



US 20070150299A1

(19) **United States**

(12) **Patent Application Publication**

Flory

(10) **Pub. No.: US 2007/0150299 A1**

(43) **Pub. Date: Jun. 28, 2007**

(54) **METHOD, SYSTEM, AND APPARATUS FOR THE MANAGEMENT OF THE ELECTRONIC FILES**

(52) **U.S. Cl. 705/1**

(76) **Inventor: Clive F. Flory, Arlington, VA (US)**

Correspondence Address:
**MAXVALUEIP CONSULTING
11204 ALBERMYRTLE ROAD
POTOMAC, MD 20854 (US)**

(21) **Appl. No.: 11/614,983**

(22) **Filed: Dec. 22, 2006**

Related U.S. Application Data

(60) **Provisional application No. 60/753,370, filed on Dec. 22, 2005.**

Publication Classification

(51) **Int. Cl. G06Q 99/00 (2006.01)**

(57) **ABSTRACT**

The primary design goals of the current system are (as a matter of example, but not limited to the following, by any means): to enable Organizations to send documents to Readers ensuring that only those authorized Readers can “read” the contents; to be a low cost, easy to use system, with zero to minimum installation requirements at the Companies and Readers end; to provide the service primarily as an ASP service with the ability to be easily deployed and maintained into an Enterprise environment; to enable Companies to send documents anywhere in the world and receive the same level of protection and comfort regardless of location of Reader; to provide a centrally managed, but distributed, Reader authentication and authorization method/process for all Companies to use in any country; to provide a central NDA (Non Disclosure Agreement) Registry for any size company; and to provide a secure guaranteed on-line signing process for business contracts and agreements.

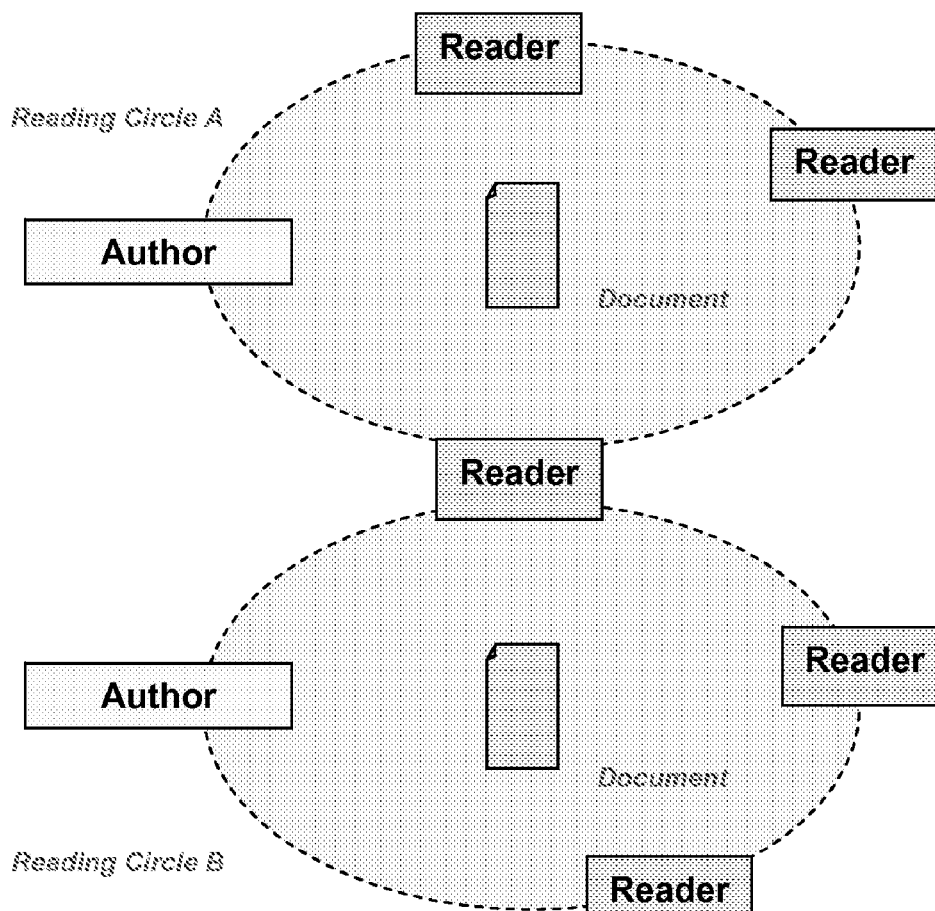


Fig. 1

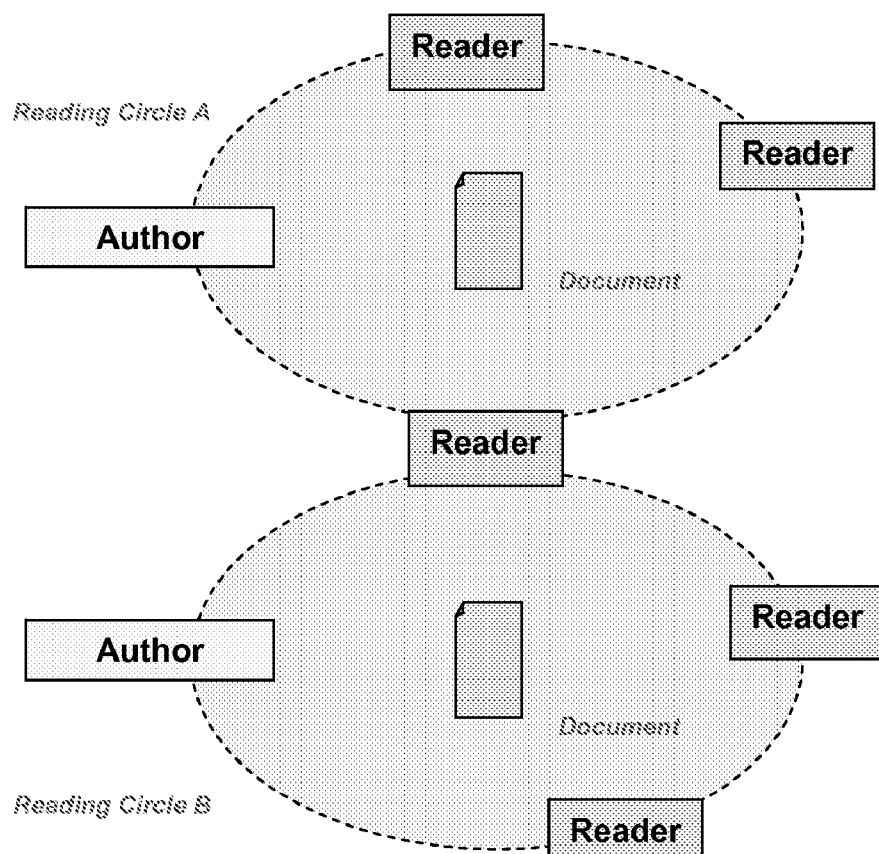


Fig. 2

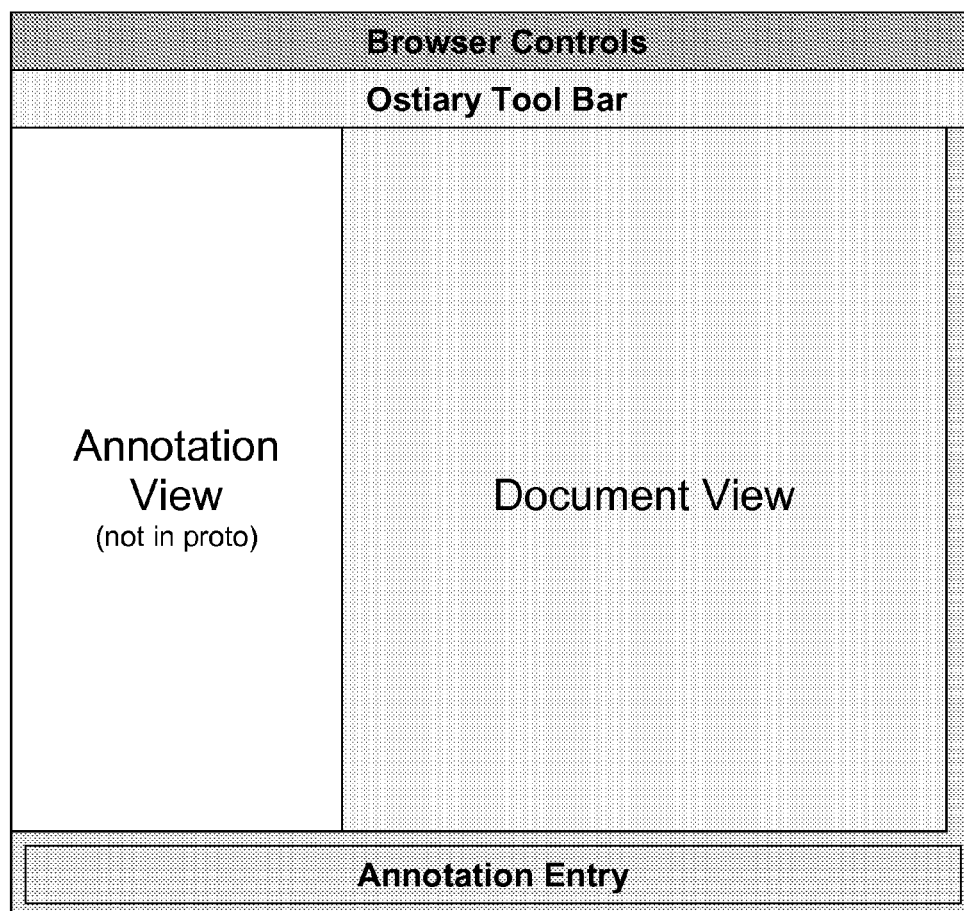


Fig. 3

The Ostiary Services

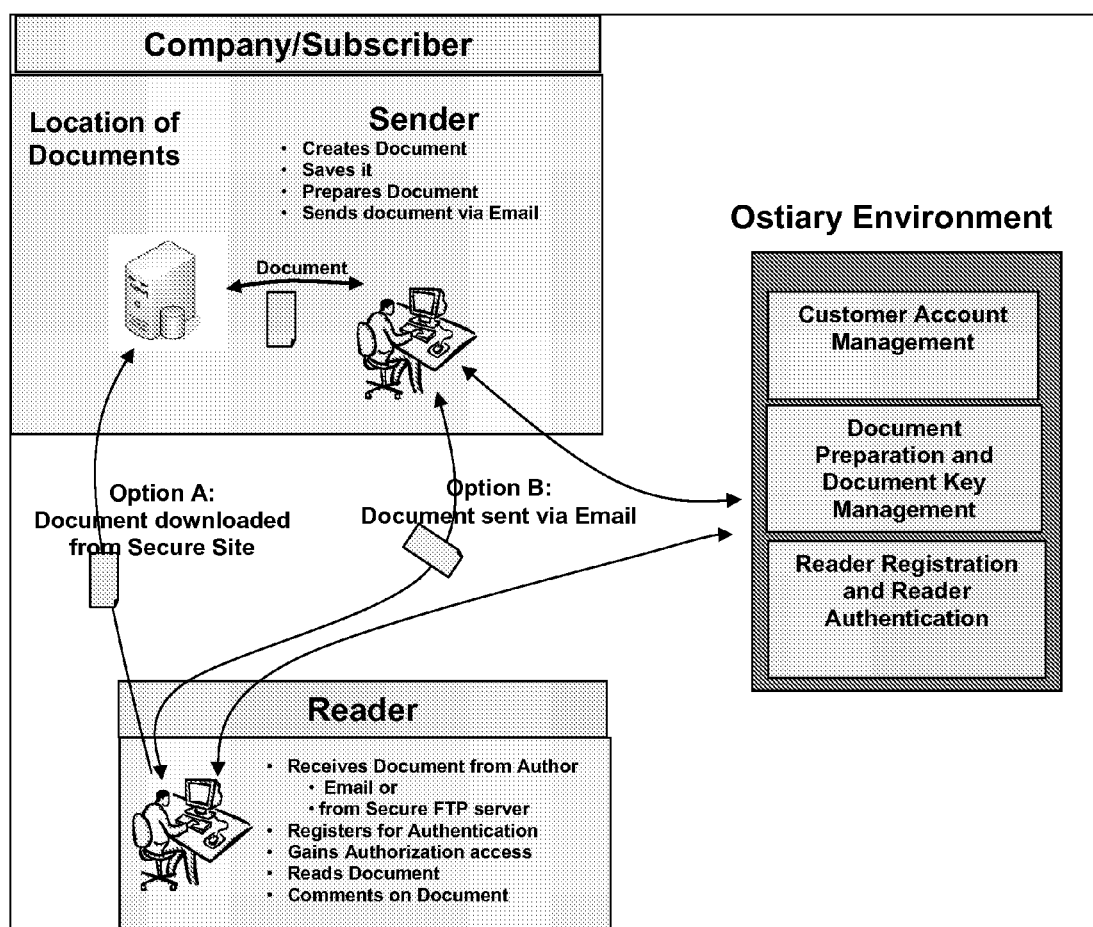


Fig. 4

All the Ostiary Service utilize the Authentication Platform.

