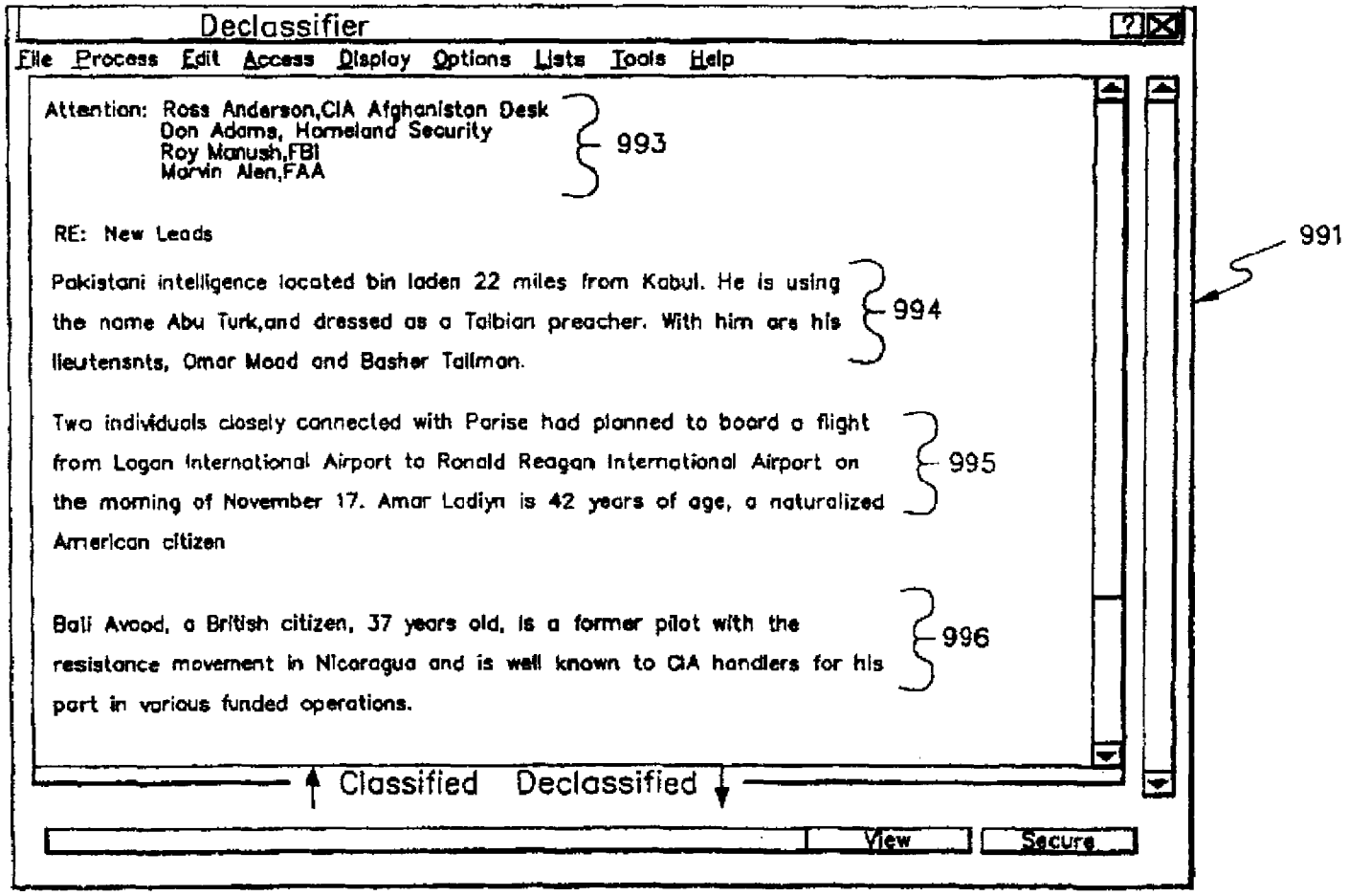

Declassifier
File Process Edit Access Display Options Lists Tools Help
Attention: Ross Anderson,CIA Afghanistan Desk
Don Adams, Homeland Security
Roy Manush,FBI
Marvin Alen,FAA
993
RE: New Leads
Pakistani intelligence located bin laden 22 miles from Kabul. He is using the name Abu Turk,and dressed as a Taibian preacher. With him are his lieutensnts, Omar Mood and Basher Tallman.
994
Two individuals closely connected with Parise had planned to board a flight from Logan International Airport to Ronald Reagan International Airport on the morning of November 17. Amar Ladiyn is 42 years of age, a naturalized American citizen
995
Bali Avood, a British citizen, 37 years old, is a former pilot with the resistance movement in Nicaragua and is well known to CIA handlers for his part in various funded operations.
996
991
Classified Declassified
View
Secure

FIG.15

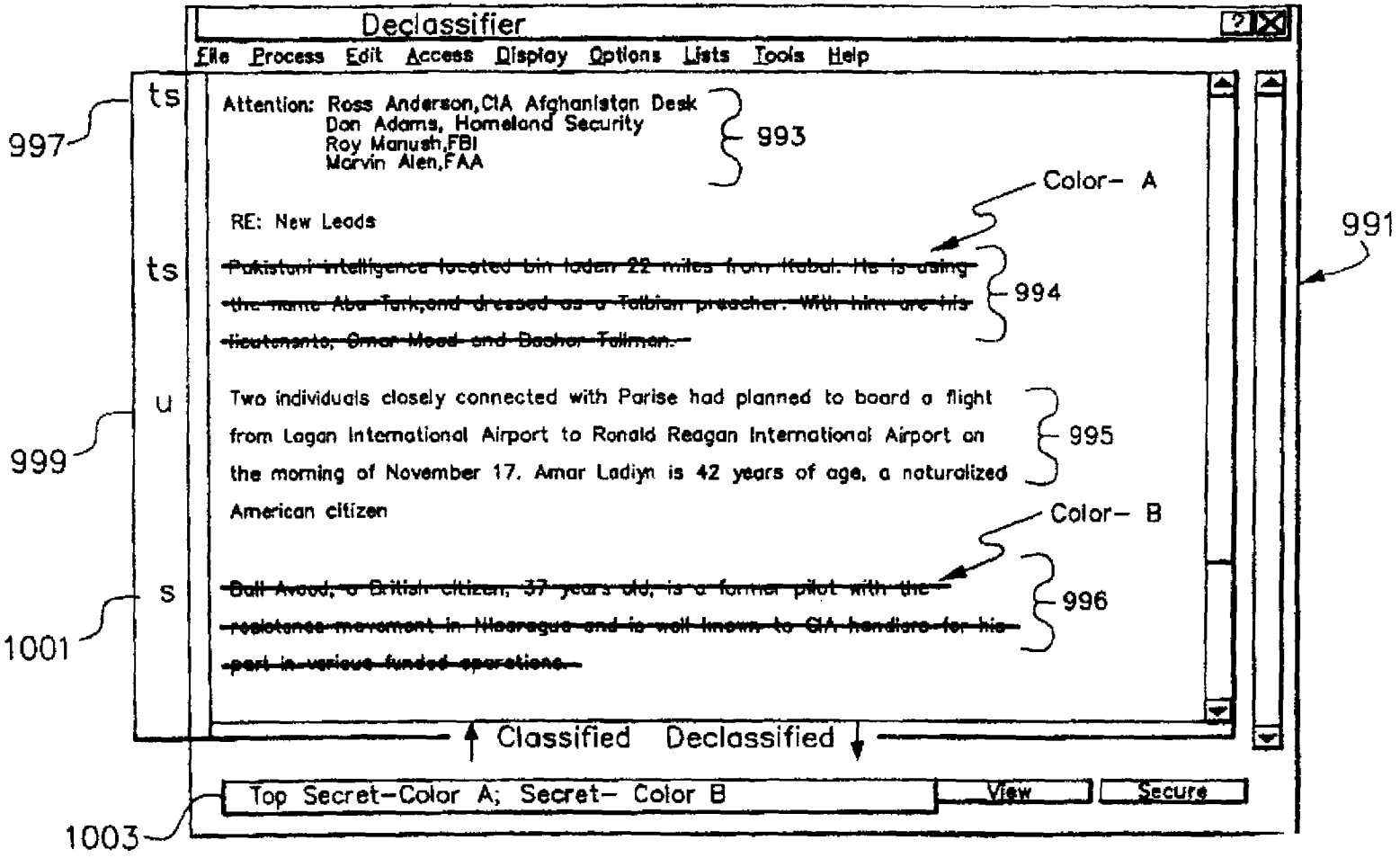

Declassifier
File Process Edit Access Display Options Lists Tools Help
997
ts
Attention: Ross Anderson,CIA Afghanistan Desk
Don Adams, Homeland Security
Roy Manush,FBI
Marvin Alen,FAA
993
Color– A
RE: New Leads
991
ts
994
999
u
Two individuals closely connected with Parise had planned to board a flight from Logan International Airport to Ronald Reagan International Airport on the morning of November 17. Amar Ladiyn is 42 years of age, a naturalized American citizen
995
Color– B
1001
s
996
Classified Declassified
Top Secret–Color A; Secret– Color B
View
Secure
1003

FIG.16

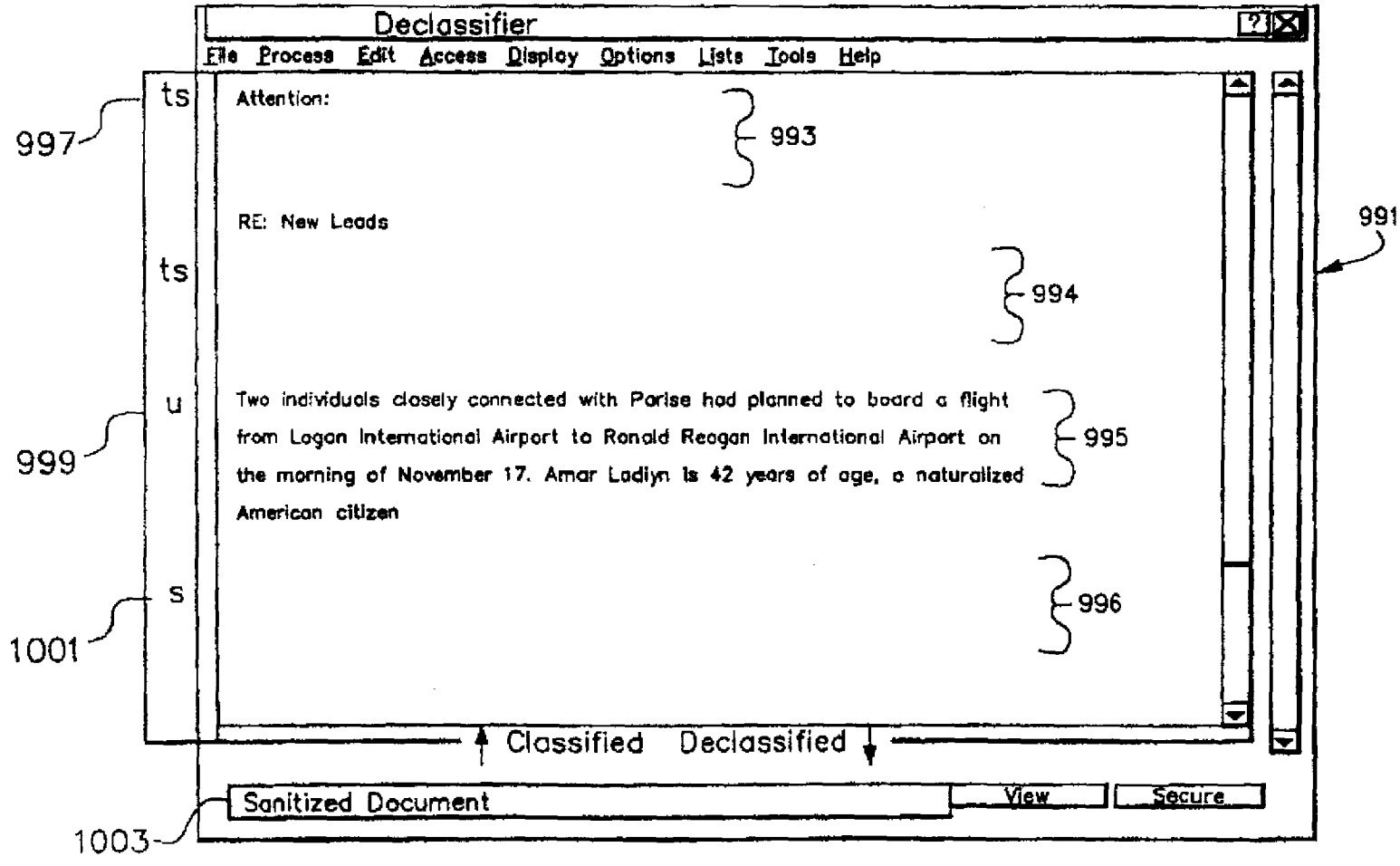

Declassifier
File Process Edit Access Display Options Lists Tools Help
ts
Attention:
993
997
RE: New Leads
991
ts
994
u
Two individuals closely connected with Parise had planned to board a flight from Logan International Airport to Ronald Reagan International Airport on the morning of November 17. Amar Ladiyn is 42 years of age, a naturalized American citizen
995
999
s
996
1001
Classified Declassified
Sanitized Document
View
Secure
1003

FIG.17

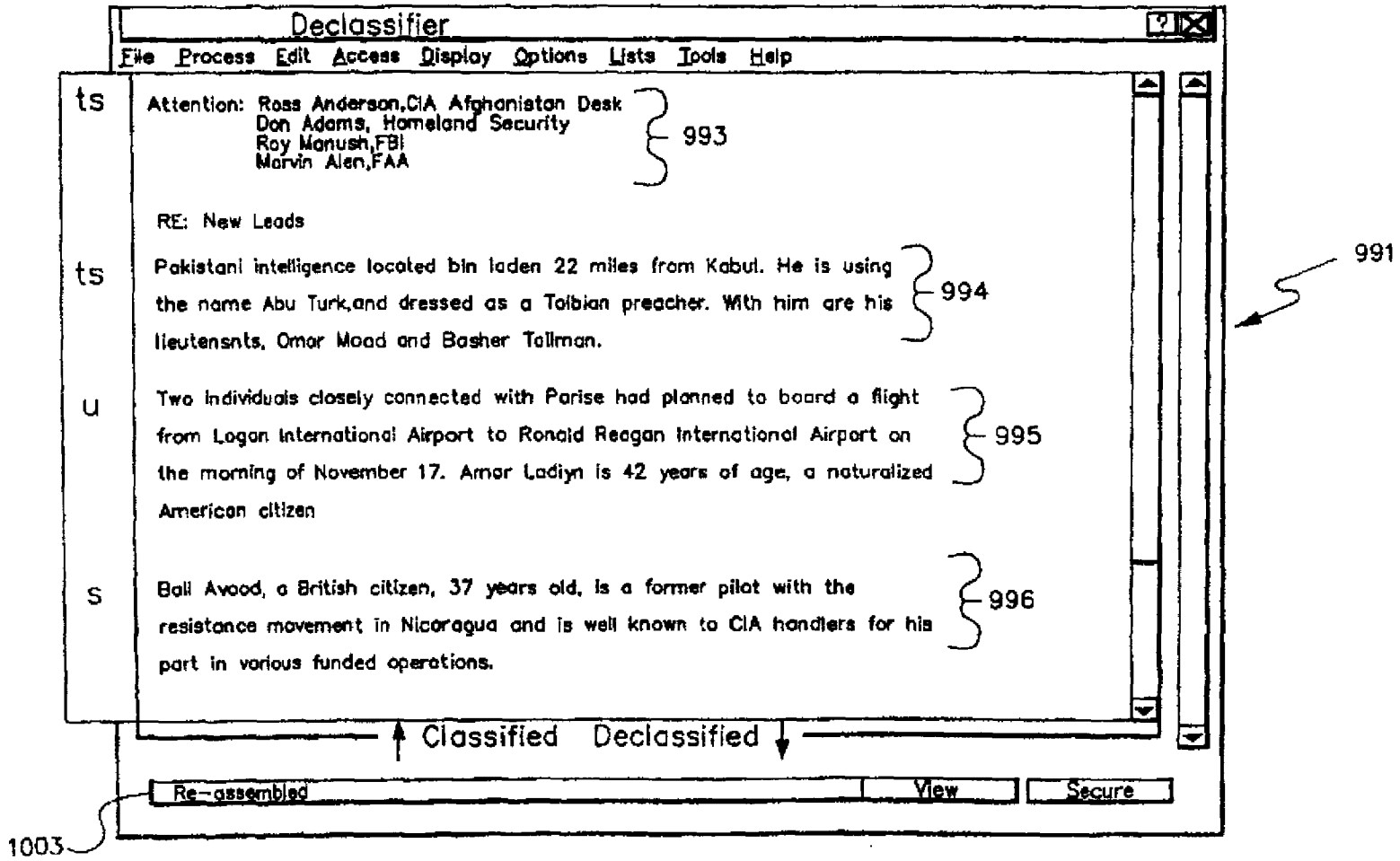

Declassifier
File Process Edit Access Display Options Lists Tools Help
ts
Attention: Ross Anderson,CIA Afghanistan Desk
Don Adams, Homeland Security
Roy Manush,FBI
Marvin Alen,FAA
993
RE: New Leads
ts
Pakistani intelligence located bin laden 22 miles from Kabul. He is using the name Abu Turk,and dressed as a Taibian preacher. With him are his lieutensnts, Omar Mood and Basher Tallman.
994
u
Two individuals closely connected with Parise had planned to board a flight from Logan International Airport to Ronald Reagan International Airport on the morning of November 17. Amar Ladiyn is 42 years of age, a naturalized American citizen
995
s
Bali Avood, a British citizen, 37 years old, is a former pilot with the resistance movement in Nicoragua and is well known to CIA handlers for his part in various funded operations.
996
991
Classified Declassified
Re-assembled
View
Secure
1003

FIG.18

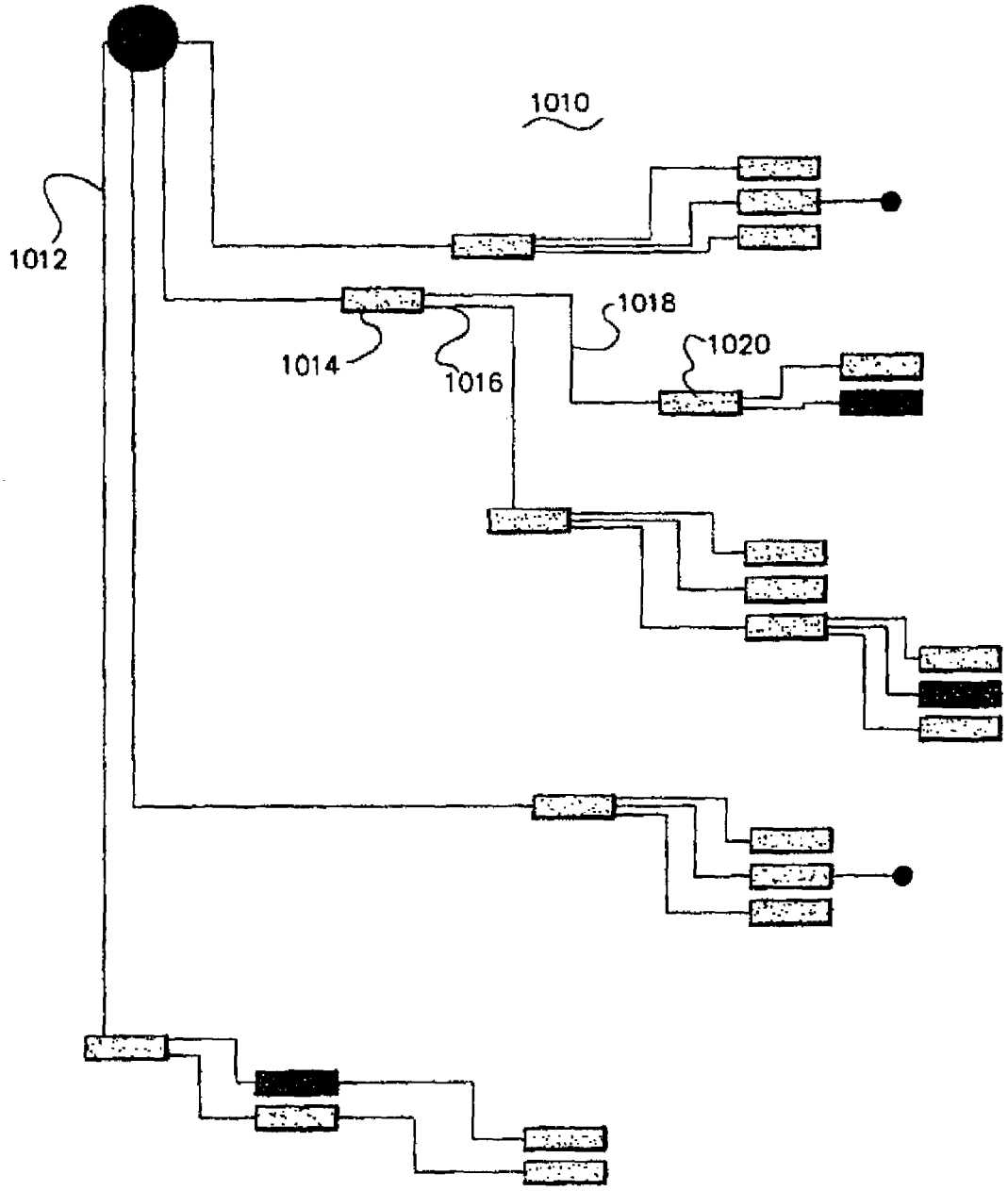


FIG.19

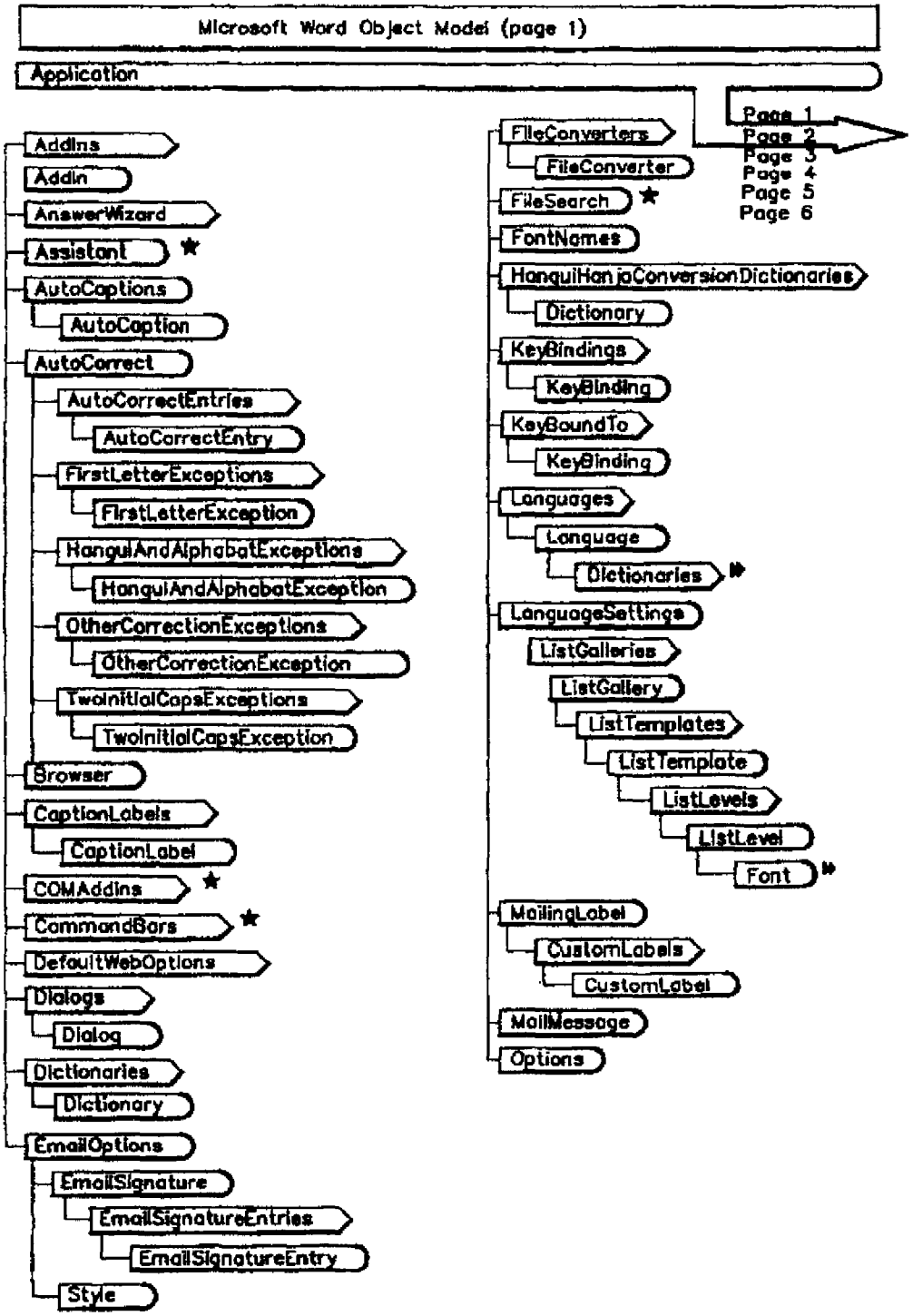

Microsoft Word Object Model (page 1)
Application
Page 1
Page 2
Page 3
Page 4
Page 5
Page 6
AddIns
Addin
AnswerWizard
Assistant
AutoCaptions
AutoCaption
AutoCorrect
AutoCorrectEntries
AutoCorrectEntry
FirstLetterExceptions
FirstLetterException
HangulAndAlphabatExceptions
HangulAndAlphabatException
OtherCorrectionExceptions
OtherCorrectionException
TwoInitialCapsExceptions
TwoInitialCapsException
Browser
CaptionLabels
CaptionLabel
COMAddins
CommandBars
DefaultWebOptions
Dialogs
Dialog
Dictionaries
Dictionary
EmailOptions
EmailSignature
EmailSignatureEntries
EmailSignatureEntry
Style
FileConverters
FileConverter
FileSearch
FontNames
HanguiHanjaConversionDictionaries
Dictionary
KeyBindings
KeyBinding
KeyBoundTo
KeyBinding
Languages
Language
Dictionaries
LanguageSettings
ListGalleries
ListGallery
ListTemplates
ListTemplate
ListLevels
ListLevel
Font
MailingLabel
CustomLabels
CustomLabel
MailMessage
Options