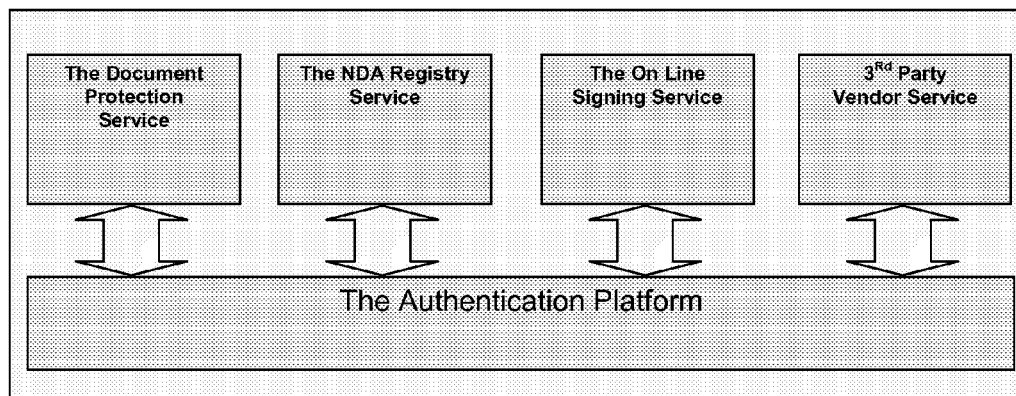


Fig. 5

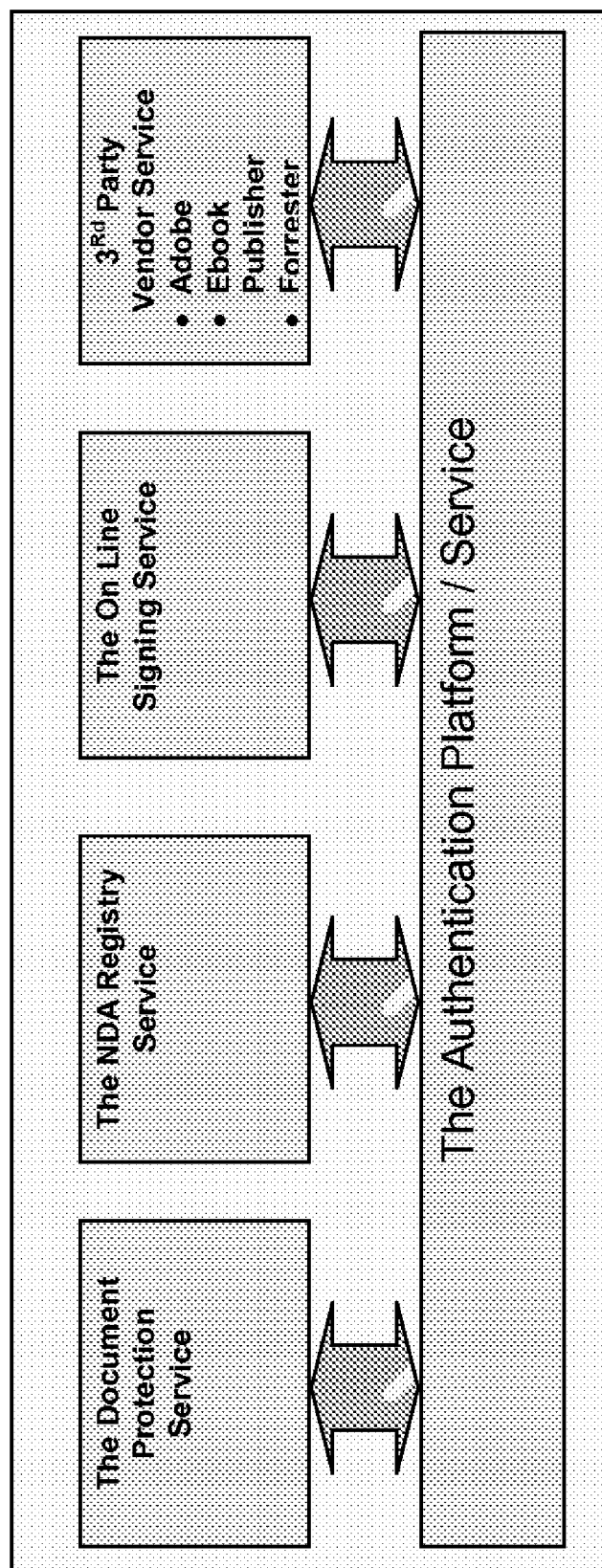


Fig. 6

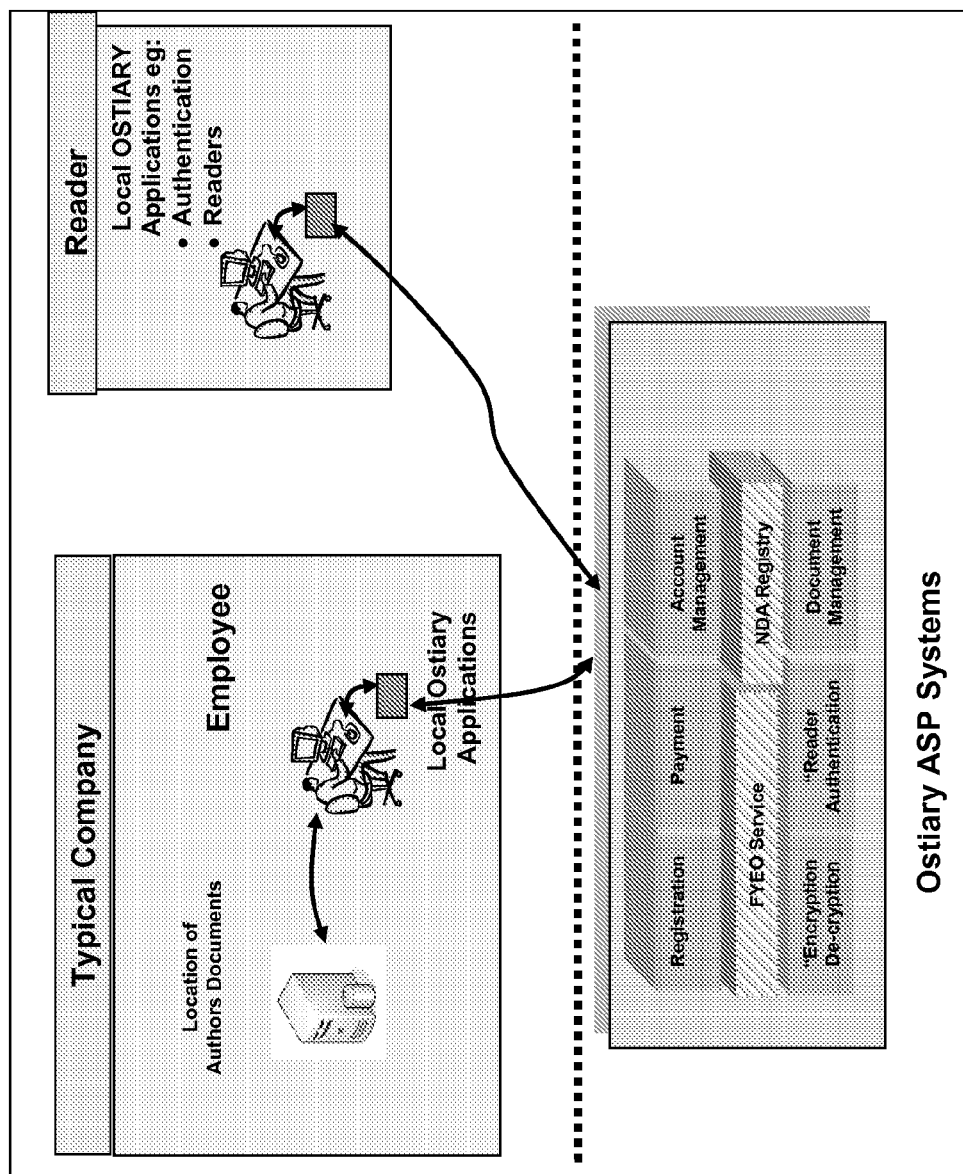


Fig. 7

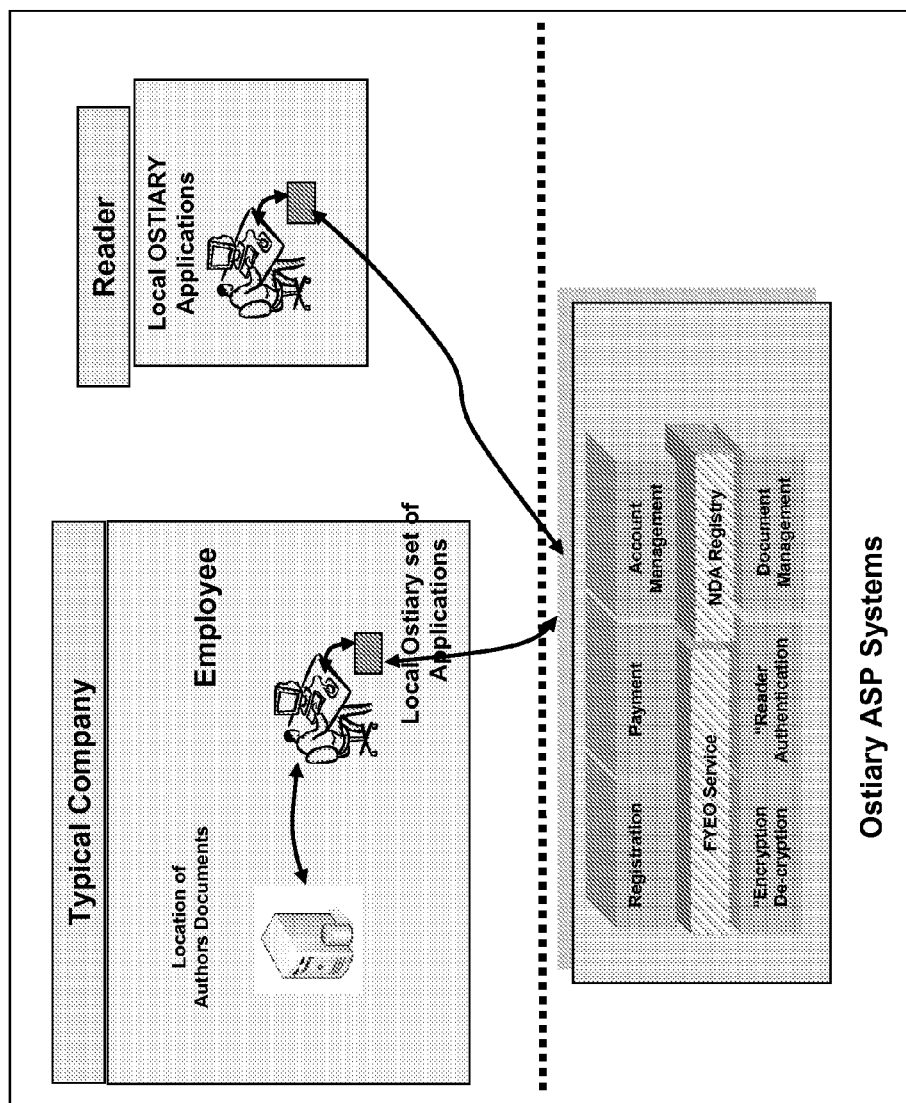


Fig. 8