FIG.20

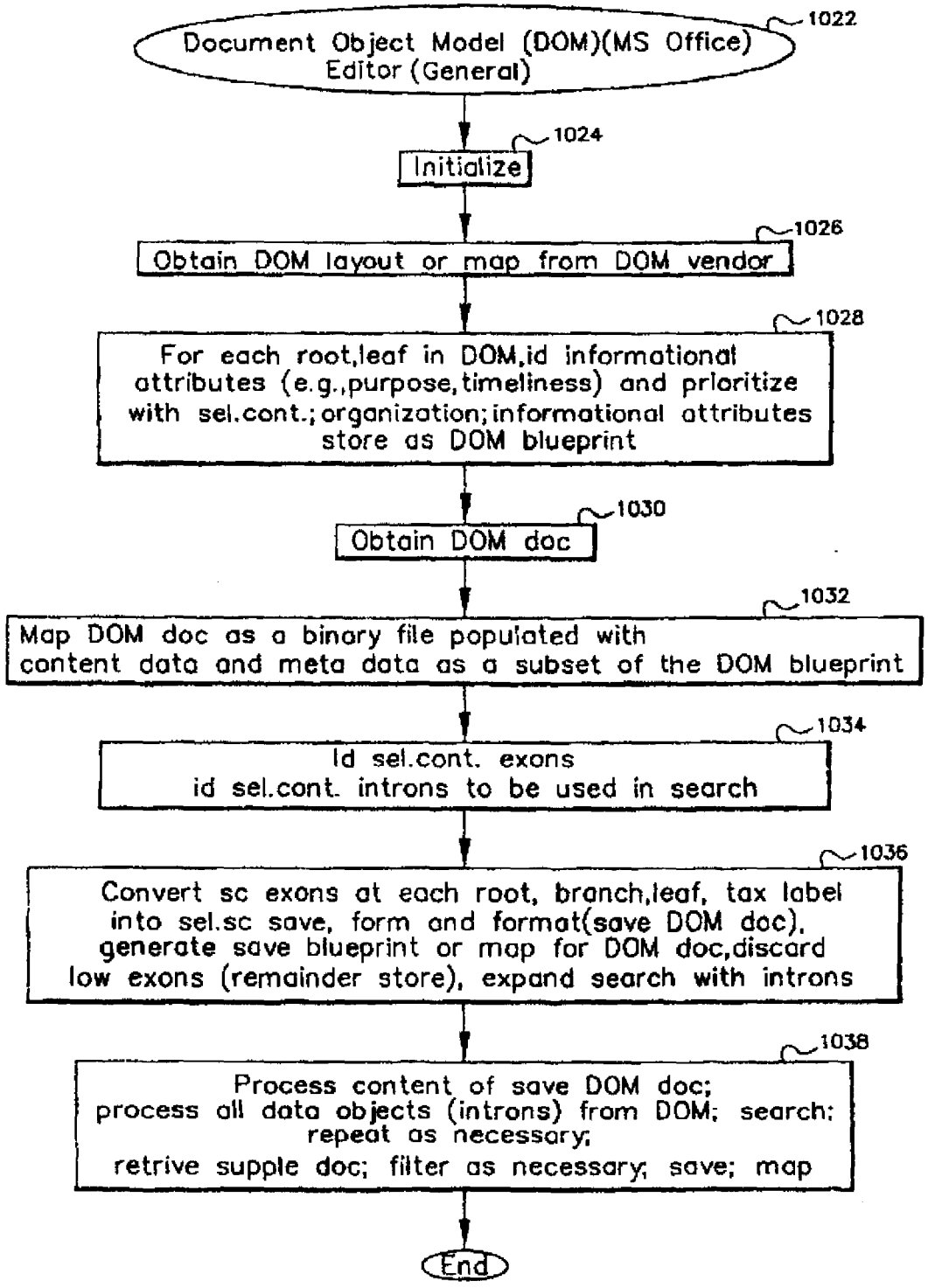

Document Object Model (DOM)(MS Office) Editor (General)
1022
Initialize
1024
Obtain DOM layout or map from DOM vendor
1026
For each root,leaf in DOM,id informational attributes (e.g.,purpose,timeliness) and prioritize with sel.cont.;organization;informational attributes store as DOM blueprint
1028
Obtain DOM doc
1030
Map DOM doc as a binary file populated with content data and meta data as a subset of the DOM blueprint
1032
Id sel.cont. exons
id sel.cont. introns to be used in search
1034
Convert sc exons at each root, branch,leaf, tax label into sel.sc save, form and format(save DOM doc), generate save blueprint or map for DOM doc,discard low exons (remainder store), expand search with introns
1036
Process content of save DOM doc;
process all data objects (introns) from DOM; search; repeat as necessary;
retrive supple doc; filter as necessary; save; map
1038
End

FIG.21

FIG.22

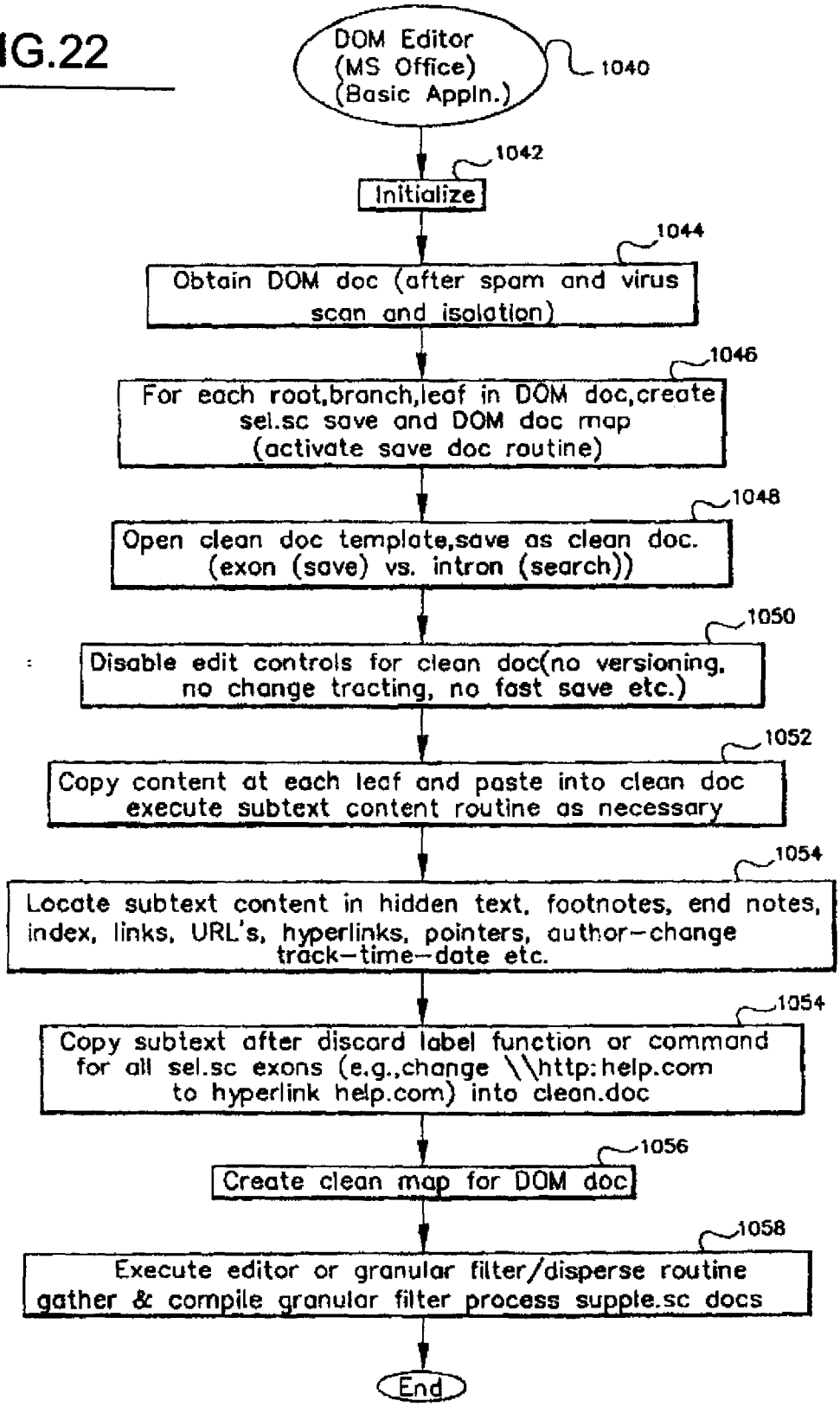

DOM Editor
(MS Office)
(Basic Appln.)
1040
1042
Initialize
1044
Obtain DOM doc (after spam and virus scan and isolation)
1046
For each root,branch,leaf in DOM doc,create sel.sc save and DOM doc map (activate save doc routine)
1048
Open clean doc template,save as clean doc. (exon (save) vs. intron (search))
1050
Disable edit controls for clean doc(no versioning, no change tracting, no fast save etc.)
1052
Copy content at each leaf and paste into clean doc execute subtext content routine as necessary
1054
Locate subtext content in hidden text, footnotes, end notes, index, links, URL's, hyperlinks, pointers, author-change track-time-date etc.
1054
Copy subtext after discard label function or command for all sel.sc exons (e.g.,change \\http:help.com to hyperlink help.com) into clean.doc
1056
Create clean map for DOM doc
1058
Execute editor or granular filter/disperse routine gather & compile granular filter process supple.sc docs
End

FIG.23 -- Table 1: Categorical Identifiers For Personal Identity

name
address(es) and variants
telephone number(s) and variants
username
biometrics
gene typing
photograph
date of birth
age
marital status
gender
sexual orientation
sexual proclivities
disabilities
tattoos
scars
visible or functional injuries
age/age range
hair color
eye color
race profile
educational history
employment history
home price
ethnicity
personal interests
personal descriptive information (e.g., SWHM 38, Professional)
physical stigmata
skill set
credit history
credit reports (formal NCR, etc.)
social security number
patient ID or other location- or process-specific
user assignment
insurance number
credit card numbers
birthplace
heritage
health history
political party
political beliefs
association(s)
frequent flyer/buyer club info
remittance advice
investigation evidence
court evidence
EDI/EDIFACT records
applications
personal web sites
Chain of trust forms
Chain of custody forms
skill set
religion
personal interests
travel log
number of siblings
business partners
business name
profession
account numbers (banking, services, suppliers)
service providers (physicians, insurers, hospitals, clinics, etc.)
X-rays
surveillance
dental charts
medical records
account balances
account transfer or transaction amounts
income range
neighborhood/city/region/country
license (driver, occupational, professional)
vehicle registration (license, tag, plate, etc.)
vehicle identification
vehicle make, type, model, color, year
date of life events
incident reports (legal, criminal, health services, news)
accident reports (auto, OSHA, EPA, EEOC, etc.)
criminal convictions
court records
abuse records
divorce proceedings
bankruptcy records
organization registrations
Corporation officers and registrations
tax records (chattel, land, local, state, Federal, and special use taxes)
property ownership
permit applications
donor lists
news reports
family history
family relationships
family health history
legal documents
consent forms
newsgroup postings

FIG.24 -- Table 2: Ranked Identity Category

name	disabilities
address	tattoos
telephone	scars
username	injuries
biometrics	age range
gene typing	hair color
photograph	eye color
date of birth	race profile
age	education
marital status	employment
sex	personal interests
sexual orientation	
sexual proclivities	

FIG.25 -- Table 3: Categorical Identifiers for Manufacturing Business

- Manufacturing
  - product brand names
  - product generic name
  - drawings
  - tools (brand names and generic names)
    - hand tools
    - software
    - machines
  - software, computer programs, etc.
  - Research and Development
    - competitors products, competitor names, patent numbers, patent titles, project names, project personnel
- Sales
  - personnel
  - competitors
  - sales data
    - quantity
    - geographic distribution
  - customers
    - names, addresses, contacts
  - sales projections
- Financial
  - chart of accounts
  - ledgers
  - financial statements
  - tax returns
- Human Resources
  - see categorical identifiers for personal identity

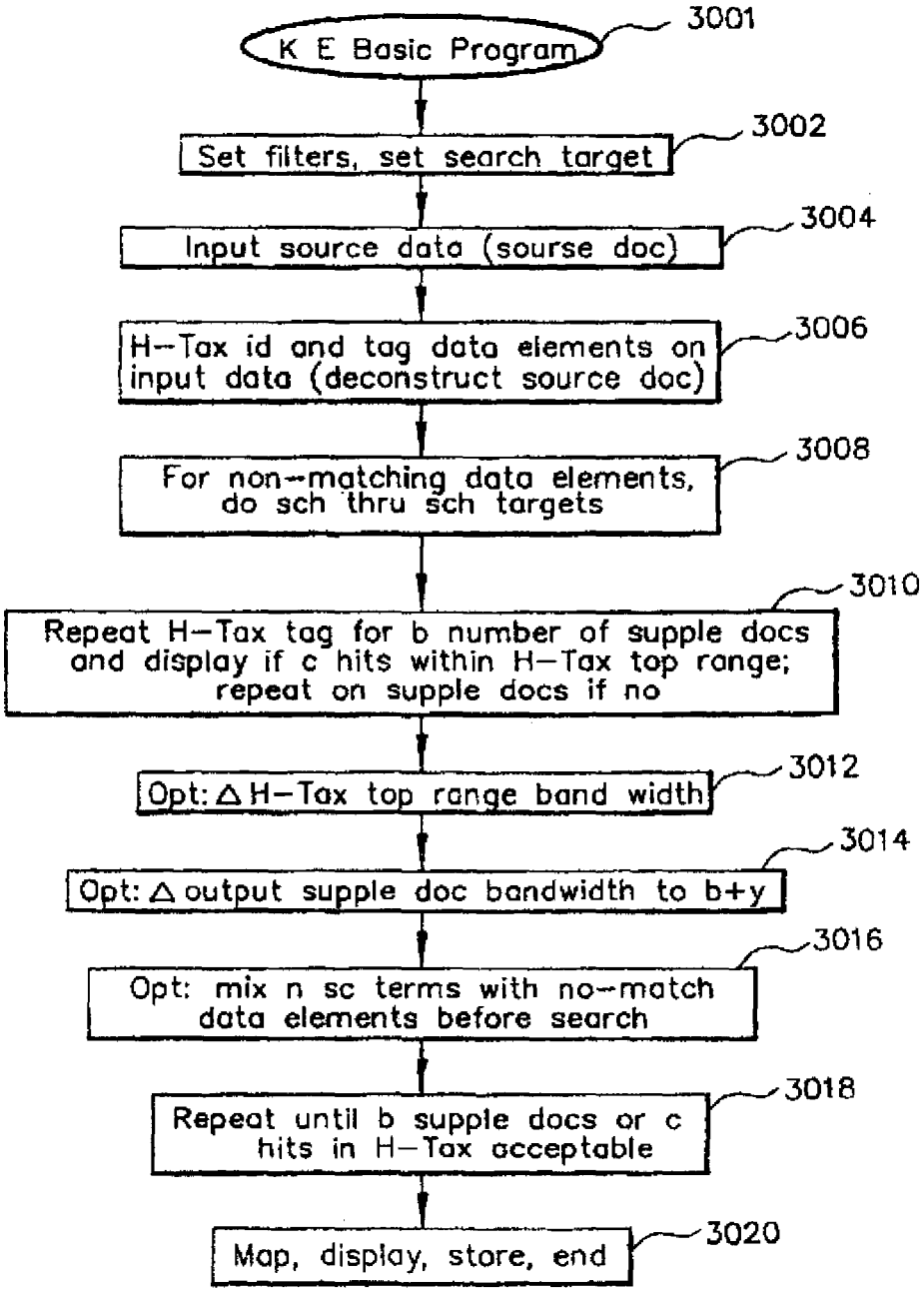

K E Basic Program
3001
Set filters, set search target
3002
Input source data (sourse doc)
3004
H–Tax id and tag data elements on input data (deconstruct source doc)
3006
For non–matching data elements, do sch thru sch targets
3008
Repeat H–Tax tag for b number of supple docs and display if c hits within H–Tax top range; repeat on supple docs if no
3010
Opt: Δ H–Tax top range band width
3012
Opt: Δ output supple doc bandwidth to b+y
3014
Opt: mix n sc terms with no–match data elements before search
3016
Repeat until b supple docs or c hits in H–Tax acceptable
3018
Map, display, store, end
3020

FIG.26

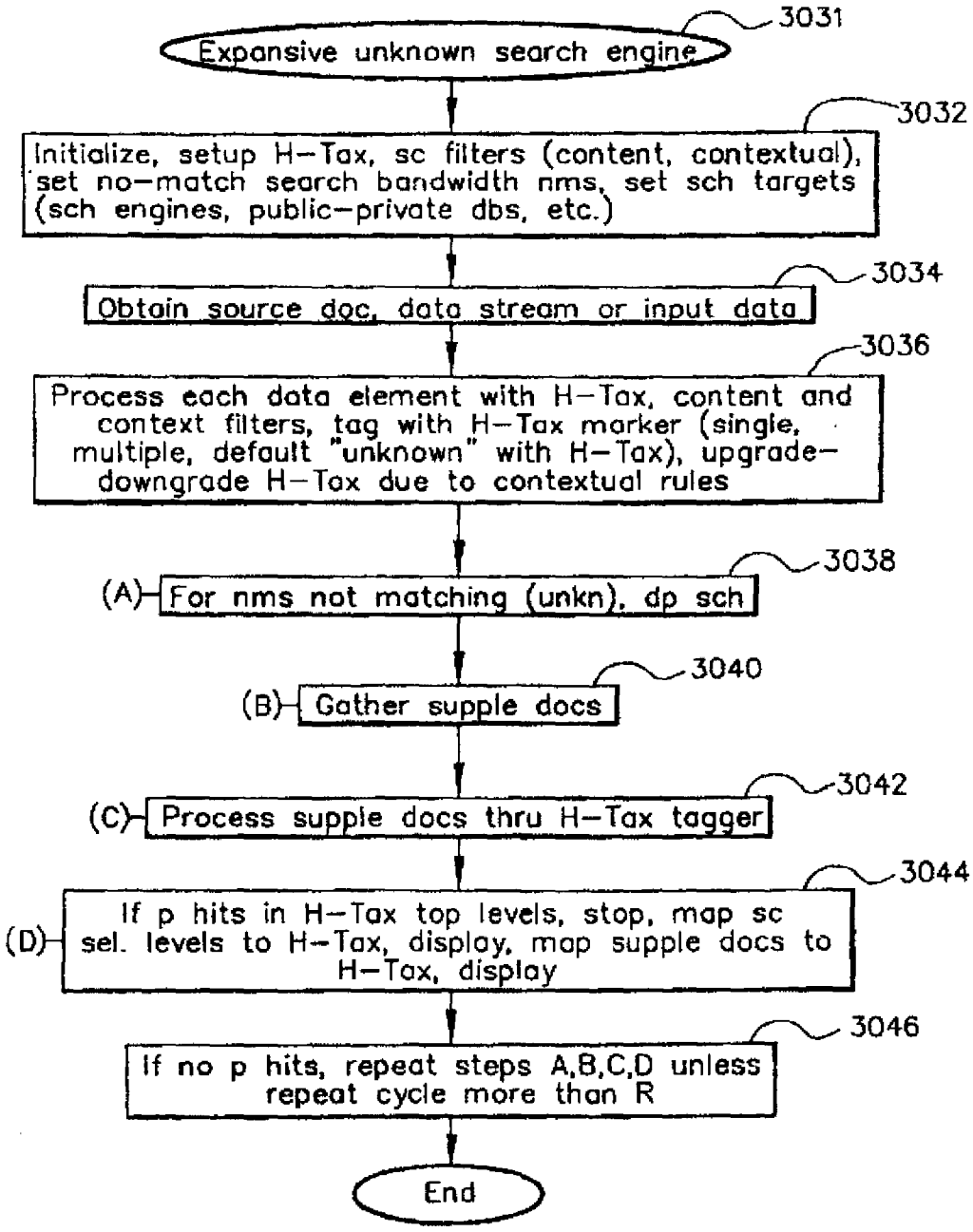

3031
Expansive unknown search engine
3032
Initialize, setup H-Tax, sc filters (content, contextual), set no-match search bandwidth nms, set sch targets (sch engines, public-private dbs, etc.)
3034
Obtain source doc, data stream or input data
3036
Process each data element with H-Tax, content and context filters, tag with H-Tax marker (single, multiple, default "unknown" with H-Tax), upgrade-downgrade H-Tax due to contextual rules
3038
(A) For nms not matching (unkn), dp sch
3040
(B) Gather supple docs
3042
(C) Process supple docs thru H-Tax tagger
3044
(D) If p hits in H-Tax top levels, stop, map sc sel. levels to H-Tax, display, map supple docs to H-Tax, display
3046
If no p hits, repeat steps A,B,C,D unless repeat cycle more than R
End

FIG.27

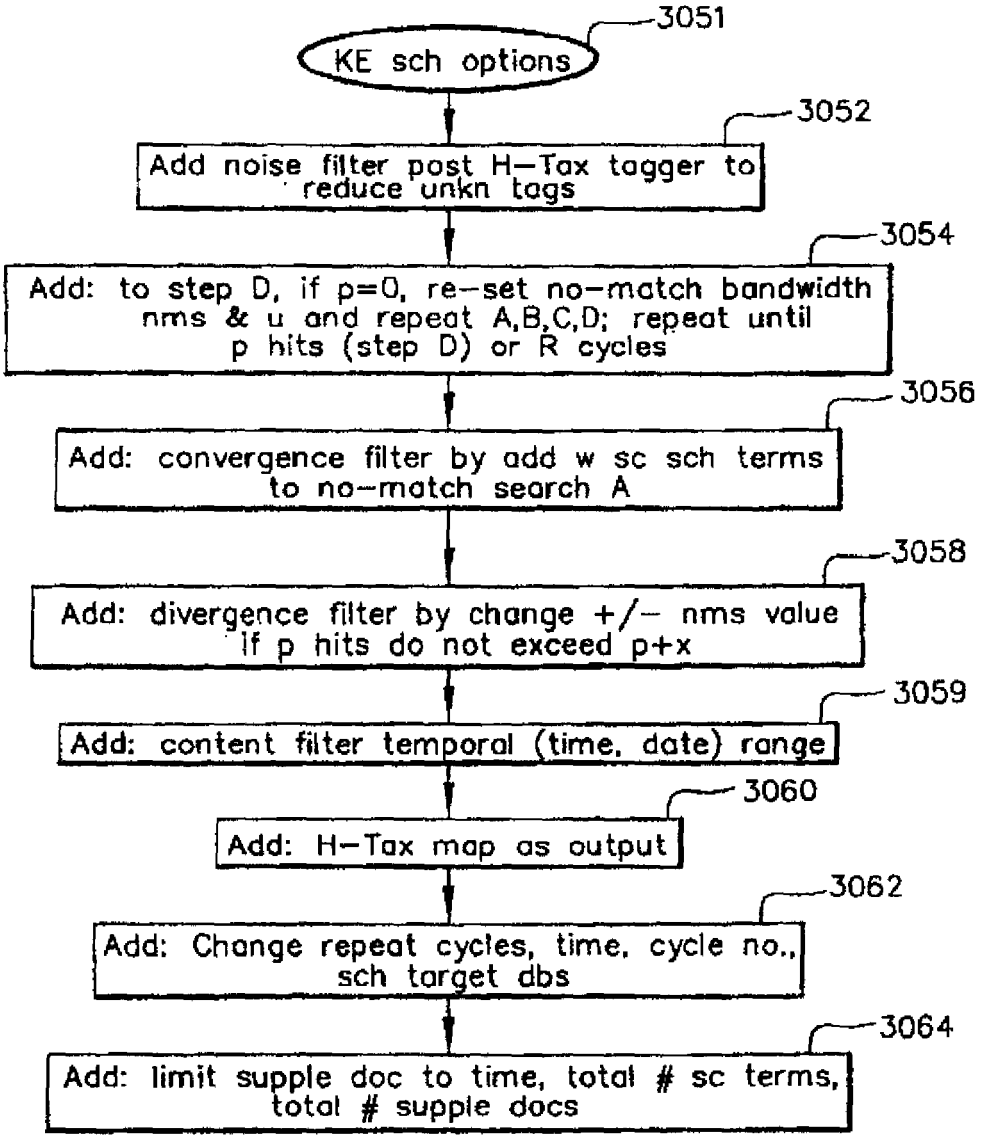

3051
KE sch options
3052
Add noise filter post H-Tax tagger to reduce unkn tags
3054
Add: to step D, if p=0, re-set no-match bandwidth nms & u and repeat A,B,C,D; repeat until p hits (step D) or R cycles
3056
Add: convergence filter by add w sc sch terms to no-match search A
3058
Add: divergence filter by change +/- nms value if p hits do not exceed p+x
3059
Add: content filter temporal (time, date) range
3060
Add: H-Tax map as output
3062
Add: Change repeat cycles, time, cycle no., sch target dbs
3064
Add: limit supple doc to time, total # sc terms, total # supple docs

FIG.28

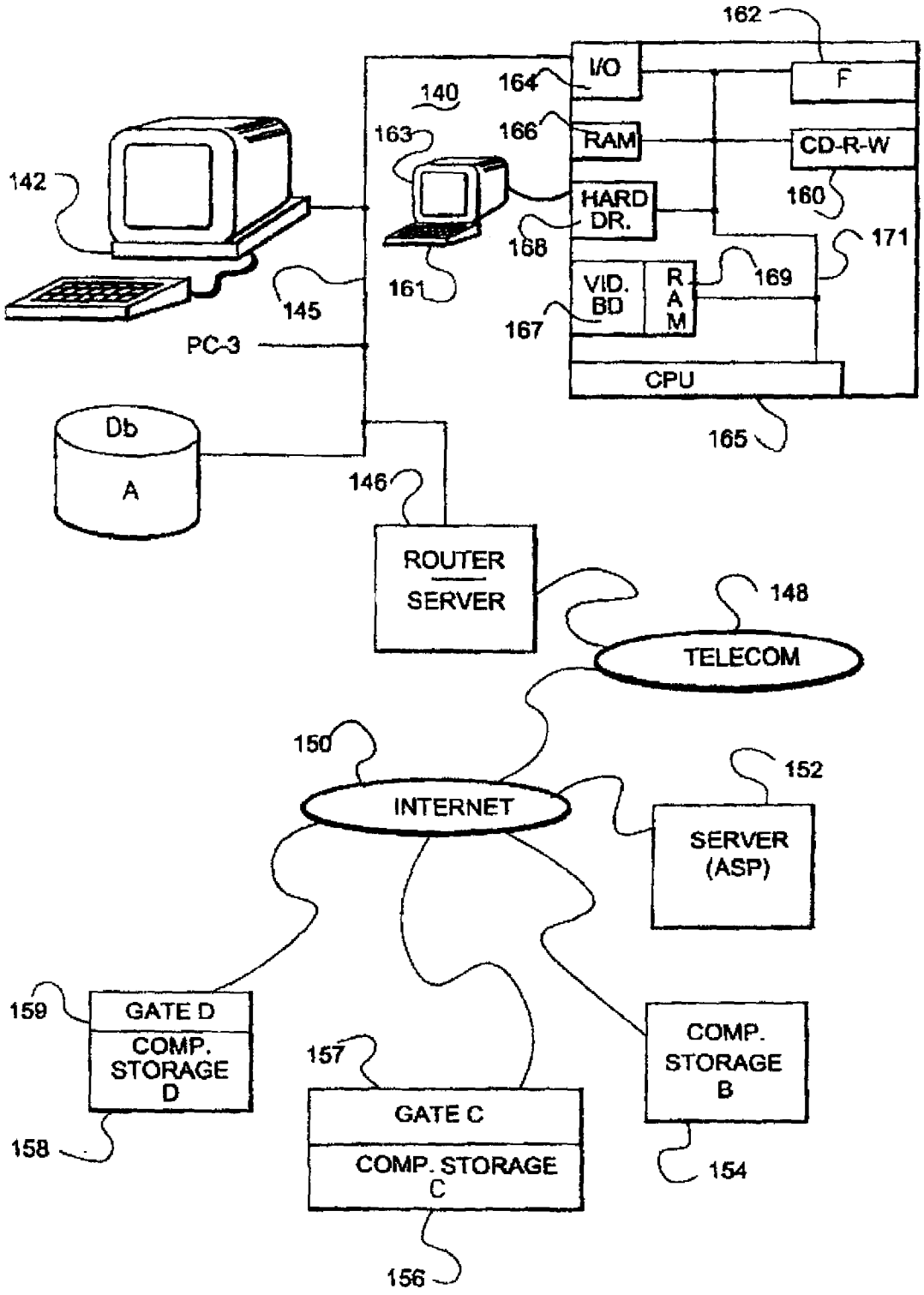

162
I/O
F
164
140
163
166
RAM
CD-R-W
142
HARD DR.
160
168
171
VID. BD
R A M
169
167
145
161
PC-3
CPU
165
Db
A
146
ROUTER SERVER
148
TELECOM
150
152
INTERNET
SERVER (ASP)
159
GATE D
COMP. STORAGE D
157
COMP. STORAGE B
158
GATE C
COMP. STORAGE C
154
156

FIG.29

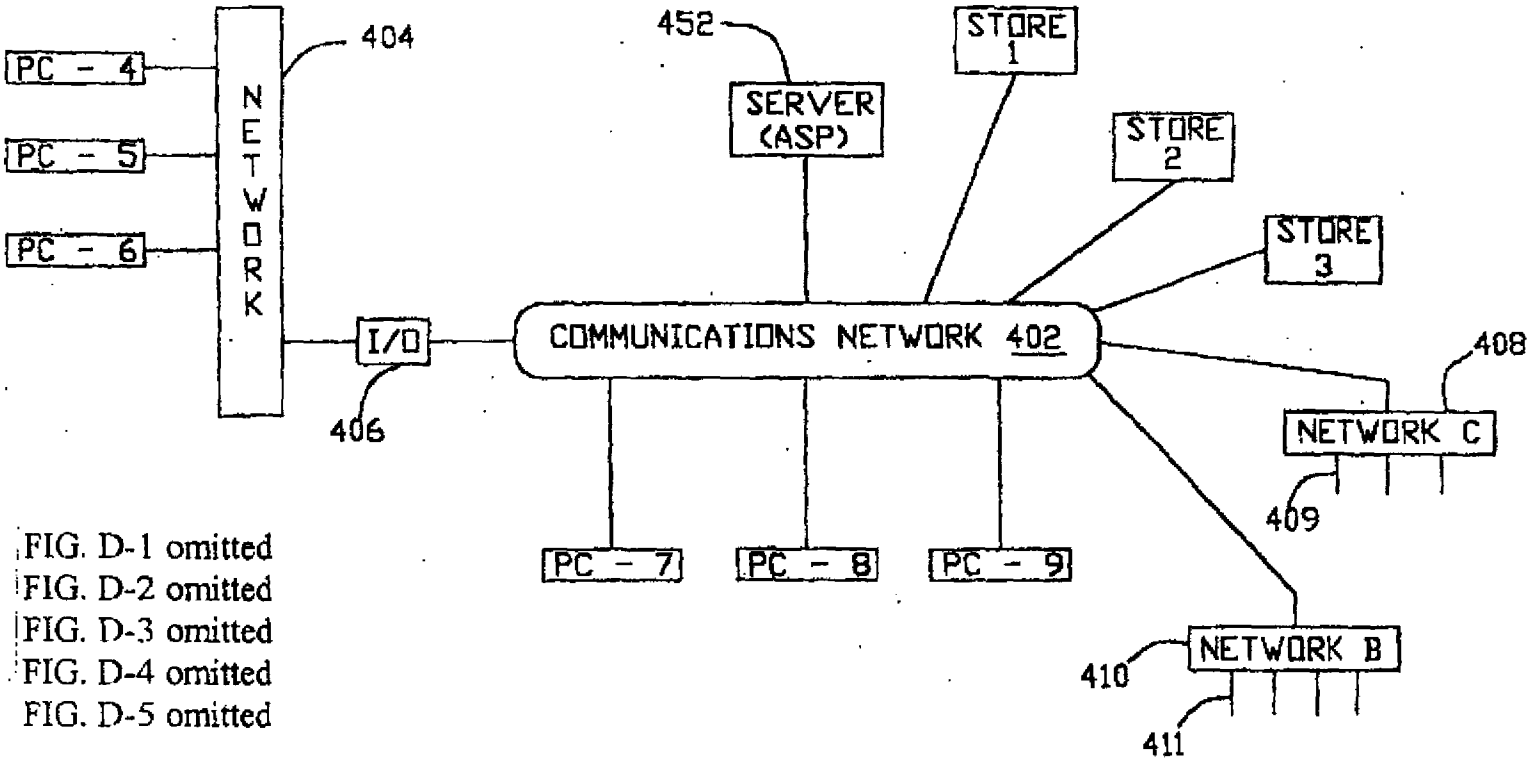
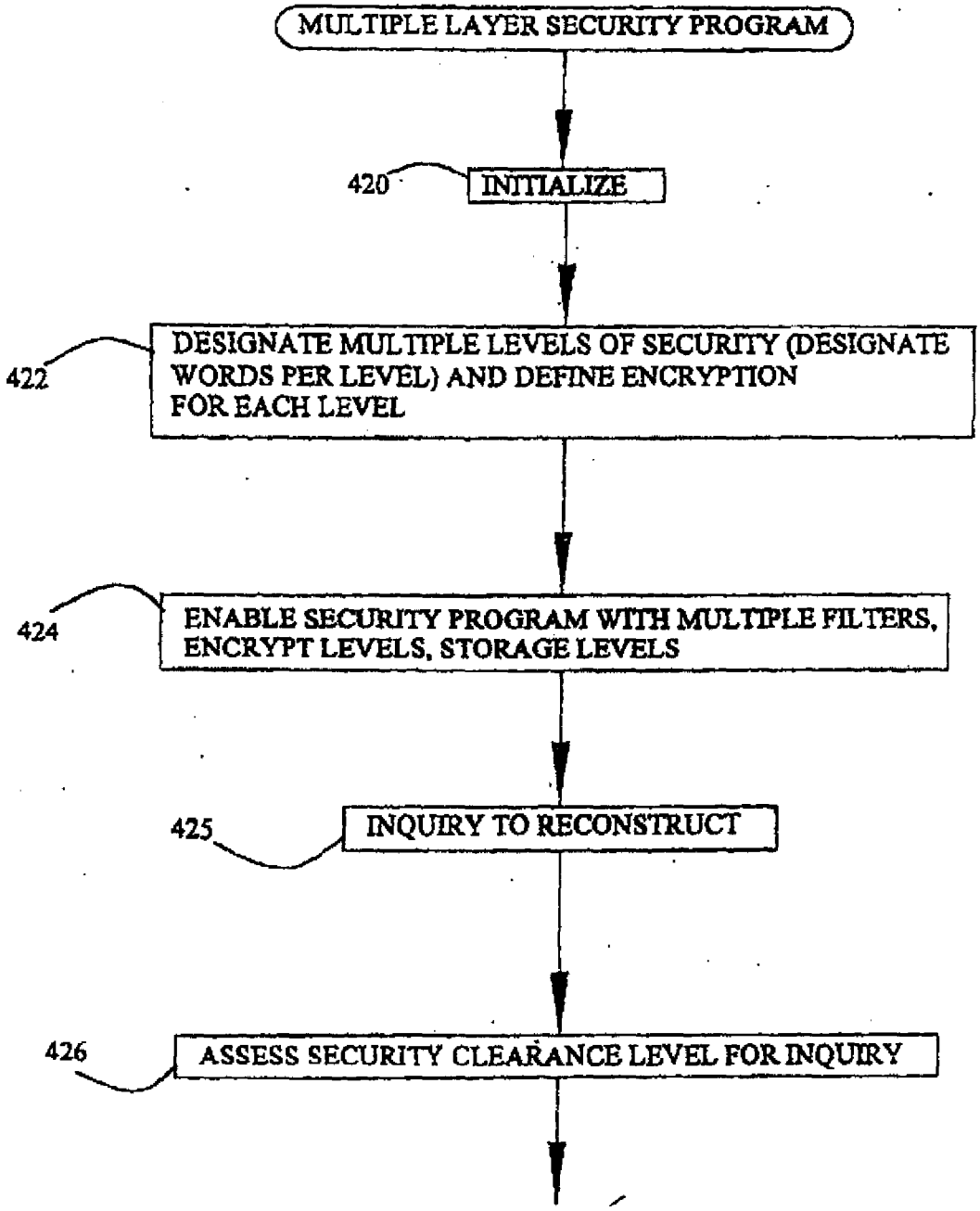


FIG. D-1 omitted
FIG. D-2 omitted
FIG. D-3 omitted
FIG. D-4 omitted
FIG. D-5 omitted

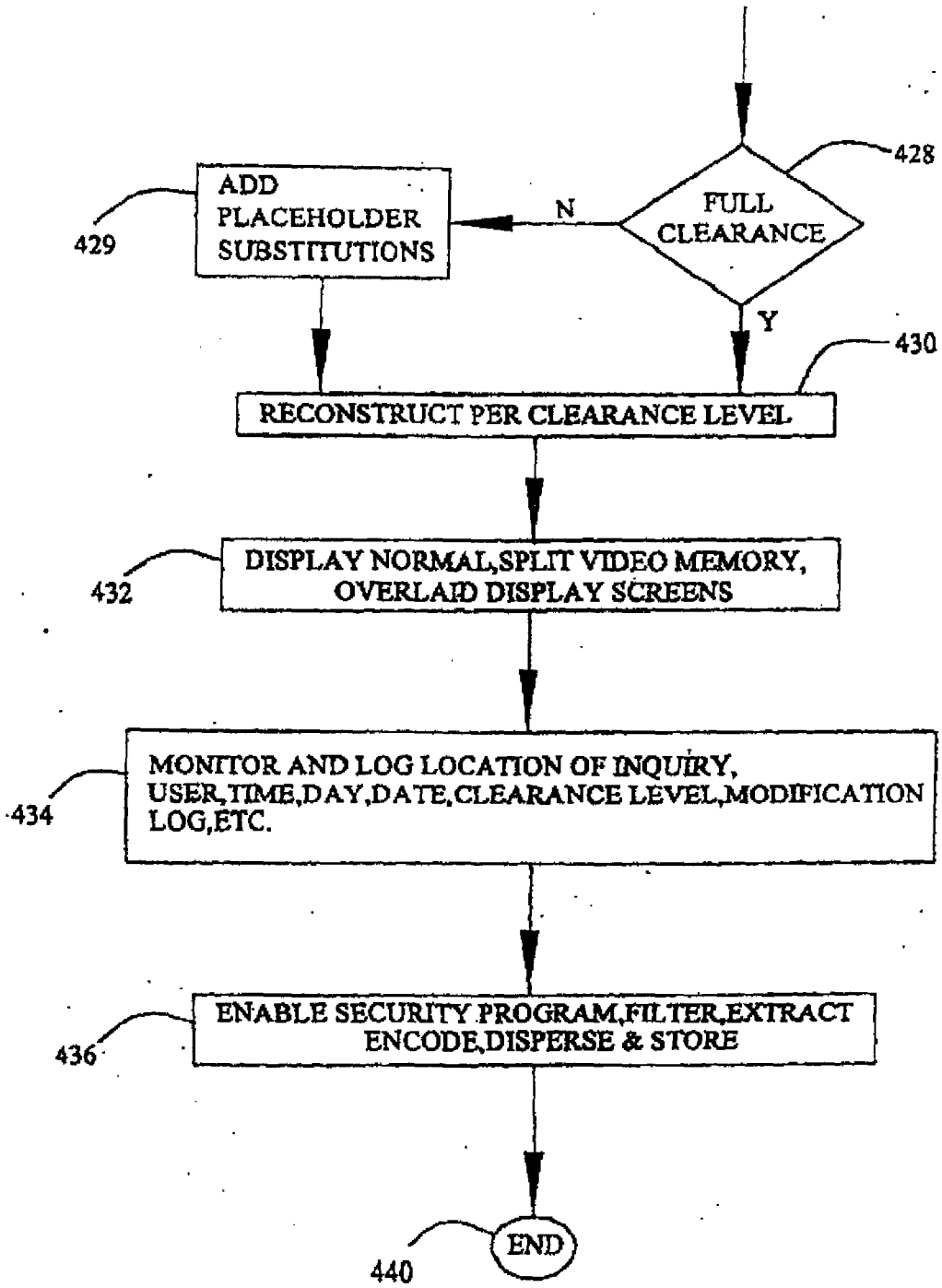
FIG.30

FIG.31a



TO FIG.31b (CONT.)

FIG.31b


428
FULL CLEARANCE
N
ADD PLACEHOLDER SUBSTITUTIONS
429
Y
430
RECONSTRUCT PER CLEARANCE LEVEL
DISPLAY NORMAL,SPLIT VIDEO MEMORY, OVERLAID DISPLAY SCREENS
432
MONITOR AND LOG LOCATION OF INQUIRY, USER,TIME,DAY,DATE,CLEARANCE LEVEL,MODIFICATION LOG,ETC.
434
ENABLE SECURITY PROGRAM,FILTER,EXTRACT ENCODE,DISPERSE & STORE
436
END
440

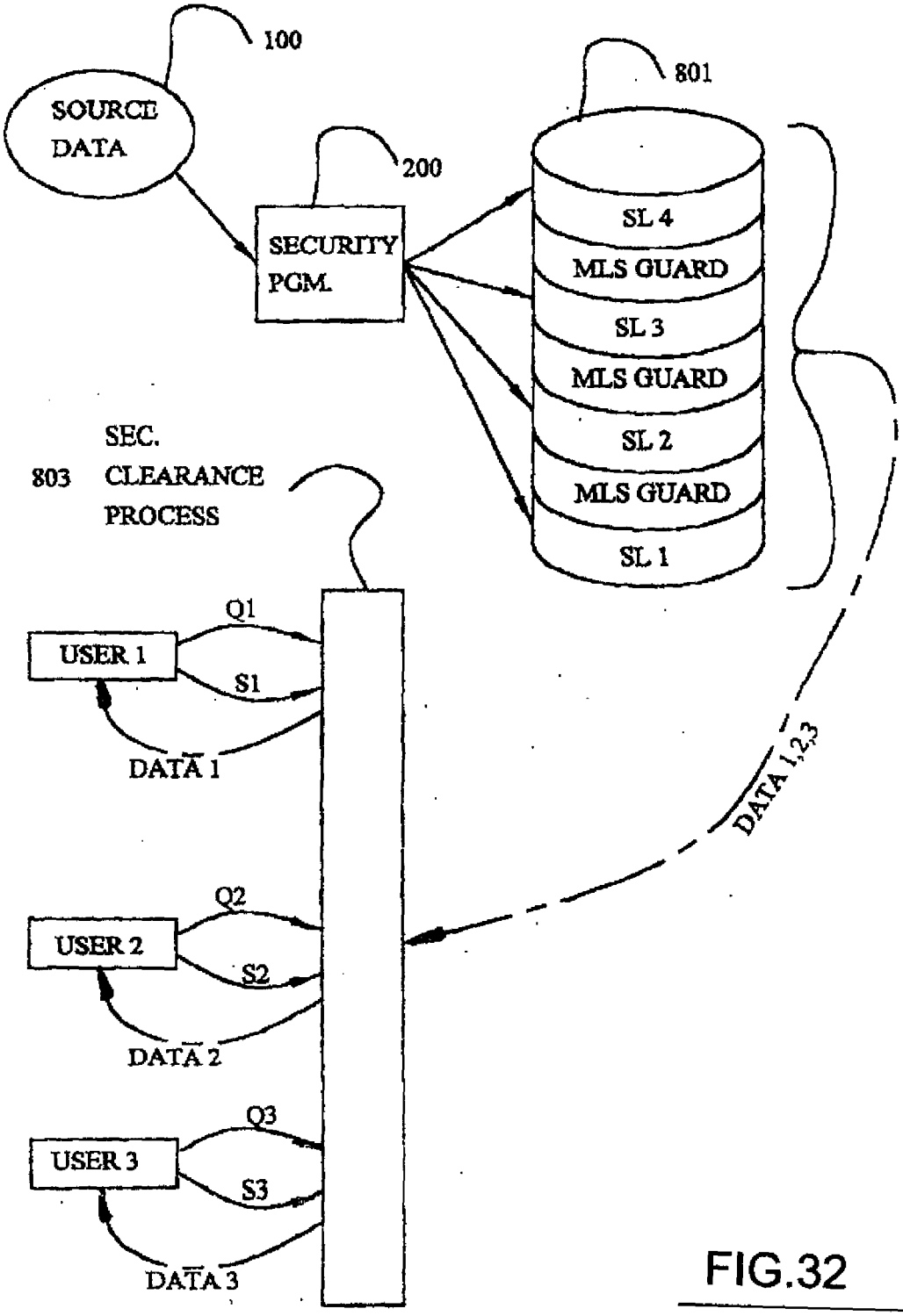

100
SOURCE DATA
200
SECURITY PGM.
801
SL 4
MLS GUARD
SL 3
MLS GUARD
SL 2
MLS GUARD
SL 1
SEC. CLEARANCE PROCESS
803
Q1
USER 1
S1
DATA 1
DATA 1,2,3
Q2
USER 2
S2
DATA 2
Q3
USER 3
S3
DATA 3

FIG.32

FIG.33a

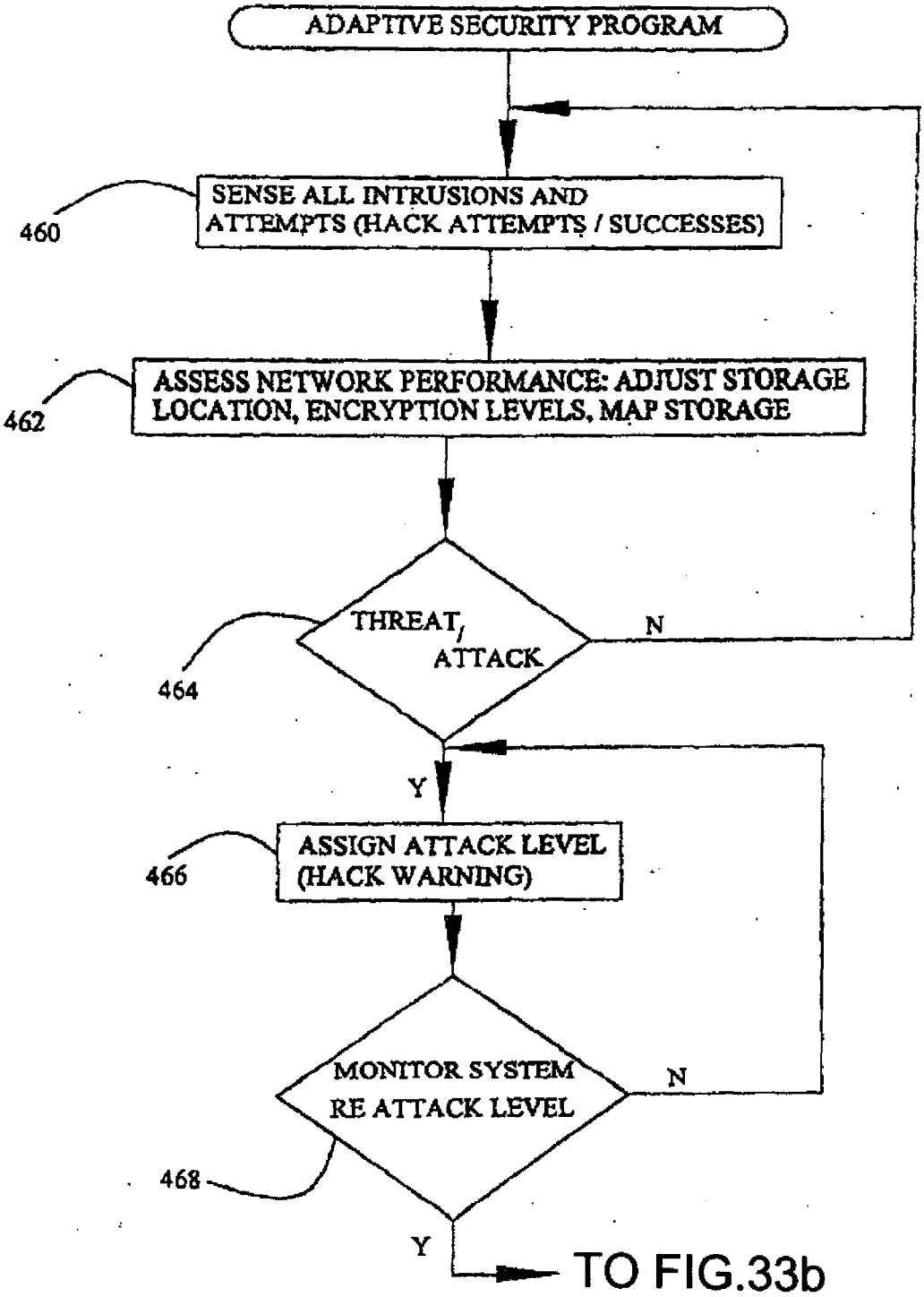

ADAPTIVE SECURITY PROGRAM
460
SENSE ALL INTRUSIONS AND ATTEMPTS (HACK ATTEMPTS / SUCCESSES)
462
ASSESS NETWORK PERFORMANCE: ADJUST STORAGE LOCATION, ENCRYPTION LEVELS, MAP STORAGE
464
THREAT, ATTACK
N
Y
466
ASSIGN ATTACK LEVEL (HACK WARNING)
MONITOR SYSTEM RE ATTACK LEVEL
N
468
Y
TO FIG.33b

FIG.33b

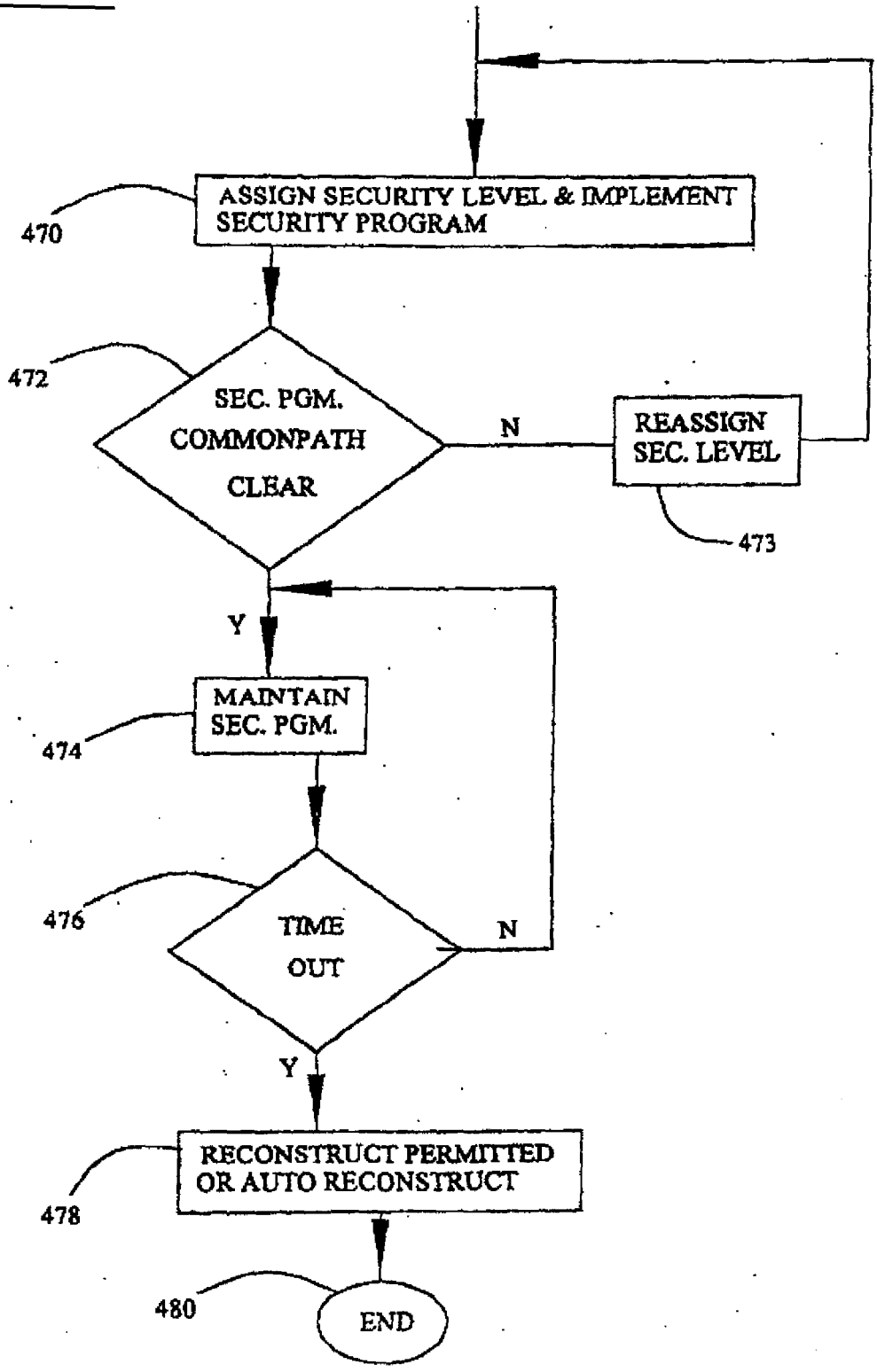

ASSIGN SECURITY LEVEL & IMPLEMENT SECURITY PROGRAM
470
SEC. PGM. COMMONPATH CLEAR
472
N
REASSIGN SEC. LEVEL
473
Y
MAINTAIN SEC. PGM.
474
TIME OUT
476
N
Y
RECONSTRUCT PERMITTED OR AUTO RECONSTRUCT
478
END
480