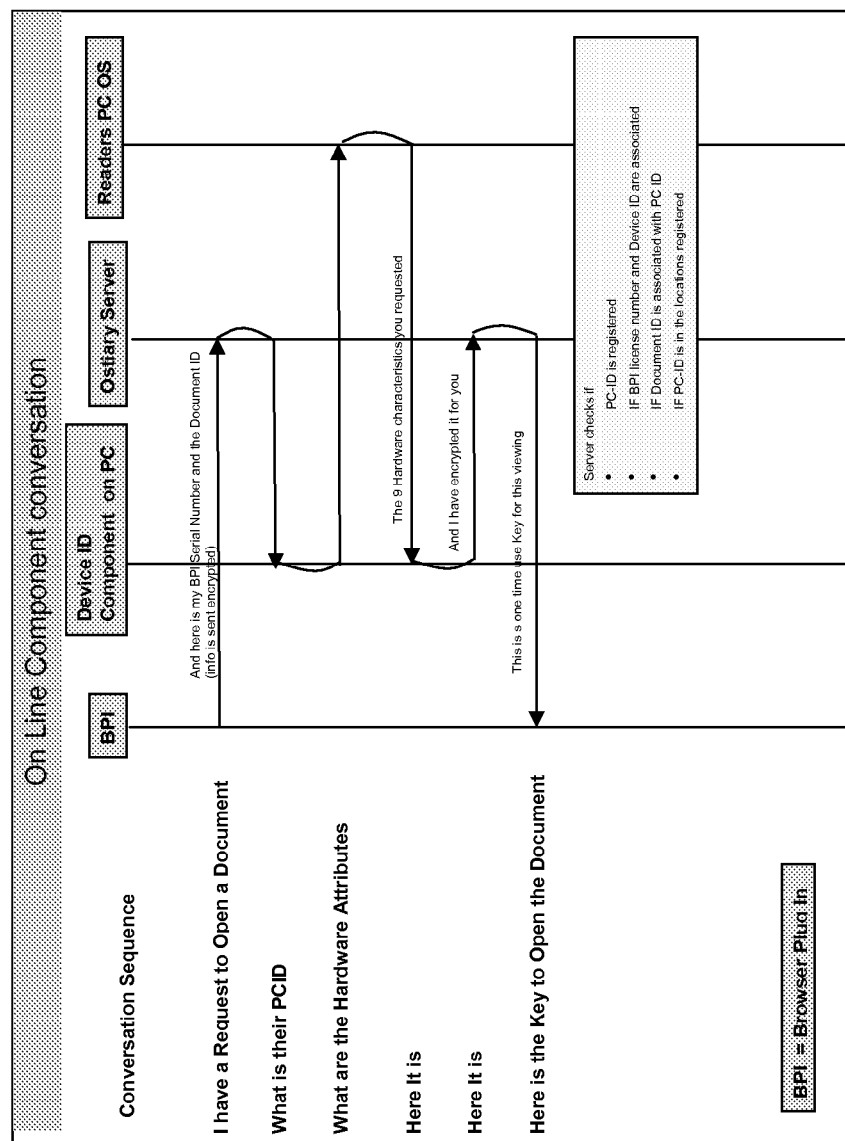


Fig. 9

Fortune 500 Environment

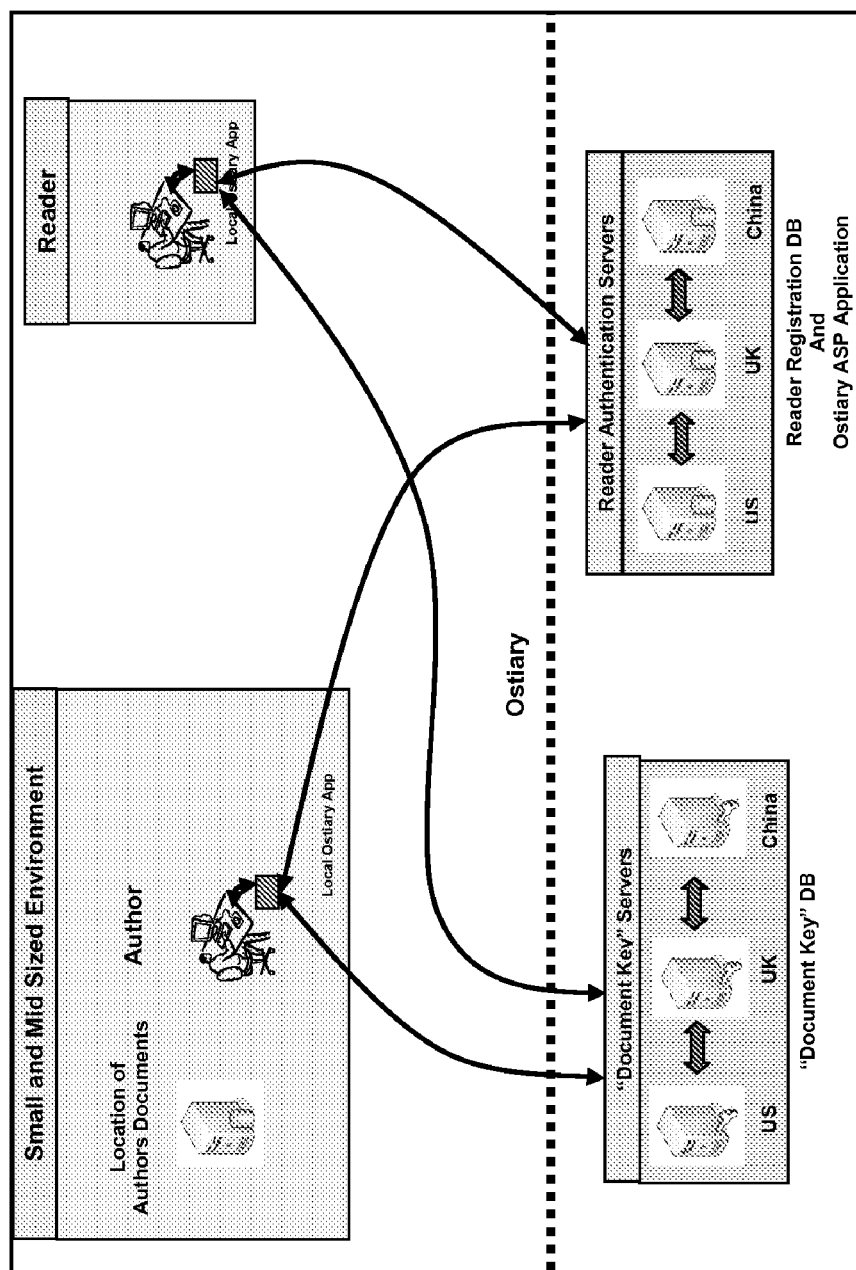


Fig. 10

Small to Mid Sized Environment

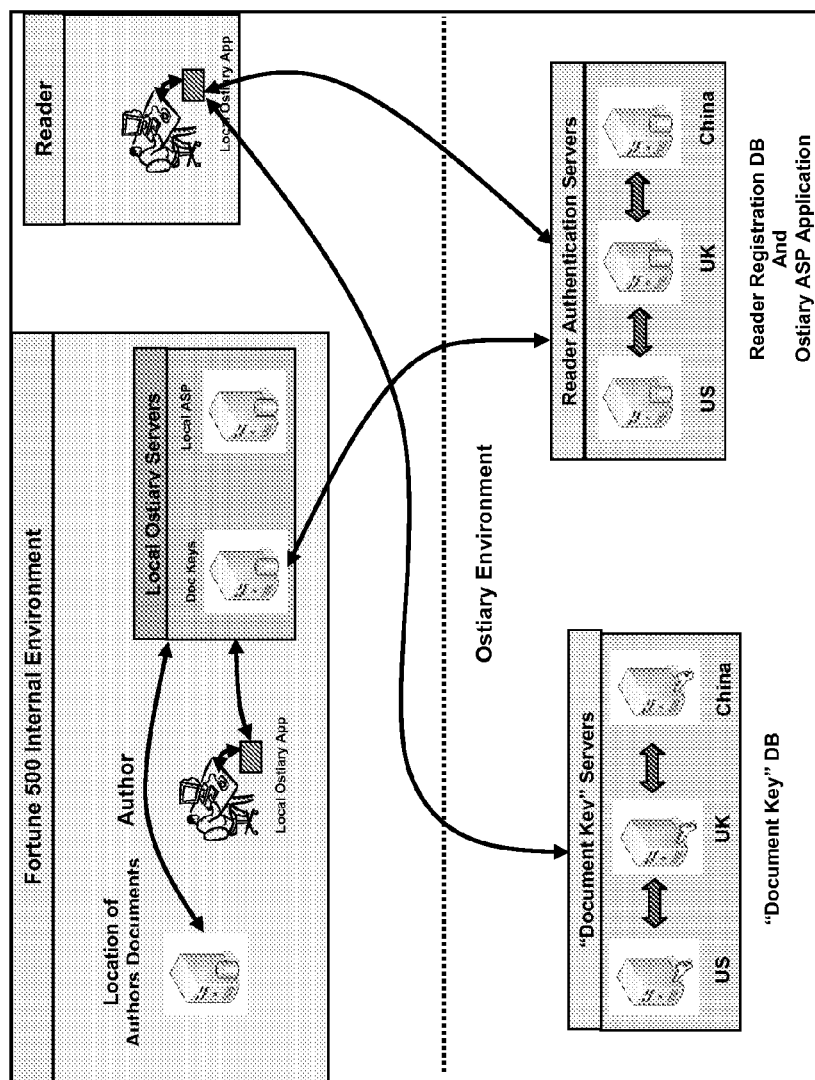


Fig. 11