FIG.34

Standard Automatic Defenses Matrix Table

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

FIG.35

Optional Automatic Defenses Matrix Table

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

FIG.36

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

FIG.37

Normal Work Mode Table

	Extraction				Storage				
	Level 1	Level 2	Level 3	Level 4	Web	Offline	Remote	Removable	Local
social security	X						X		
credit card	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 cap			X					X	
currency				X					X
postal code				X					X
address				X					X
location				X					X
date				X					X

FIG.38

Threat Mode Table

	Extraction Level 1	Level 2	Level 3	Level 4	Storage Web	Offline	Remote	Removable	Local
social security	X							X	
credit card	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

FIG.39

Attack Mode Table

	Extraction Level 1	Level 2	Level 3	Level 4	Storage Web	Offline	Remote	Removable
social security	X					X		
credit card	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	

FIG.40

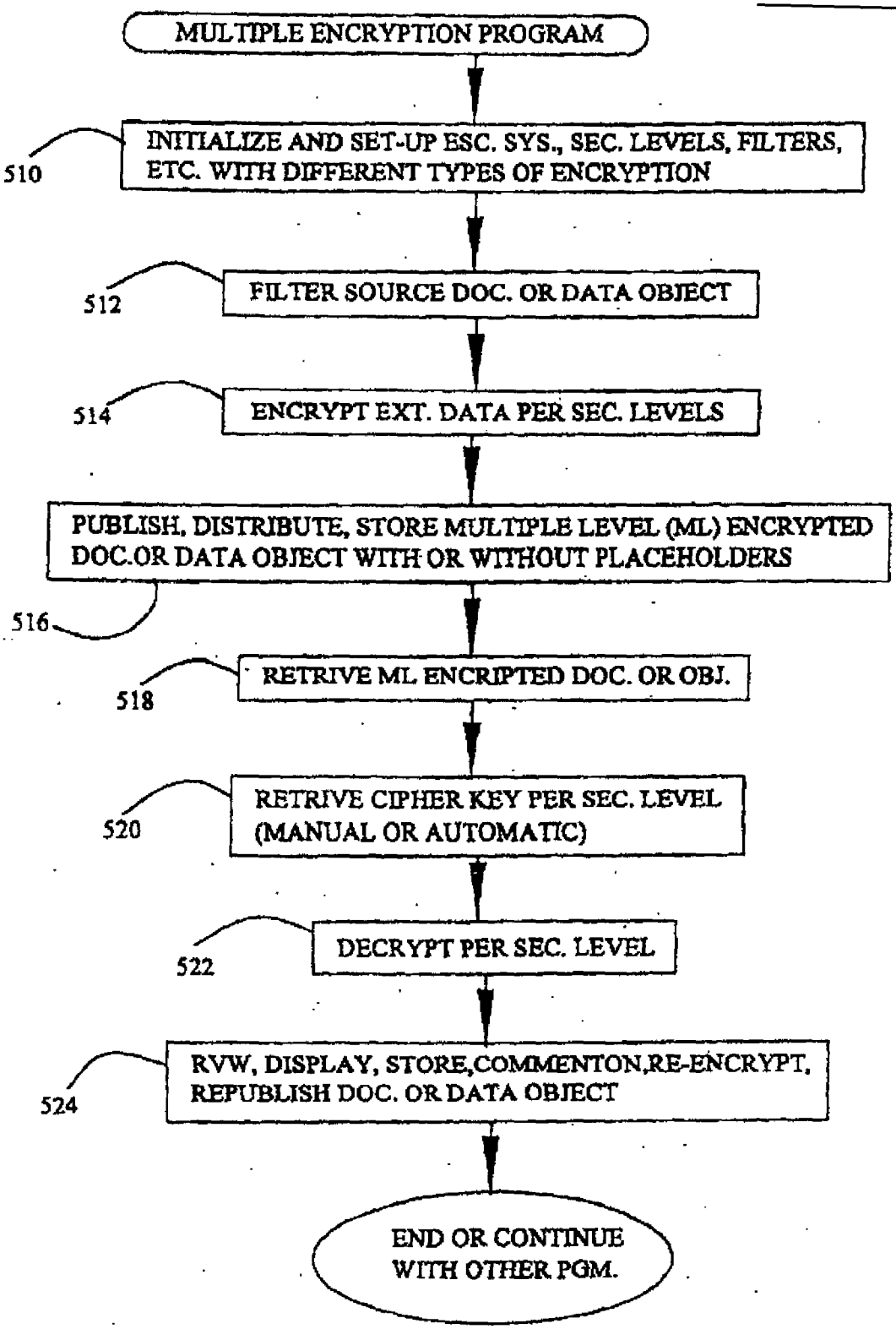

MULTIPLE ENCRYPTION PROGRAM
510
INITIALIZE AND SET-UP ESC. SYS., SEC. LEVELS, FILTERS, ETC. WITH DIFFERENT TYPES OF ENCRYPTION
512
FILTER SOURCE DOC. OR DATA OBJECT
514
ENCRYPT EXT. DATA PER SEC. LEVELS
516
PUBLISH, DISTRIBUTE, STORE MULTIPLE LEVEL (ML) ENCRYPTED DOC.OR DATA OBJECT WITH OR WITHOUT PLACEHOLDERS
518
RETRIVE ML ENCRIPTED DOC. OR OBJ.
520
RETRIVE CIPHER KEY PER SEC. LEVEL (MANUAL OR AUTOMATIC)
522
DECRYPT PER SEC. LEVEL
524
RVW, DISPLAY, STORE,COMMENTON,RE-ENCRYPT, REPUBLISH DOC. OR DATA OBJECT
END OR CONTINUE WITH OTHER PGM.

FIG.41

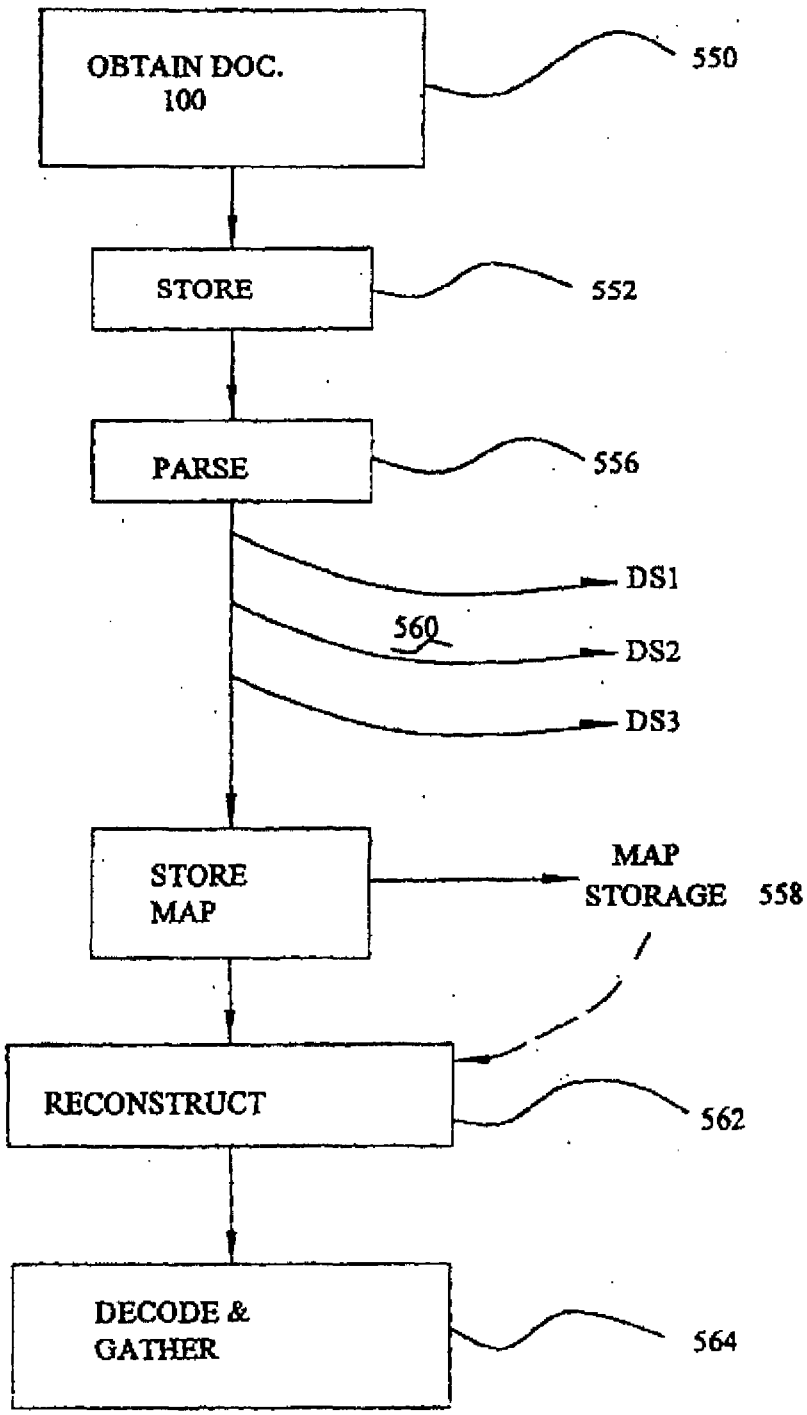

OBTAIN DOC. 100
550
STORE
552
PARSE
556
DS1
560
DS2
DS3
STORE MAP
MAP STORAGE 558
RECONSTRUCT
562
DECODE & GATHER
564

FIG.42

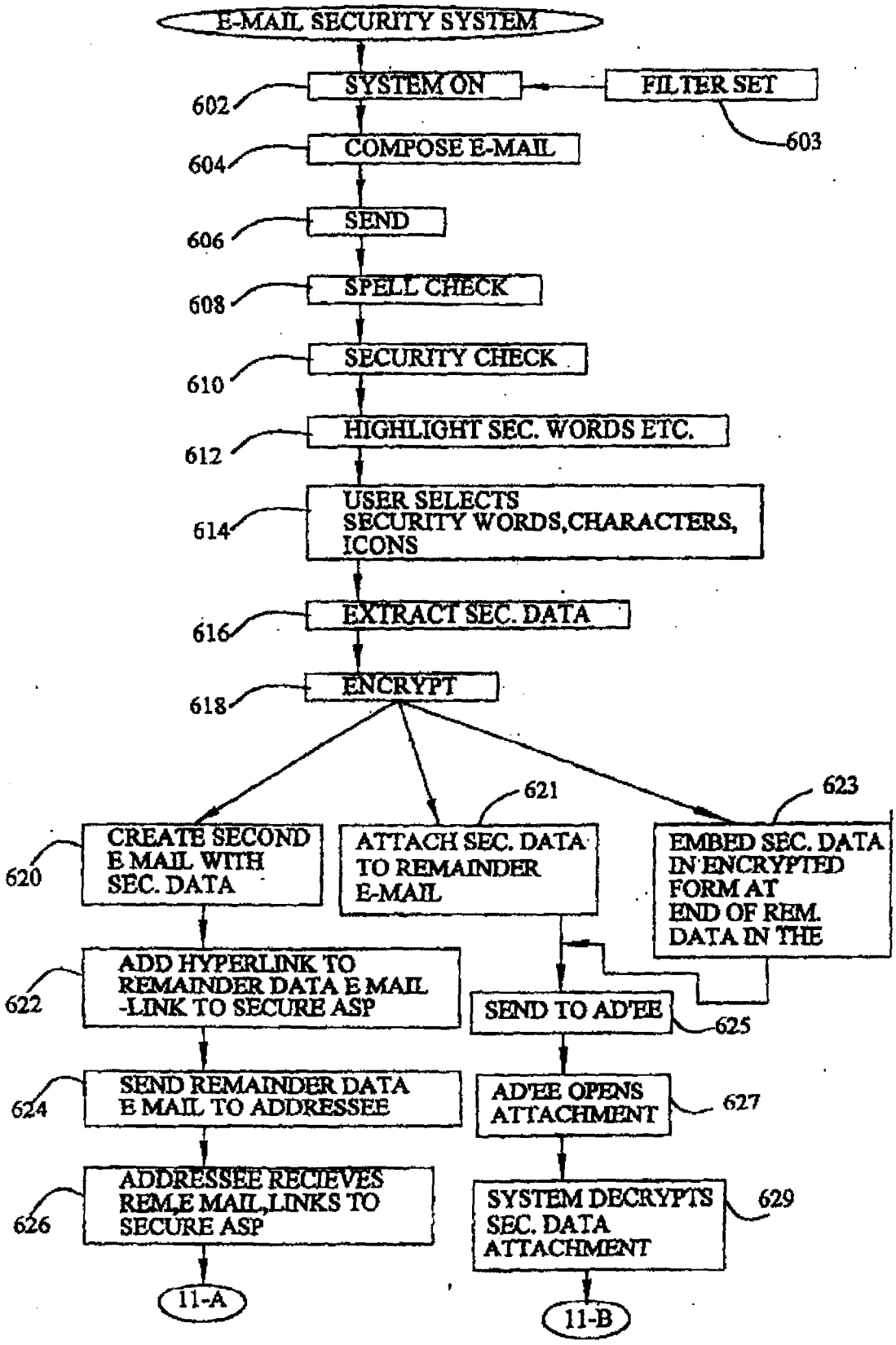

E-MAIL SECURITY SYSTEM
SYSTEM ON
FILTER SET
602
603
COMPOSE E-MAIL
604
SEND
606
SPELL CHECK
608
SECURITY CHECK
610
HIGHLIGHT SEC. WORDS ETC.
612
USER SELECTS SECURITY WORDS,CHARACTERS, ICONS
614
EXTRACT SEC. DATA
616
ENCRYPT
618
621
623
CREATE SECOND E MAIL WITH SEC. DATA
620
ATTACH SEC. DATA TO REMAINDER E-MAIL
EMBED SEC. DATA IN ENCRYPTED FORM AT END OF REM. DATA IN THE
ADD HYPERLINK TO REMAINDER DATA E MAIL -LINK TO SECURE ASP
622
SEND TO AD'EE
625
SEND REMAINDER DATA E MAIL TO ADDRESSEE
624
AD'EE OPENS ATTACHMENT
627
ADDRESSEE RECIEVES REM,E MAIL,LINKS TO SECURE ASP
626
SYSTEM DECRYPTS SEC. DATA ATTACHMENT
629
11-A
11-B

FIG.43

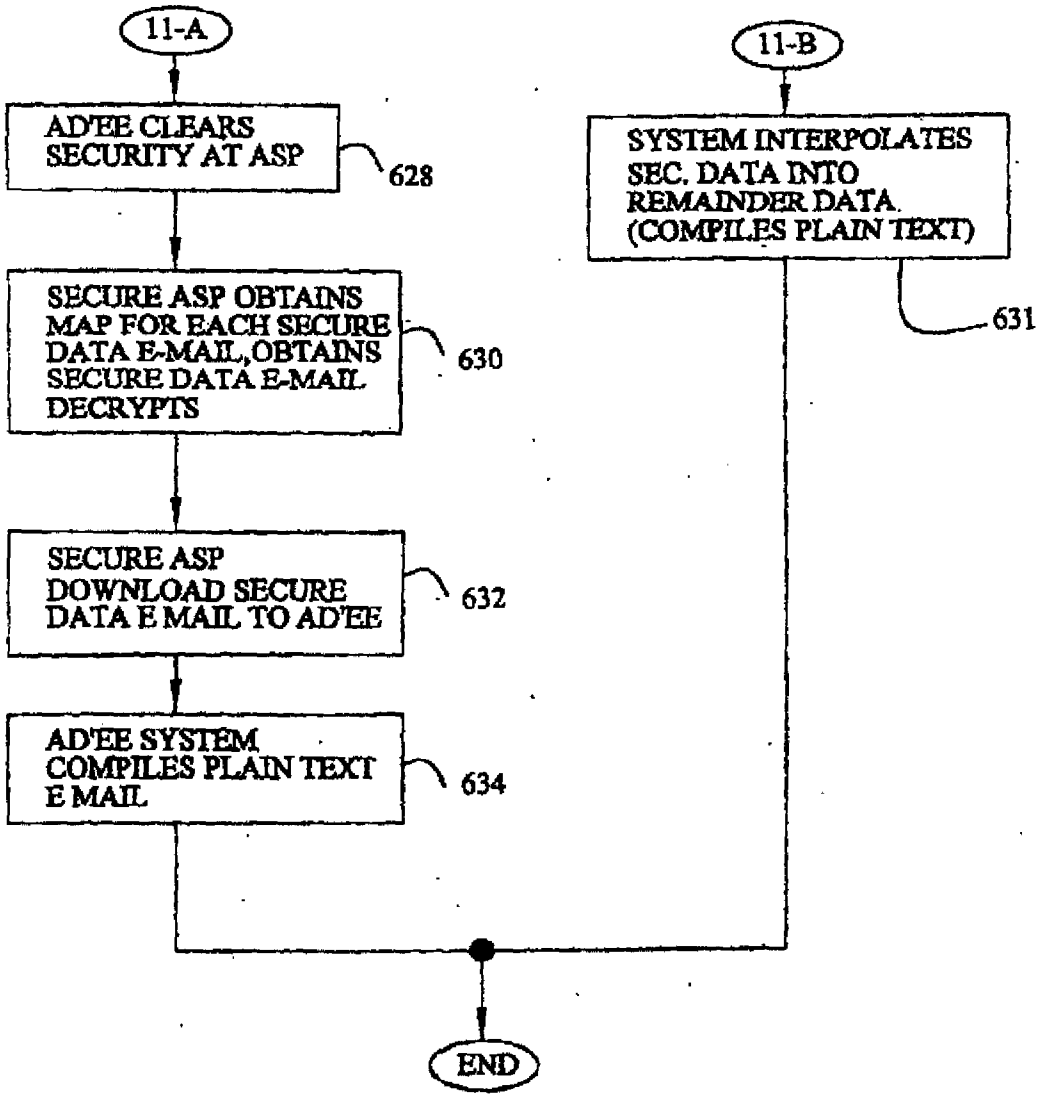

11-A
AD'EE CLEARS SECURITY AT ASP
628
SECURE ASP OBTAINS MAP FOR EACH SECURE DATA E-MAIL, OBTAINS SECURE DATA E-MAIL DECRYPTS
630
SECURE ASP DOWNLOAD SECURE DATA E MAIL TO AD'EE
632
AD'EE SYSTEM COMPILES PLAIN TEXT E MAIL
634
11-B
SYSTEM INTERPOLATES SEC. DATA INTO REMAINDER DATA. (COMPILES PLAIN TEXT)
631
END

FIG.44a

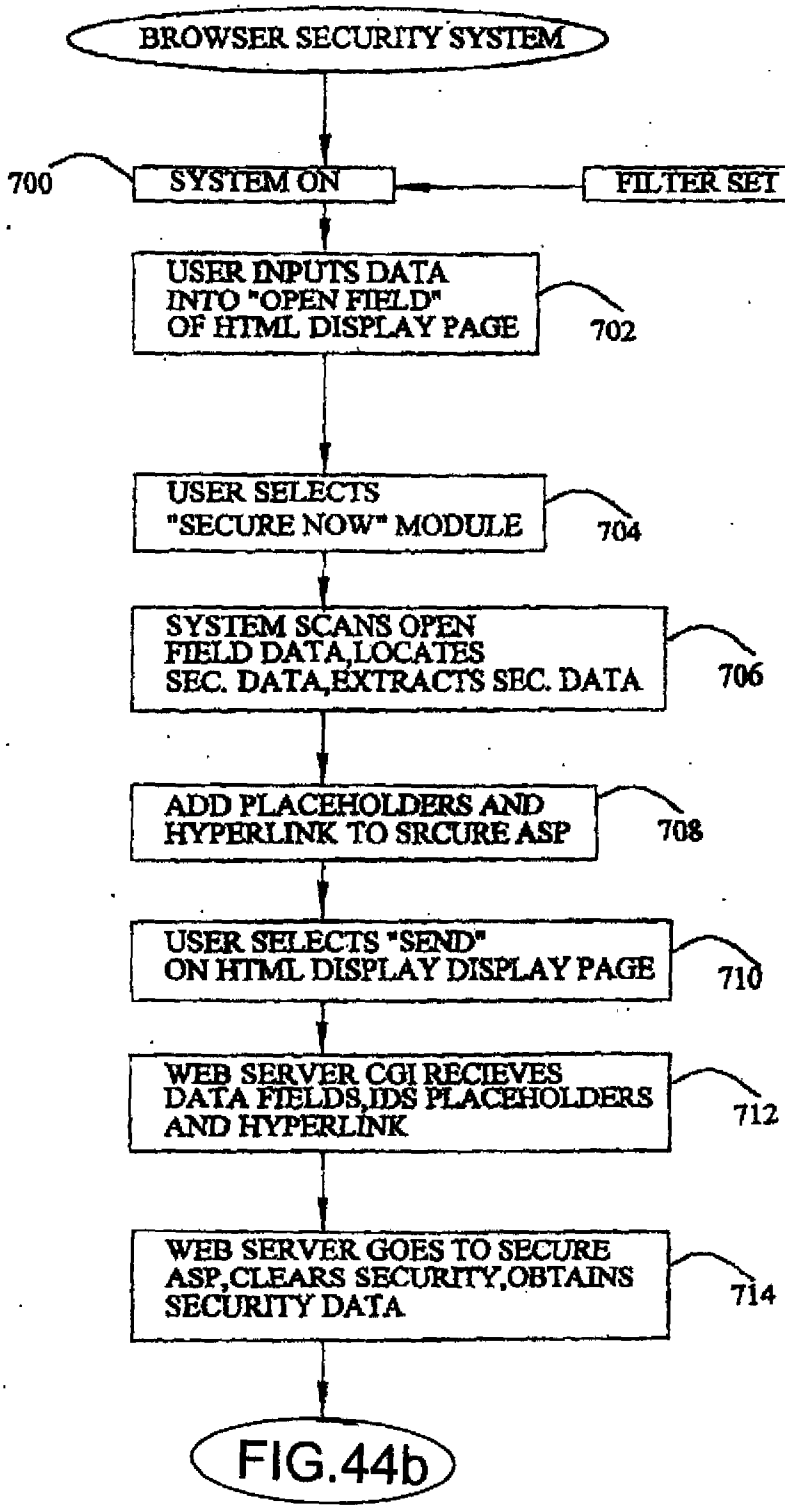


FIG.44b

FIG.44b

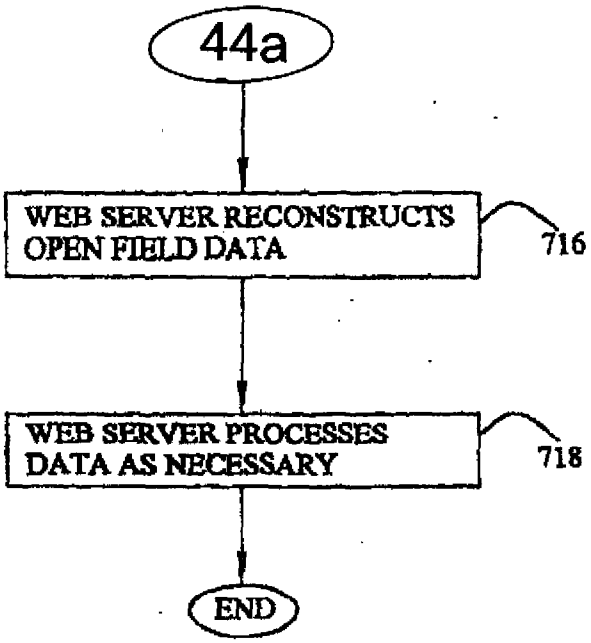
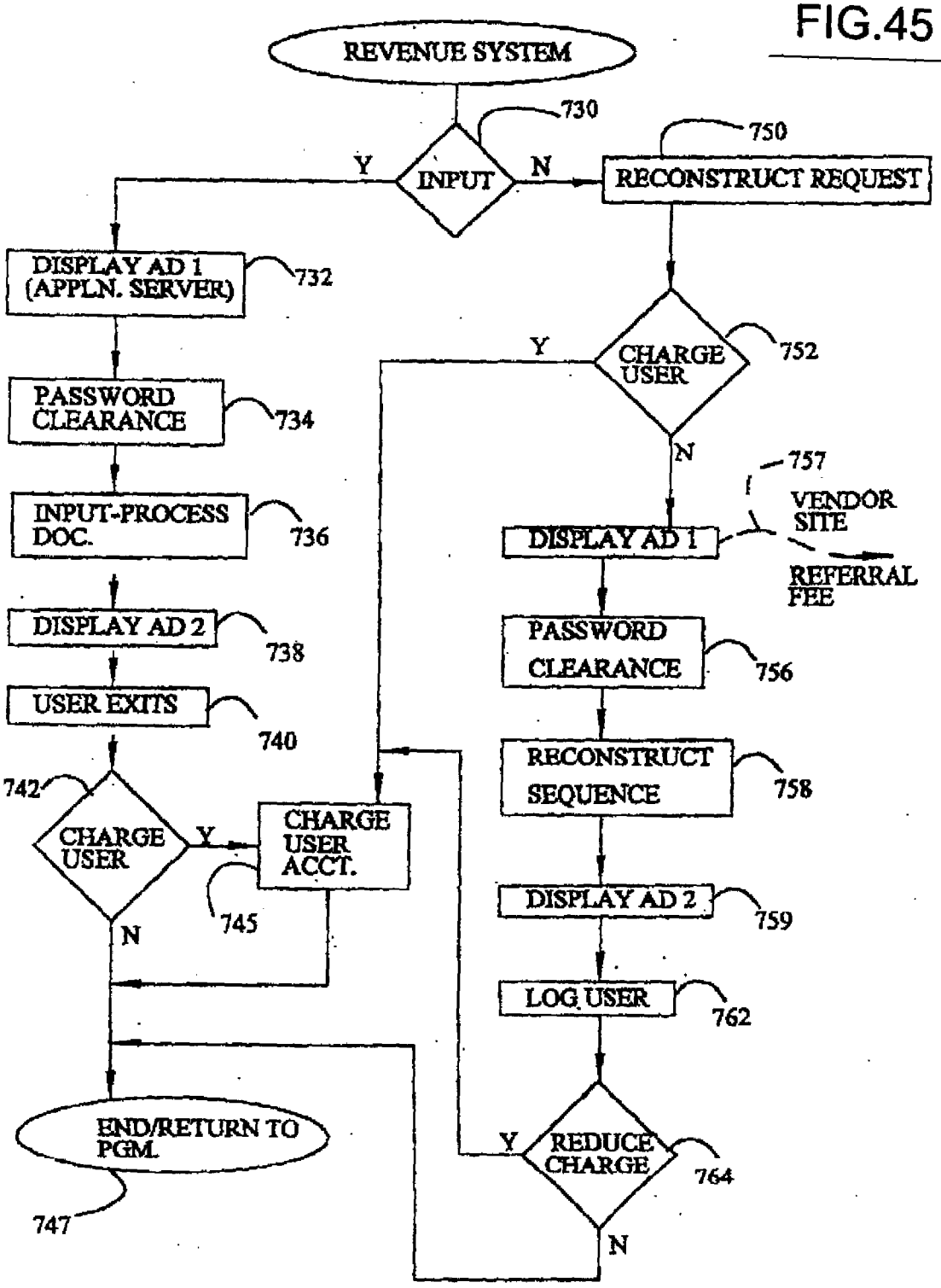