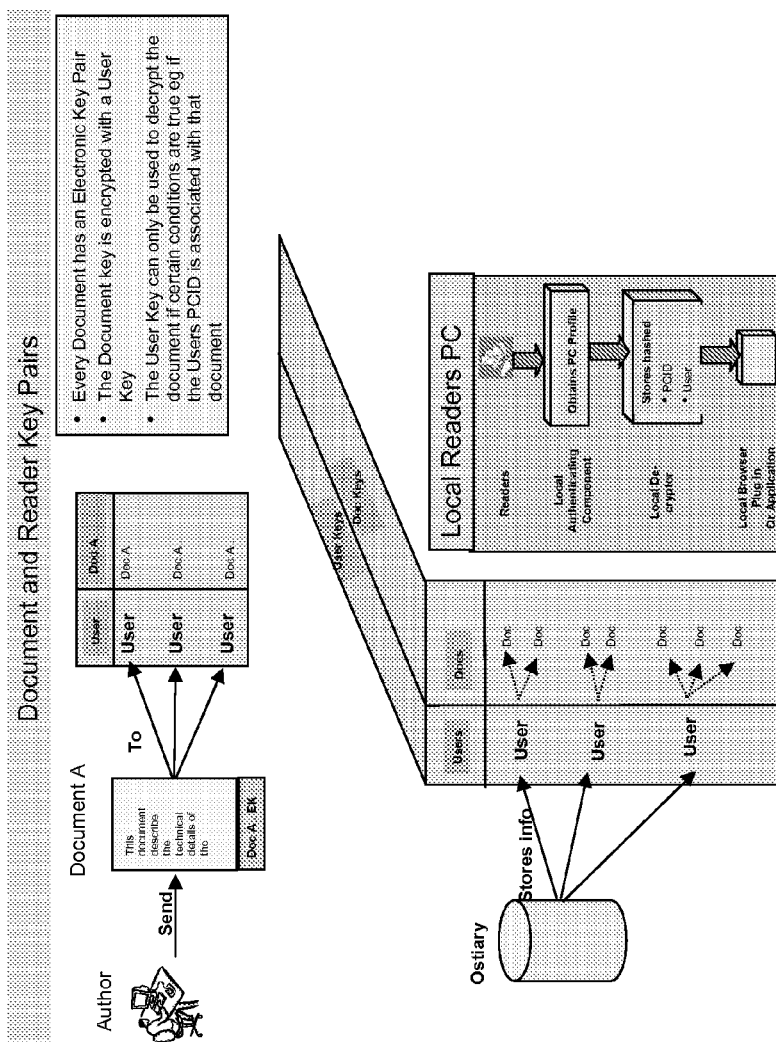


Fig. 12

Example of Screen

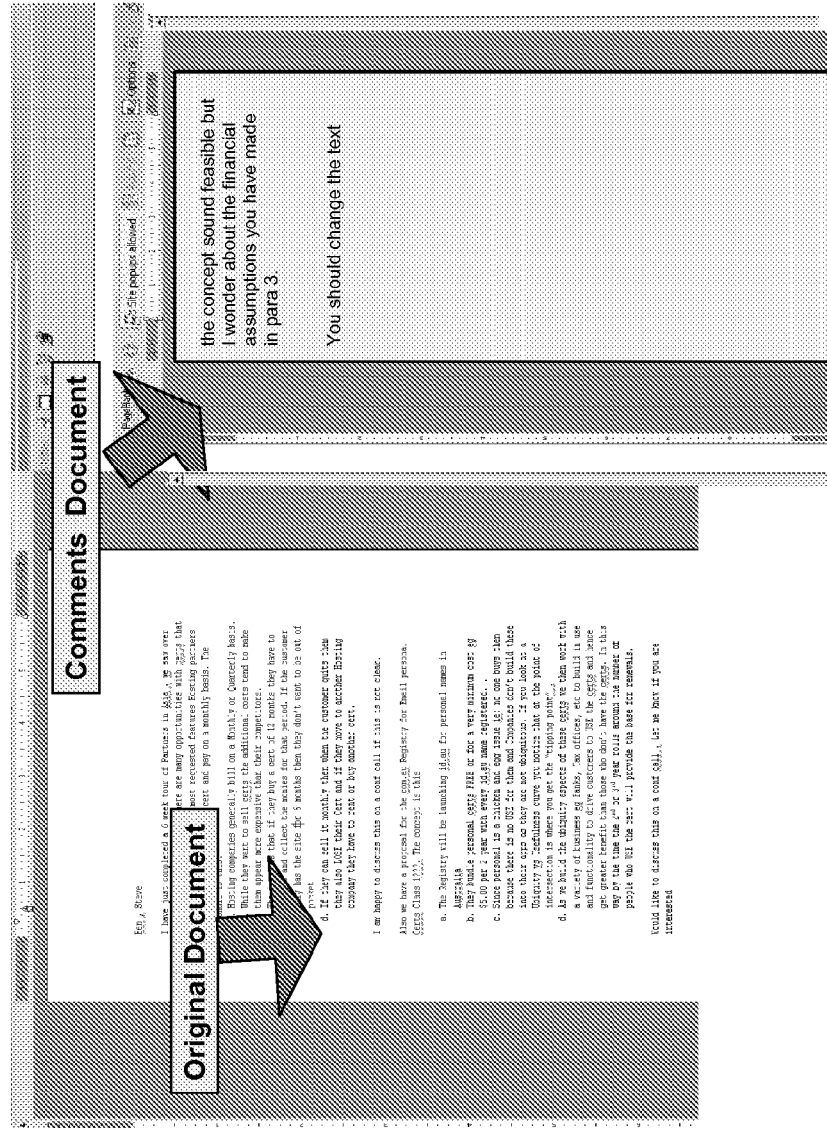


Fig. 13

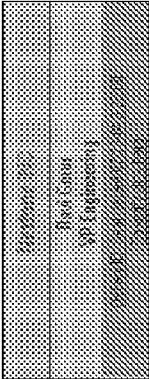
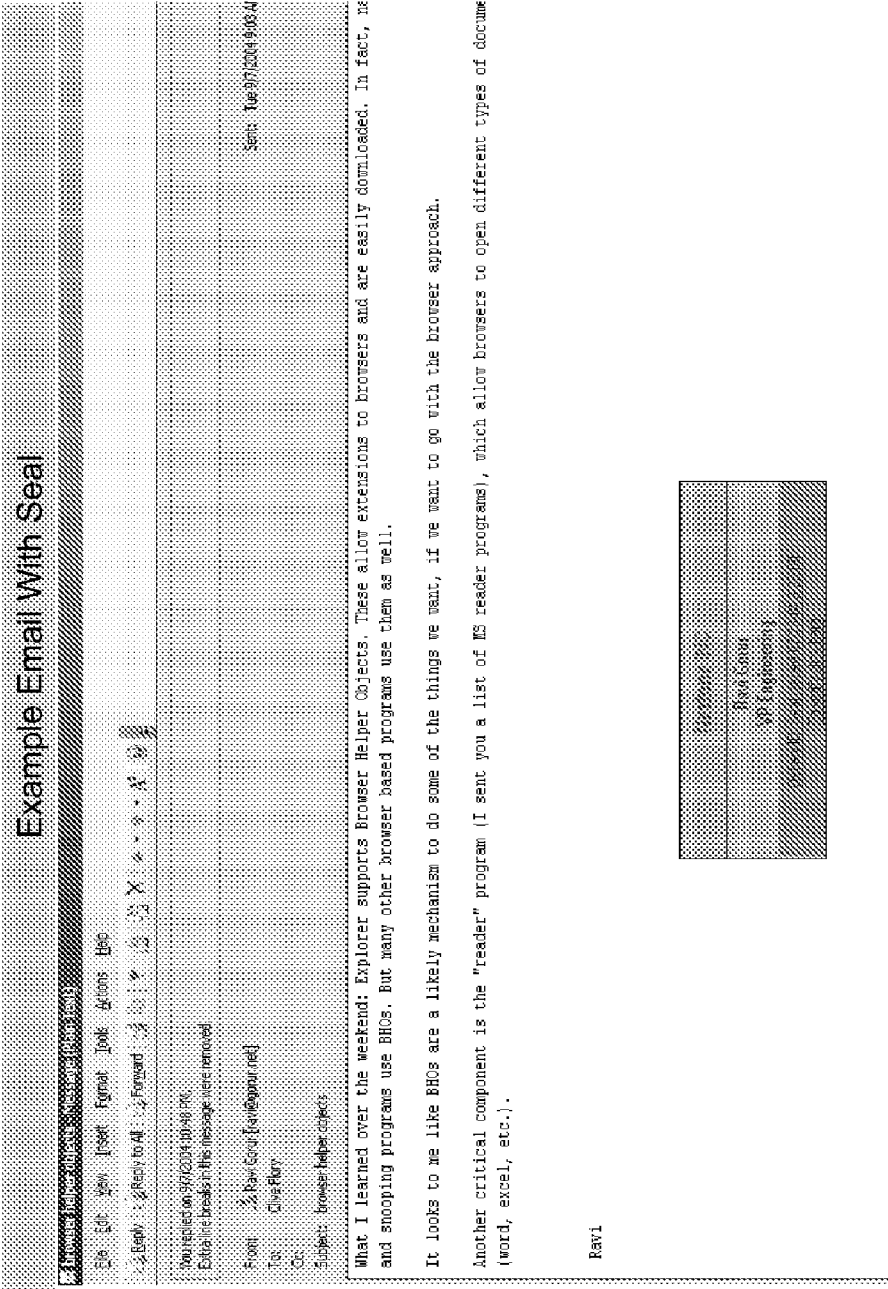