44a
WEB SERVER RECONSTRUCTS OPEN FIELD DATA
716
WEB SERVER PROCESSES DATA AS NECESSARY
718
END

FIG.45


REVENUE SYSTEM
730
INPUT
Y
N
750
RECONSTRUCT REQUEST
DISPLAY AD 1 (APPLN. SERVER)
732
PASSWORD CLEARANCE
734
INPUT-PROCESS DOC.
736
DISPLAY AD 2
738
USER EXITS
740
742
CHARGE USER
Y
CHARGE USER ACCT.
745
N
END/RETURN TO PGM.
747
CHARGE USER
752
Y
N
757
VENDOR SITE
DISPLAY AD 1
REFERRAL FEE
PASSWORD CLEARANCE
756
RECONSTRUCT SEQUENCE
758
DISPLAY AD 2
759
LOG USER
762
Y
REDUCE CHARGE
764
N

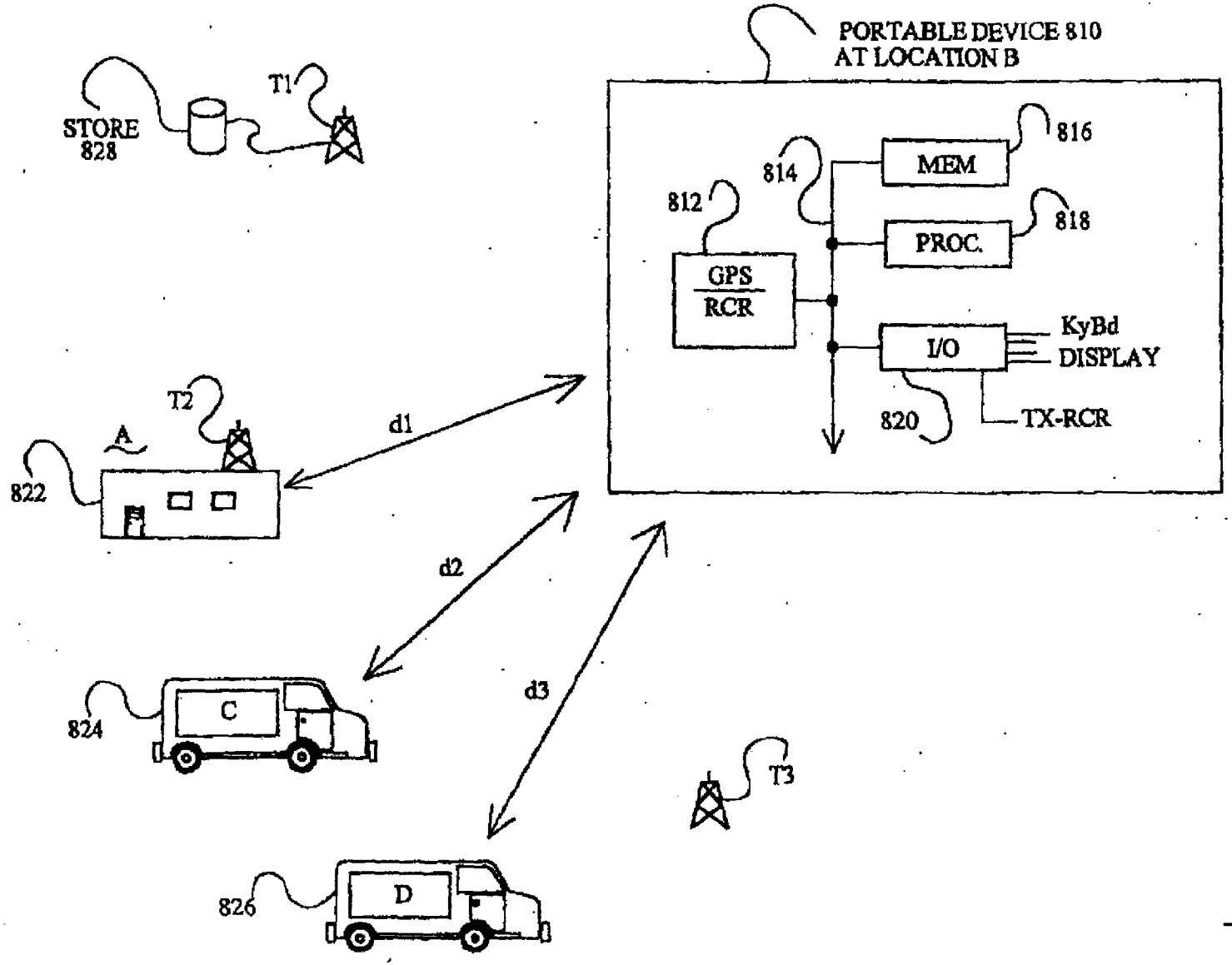

PORTABLE DEVICE 810
AT LOCATION B
816
MEM
814
812
818
PROC.
GPS
RCR
I/O
KyBd
DISPLAY
820
TX-RCR
T1
STORE
828
T2
A
822
d1
d2
d3
824
C
T3
826
D

FIG.46

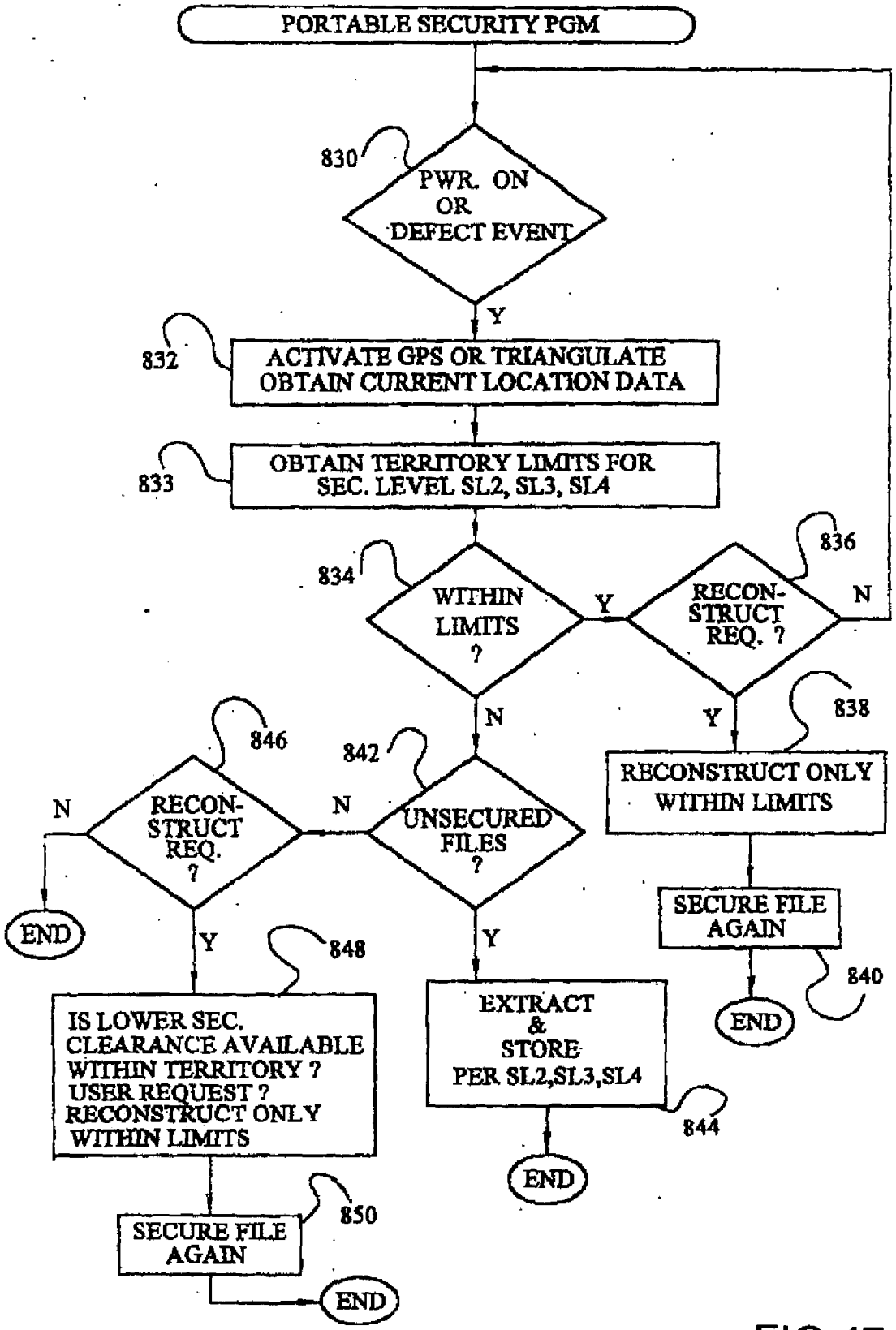

PORTABLE SECURITY PGM
830
PWR. ON OR DEFECT EVENT
Y
832
ACTIVATE GPS OR TRIANGULATE OBTAIN CURRENT LOCATION DATA
833
OBTAIN TERRITORY LIMITS FOR SEC. LEVEL SL2, SL3, SL4
834
WITHIN LIMITS ?
Y
836
RECON-STRUCT REQ. ?
N
N
Y
838
RECONSTRUCT ONLY WITHIN LIMITS
842
UNSECURED FILES ?
N
846
RECON-STRUCT REQ. ?
N
END
Y
848
IS LOWER SEC. CLEARANCE AVAILABLE WITHIN TERRITORY ? USER REQUEST ? RECONSTRUCT ONLY WITHIN LIMITS
SECURE FILE AGAIN
850
END
Y
EXTRACT & STORE PER SL2,SL3,SL4
844
END
SECURE FILE AGAIN
840
END

FIG.47

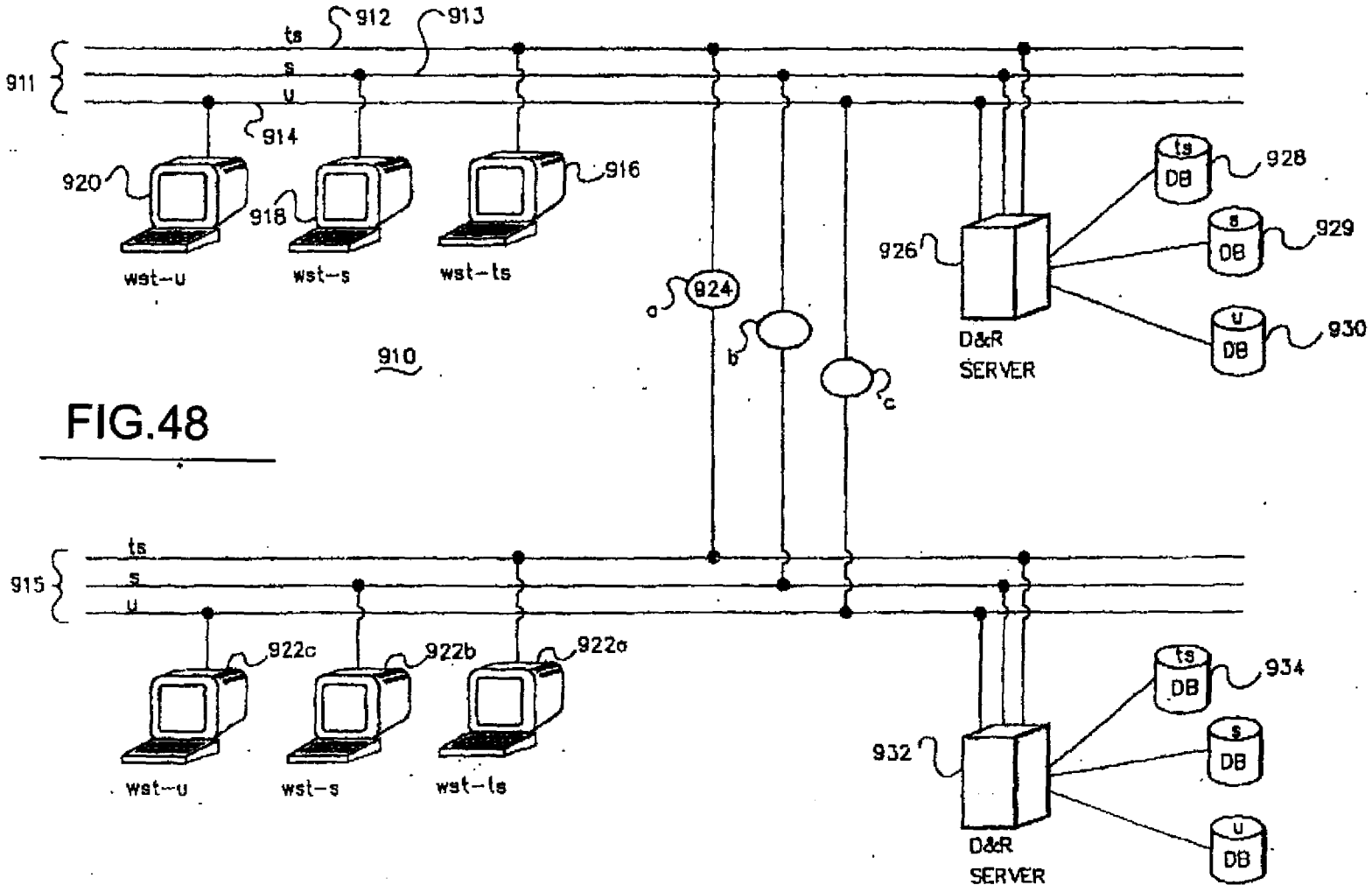

911
ts
s
u
912
913
914
920
918
916
wst-u
wst-s
wst-ts
910
924
a
b
c
926
D&R
SERVER
ts
DB
928
s
DB
929
u
DB
930
915
ts
s
u
922c
922b
922a
wst-u
wst-s
wst-ts
932
D&R
SERVER
ts
DB
934
s
DB
u
DB

FIG.48

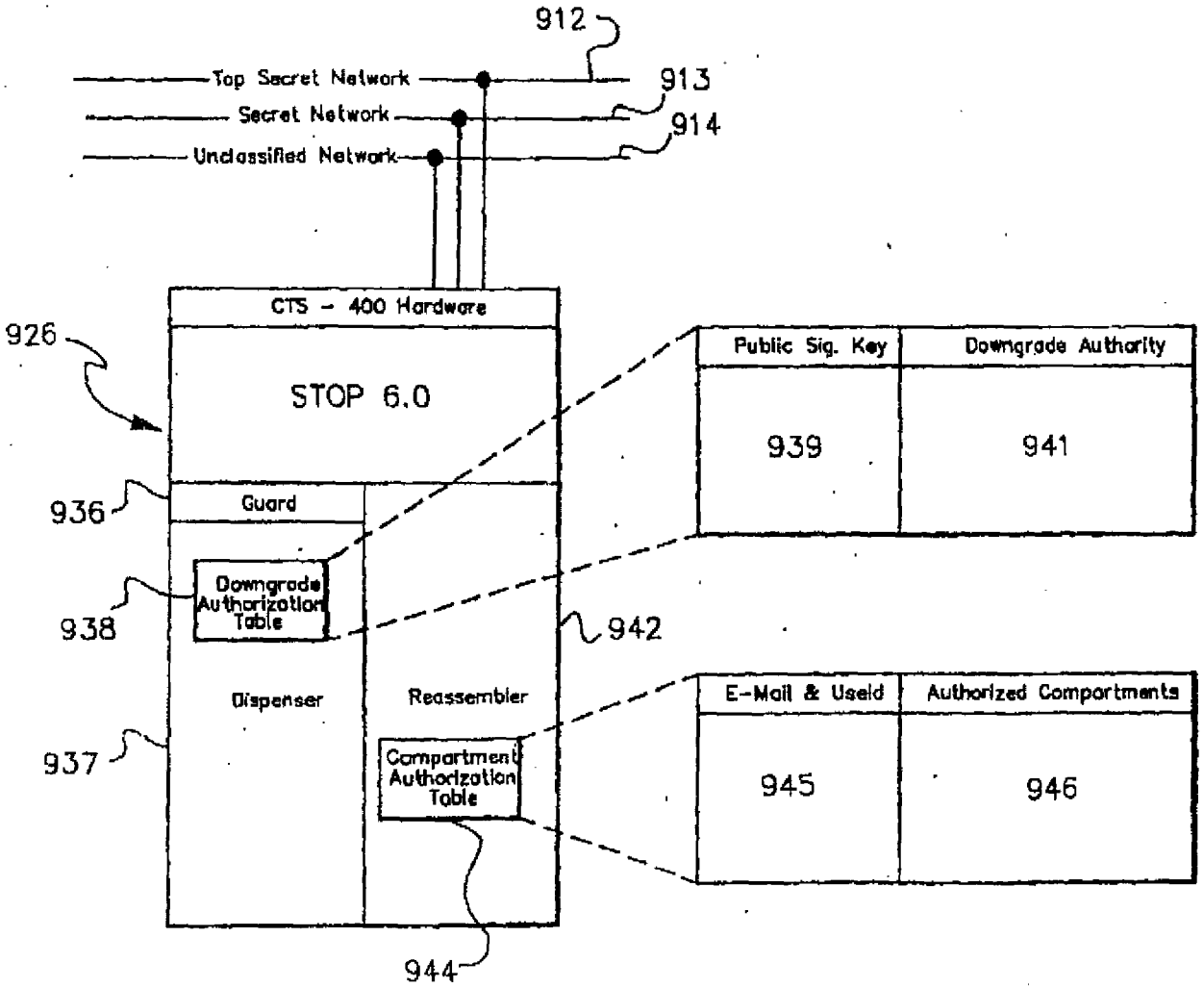

912
Top Secret Network
913
Secret Network
914
Unclassified Network
CTS - 400 Hardware
926
STOP 6.0
936
Guard
938
Downgrade Authorization Table
942
Dispenser
Reassembler
937
Compartment Authorization Table
944
Public Sig. Key
Downgrade Authority
939
941
E-Mail & Useid
Authorized Compartments
945
946

FIG.49

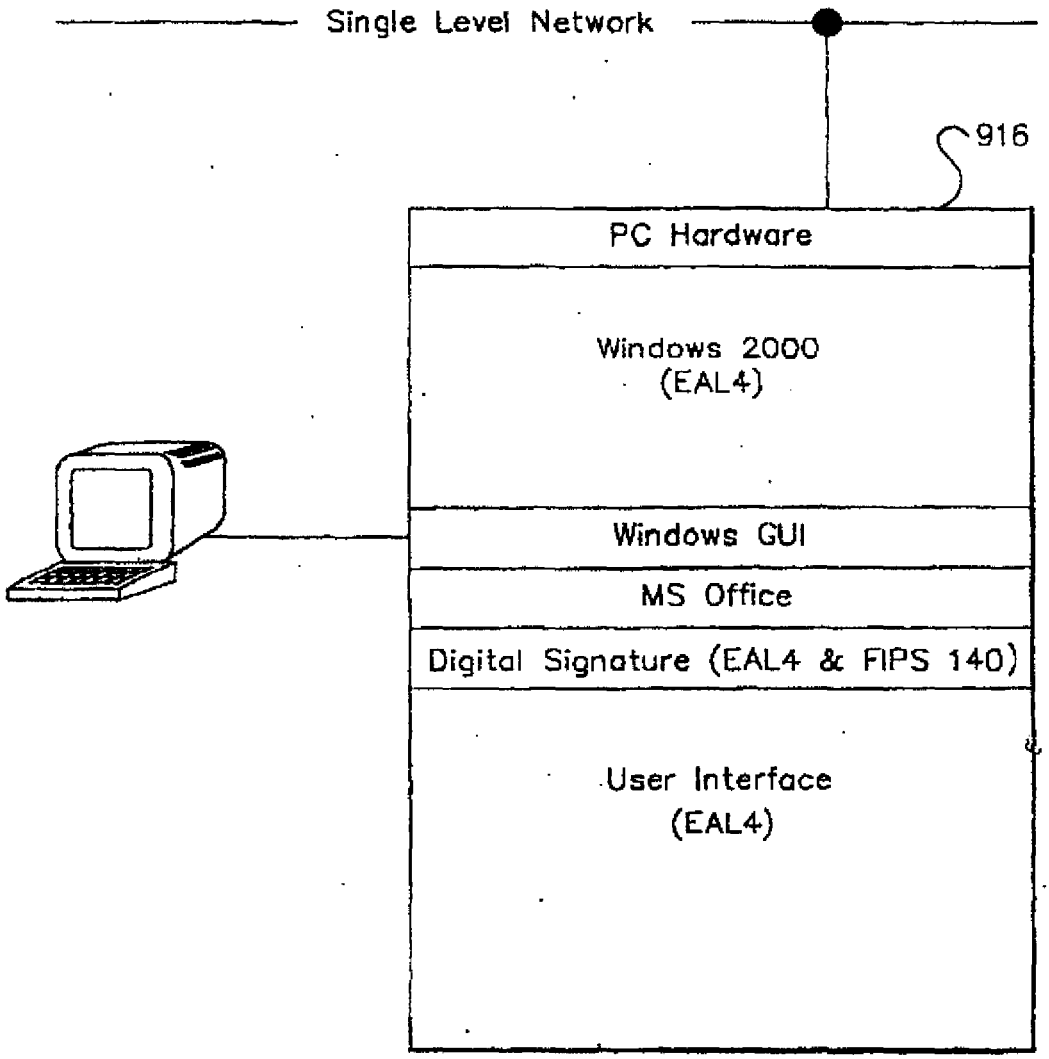

Single Level Network
916
PC Hardware
Windows 2000
(EAL4)
Windows GUI
MS Office
Digital Signature (EAL4 & FIPS 140)
User Interface
(EAL4)

FIG.50

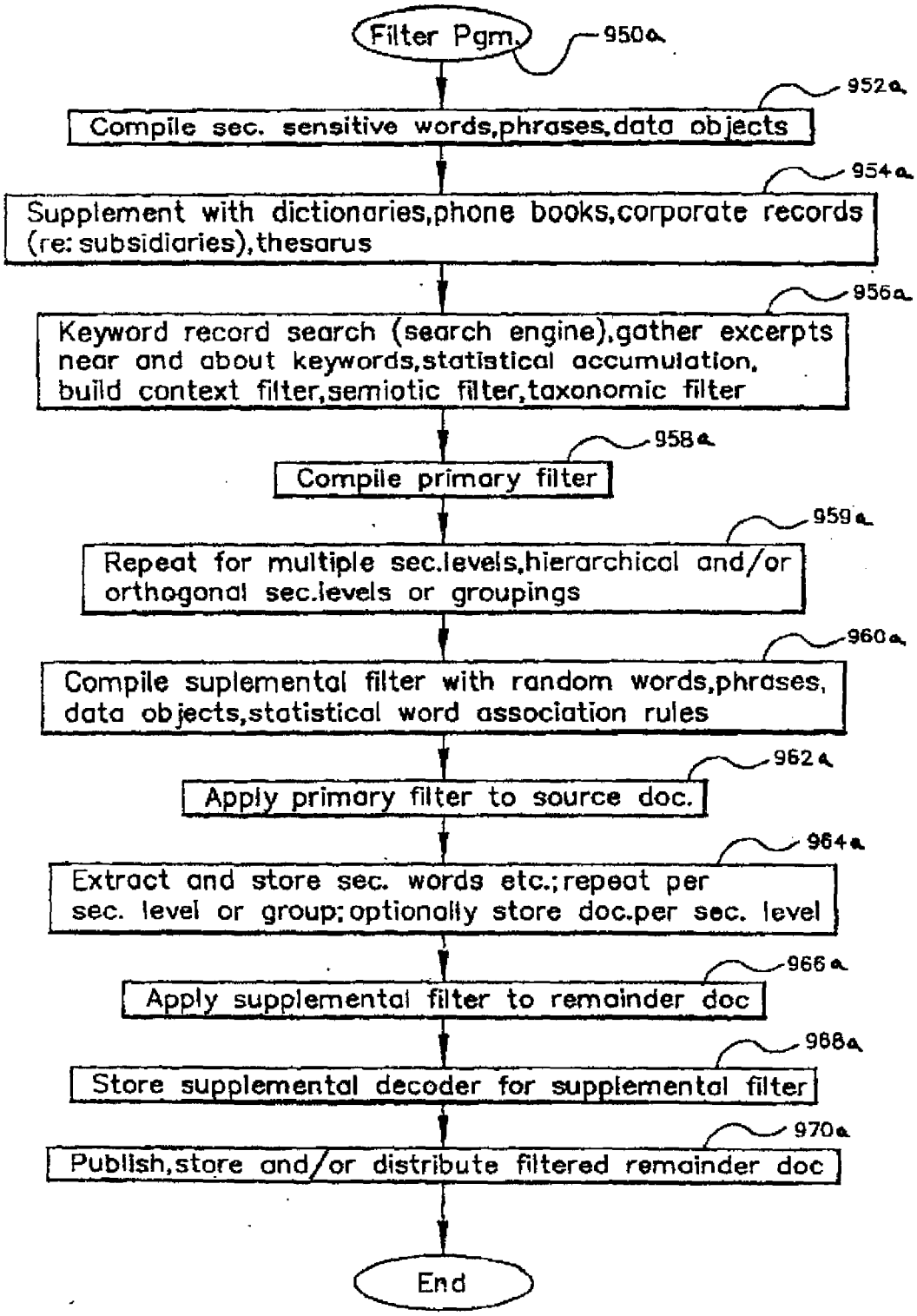

Filter Pgm.
950a
Compile sec. sensitive words,phrases,data objects
952a
Supplement with dictionaries,phone books,corporate records (re: subsidiaries),thesarus
954a
Keyword record search (search engine),gather excerpts near and about keywords,statistical accumulation, build context filter,semiotic filter,taxonomic filter
956a
Compile primary filter
958a
Repeat for multiple sec.levels,hierarchical and/or orthogonal sec.levels or groupings
959a
Compile suplemental filter with random words,phrases, data objects,statistical word association rules
960a
Apply primary filter to source doc.
962a
Extract and store sec. words etc.;repeat per sec. level or group;optionally store doc.per sec. level
964a
Apply supplemental filter to remainder doc
966a
Store supplemental decoder for supplemental filter
968a
Publish,store and/or distribute filtered remainder doc
970a
End