Fig. 14

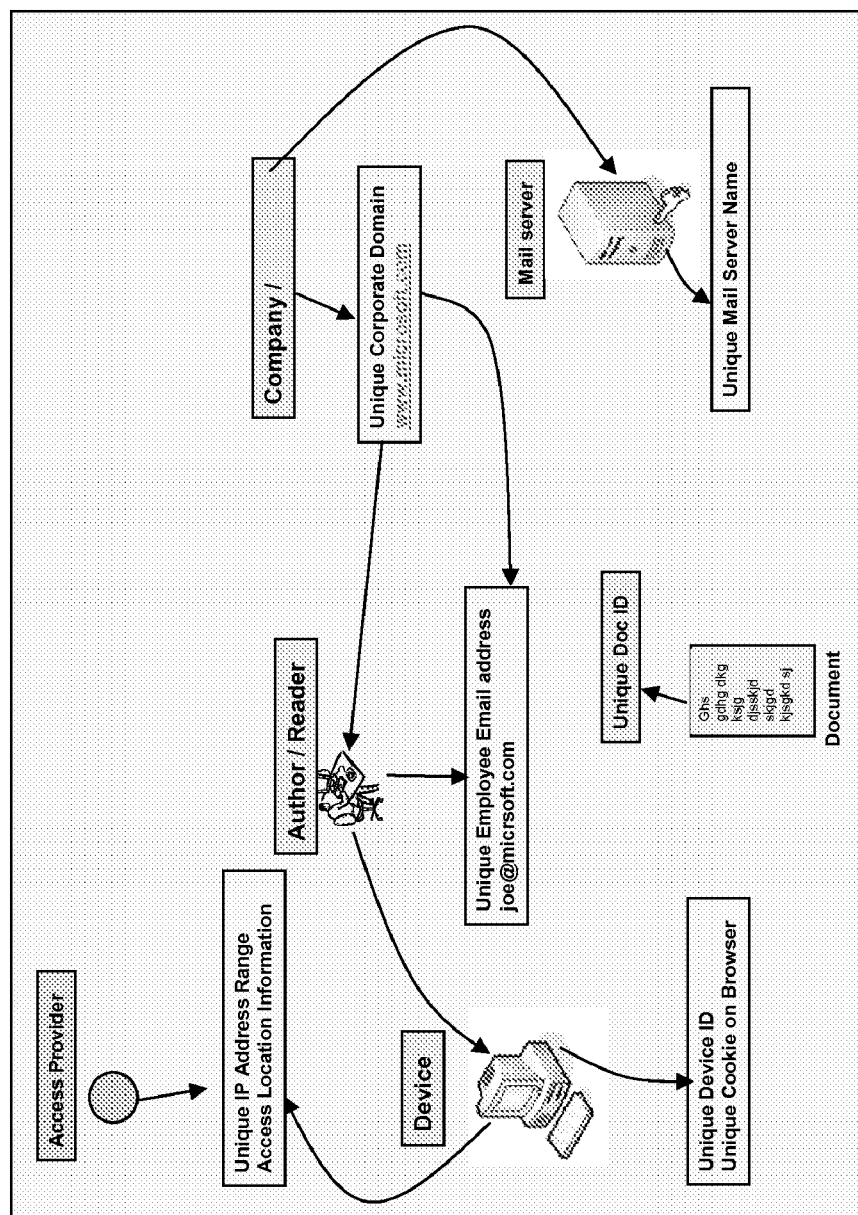


Fig 16

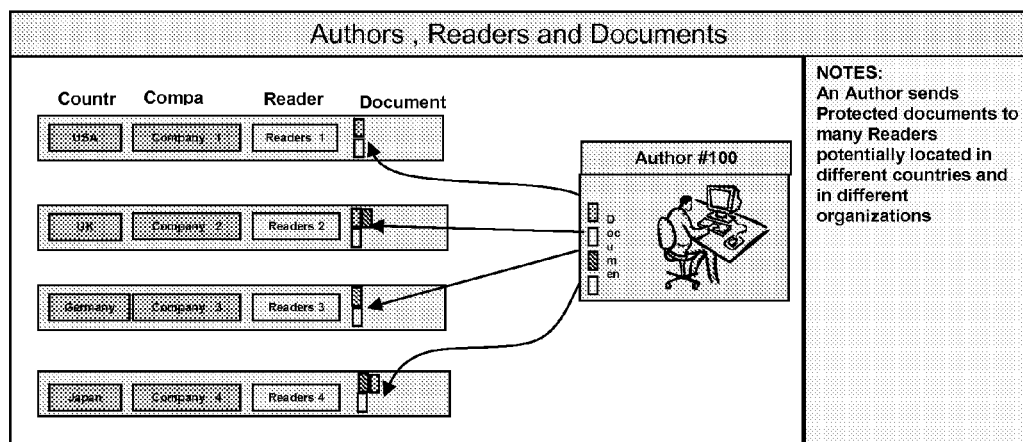


Fig 17

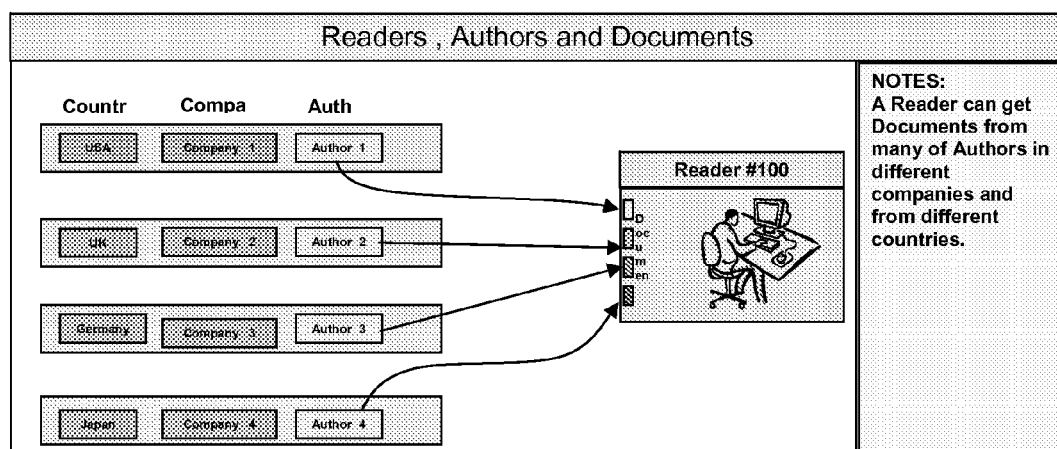
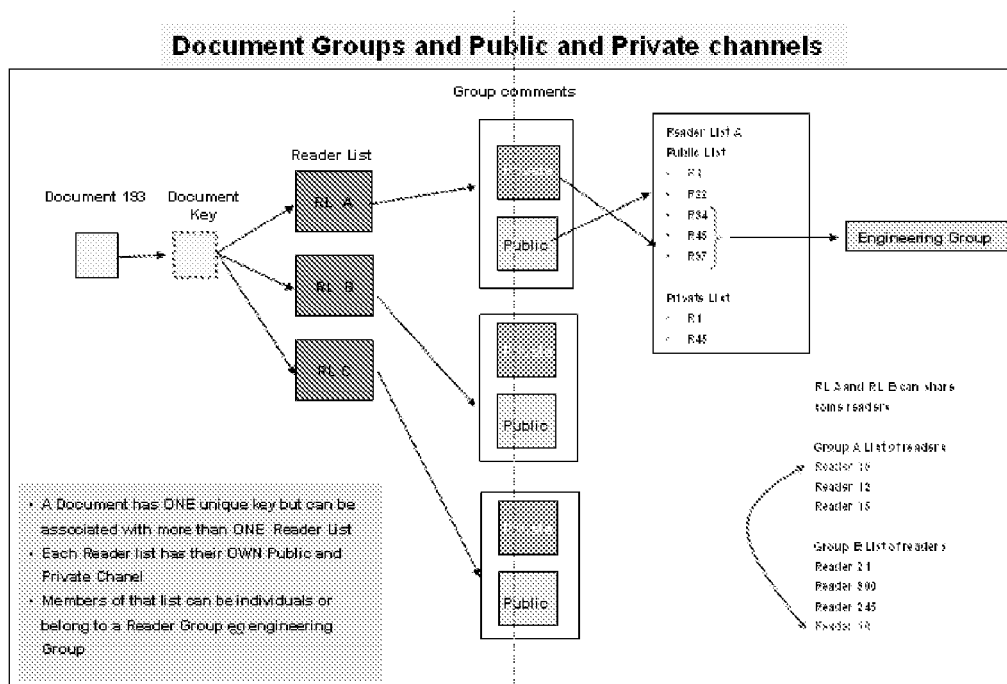


Fig 18



METHOD, SYSTEM, AND APPARATUS FOR THE MANAGEMENT OF THE ELECTRONIC FILES

RELATED INVENTION(S)

[0001] The present application is related to the U.S. provisional application, Ser. No. 60/753,370, filed Dec. 22, 2005, titled "Method and systems for network-based management of electronic files," with the same inventor and the same assignee.

BACKGROUND

[0002] The present invention relates generally to the management of the electronic files, and more particularly, to methods and systems for network-based management of shared electronic files.

The Business Problem:

[0003] Most business is conducted within a closed circle of trusted people, where the sharing of sensitive and confidential business information through the exchange of documents, a web site, an exposed business blog is a natural part of the way business is conducted. Digital documents increasingly contain the most detailed and sensitive business information so, ensuring that such documents are seen only by the intended audience, has become a major concern. This is particularly true when documents, web sites, blogs are shared between businesses.

[0004] The digital world makes For Your Eyes Only (FYEO) document security difficult to setup and maintain. Most have tackled the FYEO issue by placing sensitive documents in file systems resembling digital fortresses, made up of expensive IT infrastructure. While these fortresses succeed in preventing any unauthorized intrusions in situ, once a document leaves these safe zones, it becomes vulnerable. Password protection is not enough because passwords are often shared. Digital certificates and public private keys are not wide spread and they don't provide "continuous and persistent" protection for the Author once the document has been opened. So persistent, continuous protection of any type of document has not been fully addressed.

[0005] To address this critical problem, Ostiary has developed this technology to ensure that any document managed by the Ostiary system maintains its FYEO status, regardless of who has the documents or where in the world they reside.

[0006] Ostiary is building an easy to use and powerful Web based service to allow employees to safely share "business sensitive" digital documents such that unwanted leaks to unauthorized people are greatly reduced. Ostiary protects sensitive digital content from unwanted eyes.

SUMMARY OF THE INVENTION

What is a Business Sensitive Document:

[0007] A business sensitive document is any document created by an application such as Word processors, Presentation applications, Spreadsheets, CAD, Design apps, which contains information that only a select and authorized group should see. There is a financial risk associated with a leak of these documents.

Examples are:

- [0008] Information about a Merger or Acquisition
- [0009] A companies Financial Information
- [0010] Proprietary information shared with a corporate partner.
- [0011] Information about a NEW product Launch
- [0012] Research information around a proposed new patent
- [0013] HR/compensation Information on employees
- [0014] An Intranet Web Site

The Primary Design Goals of the System:

- [0015] To enable Organizations to send documents to Readers ensuring that only those authorized Readers can "read" the contents. This is the FYEO service
- [0016] To be a low cost, easy to use system with zero to minimum installation requirements at the Companies and Readers end
- [0017] To provide the service primarily as an ASP service with the ability to be easily deployed and maintained into an Enterprise environment
- [0018] To enable Companies to send documents anywhere in the world and receive the same level of protection and comfort regardless of location of Reader
- [0019] To provide a centrally managed but distributed Reader authentication and authorization method/process for all Companies to use in any country
- [0020] To provide the foundation of a Reader, Document delivery agent, digital Identity created from a composite of elements.
- [0021] To leverage the elements of the inherent structure of the public Internet to achieve the goals
- [0022] To provide a central NDA (Non Disclosure Agreement) Registry for any size company
- [0023] To provide a secure guaranteed on-line signing process for business contracts and agreements
- [0024] To provide an asynchronous threaded messaging system/method that links the threaded message to a document, a page in a document and a section of a page in a document
- [0025] To provide a method to segregate threaded document messages into two or more "message" channels such as Private and public channels.
- [0026] The document below separates the FYEO service from the NDA Registry Service even though at some level they are linked. Neither of these services are dependant on each other and it is envisaged that customers will take up one or the other or both: A process to ascertain the identity of a person of specific information; and ascertain the source of a document and that it has not been modified.
- [0027] The main aim of the invention is to provide an Author or publisher persistent and perpetual control on the access to their digital object creation and the rights and privileges once access has been granted. This control is governed by an authentication mechanism

- that requires the accessor to present sufficient identity elements as needed by the Author or publisher for a particular digital object to determine access rights. Once access rights are granted then the systems provides the mechanism for persistent and perpetual control of the accessor's rights and privileges during the access session.
- [0028] Furthermore the system provides the mechanism to enable Authors and publishers to allow accessors to discuss aspects of the digital object by making comments and responses to comments as threaded messages or conversations that are linked to all or specific parts of the digital object.
- [0029] Furthermore the system provides a mechanism that enables ALL participants Authors, Publishers and Accessors the means to view and manage the interactions that occur during a discussion around an object.
- [0030] Furthermore the system leverages the built up identity of a user and utilizes this to enable a digital object to be signed such that WHO signed is unambiguous. This enables the system to serve in court as a witness to a signature event
- [0031] Furthermore the system enables discussions around a digital object to be segregated into separate channels that are deemed public for all participants to see or private for a select group to see
- [0032] Furthermore the system provides a mechanism that enables Authors to manage different versions of the same original digital object
- [0033] Furthermore the system provides a mechanism that enables the Author to secure a digital object ONCE thus generating ONE unique key while enabling one or more segregated readers to have access to the digital object thus sharing the unique key while being separated by a virtual wall. Once separated ALL conversations and discussions made by the separated groups remain separated even though its around the SAME document
- [0034] Furthermore the system provides the mechanism to enable an Author to deliver the digital object and get a receipt of delivery and receipt of initial access.
- [0035] Furthermore the system provides the mechanism to alert the Author when there has been an unauthorized access attempt by a member of the Ostiary community
- [0036] Furthermore the system provides a mechanism to enable the Author AND the Readers to be notified on key events that occur around the digital object such as Who opened the object and when, Who made a comment or response and when, who signed and when, who has NOT commented
- [0037] Furthermore the system uses a Ostiary Client which can be expressed as a desktop application or a browser based plug-in provides the functionality to render or play the appropriate digital object
- [0038] Furthermore the system provides a mechanism to enable authors and readers to link digital objects to each other like citations or web sites
- [0039] Furthermore the system provides a mechanism to enable users to have access to the system regardless of how many email IDS they have or devices they use
- [0040] Furthermore the system enables an Administrator to change the Author ownership of one more object access keys without being able to access the objects themselves.
- [0041] Furthermore the system has the means to provide a network view of the relationships authors and readers have to each other through the degree if object exchange AND discussion (comment/response) intensity
- [0042] Furthermore the system provides a mechanism to enable authors and readers to have their personal address books synchronized when changes are made in any related address book
- [0043] Furthermore the system provides a mechanism to enable Readers in a circle to inherit keywords applied by the author and add their own
- [0044] Furthermore the system is able to use any type of Identity method or combination (Email ID, Password, Biometrics , digital certificates, cell phone id, USB number generator etc) as part of the authentication process
- [0045] Furthermore the system enables a federated approach to the authentication of users so identity servers can be distributed and managed by one or many groups including corporations themselves
- [0046] Furthermore the system enables a federated approach to managing digital object keys so keys can be managed by groups that generate the object keys such as corporations
- [0047] Furthermore the system enables the federated approach to managing the comments response messaging threads so these threads can be managed by groups that generate the message threads for the digital objects that they control
- [0048] Furthermore the system provides the mechanism to move a threaded conversation from version to version of a digital object
- [0049] Furthermore the system manages the registered Authors and readers as part of a community
- [0050] Furthermore the system has a mechanism that enables 2 or more participants to share the simultaneous viewing of a document inside the Ostiary viewer where one of the participants has the control of the document and controls the changes, actions, movements of the document that others can see, similar to a proxy for the other one. The action of one is displayed simultaneously in another site, as well. The history of the interactions is expressed in a network of the relationships.
- [0051] The frequency of interactions for one or more documents is expressed as the intensity of the relationships, and over time, for each person, we will have a network of the relationships. (shared network)
- [0052] In a document, at the comment level, the more comments one has for another person, the stronger the

communication relationship becomes between those two people. (Communication Network)

- [0053] When an author creates a web log or a document, the frequency of the usage of the keyword is an indication of the interest level for the author with respect to that subject matter. This can be used for citation, labeling, or categorizing, which can be used for many purposes, such as marketing.
- [0054] Classification can also be done for two or more keywords sharing some basic or fundamental concepts, based on the proximity of those concepts, e.g. to be able to classify the blogs.
- [0055] Dashboard reflects the history and activities. In particular, it is dynamically changing. For example, if a comment comes in, the item goes up in the list.
- [0056] Furthermore users in a shared conference and pass control to participants in the conference
- [0057] Furthermore the system has the mechanism to apply user created keywords to a digital object to enable grouping objects around those keywords
- [0058] Furthermore the system has the mechanism to enable participants of a shared object to share inherit the Authors keywords
- [0059] Furthermore the system has the ability for a group to expose and analyze the social interactions that arise from the shared objects
- [0060] Furthermore the system has the mechanism to expose the intensity of the interactions a user has to the System, a group, a organization to individuals
- [0061] Furthermore the system has the mechanism to display all a users activity in a dashboard that dynamically displays the changes to the states of the secured objects as they occur
- [0062] Furthermore the system has a mechanism to keep the location of a digital object and use this information wherever needed
- [0063] Furthermore a digital Object Key is linked to one or more of a user's Identity Elements. The primary and initial identify element is a users email ID
- [0064] Furthermore the system has the mechanism that enables an Author to let other Readers ADD additional readers to a secured Digital object
- [0065] In a complex situation, one may have many e-mail accounts or devices, for example. To better manage those, it is easier to correspond the unique physical attributes of a user to the many digital attributes and multiple accounts.
- [0066] Another important feature is the concept of Team-Mail, in which there is only one copy of the e-mail stored for all the recipients or users. Thus, this saves a lot of disk space. Also, there is less confusion about the version of the e-mail. In addition, the user can start from any thread in a sequence or responses, displayed in an orderly manner, and everybody else can do the same. Therefore, the size of the thread does not increase exponentially, like in a conventional e-mail. Thus, the organization is much more superior to the conventional e-mail. Inherently, the Team-mail is very secure, in that it cannot forwarded arbitrarily to a third party. Thus, our system can benefit from all of those inherent secure features.

[0067] For example, in case a person is included in a list of e-mail recipients, in the conventional e-mail system, there is no way to recover from that mistake, from the provider's point of view. However, in our system, this can be done easily, by removing the name of the wrong recipient from the list of the Team-mail (i.e. removing the access for that person), even if the mail has already been opened.

[0068] Note that services, rights, documents, and contents, each or all, can have hierarchical structure or composite structure. The rights can be delegated to others. The rights can expire or withdrawn. The service can include some codes that are executable, and can do a function or a task. The rights can be assigned based on role or context, such as in a company, for example, the CEO's rights. The database can hold the rights and name of entities involved.

BRIEF DESCRIPTION OF THE DRAWINGS

[0069] FIGS. 1-3 show the overview of the system.

[0070] FIGS. 4-8 show the details of the components of the system.

[0071] FIGS. 9-18 show some applications, examples, and details of the system.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

An Overview of the Ostiary System:

[0072] The following is a brief introduction and overview of the Ostiary System:

The fundamental Objects in the System:

[0073] The Ostiary set of services deals with the following fundamental objects that are the

Primary objects in the overall system:

[0074] Organization (sending and receiving)

[0075] People

[0076] Senders: Employees of Organizations that send documents

[0077] Readers: Authorized People that receive documents etc to read, comment, sign etc

[0078] Digital objects such as Business Documents (legal contracts, Engineering Specifications, Business Plans, Financial Spreadsheets), Music files, Video files, Web sites

[0079] Devices that are used to access, and ultimately read, play, view these digital objects. Such as :Laptop PCs, Desk Top PCs, Hand Held devices, and Cell phones,

[0080] Readers Digital IDs . This is an ID made up of a composite of elements, such as

[0081] Device characteristics used to Read the documents

[0082] The official Email addresses of the Reader Employee or their personal address.

[0083] Location of Readers

[0084] Physical characteristics such as Fingerprint

What Triggers the Need for such a Service?

[0085] Essentially the services start when an Organization has a need to send someone a Document or file or web site that requires:

[0086] a. authentication prior to access, or/and

[0087] b. On going protection from unauthorized Access

[0088] But before a document can be sent, it has to get Ostiarised, i.e. the process of:

[0089] Registering the document

[0090] Registering its authorized Readers

[0091] Encrypting the document

[0092] Establishing the documents access and usage policy

[0093] Setting the Notifications

[0094] Setting the documents keywords

How does the Service Start?

[0095] Before anything happens, an organization has to be a Registered as a subscriber to the service.

How does an Organization Register for Service?

[0096] To register an Organization, it goes to the www.os-tiary.com web site and goes through the New Organization Subscription Process. Once the Origination has been registered, then their employees can be registered for use.

How do Employees Register to use the System?

[0097] To register, an Employee will go to the www.os-tiary.com web site and go through the

New Employee Registration Process.

[0098] Once the Origination has been registered then their employees can be registered for use. Once the Employee has been registered then they can start to use the Ostiary system to Protect their documents

How is the Document Protected?

[0099] The digital objects or document delivered is never in its native form but has been processed in a way that enables only authorized Readers to:

[0100] Open the document

[0101] View the contents

[0102] Make Comments

[0103] Sign

[0104] Approve

[0105] The process of protecting the document is called "Ostiarising the document", and essentially, it is a process that does the following:

[0106] Encrypt the document and generate the document keys

[0107] Compress the document

[0108] Generate a copy with a .ots extension e.g. "My Document.doc gets a My Document.ots generated"

[0109] Once a sensitive document is protected then it can be sent to Readers for use.

Who can Read these Documents?

[0110] If a document is sent out to a Reader they will not be able to read the document unless they are registered by the Author in the Ostiary system as being authorized to Read such document.

How is "Authorized Readership" Registration Done?

[0111] When the author secures a document the "list of Authorized readers selected get registered at the time of securing

[0112] If an Author wants to ADD a new reader they add then at any time after the initial Securing of the document

[0113] If an author wants to remove a Reader they can remove the reader at any time after they have secured one after the reader has received and opened the document:

How does the Reader get the Document?

[0114] The way a Reader gets the document is by

[0115] An Email transmission by the Sender with the document attached using any email system

[0116] Picking up the file from some server where the reader has access

[0117] The System delivering it directly to a Readers email

How will a Reader Read an Ostiarised Document?

[0118] To be able to read a Ostiary secure document that a Reader has received, the following conditions have to be true

[0119] STEP 1: The Reader has to be listed as an authorized reader for that particular document. This list is always established by the Author

[0120] STEP 2: The Reader has to have the necessary Ostiary software and components installed on their device (PC, Blackberry). Typical components are

[0121] local Authentication component

[0122] the Reader/Player application

[0123] STEP 3: The Reader and their Digital ID has to be a registered in the Ostiary Authentication System

[0124] Step 1 will be performed by the Sender.

[0125] Steps 2 and 3 will be performed by the Reader in that sequence.

How does the Reader get Registered in the Ostiary Authentication System?

[0126] When a Reader is invited to view a Digital Object this triggers a registration process for them

How does the Reader Get Initially Authenticated AND How does their Digital ID get Generated?

[0127] The Readers initial Authentication Process involves the generation of their Digital ID.

Can a Reader make Comments on a Protected Document?

[0128] The rights to make comments on a document are controlled by the Author. The system provides a mechanism to enable this .

What is the CORE Business Process in the Ostiary System?

[0129] The CORE business process is as follows:

- [0130] a. Selecting an Object to be protected This is done by the Author/Publisher
- [0131] b. Adding a list of Authorized users from an Address book
- [0132] c. Setting the rights and privileges for the list of authorized users
- [0133] d. Setting the Keywords for the digital object to enable easy search
- [0134] e. Setting Notifications to enable notifications on events around a specific Digital Object
- [0135] f. The Reader Registration process, Software Installation and Reader ID creation process.
- [0136] g. The Authenticating a Reader process when they try to open a document

System:

[0137] FIGS. 1-3 show the overview of the system. FIGS. 4-8 show the details of the components of the system. FIGS. 9-18 show some applications, examples, and details of the system. The details are described below.

[0138] Our system, the subject of the current invention, the Ostiary ASP, delivers the following services through the web:

Document Services:

- [0139] 1. Allows the safe and secure sharing of documents of all common types, distributed by Authors, to an authorized set of Readers defined by the authors.
- [0140] 2. Prevents unwanted copying, printing, or otherwise sharing of these documents by authorized Readers.
- [0141] 3. Allows users (Readers and Authors) to sign documents to provide a mechanism for on-line document acceptance by authenticated users.
- [0142] 4. Allows Authors to track documents through an audit trail. Supports non-repudiation as part of the audit mechanism.
- [0143] 5. Allows Authors to set privilege policies on a per document basis. These include settings for access period, access count, etc.
- [0144] 6. Uniquely identifies every document and provides a simple versioning system. Allows the automatic notification of the availability of new versions to Readers.
- [0145] 7. Allows document annotations and the secure sharing of annotations by authors and readers.

Definitions:

[0146] Users: All users of the Ostiary system are registered, identified by email address and password and have at least one associated PC/device ID. The Ostiary client must be installed on the registered user's device(s). Ostiary associates the user with this device(s). The Ostiary Client is capable of providing all (or some) services.

[0147] Ostiary Browser Ostiary Client (OBP): A special browser based program that delivers all document services to Authors and Readers.

[0148] Ostiary Password: All access to the Ostiary system requires a password. Ostiary Documents: documents of all common types (Word, Excel, PowerPoint, HTML and PDF) identified, encrypted and specially packaged by the Ostiary System for restricted access by a Reading Circle.

[0149] Accounts and Account Holders: Registered Users with subscription services (those that require payment) belong to accounts and are Account Holders. An Account may include multiple registered users. An Account has billing information (name, address, etc.). The Registered User that opens the account is automatically the administrator of the account and can add/delete other Account Holders.

[0150] User Roles: A Registered User is capable of the following roles.

[0151] Author: A role restricted to Registered Users that are Account Holders. An Author has publishing and signature privileges. Publishing allows authors to secure documents through Ostiary encryption and distribute the document to any number of authorized Readers (see below). Signature privileges allow authors to sign documents.

[0152] Reader: A role for Registered Users that may or may not be Account Holders. A reader has the privilege, assigned by an Author, to view a document.

[0153] Note that an Account Holder may be an Author and/or a Reader.

[0154] Reading Circle: The group of people with authorized access to one Ostiary Documents (for simplicity at this point, we will assume one document per Circle, but it can be more than 1 documents.). The group is comprised of one Author and zero or more Readers admitted by the Author to the circle. The author determines the privileges for document access by readers. Note that a user who is an Account Holder may play an Author role in one Reading Circle and a Reader role in another Reading Circle.

[0155] Authenticated Users: Ostiary will validate registered users on every access to the server; i.e., this is the on-line state of a registered user that has access to system services (document protection, etc.).

The System Supports the Following Setups:

[0156] 1. Setup

[0157] a. An Ostiary Server (PC).