FIG.51

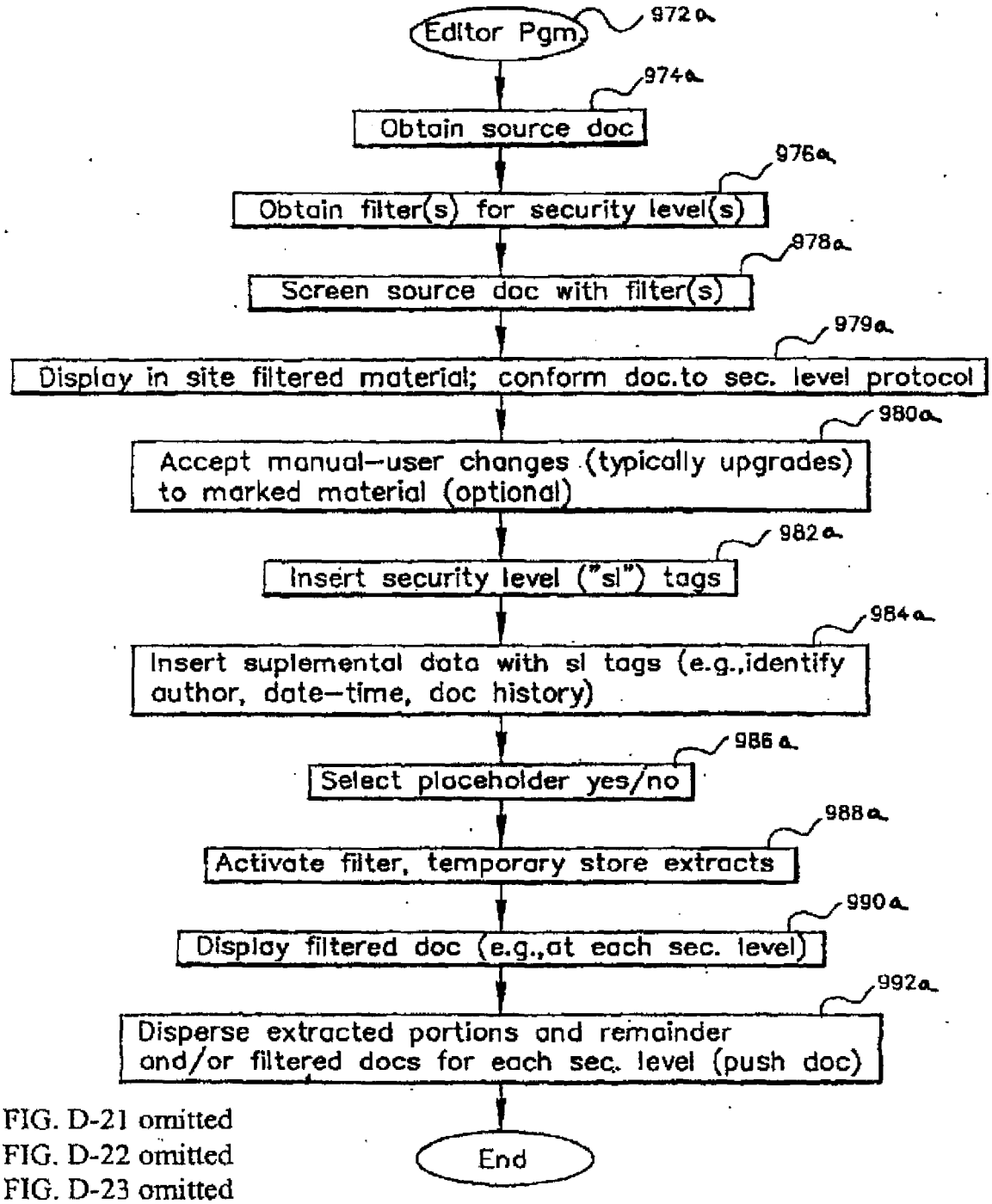


FIG. D-21 omitted
FIG. D-22 omitted
FIG. D-23 omitted

FIG.52

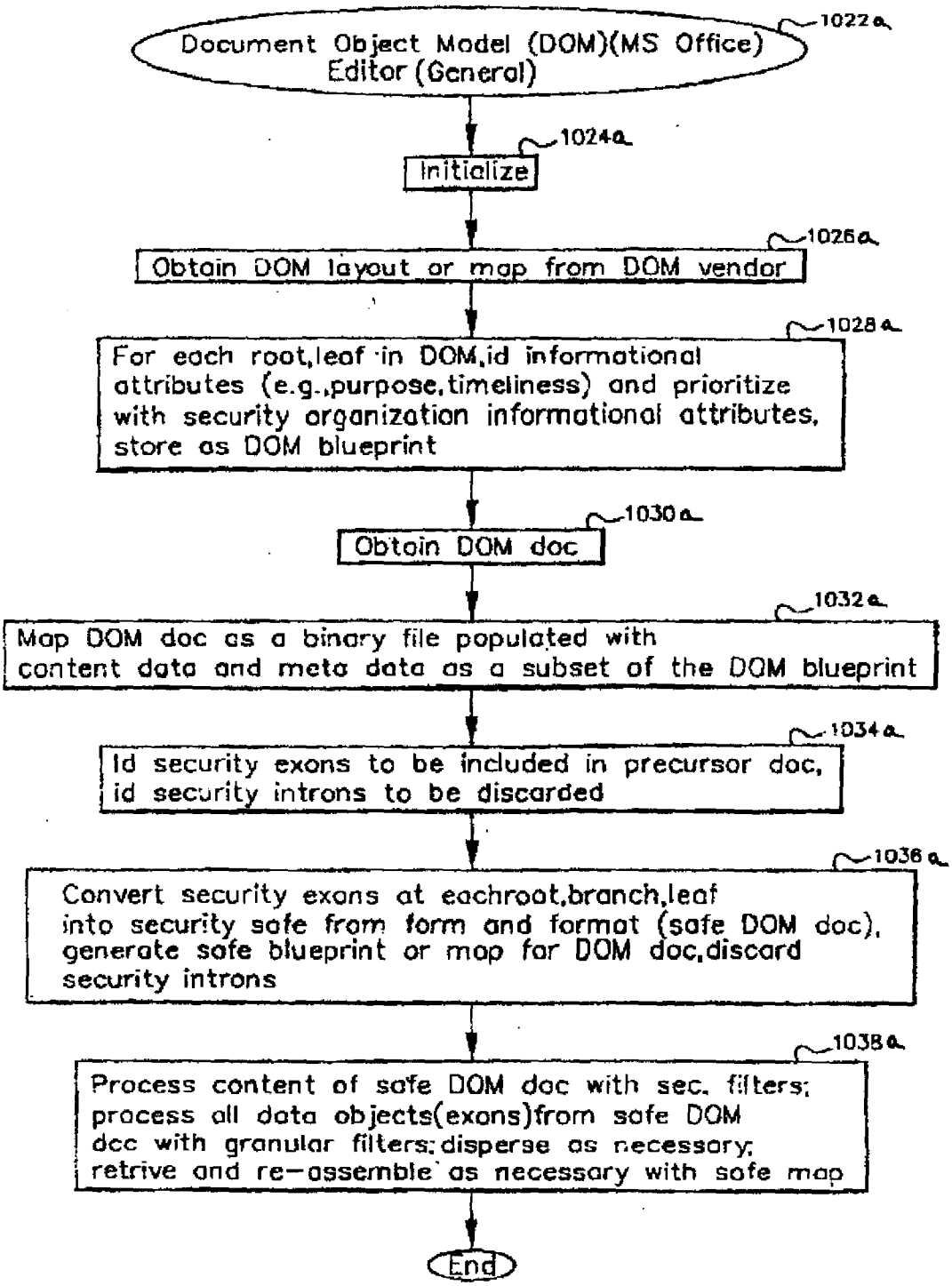
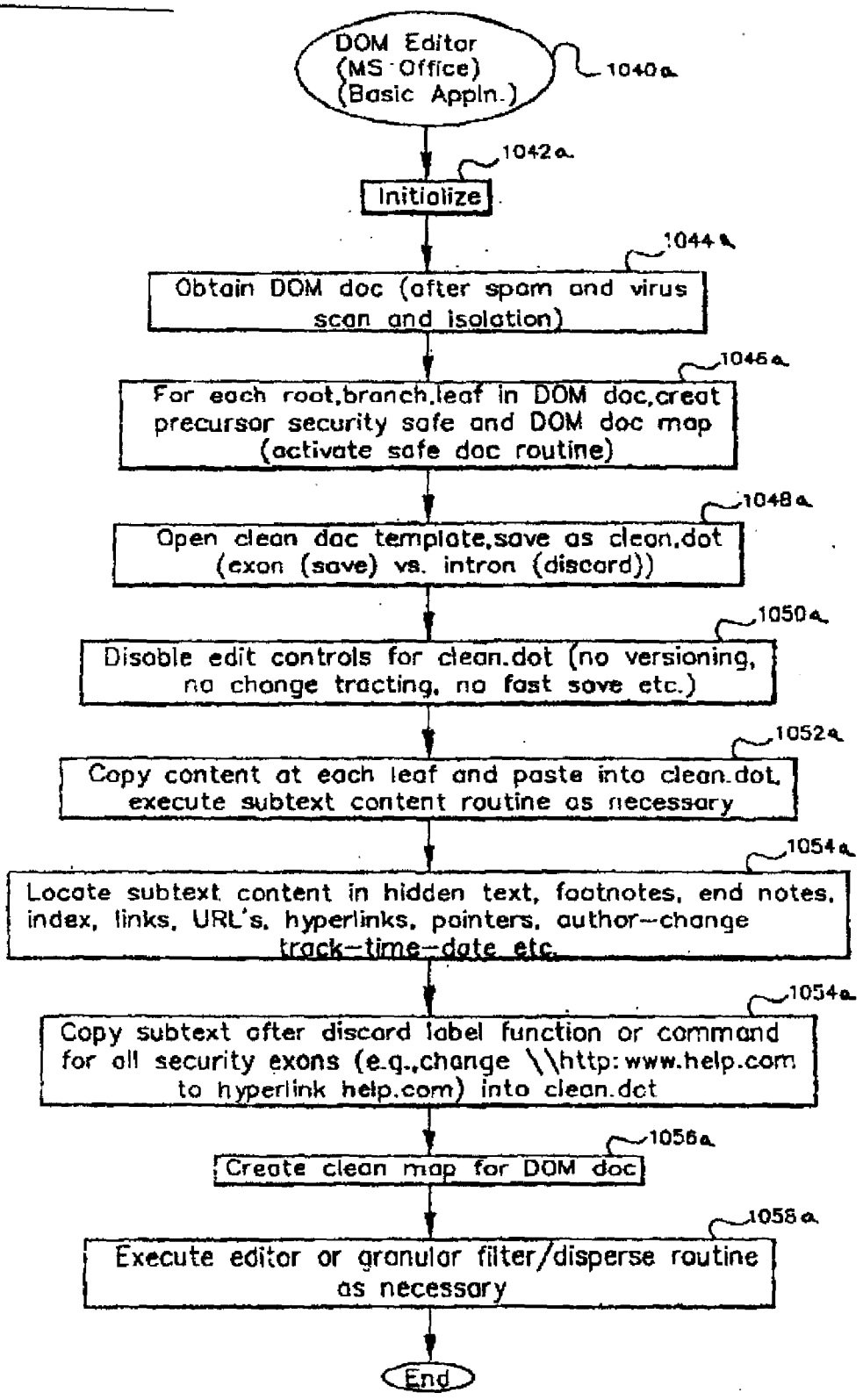

Document Object Model (DOM)(MS Office) Editor (General)
1022a
Initialize
1024a
Obtain DOM layout or map from DOM vendor
1026a
For each root,leaf in DOM,id informational attributes (e.g.,purpose,timeliness) and prioritize with security organization informational attributes, store as DOM blueprint
1028a
Obtain DOM doc
1030a
Map DOM doc as a binary file populated with content data and meta data as a subset of the DOM blueprint
1032a
Id security exons to be included in precursor doc, id security introns to be discarded
1034a
Convert security exons at eachroot,branch,leaf into security safe from form and format (safe DOM doc), generate safe blueprint or map for DOM doc,discard security introns
1036a
Process content of safe DOM doc with sec. filters; process all data objects(exons)from safe DOM doc with granular filters; disperse as necessary; retrive and re-assemble as necessary with safe map
1038a
End

FIG.53

FIG.54


DOM Editor
(MS Office)
(Basic Appln.)
1040a
1042a
Initialize
1044a
Obtain DOM doc (after spam and virus scan and isolation)
1046a
For each root,branch,leaf in DOM doc,creat precursor security safe and DOM doc map (activate safe doc routine)
1048a
Open clean doc template,save as clean.dot (exon (save) vs. intron (discard))
1050a
Disable edit controls for clean.dot (no versioning, no change tracting, no fast save etc.)
1052a
Copy content at each leaf and paste into clean.dot, execute subtext content routine as necessary
1054a
Locate subtext content in hidden text, footnotes, end notes, index, links, URL's, hyperlinks, pointers, author–change track–time–date etc.
1054a
Copy subtext after discard label function or command for all security exons (e.g.,change \\http:www.help.com to hyperlink help.com) into clean.dot
1056a
Create clean map for DOM doc
1058a
Execute editor or granular filter/disperse routine as necessary
End

Electronic Acknowledgement Receipt

EFS ID:	15646089
Application Number:	12453124
International Application Number:	
Confirmation Number:	8996
Title of Invention:	DIGITAL INFORMATION INFRASTRUCTURE AND METHOD FOR SECURITY DESIGNATED DATA AND WITH GRANULAR DATA STORES
First Named Inventor/Applicant Name:	Ron M. Redlich
Customer Number:	4897
Filer:	Robert C. Kain
Filer Authorized By:	
Attorney Docket Number:	6851-08-CIP
Receipt Date:	30-APR-2013
Filing Date:	29-APR-2009
Time Stamp:	10:36:37
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	Specification	6851-08-cip-Sub-Spec-Notice-File-Sub-Spec-20130430-a.pdf	26506 13386099b53c690d75cd196e334dc27be52f0d7c	no	1

Warnings:	
Information:	

2	Specification	6851-08-CIP-pa-sub-spec-b.pdf	3196442 12eee2d0593121c8b020c9e6b136f05a9379ba76	no	924
Warnings:					
Information:					
3	Specification	6851-08-cip-Sub-Spec-Notice-File-Marked-Spec-20130430-c.pdf	26402 ecc7cd6cd715c7941e48419cc26c719b610069c8	no	1
Warnings:					
Information:					
4	Specification	6851-08-CIP-pa-sub-spec-d.pdf	3196438 a55731851d06e0b62112213c1e40f9f1d8cc9226	no	924
Warnings:					
Information:					
5	Miscellaneous Incoming Letter	6851-08-cip-Sub-Spec-Notice-File-Marked-Dwgs-20130430-e.pdf	26637 2de14ae9dd47c912e25b336f4862a2a2020a7e11	no	1
Warnings:					
Information:					
6	Drawings-only black and white line drawings	6851-08-cip-Sub-Spec-Marked-Dwgs-20130430-f.pdf	812151 47d5db2898d8158aeb75fc4705fb265f03fb6602	no	59
Warnings:					
Information:					
7	Miscellaneous Incoming Letter	6851-08-cip-Sub-Spec-Notice-File-Corr-Dwgs-20130430-g.pdf	26606 4bbedb17fdbe710452c560fce23b547492fb1c9f	no	1
Warnings:					
Information:					
8	Drawings-only black and white line drawings	6851-08-cip-Sub-Spec-Corr-Dwgs-20130430-h.pdf	840275 c75b93384d6caa6276cbcd75b3a473e0db1eaa98	no	59
Warnings:					
Information:					
		Total Files Size (in bytes):	8151457		

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.

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

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

Serial No. 12/453,124

Examiner D. Lazaro

Confirmation No.: 8996 Group Art 2455

Filed: April 29, 2009

For: Digital Information Infrastructure and Method
for Security Designated Data and with Granular Data Stores (as amended)

NOTICE OF FILING SUBSTITUTE SPECIFICATION - CLEAN SPECIFICATION

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

Pursuant to 37 C.F.R. sec. 1.125, Applicant hereby submits a clean version of the substitute specification. A marked version of the specification is filed separately. No new matter is added to this specificaiton by the changes to the specification.

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

K:\RCK\CLIENTS\Redlich\Patents\6851-08-cip-Sub-Spec-Notice-File-Sub-Spec-20130430.wpd

Digital Information Infrastructure and Method for Security Designated Data and with Granular Data Stores

[0001] This is a continuation-in-part patent application based upon and claiming the benefit of Serial No. 11/746,440 filed May 9, 2007 which was regular patent application based upon provisional patent application serial no. 60/883,522 filed January 5, 2007, the contents of both applications are incorporated herein by reference thereto.

A.0 Introduction

[0002] The present invention relates to information management data processing modules and computer software system and method enabling protection of confidential information, identification of such information, identification of select content, classification for the same, and security system for the same. Businesses and enterprises use information in many different types of forms and format. Structured information is typically data found in database or spreadsheet formats or stored in self-defining formats wherein the information is managed by a software application. A further example of self-defining format is XML documents in format schematics. Some information is "semi-structured" wherein the information has certain defined fields such as email and the structured data fields from, to, cc, bcc and subject, but the body of the email message is unstructured. Unstructured information includes documents generated by end users with the assistance of applications program such as Microsoft OFFICE, word processing programs, image processing programs (ADOBE), files downloaded from the Internet, audio and video files etc. Enterprises focus their attention on mission critical applications and data relative thereto which is often located in structured databases or other structured data formats. However, a large majority of information is contained in unstructured or semi-structured formats. There are significant risks involved in handling and locating confidential information in these information files as well as identifying and handling intellectual property data in those files.

[0003] The content of these information files are important from a legal standpoint, a data security standpoint, and a government regulation or compliance standpoint. Although the content of the information files may be searched and indexed, the resulting information must then be classified. The enterprise must establish policies which dictate how the information files are handled in light of legal, security and compliance risk factors. Further, enterprise policies regarding information or document retention and immutability (the degree and extent that a particular document or information file may be changed) must be established and enforced.

[0004] Simply indexing the content of an information file is not adequate. Semantic analysis, key word tagging and classification categorization (taxonomic analysis) should be conducted. Information tools and computer programs and methods should enable the users (an enterprise) to analyze, categorize and actively manage unstructured information in the enterprise. Theft or accidental loss of customers' information or employees' private information is no longer acceptable. Laws mandate disclosure of such data loses. Further, the public is acutely aware of identity theft and privacy issues. Also, theft or misuse of intellectual property and other confidential business information is a mission critical aspect of many enterprises. To complicate matters, businesses and enterprises do not operate closed informational systems but often times invite partners, customers, vendors, contractors and other third parties to participate in the enterprise informational system. Therefore, most enterprises operate an open ecosystem informational structure. Employees of the enterprise in addition to its partners, customers, vendors and others participate in the production of information and the use/and consumption of information.

[0005] In the past, most commentators believed that a breach of confidentiality and misuse of data was a result of an outsider "hacker" getting access to enterprise information by penetrating a

firewall or other security system. However, there is a greater risk to the enterprise that rogue insider will take the information and misuse that information. Further, trusted employees constantly copy files onto laptops, PDAs (personal data assistance), USB thumb drives (flash memory), CDs and other removable media in order to fulfill the tasks assigned by the enterprise. This portable data can be easily misplaced or stolen. Further, the ease of electronic transfer of documents to others exposes the information contained therein to mis-directed addresses, as well as unauthorized theft and misuse.

[0006] Therefore, enterprises and organizations must manage the access to the information and use of the information and monitor such access and use and audit (log) these activities. A system of information rights management should concern the following aspects: (1) control who can open, print or edit a document or information file; (2) prevent or limit distribution of the information file; (3) enable the enterprise to change permissions on an information file per enterprise policy or changed conditions; and (4) maintain an audit trail of such activity.

[0007] The information infrastructure tools also must accommodate the changeable value of information over the life cycle of the information file. Although the information and content of the file does not change, the value of the information changes due to contextual events and external environmental conditions. External events which change the value of information and information file can be summarized as follows: (a) creation and modification and use of the information in the information file as it is processed by the enterprise; (b) completion of the project or event associated with the information file; (c) government regulations imposed on the information; (d) legal actions associated with the content of the information file and financial audits related to such information; (e) distributing the information in the information file to individuals with different access or security clearances or rights; (f) distribution of the information, both physically and electronically, to others who are not in the

enterprise; (g) the types and operation of storage devices and the media which retain the information files; (h) the discovery of new uses for the information content in the file; (i) new software applications which replace obsolete applications; (k) personnel changes within the enterprise and associated changes and permissions to access, control and modify the information file; (l) expansion and contraction of the enterprise itself (organizational changes) and the changeable nature of business relationships with partners, customers and suppliers.

[0008] In view of the foregoing, it is necessary to have an information classification system or engine which automatically categorizes information in unstructured information files and labels the same and permits the enterprise to establish a policy for that information and implement the policy recommendation with specific actions to ensure that the information is properly handled, distributed, retained, deleted (document retention) and otherwise managed.

Objects of the Invention

[0009] It is an object of the present invention to provide a system operator or CIO with data processing tools to manage and organize data processed by an enterprise.

[0010] It is a further object of the present invention to provide tools for securing secret or security sensitive sec-con data in the enterprise computer system and to locate, identify and secure select content SC which may be of interest or importance to the enterprise.

[0011] It is an additional object of the present invention to employ a dynamic, adaptive filter to enhance select content (SC) collection, to employ classification systems to organize such SC, and, in some cases, to do so continuously.

[0012] It is a further object of the present invention to assist in data processing or manipulation including processes such as coping, data extraction, data archiving, data distribution, data destruction

(a document retention process), inter-enterprise and intra-enterprise data distribution, data access request processing, and data distribution denials.

Summary

[0013] The present invention is a method of organizing and processing data in a distributed computing system. The invention is also implemented as a computer program on a computer medium and as a distributed computer system. Software modules can be configured as hardware. The method and system organizes select content which is important to an enterprise operating said distributed computing system. The select content is represented by one or more predetermined words, characters, images, data elements or data objects. The computing system has a plurality of select content data stores for respective ones of a plurality of enterprise designated categorical filters which include content-based filters, contextual filters and taxonomic classification filters, all operatively coupled over a communications network. A data input is processed through at least one activated categorical filter to obtain select content, and contextually associated select content and taxonomically associated select content as aggregated select content. The aggregated select content is stored in the corresponding select content data store. A data process from the group of data processes including a copy process, a data extract process, a data archive process, a data distribution process and a data destruction process is associated with the activated categorical filter and the method and system applies the associated data process to a further data input based upon a result of that further data being processed by the activated categorical filter utilizing the aggregated select content data. In effect, the system and process translates the sec-con or SC data and then stores the same in certain locations or secure stores. In this manner, a transformation of the data is achieved. By transposing the sec-con or SC data, higher levels of organization are realized or higher levels of security are implemented.

[0014] The enterprise designated filters screen data for enterprise policies such as a level of service policy, customer privacy policy, supplier privacy policy, enterprise human resource privacy policy, financial data handling policy, public company reporting policy, health care regulation policy, technical innovation policy, competitive reporting policy and document or data retention policy.

[0015] In another embodiment, the method and system extracts security sensitive content from a data input to obtain extracted security sensitive data for a corresponding security level and remainder data. This extracted security sensitive data is stored in a respective security sensitive extract store. Remainder data is stored in the distributed computer system. Distribution of the data input with respect to said distributed computing system is limited based upon throughput from at least one of the enterprise designated filters. The controlled release of corresponding extracted security sensitive data from the respective extract stores with the associated security clearances for corresponding security levels is permitted by the system. In this manner, security sensitive content is separately stored apart form the select content, which is stored in select content data stores.

Table of Contents

AAA.1.0.0 DigitalDoors Capabilities

AAA.1.1.0 Architecture Specifications

AAA.1.2.0 Scalability

AAA.1.3.0 Product and Process Overview

AAA.1.4.0 DigitalDoors implementation options:

AAA.1.5.0 The Key for Net-Centric security

AAA.1.6.0 Active defense and counterattacks versus common passive defense

AAA.1.7.0 Technical Basis for DigitalDoors Technology

AAA.1.8.0 Granular data control

AAA.1.9.0 Collaboration will consist of:

AAA.1.10.0 Granular tagging with metadata

AAA.1.11.0 Coalition And Multinational Cross Domain Collaboration

AAA.1.12.0 Incorporation into a trusted OS

AAA.1.13.0 Survivable infrastructure

AAA.1.14.0 Net Centric capabilities

AAA.1.15.0 DigitalDoors Services overview

AAA.1.16.0 DigitalDoors implementation options:

AAA.1.17.0 defenses against outs

AAA.1.18.0 collaboration elements:

AAA.1.19.0 DigitalDoors cornerstones

AAA.1.20.0 Granular content control

AAA.1.20.1 Cross domain

AAA.1.21.0 Security services

AAA.1.22.0 solutions to vulnerabilities

AAA.1.23.0 Replication for perpetual data availability

AAA.1.24.0 Solving net centric needs

AAA.1.25.0 Secured Discovery and publishing services

AAA.1.26.0 Publishing;

AAA.1.27.0 Meta data Posting

AAA.1.28.0 Secured Mediation services for information sharing

AAA.1.29.0 Other services

AAA.1.30.0 Secured perpetual storage services

AAA.1.30.1 Meta data posting

AAA.1.31.0 Secured enterprise management services

AAA.1.32.0 Access enforcement:

AAA.1.33.0 Real time granular audit of all critical content in network

AAA.1.34.0 Applications for operating an assured environment services-

AAA.1.35.0 Processing

AAA.1.36.0 Providing scalability, reliability, resilience, fault tolerance, speed

AAA.1.37.0 Enabling generic and standardized data distribution services

AAA.1.38.0 Storage

AAA.1.39.0 Metrics

AAA.1.40.0 Technical specifications, operating parameters, and network design specifications

AAA.1.41.0 DigitalDoors Operating Parameters:

AAA.1.42.0 DigitalDoors Network Design Specifications:

AA.1.0.0 Background: Formlessness for Security

AA.1.1.0 Introduction

AA.1.2.0 Definition

AA.1.3.0 Formlessness

AA.1.3.1 How DigitalDoors Applies Formlessness

AA.1.4.0 Formlessness as Security for Maps.

AA.1.4.1 History and Concept

AA.1.5.0 Security through: dispersion, formlessness, reversible chaos

AA.1.6.0 Formlessness to secure maps

AA.1.7.0 Formlessness by breaking context - hiding is not enough

AA.1.8.0 Differentiation between Obscurity and Formlessness

AA.1.8.1 Obscurity

AA.1.8.2 Formlessness without context

AA.1.8.3 Proverbial versus Actual Context Change

AA.1.8.4 Obscurity and Formless Differentiation

AA.1.8.5 Recovering from Obscurity and Formlessness

AA.1.8.6 Formlessness through Microperimeterization

AA.1.8.7 Formlessness the difference between Dispersion and Hiding

AA.1.1.8 Dispersion as Asymmetric warfare

AA.1.9.0 Overview of Formlessness:

AA.1.9.1 The DigitalDoors Formlessness Doctrine

AA.1.9.2 Establishing Formlessness:

AA.1.9.3 Defending intellectual property and trade secrets:

AA.1.9.4 Defending information in web sites:

AA.1.9.5 Legal defenses with formlessness:

AA.1.9.6 Measurement of the information inventory for risk:

AA.1.9.7 Monetizing the information inventory:

AA.1.9.8 The Global Information war

AA.1.10.0There is a need for a technological paradigm change.

AA.1.11.0 DigitalDoors Hierarchical Security Sanitization and Reconstitution

AA.1.12.0 Methodology Overview:

AA.1.13.0 A new IT paradigm

AA.1.14.0 Taking advantage of a major economic imbalance

AA.1.15.0 Monetizing the organization's information assets:

AA.1.16.0 Information disassembly and Reassembly

AA.1.16.1 Disassemblying Information

AA.1.16.2 The reasons for disassembly

AA.1.16.3 Finding Value within Information

AA1.16.4 TheDoctrine behind DigitalDoors

AA.1.16.5 Reconstituting Information

AA.1.16.6 Directory Files

AA.1.16.7 A compound data stream that can be stripped into granular items

AA.1.16.8. Data Unification

AA.1.16.9 Conclusion

AA.1.17.0 A New Information Security Paradigm: Neutralize the Loss of Perimeter

AA.1.18.0 Why security is ignored

AA.1.19.0 Security integration and the lack of attention to it

AA.1.20.0 Security as the future foundation for information

AA.2.0.0Design and implementation

AA.2.1.0 Implementation of Granular data control in data streams

AA.2.2.0 Brief Functional Overview

AA.2.2.1 Brief Structural Overview

AA.2.2.2 Remote Storage Overview

AA.2.2.3 Operating Parameters

AA.2.2.4 Network Design Specifications

AA.2.2.5 Operating Parameters

AA.2.2.6 Network Design Specifications

AA.2.2.7 Remote Storage Infrastructure

AA.2.2.8 Brief Structural Overview

AA.2.2.9 Remote Storage Overview

AA.2.3.0 Upfront Processing

AA.2.4.0 Proxy architecture

AA.2.5.0 Reclassification- Reconstitution

AA.2.5.1 ReClassification

AA.2.5.2 Recovery Information

AA.2.5.3 Processing with DeClassified Data

AA.2.5.4 Content Filtering

AA.2.5.5 Channel Transmission Protection

AA.2.6.0 The Recovery map

AA.2.6.1 Map Structure Variants and Granularity

AA.2.7.0 Concurrency in granular data control

AA.2.8.0 DeClassifying and ReClassifying E-Mail

AA.2.8.1 Generation and Distribution

AA.2.8.2 Receiving and ReClassification

AA.2.8.3 Forwarding and Redelivery of E-Mail

AA.2.8.4 Content Filtering

AA.2.8.5 Processing E-Mail

AA.2.9.0 Declassifying and ReClassifying while Browsing the web

AA.2.9.1Generation and Distribution:

AA.2.9.2 Receiving and ReClassification

AA.2.10.0 Creating multiple levels of categorization

AA.2.11.0 Out-of-Channel Multitier Tagging

AA.2.12.0 Multitier Hierarchical Overlapping Tag Structure

AA.2.13.0 Dictionary Encoding AA.2.14.0 Declassification and scrubbing of maps

AA.2.14.1 Channel Transmission Protection:

AA.2.15.0 Distribution of MS word

AA.2.16.0 Filters, sieves and capabilities

AA.2.16.1 The DigitalDoors classification metadata can be transitory.

AA.2.16.2 Applicability of Sieves and Filters

AA.2.16.3 Manual, Assisted, an Automated Modes

AA.2.16.4 Dictionaries

AA.2.16.5 My Word List

AA.2.16.6 My Group List

AA.2.16.7 My Category List

AA.2.16.8 My Policy List

AA.2.16.9 AutoSEC

AA.2.16.10 OPSEC

AA.2.16.11 COMSEC

AA.2.16.12 Manual Selection

AA.2.16.13 Manual Mouseover Selection

AA.2.16.14 Tearline Creation

AA.2.16.15 Other configurations

AA.2.16.16 Accuracy and Granularity

AA.2.17.0 Automating filters and sieves

AA.2.17.1 Classification Conflict Resolution

AA.2.18.0 Processing sets

AA.2.18.1Collections

AA.2.18.2 Sets

AA.2.19.0 Failure of best of breed security

AA.2.20.0 Integrated Single Files, Attachments, and Links

AA.2.20.1 Stream Outputs

AA.2.21.0 Hierarchical Security Sanitization and Reconstitution

AA.2.22.0 Software implementation

AA.2.23.0 Software operations: Sensitivity Level Hierarchy and tear line

AA.2.23.1 Secure Editor application

AA.2.23.2 DeClassifying and ReClassifying while Browsing the web

AA.2.23.3 Generation and Distribution:

AA.2.23.4 Receiving and ReClassification

AA.2.24.0 DeClassification Mapping - Channels mapping

AA.2.24.1 Channel Transmission Protection:

AA.2.25.0 Security by dispersion – the cloud

AA.2.26.0 Semantics dictionaries AA.3.0.0 Privacy and security:

AA.3.1.0 Context: The difference between Security and Privacy

AA.3.2.0 Security and privacy: protecting the crown jewels

AA.3.3.0 Surrogate Keywords as unique identifiers for privacy and security

AA.3.4.0 The Metrics of Privacy: Identification, De-Identification, and Permitted versus Forced Re-Identification

AA.3.4.1 Privacy overview

AA.3.4.2 Data Ownership

AA.3.3.3 Definition of Identity

AA.3.4.4 Uniqueness

AA.3.4.5 Sufficiency

AA.3.4.6 Direct and Indirect Identification

AA.3.4.7 Unique Identification and Subset Identification

AA.3.4.8 Indirect Identity Information Sources

AA.3.4.9 Definition of Privacy

AA.3.4.10 Implementing Privacy Policy

AA.3.4.11 Privacy Measurements

AA.3.4.12.Measuring Privacy

AA.3.4.13 Measuring Uniqueness of Identification

AA.3.4.14 Density of Identification

AA.3.4.15 Inference

AA.3.4.16 Conclusion

AA.3.5.0 Personally identifiable information: Meta PII

AA.3.6.0 Categories of Personally Identifiable Information (PII)

AA.3.6.1 Technical Identifiers

AA.3.7.0 Toxic spill of personally identifiable information (PII)

AA.3.8.0 From aggregation, inference, reidentification to Anonymity

AA.39.0 Control personally identifiable information (PII) through granular data control

AA.4.0.0 Classification and categorization:

AA.4.1.0 Multiple Hierarchical Tagging and Data Extraction

AA 4.2.0 Commonality of Data: categorization, a multitier hierarchical overlapping tag Structure

AA.4.3.0 Categorization structure tagging, risk measurement and context

AA.4.4.0 Data and Metadata Granularity for decomposition to break context

AA.4.5.0 In-Channel and Out-of-Channel Tags

AA.4.6.0 Capitalization is content-, context-, and concept-driven

AA.4.6.1 Categorization Specialization

AA.4.6.2 Semantic Parsing Rules

AA.4.6.3 Process

AA.4.6.4 Conclusion

AA.4.7.0 Data classification – the leakage threat

AA.4.8.0 Semantics dictionaries

AA.4.9.0 Difference between Content, Context, and Concept

AA.4.10.0 Classification as Proxy for Scarcity

AA.4.11.0Threats of Meta Data

AA.4.12.0 Degrees of data structure

AA.5.0.0 Defining Information

AA.5.1.0 The meaning of information and related context risk

AA.5.2.0 Content Concept and Context - Correcting the Security Gap for Data Object Models

AA.5.3.0 The Structure of Information

AA.5.3.1 Information Structure

AA.5.3.2 DNA versus RNA

AA.5.3.3 Granular Content

AA.5.4.0 Implementing of MS Office

AA.5.4.1 Microsoft Office Suite and Applications

AA.5.4.2 Repress Thoughts of Banishing MS Office

AA.5.4.3 Office Versions, Releases, and the Data Object Models

AA.5.4.4 Content Security

AA.5. 4.5 Implementing Document Protection

AA.5.4.6 Conclusion

AA.5.5.0 The contextual information matrix

AA.5.6.0 Future direction for information awareness

AA.5.7.0 Unstructured data

AA.5.8.0 Information measurement and management

AA.5.9.0 MS Office Document Structure: Protection and Processing

AA.5.9.1 The MS Office Object Model

AA.5.10.0 The criticality of right context

AA.6.0.0 Search and data mining

AA.6.1.0 Meta Data Hound search - Adjacency with Permutations and Combinations

AA.6.2.0 Search Convergence and Search Divergence

AA.6.3.0 Convergent search

AA.6.3.1 Divergent Search Paradigm

AA.6.4.0 Data mining and inference attacks

AA.6.5.0 Metaseaerch data mining

AA.6.5.1 Description of the DigitalDoors Metasearch Process

AA.6.5.2 Combinations and Permutations

AA.6.5.3 Automated Contextual Pruning

AA.6.6.0 Knowledge Discovery: Search Convergence and Divergence

AA.6.6.1 Initial Process

AA.6.6.2 DigitalDoors MetaSearch

AA.6.6.3 MLS-Compliant Search and Distributions

AA.7.0.0 Security:

AA.7.1.0 Security Keystone overview

AA.7.1.1 Security

AA.7.2.0 Malware attack the tentacles of Insecurity

AA.7.3.0 Security is broken

AA.7.4.0 Meta data dangerous double hedge sword

AA.7.5.0 The transition content security via Data Leakage Prevention

AA.7.6.0 The failure of best breed security

AA.7.7.0 Why Security of information

AA.7.8.0 Security as an open set

AA.7.9.0 Dangers in information interactions, the need for granular content isolation

AA.7.10.0 Prevention of leakage through context and range control

AA.7.11.0The vulnerability of perimeter security and the need for granular data control

AA.7.12.0 Leakage from Data combination

AA.7.13.0 The Risks from XML

AA.7.14.0 The risks of new information infrastructures

AA.7.15.0 Granular content dispersion as security

AA.7.16.0 Security by the One-Time Pad

AA.7.16.1 Perfect Secrecy

AA.7.17.0 Risk in repurposing of information

AA.7.18.0 The ineffectiveness of Perimeter security

AA.7.19.0 Deficiencies in perimeter security and encryption

AA.7.20.0 The breakdown of perimeter security and the need for Dispersion

AA.7.21.0 Asymmetric Security

AA.7.22.0 Dispersal security versus perimeter security

AA.7.23.0 Metadata risks, the need for a lockdown

AA.7.24.0 Competitive Analysis of Security Methods

AA.7.24.1 security Technology

AA.7.24.2 Encryption and Security History

AA.7.24.3 Cipher Science

AA.7.24.4 integrating disciplines

AA.7.24.5.Unique Architecture

AA.7.24.6 DigitalDoors versus Other Technologies

AA.7.25.0 Security by dispersion to the cloud

AA.7.26.0 Defenses in Depth: layered security

AA.7.26.1 Why layered security works

AA.2.27.0 Perimeter security, the failure of the Sandbox

AA.2.28.0 The critical danger of Commercial off the shelf software

AA.2.29.0 COTS Implementation

AA.7.29.1 Unfolding Catastrophe

AA.7.30.0 DigitalDoors Access and Rights

AA.7.30.1 Authorization

AA.7.30.2 Authentication Database

AA.7.30.3 Registration/ Rights database

AA.7.30.4 Location Map Database(s)

AA.7.30.5 Architecture Overview

AA.7.30.6 Primary Benefits

AA.7.31.0 Securing the Internet

AA.7.32.0 Spread of viruses within meta data

AA.7.33.0 Touchpoints and gateways as back doors

AA.8.1.0 Multi level Security Information Sharing:

AA.8.1.1 Information sharing overview

AA.8.2.0 Multi Level Security: new concepts for information sharing

AA.8.3.0 Information sharing through granular content control

AA.8.3.1 Gaps in Controls

AA.8.3.2 Risks from Distributed Stovepipes and Silos

AA.8.4.0 The Failure of Tag Reflexivity for Information Sharing

AA.8.4.1 Tag Reflexivity

AA.8.5.0 Multi Level Security needs to adopt granular data control to achieve its objective

AA.8.6.0 Accommodating the Bell LaPadula model

AA.8.6.1.0 Maps and Recovery Information

AA.8.7.0 Challenges of Multi level security information sharing

AA.8.8.0 Implementing Cross-Domain MLS Information Flow

AA.8.9.0 Multi level Security for the Internet

AA .8.9.1 Cultural and Technical Constraints

AA.8.10.0 A Paradigm Shift

AA.8.11.0 Implementing Cross-Domain Information Flow - Multi level security

AA.8.12.0 Negotiated multi level information sharing

AA.8.13.0 Security through information Distribution

AA.8.14.0 Implementation of information sharing with Rigorous Protections

AA.8.14.1 General Concept

AA.8.14.2 Implementation map

AA.8.14.3 Technical Implementation

AA.8.14.4 A Tool in a Toolbox

AA.8.14.5 Maturity of the Paradigm Shift

AA.9.0.0 Intangibles:

AA.9.1.0 Creation and production of intangibles

AA.9.2.0 Intangible data assetization

AA.9.2.1 Assetization for Asset Monetization

AA.9.2.2 Differential Valuation

AA.9.2.3 Conclusion

AA.9.3.0 The Intangible assets production model

AA.9.4.0 Monetary information valuation

AA.9.4.1 Monetary Valuation Methodology

AA.9.4.2 Weighting Content, Context, and Concept

AA.9.4.3 Discovering and Monetizing the Intangibles

AA.9.4.4 Static and Dynamic

AA.9.4.5 Conclusion

AA.9.5.0 Assetitization of intangible content

AA.9.5.1 Definitions

AA.9.5.2 Conclusion

AA.9.6.0 Attribution of monetary value to information

AA.9.6.1 Monetization

AA.9.6.2 Contextual Conflicts

AA.9.6.3 DigitalDoors Methodology

AA.9.6.4 Weights

AA.9.6.5 Hierarcharchial Assignments and Enhancements

AA.9.6.6 Conclusion

AA.9.7.0 Information Lifecycle Valuation

AA.9.8.0 Security Gaps: Binding Infrastructure with Process with User with Data .The need for a new intangibles production model

AA.9.9.0 Intangible Trade secrets

AA.9.9.1 Background

AA.10.0.0 Introduction to the Digitaldoors Dictionary

AA.10.1.0 DigitalDoors Dictionary

A.1 Creating An Information Infrastructure

A.2 Sampling and Creation of a Simple Info Infrastructure

A.3 System Tools and Processing Methods for an Information Infrastructure

A.4 Information Dispersal - Basic

A.5 Alternative to Information Dispersal Algorithm

A.6 Adding Prior Art Information Dispersal Algorithms to Granular Data Dispersion

A.7 Automatic Dispersal of Data to Remote Storage Locations

A.8 Dispersal - Breaking Down the Context of Data Streams while Maintaining Access to the Content of its Parts

A.9 Granular Tagging - Basic

A.10 Automated Granular Data Level Manipulation

A.11 Process for Creation of Automated Granular Tagging and Labeling

A.12 Process for Creation of Automated Tagged Tear Lines

A.13 Category Tags as Placeholders in Databases

A.14 Controlled Release - Basic

A.15 Layered Build-up of Data Streams, Layer upon Layer

A.16 Granular Data Release from Third Party Repository

A.17 Creation of Modular Data Components from Granular Data Streams

A.18 "Rolling" Exposure of Granular Data Streams

A.19 Controlled Release of Extracts after Verification

A.20 Multi Purpose Usage of Filtering and Extraction Process

A.21 Filtering and Copying "Selected Data"

A.22 Combined Process of Extracting Part of the " Selected Data" and Copying Parts of the "Selected Data"

A.23 Data Mining Search Results Basic - Distribution as Multi Level Security Versions

A.24 Data Mining - A Search Creating Automatically Key Words

A.25 Data Mining - Continuous Data Mining with Query Refinement

A.26 Automatic Continuous Search – with Divergence and Convergence

A.27 Distributed Data Mining

A.28 Content Inference Engine - Basic

A.29 An Inference Engine - Searching for the Unknowns

A.30 Securing Information Sharing with an Inference Engine

A.31 Automatic Web Data Inference Crawler Robots

A.32 Changeable Data Classifications Based on Content Inference Threats

A.33 Search Operations Creating New Continuously Growing Digital Data Streams

A.34 Distributed Searches from Different Storage Nodes

A.35 Storage of Separated Data Pieces in One Location

A.36 Storage of Granular Data Streams - Basic

A.37 Configuration of Granular Data Streams Dispersal to Distributed Storage Stores

A.38 Granular Data Stream Transport

A.39 Shuttling Data and Granular Data Streams Between Distributed Storage Stores

A.40 Replication of Granular Data Streams with Minimal Security Risk

A.41 Anonymizing Classified and Unclassified Storage Stores

A.42 Controlled Release of Granular Data Streams - Granular Data Manipulation and Control

A.43 Sanitization Process with Inference Filtering - Basic

A.44 Process for Sanitizing Data on the Network for Privacy Security and Survivability

A.45 Automated Sanitization of Important Data

A.46 Sanitization of Non-Important Data

A.47 Release of Granular Data Streams in With Increasing Levels of Access Identifiers

A.48 Release of Granular Data Streams After Obtaining Consideration

A.49 Secured Release of Granular Data Streams into Multiple Screens

A.50 Ecosystem Based on "Granular Data Control" - Basic

A.51 Eco System for Information Superiority and Survivability Based on "Granular Data Control"

A.52 System and Method for Minimizing Data Exposure

A.53 Creating "Digital Doors" for Access and Controlled Release in a Data Stream

A.54 General Aspects - Basic

A.55 Automatic Creation of a User or Object's Identification Profile

A.56 Copying Filtered Granular Data and Dispersing

A.57 Combining Extraction and Copying for Filtering of Filtered Granular Data

B.1 Basic Operational Theory of Secure or Select Data Storage

B.2 General Operation

B.3 System Configurations

B.4 Input or Initial Processing Considerations (Basic Filter Modules)

B.5 Storage

B.6 Extraction and Storage Enhancements

B.7 Basic Reconstruction

B.8 Reconstruction Techniques

C.0 Testing the Security System

C.1 The Etiology of Information

C.2 Metasearch Engine for Knowledge Discovery: Search Convergence and Divergence

C.3 Initial Process - Metasearch Engine and Knowledge Expander

C.4 Simple Metasearch Engine

C.5 Automatic Metatagging

C.6 Automatic secondary tagging of a "range"

C.7 MLS, Multi-level Security-Compliant Search and Distributions

C.8 Benefits of the Metasearch - Knowledge Expander

C.9 Information Life Cycle Engine

C.10 Information Life Cycle Searches

C.11 Search With Prioritized Classifications

C.12 Simple Filters

C.13 Complex Filters

C.14 The Editor As An Information Expander

C.15 Document Object Model (DOM) - Protection and Processing

C.16 Recognizing The Document Object Model (DOM)

C.17 Content

C.18 DOM Process Editor

C.19 Five Informational Attributes

C.20 Select Content Introns and Exons

C.21 Hierarchical Taxonomic Class Examples

C.22 Knowledge Expander (KE) Basic Program

C.23 Secured Metasearch Engine Based on Granular Data Control

D.1 Secure Editor, DOM Editor (General) and DOM Editor Applied as Extractor Modules

D.2 Applications of the Secure and SC Data Systems

D.3 Automatic Features

D.4 Multiple Security Levels

D.5 Sharing Data with Different Security Levels - Data Mining

D.6 Multilevel Security through Sanitization with Reconstruction of Sanitized Content

D.7 Multiple Independent Levels of Security (MILS)

D.8 MLS Server and Workstation Components

D.9 Flexibility of the Present MLS Approach

D.10 Multiple Extraction Filters and Application Outline

D.11 Multiple Security Features for Data

D.12 Adaptive Data Security -Event Responsive System

D.13 Email, Web-based and Other Types of Applications

D.14 Portable Computing Device Environment

E.1 General System Comments

Brief Description of the Drawings

[0016] 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:

[0017] FIGs.1a and 1b diagrammatically illustrates a basic system diagram, method and flow chart for an information infrastructure.

[0018] FIG. 2 diagrammatically illustrates a basic information life cycle process or system wherein secure content (sec-con) and select content (SC) is separately stored per categorical filters operable by the enterprise.

[0019] FIG. 3 diagrammatically illustrates a simplistic dynamic filter and select content (SC) storage coupled to a data processing event.

[0020] FIG. 4 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.

[0021] FIG. 5 diagrammatically illustrates a system diagram showing reconstruction of the data, various security clearances and both electronic reconstruction and visual reconstruction.

[0022] FIG. 6 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.

[0023] FIG. 7 diagrammatically illustrates a basic flowchart showing reconstruction for various security levels.

[0024] FIG. 8 diagrammatically illustrates interleaving distinct data into different memory locations in a video memory.

[0025] FIG. 9 diagrammatically illustrates a flowchart showing one embodiment of the principal portions of the data security program.

[0026] FIG. 10 diagrammatically illustrates a flowchart showing the basic elements of the reconstruction process for the data security program.

[0027] FIG. 11 diagrammatically illustrates deconstruction of an input document into segments.

[0028] FIG. 12a diagrammatically illustrates the information life cycle knowledge expander (KE) search engine process.

[0029] FIG. 12b diagrammatically illustrates the KE process of using search terms, data collection and depth-of-search control.

[0030] FIG. 12c diagrammatically illustrates the KE process for the primary search results.

[0031] FIG. 12d diagrammatically illustrates the KE process for the output representation of search term data and search result data of supplemental documents.

[0032] FIG. 13 diagrammatically illustrates a filter program.

[0033] FIG. 14 diagrammatically illustrates an editor program.

[0034] FIGs. 15, 16. 17 and 18 diagrammatically illustrate extraction of select content (SC) and a hierarchical taxonomic system based upon TS, T, C and UC security code classifications.

[0035] FIG. 19 diagrammatically illustrates a data object tree or map for a document model (DOM).

[0036] FIG. 20 diagrammatically illustrates varies metadata levels in the DOM.

[0037] FIG. 21 diagrammatically illustrates a DOM editor process.

[0038] FIG. 22 diagrammatically illustrates another DOM editor process.

[0039] FIGS. 23, 24 and 25 show examples of categorical identifiers, ranked id categories and categorical ids for a business.

[0040] FIG. 26 diagrammatically illustrates a basic KE search process.

[0041] FIG. 27 diagrammatically illustrates an expanded KE search process.

[0042] FIG. 28 diagrammatically illustrates KE search process options.

[0043] FIG. 29 diagrammatically illustrates a hardware implementation for the KE search system.

[0044] FIG. 30 is a computer network diagram showing various user communities.

[0045] FIG. 31a, 31b diagrammatically illustrates a flowchart showing the key component steps for the multiple layer security program for the community of users.

[0046] FIG. 32 diagrammatically illustrates a multiple level security system accessed by users having different security clearances (which also represents a data mining system and operation).

[0047] FIG. 33a, 33b diagrammatically illustrates a flowchart showing the key components of an adaptive security program adaptable to various levels of electronic attacks, hacker or hack attacks.

[0048] FIGs. 34 to 39 show tabular examples of attack and response levels for Standard Automatic Defenses Matrix; Optional Automatic Defenses Matrix; Security Meter Module; Normal Work Mode; Threat Made Table; and, Attack Mode.

[0049] FIG. 40 diagrammatically illustrates a flowchart showing the key components of a multiple encryption program using multiple types of encryption in one document or data object. Encryption may include data compression and/or expansion or parsing techniques.

[0050] FIG. 41 diagrammatically illustrates a chart showing the key components of the parsing, dispersion, multiple storage and reconstruction (under security clearance) of data.

[0051] FIGS. 42 and 43 diagrammatically illustrate a flowchart showing the key components of one embodiment of the e-mail security system (jump points 42 and 43 link the flow charts).

[0052] FIGS. 44a and 44b 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).

[0053] FIG. 45 diagrammatically shows several revenue systems which may be employed with the data security systems described herein.

[0054] FIG. 46 diagrammatically illustrates a portable computing device (or the critical parts

thereof, see FIG. B-2 for further details) associated with the portable data security locator system and method.

[0055] FIG. 47 diagrammatically illustrates a basic flow chart for the portable security system program in accordance with the basic principles of the present invention.

[0056] FIG. 48 diagrammatically illustrates a MILS or multiple independent levels of security computer network with three (3) sub-networks at security levels top secret TS, secret S, and unclassified U.

[0057] FIG. 49 diagrammatically illustrates a security guard computer useful in the network of FIG. 48.

[0058] FIG. 50 diagrammatically illustrates a workstation useful in the MILS network.

[0059] FIG. 51 diagrammatically illustrates a filter program flow chart.

[0060] FIG. 52 diagrammatically illustrates a basic security editor program.

[0061] FIG. 53 diagrammatically illustrates a general flow chart for a comprehensive filter operable on a document DOM.

[0062] FIG. 54 diagrammatically illustrates a basic application of the comprehensive DOM editor.

[page left blank]

EX. 1002, Page 2565

Detailed Description of the Preferred Embodiments

[0063] The present invention relates to an information infrastructure with many different features and characteristics. The infrastructure is a system, a methodology and a process implemented 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 the functions described herein. An Abbreviations Table is provided at the end of this specification. Also, the General System Comments section E.1 describes certain aspects relative to the implementation of this invention. In the drawings, and sometimes in the specification, reference is made to certain abbreviations. The Abbreviations Table (section E.1) near the end of the specification and the Digital Doors Dictionary at section AA.10.1.0 provide some correspondence between the abbreviations and the item or feature.

AAA.1.0.0 DigitalDoors Capabilities

[0064] DigitalDoors delivers security solutions which conform to the secured information sharing requirements as stated in the Presidential Executive Order 13356 of 8.27.04 and in the Senate's National Intelligence Reform Act passed in September 2005.