[0158] b. Two or more Ostiary User-Devices running Windows.

[0159] c. One PC, running Windows, used as the Author's User-device. This device is pre-loaded with the Ostiary Browser Ostiary Client and connected to the server via a LAN. The Author has been registered into the Ostiary system.

- [0160] d. Two PCs, running Windows, used as Readers' devices, connected to the server via a LAN. One of these devices is not registered into the system (no Ostiary Plug-in). This is the Target Reader. The other is registered: this is the Invalid Reader.
- [0161] 2. Author prepares the document through the plug-in
 - [0162] a. The Author logs into Ostiary, through Explorer/plugin.
 - [0163] b. A document on the Author-device is selected for preparation
 - [0164] c. The Author follows a wizard driven process to prepare the document
 - [0165] i. The Target Readers is defined with email addresses (one reader is entered)
 - [0166] ii. The Document security settings are set (non-operational)
 - [0167] iii. The prepared document is saved
 - [0168] d. The prepared document is emailed to the target reader (this reader is NOT registered).
- [0169] 3. Target Reader (not registered), saves document from email. He opens the document (must be connected to the server).
 - [0170] a. Explorer is invoked. The browser notifies the user that the Ostiary Ostiary Client is required and must be downloaded from a specific location (server).
 - [0171] b. The user downloads the browser plug-in.
 - [0172] c. The Ostiary Client then uses a wizard process to take the user through the registration process including password.
 - [0173] d. Once complete, the Ostiary Client gets the document key from the server and allows the Reader to view the document.
 - [0174] e. The Reader will not be able to cut, copy or print the document.
- [0175] 4. Invalid Reader
 - [0176] a. The Target Reader forwards the document (encrypted) to the Invalid Reader (who is already registered).
 - [0177] b. The Invalid Reader opens the document.
 - [0178] c. The Ostiary Client immediately warns the user that he is not authorized to view the document. The Ostiary Client also asks the reader whether permission from the Author should be obtained. The Reader responds with a "yes".
 - [0179] d. The server delivers an email to the Author with the request to authorize the new Reader.
 - [0180] e. The Author Responds to the email with a Yes.
 - [0181] f. The Invalid Reader is delivered the Keys to allow him to view the document after password entry.

Document Requirements

- [0182] Prepared documents have the following properties:
 - [0183] 1. HTML formatting/wrapper
 - [0184] 2. Document image clear-text is encrypted and embedded within the wrapper
 - [0185] 3. Embedded document image is uniquely identified. This is sent to the server by the plug-in.
 - [0186] 4. Image (document converted to image)
 - [0187] a. Includes "Powered by Ostiary" Header, timestamp, author, etc.
 - [0188] b. Includes watermark, under control of Author (HTML background)

Ostiary Client Requirements

- [0189] The Ostiary Ostiary Client performs the following functions for all users (Authors and Readers)
 - [0190] 1. Registration of the user: this establishes the device/user linkage.
 - [0191] 2. Password protection for Ostiary document viewing and server access
 - [0192] 3. View user information delivered from server on web pages
 - [0193] 4. Tool bar for document viewing and preparation (authors)
 - [0194] 5. Document viewer:
 - [0195] a. Page up/down (tool bar buttons and keys)
 - [0196] b. Support for scrolling with scroll wheel and up/down arrow keys
 - [0197] c. No Cut/Copy functions
 - [0198] 6. Annotation capability
 - [0199] 7. Disable Browser Print operation
 - [0200] 8. Author Specific requirements
 - [0201] a. Document preparation (wizard)
 - [0202] b. Document control: disable, add users, etc.

Document Services

- [0203] Document services are initiated by Authors and spread to the Readers within a Reading Circle. All services around a document require an Author.

Overview of Document Services

Protection and Distribution

Document protection and Distribution is Delivered as Follows:

- [0204] 1. Preparation phase:
 - [0205] a. An Author prepares a document through the Ostiary Browser Ostiary Client (OBP). This operation requires login to the Ostiary Server and authentication (must be connected to the Inter/Intranet).
 - [0206] b. The Author defines the Reading Circle: the Author is the first and default member. Readers are

included by the author listing their email addresses with one of the following mechanisms:

- [0207] i. Typing in the list of specific addresses via a web-page on the Ostiary server. Optionally, the user may type a domain address which allows all Users with the domain address access.
- [0208] ii. Picking from an Author pre-defined list of Reading Circles on the server web-page.
- [0209] iii. Passively collecting a list of email addresses from the "To:" field on an Outlook email with the Ostiary Document attachment: this will require a special Ostiary Client on Outlook.
- [0210] iv. Other mechanisms.
- [0211] c. The Author defines if this is a new version of an existing document.
- [0212] d. The Author defines document privileges in the Reading Circle (associated with the document):
 - [0213] i. Printing: No by default
 - [0214] ii. Cut/Copy: No by default
 - [0215] iii. Days of access: unlimited by default
 - [0216] iv. Off-line mode: No by default
- [0217] v. Annotation Mode:
 - [0218] 1. No Annotation (default)
 - [0219] 2. Author only: author receives all annotation entered by Readers, not viewable by Readers (except that the originator can view his annotation).
 - [0220] 3. Full Circle: all members view/edit annotation.
- [0221] e. The document is stored in some location desired by the Author. Optionally, the Author may define a link that points to the public location of the protected document (a document server) for use during versioning.
- [0222] 2. Once preparation is complete, the author may send the prepared document by email to the Reading Circle. Any user defined in the Reading Circle as a Reader will be given access to the document once the Reader has been authenticated by the Server when the user trust to open the document. The User/Reader must be connected to the Inter/Intranet and login to the Ostiary service for the authentication process.
- [0223] 3. Any additional users included on the distribution list, initially or later, will require an additional authorization step by email, as follows: if a user, not in the Reading Circle, attempts to view the document:
 - [0224] a. The Server initially denies access to the user, indicating that the Author must allow access
 - [0225] b. The Server sends an email to the Author requesting that the user requests to be a Reader (i.e., part of the Reading Circle)
 - [0226] c. The Author accepts or declines the user into/from the Circle, via a response to the email (clicking "yes" or "no" link)

- [0227] d. The Authors decision is forwarded to the User requesting access. If accepted into the Circle, the Reader may access the document.

[0228] Note that Ostiary does not store the document on the server. All encrypted documents are stored by the user.

Document Services

[0229] The following services are provided on a per document basis.

Versioning:

- [0230] 1. Each document is identified with a unique fingerprint (digest). Ostiary allows the Author to define document versions based on the unique fingerprint.
- [0231] 2. When on-line Readers access an old version of a document, they are warned by the system that a new version is available. The system will provide the user with a URL where the NEW version can be downloaded .

Annotation:

- [0232] 1. The Ostiary Client allows the users in the Reading Circle to add annotation notes alongside the document.
- [0233] 2. The annotation is collected and displayed to the Author or all members of the Circle by the server. The server performs the annotation information exchange; therefore, online access is required to retrieve annotations.
- [0234] a. Is offline annotation entry allowed? Yes.
- [0235] b. Are annotations securely stored and transmitted? Yes.
- [0236] 3. The display of annotation is through an Ostiary client (desktop or browser based). Annotations are location sensitive: they are associated with a particular cursor position in the document. They are displayed on a per-page basis. Entry is through a third smaller text entry field.
- [0237] 4. Once saved, annotations are transmitted immediately. The server stores and forwards the information.
- [0238] 5. Annotations may be deleted/modified by users who enter them. Thus the server presents the "latest" version of comments. An audit trail is not maintained. Watermarks and other overlays can also be used.

The Ostiary Client

[0239] The Ostiary Client can be expressed as a desktop application written in any language as well as a Browser plug in or a Ajax based client. It provides all services to the Author and Reader. Regardless of method of construction the Ostiary Client provides the following

- [0240] 1. Registers Readers
- [0241] 2. Authenticates users with Server support .
- [0242] 3. Encrypts and prepares documents with server support.
- [0243] 4. Decrypts and digitally protects documents.
- [0244] 5. Prevents cut/copy and print (as configured)

[0245] 6. Allows entry and viewing of comments, responses and annotation

[0246] 7. Allows signature operations

[0247] The Ostiary Client creates multiple frames. The annotation and document view frames are operated with a single scroll-bar. Annotation entries are identified by users.

[0248] The Ostiary Security Infrastructure:

[0249] The Ostiary Security Infrastructure contains 5 logical Pillars that act as the foundation for all current or future services. The five pillars are:

TABLE 1

The five pillars.	
Pillars	Description
Secure and Share	Secure any document and safely Share it outside your firewall (supports Microsoft Word, Excel, PowerPoint, Project, and Visio, Adobe PDF, AutoCAD, TIFF, JPEG)
Review and Comment	Gather, Review, Comment, Respond and Approve Comments in real time
Track and Audit	Know WHO opened, forwarded, commented on WHAT documents and WHEN
Manage and Control	Manage and control Readers rights and privileges at ANY time
Sign and Approve	Digitally sign and approve documents, comments, actions

[0250] These five pillars enable Ostiary to customize and target multiple solutions and market segments using the same underlying components and platform.

[0251] The Ostiary Dashboard—provides full Audit Trail of who did what and when:

[0252] The Ostiary Server is aware of all events that take place around a document. It knows who created a document, who received it, who opened it, when it was opened, how many times it was opened, when an unauthorized access was made and by whom, who commented, who has not, how many responses have been received, who has signed, etc. In this way, Ostiary constructs a detailed Audit Trail of all events, and provides this information to users via a Dashboard accessed from any Browser.

Full Audit Trail and Visibility:

[0253] This FedEx Tracking System capability provides a user with complete visibility of where a Digital Object is. Similarly, the Ostiary System provides the Author with complete visibility as to who received, who opened, who printed, who commented on a document

The Following are the Key Service Offerings:

[0254] Document Security—Securing any document outside as well as within the corporate firewall.

[0255] Document Audit and Compliance—Maintaining an audit trail on document events (WHO opened, printed or commented on WHAT document and WHEN).

[0256] Secure Collaboration—Gather, review, respond and approve comments from a group of people (colleagues, customers, business partners, suppliers) in real time, anytime, anywhere.

[0257] Document Approvals and Digital Signatures - Automating the signature and approval process on documents such as: NDAs, HR offer letters, Purchase Orders, Procurements and other legal agreements.

[0258] Secure Discussions Blogs—The ability to create a topic or discussion, invite a group of participants and ensure that the discussion is secure and without the headaches that Email provides.

[0259] Ostiary is addressing a market where the users are dispersed throughout the world and rely on multiple devices to communicate and stay in touch. Ostiary has designed the service such that users will be able to receive critical comments, respond to comments, sign and approve aspects of the document from any device, regardless of where they are. Devices supported are wireless devices, such as BlackBerry and Wireless PDAs.

[0260] There are two KEY participants in the model:

[0261] Authors—Authors initiate the process by sending Readers secured documents, and determining their Rights and Privileges : Life of document, Comments required, Printing, signature required, etc.

[0262] Readers—Readers receive documents with their level of access having been determined by the Author.

[0263] Authors subscribe and PAY for the service while Readers use it FREE. Readers have to go through a “one time” registration process. Once registered in the Ostiary Global Authentication server, they will be able to open secured documents sent to them by ANY subscribing author.