[0065] DigitalDoors delivers information assurance through security processes that secure automatically (or manually) the data content elements. This simultaneously enables data security, data privacy protection, secured sharing and collaboration, and survivability within a unified infrastructure.

[0066] DigitalDoors technology provides security against insiders and augments traditional perimeter-based security methods. It represents a major step toward granular data content security and secured leveled information sharing necessary for unified national security and protection of privacy. It introduces granular content security and privacy protection, while enabling data sharing without

exposures of source, methods, and activities.

[0067] DigitalDoors is inherently platform-independent and process-independent; it is a single enterprise-wide solution for all types of platforms, network infrastructures, cross-platform distribution, extended information workflows, and traditional data processing operations. The DigitalDoors technology is fully flexible and compliant with existing and developing standards for databases, XML, and hierarchical metadata, as specified in this document.

[0068] Given the practical implementation of data security at a granular data level and the modular, multi-platform initiative, the core taxonomic technology enables anonymous information sharing so that organizations can share information to connect the dots in a practical, sustainable, and effective process.

AAA.1.1.0 Architecture Specifications

[0069] DigitalDoors configuration is robust enough to support security while maintaining data structures consistent with legacy data operations, traditional desktop applications, and most structured and formatted data types. Support for HTML and XML is available at this time. Specifically, DigitalDoors will operate with SOAP, WSDL, UDDI, WS-Interoperability, XACML, PKI, XKMS, X-KRSS, biometric, SAML, and most other web-enabled architectures, trusted platforms, Unix, Linux, as well as host-based legacy environments. The technology is feasible within or across domains, and can function within multiple level trusted domains.

[0070] In DigitalDoors existing network, system, data processing, ID assurance, encryption technology, Internet-based transaction processing, messaging, and database activities coexist with limited workflow complications. DigitalDoors reviews data sensitivity level at the payload and messaging level; as a result, it can interoperate with the GIG transport services, with core enterprise

services, and any community of interest.

AAA.1.2.0 Scalability

[0071] DigitalDoors is scalable both vertically and horizontally, or any mix thereof. The functions can be run centralized or dispersed, or both. It can run as hardware or software. As software, it can run on low-end user desktops, servers, appliances, or massively-parallel hosts. Complex processes (or sense CPU-bound processes) can be offloaded to coprocessors or grid-based resources. Demonstrations show functionality on past generation PC hardware without any peculiar software or hardware, thereby confirming a simple scalability scenario. DigitalDoors is also designed from the ground up with networking awareness and sensitivity level awareness to support single user environments, networked client-server infrastructures,and complex distributed GIG-type scenarios. Location references support local and fully-qualified paths, X-paths, X-pointers, and other long addressing methods.

AAA.1.3.0 Product and Process Overview

[0072] DigitalDoors provides Defense in Depth security capabilities which ensure the Integrity and continuity of the information environment and the information it stores, processes, maintains, uses, shares, disseminates, disposes, displays, or transmits.

[0073] DigitalDoors presents solutions to the following vulnerabilities in networks, computing infrastructure, core services and discreet systems:

Creation of many single points of failure in a net centric environment

Survivability and lack of constant data availability

Lack of resiliency against attacks including denial of service attacks

Unsecured collaboration and cross domain data exchange leakage

Protection against insider attacks,

Defense against malicious traffic

Defense against war operations including spy ware

AAA.1.4.0 DigitalDoors implementation options:

[0074] It is an add security capability which can be overlaid and integrated into existing security management systems. It can function as a stand alone security service.

AAA.1.4.0 Perpetual Data Availability

[0075] DigitalDoors delivers basic security Access Management capabilities, however it goes far beyond that and delivers the capability for perpetual data availability. Perpetual data availability enables access to data even when different storage servers are attacked or compromised. Single points of failure, are eliminated by dispersing the data into different storage servers. To eliminate the risk in replication of the data the documents /data streams are split into granular data segments (both data and metadata).

[0076] Compromise of an encrypted granular data segment on a compromised server can't compromise the entire document or data stream.

AAA.1.5.0 The Key for Net-Centric security

[0077] Net-Centric security will be based on granular content control. DigitalDoors products are based on breakthrough patented technologies, which deliver comprehensive solutions to critical net centric needs. The products deliver maximum security, survivability and collaboration capabilities through the introduction of security at the granular data level within documents and data streams. The process can be outlined as follows:

[0078] DigitalDoors creates automatically or manually a sanitized version of the original document and/or a data stream, which contains no sensitive data.

[0079] The system in essence creates a "lowest common denominator" a non classified, sanitized document.

[0080] That document version can be shared with many users including those with low or no clearances.

[0081] The critical granular content within the document or data stream is tagged, encrypted, extracted and dispersed to distributed storage.

[0082] The result: a remainder unclassified sanitized document/ data stream with its critical /classified components stored in distributed storage.

[0083] An attack will not cause damage or only very limited damage since the critical classified granular content is not in the original document.

[0084] The sanitized document will be upgraded for each specific user according to his security level and role at wire speed. Sanitized, declassified documents and/or data streams will be converted back into classified documents, at wire speed, when a user presents his identification.

[0085] The reconstitution will take place based on the clearance levels and roles of each user.In essence different versions of the original document/ data stream will be reconstructed according to the rights of each different user.

[0086] Users who present their credentials will see instantly those missing parts of the document that they are allowed to see. As an example a mid level intelligence analyst will see the most of the elements reconstituted back into the document while a local commanding officer will see a reconstituted version with all the original elements.

[0087] The remainder document is a critical element presented by DigitalDoors. The remainder document enables not only wide secured sharing but also a centralized management of documents and/or data streams while the secure elements are decentralized to avoid single points of failure. This includes solutions against malicious traffic:

AAA.1.6.0 Active defense and counterattacks versus common passive defense

[0088] Critical content is not there, creation of air gaps. Work within all 7 OSI layers with filters will process every header and payload packet.

[0089] Firewalls and intrusion detection appliances are not successful in detouring major malicious attacks. There are different systems analyzing packets headers and payloads for malicious data blocking. DigitalDoors takes a different approach. DigitalDoors sees those data blocking efforts as passive defenses. Passive defenses have been proven to be much less useful than active defenses and counterattacks. In active defenses, the defender takes advantage of the terrain and other elements.

[0090] DigitalDoors was designed to operate as an active defense and as counterattack. It assumes that even the best of breed systems will not be able to block thoroughly the growing number and sophistication of malicious traffic.

[0091] The basic assumption is that the attacker will always be a step ahead of the defender. DigitalDoors therefore creates the ultimate last line of defense by having the critical elements of content extracted to dispersed secure storage locations.

[0092] In essence DigitalDoors creates air gaps. Malicious attacks might hurt the non-critical remainder content but the critical content is kept away in highly secure distributed storage locations unknown to the attackers.

[0093] Controlled release of critical content from storage locations will take place only after

extensive scans for malicious attacks.

[0094] DigitalDoors standard functionality is focused at ISO layer 7 and above; specifically, it is intended to function within the presentation and application layers of the ISO model and protect data within infinitely granular hierarchies. As more traditional networking filter implementation, it functions and can be separately implemented at layers 1 through 6. With the filters, each bit it comes into contact with, header or payload is analyzed. Malicious elements are filtered out at wire speed. DigitalDoors will add on the best of brand malicious filtering capabilities after their certification by DoD. The DigitalDoors new version will enable malicious attacks to trigger DigitalDoors defenses-in-depth's last line of defense. Intrusion detection alerts will trigger a double-tiered defense:

[0095] Substantial extractions of content from documents, data streams will take place. The extracted critical content will be transported to distributed storage.

[0096] The release of content from storage for reconstitution in documents and data streams will be stopped or minimized.

AAA.1.7.0 Technical Basis for DigitalDoors Technology

[0097] DigitalDoors is a novel but practical combination of well-known computing disciplines, including secret sharing, information dispersal algorithms, distributed computing and best of breed security methodologies. In essence, the system creates virtual "digital doors" in documents and data streams. Those digital doors establish security and enable secured collaboration through defenses-in-depth capabilities to ensure end to end integrity, continuity of the data in storage and in transfer. DigitalDoors offers distinct core solutions and advantages that are not solved by DOD initiatives and products like CIBIS, CASPER, cross domain guards, and best of breed commercial products.

[0098] DigitalDoors contributes to the security by implementation of granular data control. The DigitalDoors solutions include the following cornerstones:

[0099] Net centricity creates major benefits but also creates dangerous risks.

[0100] The key to manage those risks is through granular control of the critical elements within the networks.

[0101] The critical element within the networks is data, which needs to be controlled granularly at the granular data level.

[0102] Therefore documents / data streams need to be parsed manually or automatically into smaller granular content parts, in order to enable granular control.

[0103] These granular content parts need to be tagged and classified per security level and role.

[0104] Users will have access to those granular tagged parts according to the rights they were assigned in their user profile.

[0105] In essence there is a need in net centric environments for recreation of various digital versions, on the fly which are reconstructed according to different users rights and roles.

[0106] Creations of on the fly versions save costs both in bandwidth storage and speed. There is no need to keep in storage many different versions and there is no need to send full documents multiple times across networks.

[0107] To counter the major security risks of net centricity the granular content parts should be tagged, encrypted, extracted, and dispersed to distributed storage locations.

[0108] Providing perpetual data availability and data survivability by replication of the different granular parts and storing the replicated copies on many servers.

[0109] Replication on many servers is enabled without security risk because the replicated items are very granular and even if they are compromised they are out of any context and do not compromise the bigger document or data stream.

AAA.1.8.0 Granular data control

[0110] There is a need to create "digital doors" in documents and data streams to enable granular control and achieve maximum collaboration, security, survivability, confidentiality, and privacy.

[0111] Digitaldoors Creates Granular Digital Rights Management for Collaboration. The core enabler of the DigitalDoors collaboration product is the creation and control of granular data segments within a document and/or a data stream. The parsing of granular content segments in a documents and/or data stream, can be done manually, automatically, or a combination of both. Metatags are assigned manually and also automatically to the newly created granular data segments. The Metatags include user roles, and define who and what processes are allowed to access each segment. When a user requests data through the discovery services, an automatic matching process will take place, matching user's profile with the metatags. The control of granular parts of content within data streams enables sharing of content with many users where each can see what he is allowed to see in a document/ data stream in accordance with his personal profile and the policy embedded into the metatags within the different content segments.

[0112] Users will be able to access the data according to their roles. For example a user with an intelligence role will be able to view the whole reconstructed content while a user with a logistics role will be able to view only a limited reconstructed version of the original content.

AAA.1.9.0 Collaboration will consist of:

[0113] User's presentation of his identification

[0114] Automatic matching of user's profile with Metatags of the different tagged segments of the document/data stream.

[0115] Wire speed reconstruction of a version of a document/ data stream according to users profile.

AAA.1.10.0 Granular tagging with metadata

[0116] Label data (and other resource) at content and context level for sensitivity, compartment, information, categorization, and other arbitrary designations

[0117] User and process clearances (inclusion and/or exclusionary) based on sensitivity, compartment, information, categorization, and other arbitrary designations

Granular Digital Rights management:

Support revocation of rights in real time

Support downgrading in real time

Support upgrading in real time

Controlled release of granular data:

Enable controlled release of data at all user , process and application levels

Enable distribution of core services and rapid information deployment to the edge

AAA.1.11.0 Coalition And Multinational Cross Domain Collaboration

[0118] DigitalDoors enables secured cross domain sharing as urgently needed in coalition and multinational cross domain collaboration. Real time ad hoc interaction between different trusted and untrusted participants is enabled in the very difficult cross domain environment. A document/ data stream is divided to parts, each part is tagged according to the security level of the content (TS, S, C, U), it can also be tagged for the roles of users that should be allowed to access it (TS a, TS b, and Sa).

AAA.1.12.0 Incorporation into a trusted OS

[0119] Incorporated with a trusted OS (for example a certified Trusted Solaris and a TCS guard) DigitalDoors enables a user to divide a document into granular content segments, tagging and encrypting each of the newly parsed parts according to the classification level of its content (TS, S, C, U) and dispersing the tagged parts to different distributed (TS, S, C, U) storage locations throughout the enterprise. The different segments can also be tagged for users roles. (TS a, TS b, S a, etc.).Users will be able to access a document or data stream they request which will be reconstituted at wire speed according to their role and clearance level.

[0120] Cross domain collaboration is enabled with connectivity of DigitalDoors products to a certified guard.

Cross domain sharing in both directions High to Low, Low to High

Secured Cross Domain sharing for US, and coalition forces

Advanced metatags for security clearness and roles

Organizational and user defined filters

AAA.1.13.0 Survivable infrastructure

[0121] DigitalDoors Creates a secured survivable information security services infrastructure that lowers costs and maximizes secure collaboration for real time situational awareness.

[0122] It Secures data at point of origination, in rest and in transit based on methods of content granularity.

[0123] Provides data confidentiality, availability, integrity, and non-repudiation to users with override functionality and lowest common denominator as failsafe

[0124] Cross-platform, cross-network, and integrates with existing identification, authentication, and authorization systems

[0125] Integrates with Cross Domain guards with EAL-4 or higher certifications

[0126] Support platform, guard, network, workflow, gateway data, and metadata interoperability for allies, partners, coalition forces

AAA.1.14.0 Net Centric capabilities

[0127] DigitalDoors suite of net centric products and services delivers the following sought solutions to critical challenges of net centric organizations:

1. Security
2. Survivability
3. Constant data availability
3. Secured collaboration/ coalition cross domain sharing
4. Automatic posting and alerting
5. Specialized discovery/data mining

[0128] The DigitalDoors evolutionary services can enable users to get the right information, at the right time, in the right format, as needed to meet operational tactical and support missions.

AAA.1.15.0 DigitalDoors Services overview

[0129] DigitalDoors is a net centric core technology which delivers among others, the following services:

1. Secured collaboration services

[0130] "The existing Collaboration capabilities are technically outdated, expensive, have serious

security flaws and do not scale well. There is the need to continually look at collaboration technology trends and potential redesigns and/or enhancements"

[0131] Global Information Grid Core Enterprise Services Strategy- Draft version 1.1a 7/9/03

[0132] Office of the Assistant Secretary of defense for Networks and information integration

[0133] The DigitalDoors product addresses each of the above limitations taking secure collaboration from an "elusive goal" to an achievable goal.

[0134] DigitalDoors products deliver an evolutionary technology, which enables secured seamless collaboration .It provides comprehensive access to information from anywhere, at any time on any device and application.

AAA.1.16.0 DigitalDoors implementation options:

[0135] It is an add on collaboration capability which can be overlaid and integrated into existing shared workspaces, whiteboards and applications etc.

[0136] Or it can function as a stand alone collaboration service.

AAA.1.17.0 defenses against outsuiders and insiders

[0137] DigitalDoors defends against possible killer collaboration traps , security killer gaps as described in the IA/ Security services segment. Possible collaboration killer gaps can be:

War operations on collaboration sessions including substitution of misinformation in sessions by outsiders or insiders

Destruction of storage and backup storage

Unavailability of data due to denial of services attacks

[0138] DigitalDoors contributes breakthrough security added value to the following

AAA.1.18.0 collaboration elements:

Session management

Text Collaboration

Audio and Video over IP Network

White boarding and annotation

Application Sharing

Application Broadcasting

Virtual spaces

[0139] DigitalDoors contributes to the security of collaboration by implementation of granular data control.

AAA.1.19.0 DigitalDoors cornerstones

[0140] The DigitalDoors solutions are based on the following cornerstones:

[0141] Net centricity creates major benefits but also creates dangerous risks.

[0142] The key to manage those risks is through granular control of the critical elements within the networks.

[0143] The critical element within the networks is data, which needs to be controlled granularly at the granular data level.

[0144] Therefore documents / data streams need to be parsed manually or automatically into smaller granular content parts, in order to enable granular control

[0145] These granular content parts need to be tagged and classified per security level and role.

[0146] Users will have access to those granular tagged parts according to the rights they were assigned in their user profile.

[0147] In essence there is a need in net centric environments for recreation of various digital

versions, on the fly which are reconstructed according to different users rights and roles.Creations of on the fly versions save costs both in bandwidth storage and speed. There is no need to keep in storage many different versions and there is no need to send full documents multiple times across networks.

[0148] To counter the major security risks of net centricity the granular content parts should be tagged, encrypted, extracted, and dispersed to distributed storage locations.

[0149] Providing perpetual data availability and data survivability by replication of the different granular parts and storing the replicated copies on many servers.

[0150] Replication on many servers is enabled without security risk because the replicated items are very granular and even if they are compromised they are out of any context and do not compromise the bigger document or data stream.

AAA.1.20.0 Granular content control

[0151] DigitalDoors creates Granular Digital Rights management for collaboration:

[0152] The core enabler of the DigitalDoors collaboration product is the creation and control of granular data segments within a documents and/or datastream. The parsing of granular content segments in a documents and/or datastream, can be done manually, automatically or a combination of both. Metatags are assigned manually / automatically to the newly created granular data segments. These metatags include also which user roles are allowed to access each segment. When a user requests data through the discovery services, an automatic matching process will take place, matching user's profile with the metatags. The control of granular parts of content within data streams enables sharing of content with many users where each can see what he is allowed to see in a document/ data stream in accordance with his personal profile and the policy embedded into the Metatags of the different content segments.

[0153] Users will be able to access the data according to their roles. For example a user with an

intelligence role will be able to view the whole reconstructed content while a user with a logistics role will be able to view only a limited reconstructed version of the original content. Collaboration will consist of:

1. User's presentation of his identification

2. Automatic matching of user's profile with Metatags of the different tagged segments of the document/data stream.

3. Wire speed reconstruction of a version of a document/ data stream according to users profile.

[0154] Granular tagging with metadata:

1. Label data (and other resource) at content and context level for sensitivity, compartment, information, categorization, and other arbitrary designations

2. Assign users and processes clearances (inclusion and/or exclusionary) based on sensitivity, compartment, information, categorization, and other arbitrary designations

[0155] Granular Digital Rights management:

1. Support revocation of rights in real time

2. Support downgrading in real time

3. Support upgrading in real time

[0156] Controlled release of granular data:

1. Enable controlled release of data at all user , process and application levels

2. Enable distribution of core services and rapid information deployment to the edge

[0157] DigitalDoors enables secured cross domain sharing as urgently needed in coalition/ multinational cross domain collaboration. Real time ad hoc interaction between different trusted and

untrusted participants is enabled in the very difficult cross domain environment. A document or data stream is divided to parts, each part is tagged according to the security level of the content (TS, S, C, U), it can also be tagged for the roles of users that should be allowed to access it (TS a, TS b, Sa). Incorporated with a certified OS (like A DIA certified Trusted Solaris and a TCS guard) DigitalDoors enables a user to divide a document into granular content segments, tagging and encrypting each of the newly parsed parts according to the classification level of its content (TS, S, C, U) and dispersing the tagged parts to different distributed (TS, S, C,U) storage locations throughout the enterprise. The different segments can also be tagged for users roles. (TS a, TS b, S a etc.).Users will be able to access a document or data stream they request which will be reconstituted at wire speed according to their role and clearance level.

AAA.1.20.1 Cross domain

[0158] Cross domain collaboration is enabled with connectivity of DigitalDoors products to a certified guard.

[0159] Cross domain sharing in both directions High to Low, Low to High

[0160] Secured Cross Domain sharing for US, and coalition forces

[0161] Advanced Meta tagging for security clearness and roles

[0162] Organizational and user defined filters

AAA.1.21.0 Security services

[0163] DigitalDoors provides Defense in Depth capabilities which are far beyond the current state of the art. Those defenses in depth ensure:

[0164] The integrity and continuity of the information environment and the information it stores, processes, maintains, uses, shares, disseminates, disposes, displays, or transmits.

AAA.1.22.0 solutions to vulnerabilities:

[0165] DigitalDoors presents solutions to the following vulnerabilities in networks, computing infrastructure, core services and discreet systems:

1. Creation of many single points of failure in a net centric environment

2. Survivability and lack of constant data availability

2. Lack of resiliency against attacks including denial of service attacks

2. Unsecured collaboration and cross domain data exchange leakage

3. Protection against insider attacks,

4. Defense against malicious traffic

5. Defense against war operations including spy ware

AAA.1.23.0 Replication for perpetual data availability

[0166] DigitalDoors delivers basic security Access Management capabilities, however it goes far beyond that and delivers the capability for perpetual data availability:

[0167] Perpetual data availability enables access to data even when different storage servers are attacked or compromised.

[0168] Single points of failure, are eliminated by dispersing the data into different storage servers.

[0169] To eliminate the risk in replication of the data the documents /data streams are split into granular data segments (both data and Meta data).

[0170] Compromise of an encrypted granular data segment on a compromised server can't compromise the entire document or data stream.

AAA.1.24.0 Solving net centric needs

[0171] DigitalDoors products are based on breakthrough patented technologies, which deliver comprehensive solutions to critical net centric needs. The products deliver maximum security, survivability and collaboration capabilities through the introduction of security at the granular data level within documents and data streams.

[0172] Firewalls and intrusion detection appliances are not successful in detouring major malicious attacks. There are different systems analyzing packets headers and payloads for malicious data blocking. DigitalDoors takes a different approach. DigitalDoors sees those data blocking efforts as passive defenses. Passive defenses proved to be much less useful then active defenses and counterattacks. In active defenses the defender takes advantage of the terrain and other elements.

[0173] DigitalDoors was designed to operate as an active defense and as counterattack. It assumes that even the best of breed systems will not be able to block thoroughly the growing number and sophistication of malicious traffic.

[0174] The basic assumption is that the attacker will always be a step ahead of the defender. DigitalDoors therefore creates the ultimate last line of defense by having the critical elements of content extracted to dispersed secure storage locations.

[0175] In essence DigitalDoors creates air gaps. Malicious attacks might hurt the non-critical remainder content but the critical content is kept away in highly secure distributed storage locations unknown to the attackers.

[0176] Controlled release of critical content from storage locations will take place only after extensive scans for malicious attacks.

AAA.1.25.0 Secured Discovery and publishing services

[0177] Provide edge users with the ability to search, mine, and pull data based on Meta data

created automatically and or manually

[0178] Providing content and context security while maintaining catalog, search, and mining services regardless of sensitivity levels

[0179] Designed to support common delivery and posting of data in real-time

[0180] The challenges:

[0181] Enable users, down to the last tactical mile, with the capability to pull whatever they want, from wherever they want, from wherever they are.

[0182] There is a need to publish content as well as post Meta data which will enable to locate the published material.

[0183] DigitalDoors discovery services enable different users across the GIG to locate relevant

[0184] Files, data bases, services, directories, web pages, data streams, by using Meta data descriptions stored in various directories, registries, catalogs, repositories.

[0185] DigitalDoors is a security based Discovery service. Discovery services can create major vulnerabilities to the GIG; an attacker who accesses successfully a Discovery service must not be permitted to access sensitive data.

[0186] The following service are available for Discovery and Publishing services:

AAA.1.26.0 Publishing;

[0187] DigitalDoors enables publishing and posting data to common storage spaces as early as possible.

[0188] The system posts sanitized versions of the documents and/or data streams (full documents if needed.)

[0189] Documents are sanitized manually or automatically and then posted automatically.

[0190] The posting can be done automatically as part of an organizational policy. The advantage of posting sanitized versions of a document is that the user maintains control of the document's critical granular content.

[0191] The viewers who are interested in a published, posted sanitized document can request from the owner or a mediating authority the missing content. The full document can be released for consideration including exchange of sought information or payment etc.

[0192] The sanitized platform document can be automatically posted within the community of interest or other places so other users can locate it easily. The posting is done automatically or manually.

AAA.1.27.0 Meta data Posting

[0193] Meta data posted in directories, registries catalogs etc. should only enable a user access to a sanitized version of the document/ data stream.

[0194] Users who are interested to see the full version of a document/ data stream will need to present identification.

[0195] The presentation of an ID will transform the sanitized, declassified documents and/or data streams back into a fuller version, at wire speed, based on their clearance levels and roles. Different versions of the original document/ data stream will be reconstructed according to the rights of each different user

[0196] Meta data is created automatically/ manually and may be posted in Meta data directories in Communities of interest or other locations.

[0197] Edge users pull capabilities at last mile.

[0198] In addition to labeling and tagging content segments, DigitalDoors scans and categorizes all content in a document/ data stream. A user can search for information based on Meta data in tags and

also by key word searching and category searching. The search results will be in delivery of a sanitized results .With presentation of identification a tailor made version will be created for each user based on his profile.

AAA.1.28.0 Secured Mediation services for information sharing

[0199] In order to enable any substantial aggregation, fusion, translation and integration of data for delivery of situational awareness support, there is a need to motivate different people in the network to share their data.

[0200] How can data owners be motivated to share with others?

[0201] DigitalDoors enables users negotiate the exchange of data, services or products in a net centric environment.

[0202] DigitalDoors Mediation services creates a framework for negotiations between parties that might not have any former relationship or trust.

[0203] The basis of all negotiations and brokering is giving users a motivation to share their data.

[0204] The consideration for data can be information, services, money etc.

[0205] A true market place, for arms length negotiations is enabled by the ability to release granular content in a controlled way following receiving of agreed upon consideration.

[0206] Data can be released in parts and in stages based on the response of the other parties. Such mediation is automated or can be done also manually.

AAA.1.29.0 Other services

[0207] Other Mediation services provided by DigitalDoors Are:

Full auditing is enabled.

Auctioning is enabled, highest bidder will get all or parts of released of data

Discovery Metadata dictionaries

Taxonomies and Ontologies.

AAA.1.30.0 Secured perpetual storage services

[0208] A net centric environment demands secure perpetual data availability. There is a need to create a survivable storage net centric environment, avoiding single points of failure.

[0209] Replication of data on distributed servers defeats single points of failure, but it creates security risks based on over exposure data. DigitalDoors overcomes the replication risks be overcome and delivers a perpetual data availability service.

[0210] DigitalDoors delivers basic security Access Management capabilities, however it goes far beyond that and delivers the capability for perpetual data availability. Perpetual data availability enables access to data even when different storage servers are attacked or compromised. Single points of failure, are eliminated by dispersing the data into different storage servers. To eliminate the risk in replication of the data the documents /data streams are split into granular data segments (both data and Meta data).Compromise of an encrypted granular data segment on a compromised server can't compromise the entire document or data stream.

AAA.1.30.1 Meta data posting

[0211] DigitalDoors enables posting data to common storage spaces as early as possible.

[0212] The system posts:

Meta data in directories, registries and

Posts / publishes sanitized documents (full documents if needed.) in public spaces in the Communities of interest.

[0213] Documents are sanitized manually or automatically and then posted automatically.