The Main Purpose of the Service and System:

[0264] The main purposed of the service and system is twofold:

[0265] to provide continued authorized access to a digital Artifact such as a digital document in an Open Digital environment

[0266] To provide the Access through an Internet based Authentication Method

Authorized Access

[0267] While the thrust of this document focuses on the authorized access of Digital Documents the principle and goals of the design is to provide the authorized access for a range of digital artifacts such as

[0268] Digital Documents in any format (e.g. word, Excel, PDF)

[0269] Music files in any format such as MP3

[0270] Video Files in any format such as MPEG

[0271] A Web Site e.g. access to your bank, your Distributors Intranet

[0272] A Image on a Web site

[0273] To a Physical Building whose locks are connected to the Internet

Authentication Method and Infrastructure

[0274] While the thrust of this design document focuses on the Authentication method in conjunction with the Document Access service the design of this component will be as a stand alone system that can be used by 3rd party vendors for authenticating user access for their own digital artifacts. Examples would be

[0275] Adobe using the Authentication method and infrastructure for PDF documents

[0276] Sony using it for managing the access to their Music files or Video files

General Design Principles

[0277] Apart from the Business functionality required a key part of the design is to ensure that the system being built

[0278] a. Scale to accommodate growth in users

[0279] b. Perform well and within Service Levels set down

[0280] c. Be Reliable such that the service can be provide with a minimum of 99.99% availability

[0281] d. Be Extensible to enable quick, dynamic changes to the components in the system as functions change (to extend or remove unwanted functionality)

The Ostiary System(s) Overview:

[0282] The FULL Ostiary Service is delivered through a collection of Systems, Sub Systems and Components.

[0283] The following is a brief description of the systems: Table 5:

System	Description
The Authentication System	The Authentication System is the central registry for ALL Readers and provides the full Authentication service based on the unique Digital ID generated from a composite of elements for each Reader
The Subscriber Registration System	The Subscriber Registration system manages the Customers Registration and Subscription process and also the Authorized Senders Registration.
The Object/Document Management System	This is the system that Registers the Document Enables the Policy, Access and Usage rights to be established Provides the Version Control capability Provides the Document Commentary capability
The NDA System	The NDA System enables two or more Companies to Register a hand signed NDA document between the two parties Digitally sign and register the Agreement Search features
The Legal Signature System	This is Service as well as a sub system that enables two or more parties to digitally sign a legal document on line. The NDA System also uses this sub system
The Billing System	This system handles all the requirements relating to billing a Customer
The On line Payment System	This system handles all the requirements relating to enabling customers to pay on line a Customer
The Reporting System	The Reporting System manages all the Reporting needs across all the services
The Customer Service Systems	The Customer Service system manages all the Customer care requirements such as
The Notification System	This is the system that handles all the notification and communication needs between Customer and Systems Customers and Readers Readers ad Customers Notifications can be via Email SMS Messages
The DNS System	This is a system outside of the Ostiary set of Systems where domain names are registered with all their related information such as Name of Registrant, MX Records, Server Records etc. This system is run by the Registries such as Verisign, Neulevel etc
The IP Geo Location System	This is a system that provides IP based Geo location information on where a person or device is at the time they are accessing the Internet. This system is provide by Digital Envoy
The Reader System	This is the system that enables the Reader to make a request to access a document and interfaces with the authentication systems and controls the policy and usage at the Reader end.
Referral System/ Tell a Friend	This system provides the ability for Readers and users to refer the service to others

[0284] Each of the Systems has Components that perform some task and communicate with each other. Some components can be part of more than one system. And system relate to other systems.

[0285] When components communicate there is a standardized format for communication. Every component can communicate but every component responds only if there is a threshold reached that triggers its response.

[0286] Following is a detailed description of the systems with respect to the

[0287] Components in the systems

[0288] What the systems do

[0289] How the system works (the Processes)

[0290] The Communications between components and system

Detailed Description of the Ostiary System(s)

The Authentication System

[0291] The heart of the Ostiary Services and systems is the Authentication Systems, whose main purpose is to ensure that authorized access is honored.

What is the Authentication System

[0292] The Authentication System is a central registry of Readers who are authorized by Senders to access and read Ostiary processed Digital Objects such as documents. The Readers go through a Registration process where

[0293] The Reader

[0294] Their email address

[0295] the device(s) that they want to use for access and

[0296] The IP Geo location of the Reader

[0297] Fingerprint

[0298] are linked to form a personal "Composite ID" or "digital fingerprint". This digital fingerprint becomes a representation of the Reader, and once this is done, then they can access any digital object from ANY Sender using a Reader appropriate for that Document.

What are the KEY Elements and Components?

[0299] The key elements and components are

[0300] The Readers Details

[0301] Their email address

[0302] The Device characteristics

[0303] Their IP Geo Location at the time of Registering

[0304] Their Biometric details

How is the Authentication Process Started

[0305] The Authentication process is triggered starts when

[0306] Self Register Process: A Reader goes to the Ostiary Web site to "self register"

[0307] Trying to Read a Ostiary Document for the first time Process: The Reader tries to open an Ostiary document for the first time

The Self Register Process

[0308] A reader can be sent to the Ostiary web site a number of ways. When the Reader gets to the web site there will be a section called Reader Registration.

[0309] When the Reader clicks on this link they will Get a Reader Registration form: "Insert Reader registration form".

The Core System

[0310] At the heart of the system are a set of Unique Identifiers for a number of Objects that are captured and related in a way that creates the Authentication system.

[0311] The Key Object IDs captured are:

TABLE 6

The Object	ID Types	Description	Example
The Document	Document ID	Every Document has a unique ID that the system generates	Hhy673b7b33bbd
The Reader	Email Address	Every Reader will have a business email address given to them by their company	bill@microsoft.com
	User Name and Password	As in most login registration systems there will be a need to capture a users User Name and Password	bgates Linux
	Users Unique Question and Responses	The system will have a set of questions that require a response that only the Reader will know. Examples are What is your mother's maiden name ? What is the city of Birth ?	
	Device	A Reader can have one or more devices to read a Document. Each Device will have a unique ID generated from the Device IDs	Kjks873buf8u8ur8
Client Application	Application Serial/ License number	Every application installed will have its own Serial/license number hat will be recorded	HYH 88U HJ3 Y6Y JJY

TABLE 6-continued

The Object	ID Types	Description	Example
Session	Session ID	Every time a Reader has to access to Ostiary Server a session is initiated	I84u8uj8ur jk8
Geo Location	Geo Location ID	Every time a Reader accesses a document they and their device are in some location. The exact location is unknown but the location of the devices Access point via their ISPs can be known to some degree	Country = State = City =

[0312] Each of the IDs that is generated are either

[0313] Fixed, i.e. a Document ID NEVER changes unless some element of the document changes

[0314] Changes, i.e. when ever a new session had been initiated

[0315] Furthermore every ID is associated and related to one or more other IDs in some way The table below shows which IDs are Fixed, which IDs Change and Which IDs are associated with which IDs. This table forms a key part of the authentication system:

[0321] Requests Reader to enter basic Reader information

[0322] Name

[0323] Position (optional)

[0324] Email address to be used

[0325] User Name

[0326] Password

[0327] Select Question

[0328] Provide response

TABLE 7

ID Type	ID Example	Fixed/Changes	Associated with
Published Objects ID	Hhy673b7b33bbd	Fixed	Readers Email
Readers Email ID	bill@microsoft.com	Fixed	Object ID Device ID
Device ID	Kjks873buf8u8ur84	Fixed	Readers Email Serial number of the App Cookies placed on the Device IP Location info based on location of App
Application ID	HYH 88U HJ3 Y6Y JJY	Fixed	Device ID
Session ID (cookie)	I84u8uj8ur jk8	Changes (when Reader makes request to access a Document)	Device ID
Location ID	Country = State = City =	Changes (ONLY when the Readers has physically moved their location of Internet access)	Device ID

The Core Process

[0316] The Publisher authorizes a Reader to have access to a set of objects by associating the Objects ID (e.g.: Doc IDs) with the Readers email address.

[0317] To get the keys to open the document a Reader has to

[0318] registers with the Ostiary Authentication system

[0319] Download the Reader Plug Ins

[0320] When a Reader Registers the process goes through the following steps

[0329] Once this is done, the system sends the reader a confirmation email with a URL The reader has to click the URL to complete the registration process When the URL is clicked the Reader is taken to a Web Registration completion page, at this stage the System:

[0330] Grabs Device Information from the Reader such as

[0331] Processor ID

[0332] Computer Model

[0333] Mac address

[0334] Etc

- [0335] And generates the Device ID
- [0336] It then Links the readers Email with that Device ID
- [0337] Asks the user to NAME the device (Work PC, Work Portable)
- [0338] It then downloads the and Installs the Reader Application on the Readers device
- [0339] It then Links the Applications Serial number with the Device ID
- [0340] It hen grabs the IP Geo Location of that Device and Links the current IP location with the Device ID
- [0341] It Places a cookie with the Device
- [0342] Links the Cookie ID with the Device

[0343] When a Reader wants to access or Read a document the following steps occur:

Step 1

[0344] The Ostiary set of Applications send the following data elements from the device to the server

- [0345] The Application serial number
- [0346] the Cookie ID from the Device
- [0347] the object ID or Document ID
- [0348] IP location data

Step 2

[0349] The server verifies that

- [0350] a. the App serial number is indeed associated with that cookie
- [0351] b. the IP location data is also associated with that serial number

[0352] If YES then it proceeds to Step 3

[0353] If NO it

[0354] Terminates or

[0355] Requests that the Reader go through a re-authentication process.

[0356] NOTE: If the IP location data is different as in the case when the Reader is traveling we will have a process to accommodate this.

Step 3

[0357] The Server now checks to see what Device ID is associated with the Cookie and App serial numbers submitted.

[0358] Once it determines this it then:

[0359] It checks to see what email addresses are associated with this device ID.

[0360] Once it Determines this, then:

[0361] If then pulls up the list of Object IDs associated with this email address,

[0362] It then checks to see if the Object ID sent to it by the Reader is on that list.

[0363] IF Yes:

[0364] It then sends the Object KEY to the Device in encrypted form.

ANTI-Fraud Detection

[0365] There are many methods we will use to detect fraudulent access

[0366] a. We will look at the location IP data and determine probabilistically if there is a Fraudulent attempt to access or not

[0367] b. Random requirement to re-authenticate

[0368] A hacker can copy the serial number and cookie information and install this on another device. This means that two or more Device with the same serial number and cookie can request access to the same document.

[0369] So the ONLY way around is for the system to randomly and automatically generate the Device ID and send this along with the Serial Number and Cookie info to the server.

[0370] In this way a hacker will only be able to get unauthorized access for a limited number of views.

[0371] Once a hacker's device has been identified we place them on a black list.

A Component View of the Systems

Location of Components

[0372] The key systems and their components are potentially located in 4 areas.

[0373] a. On the Senders Local PC

[0374] b. On the Readers Local PC

[0375] c. On the Ostiary Service Platform in the Ostiary Data Centers

[0376] d. On some server inside the Senders Organizations firewall (this is an option, and not mandatory)

The Key Components List

[0377] The system contains the following major components

[0378] Ostiary Server Side Components

TABLE 8

Components	Brief Description of Components Service
Subscription	This component manages and provides the following services Subscription Service De-registration Service Renewals Service Aspects of the system

TABLE 8-continued

Components	Brief Description of Components Service
Registration	This component is a subset of the Subscription component as it manages and provides service during the Registration and DE-Registration process ONLY all aspects Manages the registration and de-registration functions of Companies Authors Readers
Service	When Users register they select a service. This component contains all the necessary functionality to enable users to select change upgrade The service they have requested
Service Levels	Determining what type of Service the user has registered for ensuring they get the right service There are various TYPES of Service and there are various LEVEL of Service User can select the levels of Security service
Policy	Every document has none or some restrictions on Who can access or view the document contents What functions are available How long can it be seen for The Document Policy component enables a Author to set these restrictions or constraints Examples of Policy settings are Disable Print Disable Save Life of Doc is 7 days Can be opened only 3 times
Billing	This takes care of the billing issues between Ostiary and the User Billing has to be a plug in as a 3 rd party vendor might want to private label the service
Payment	Needs a Payment mechanism for users to pay online
Document Preparation Component	This component manages the process of preparing a document for the FYEO service. This component does the following Scans Doc for Viruses Encrypts Places doc in a location
Server Side Authentication	For a Reader to gain access to view the contents of a document they first have to be Authenticated prior to authorized access See The Authentication Process
Server Side Encryption/Decryption	Every Document that is sent is encrypted The key to Decrypt is sent only after the Authentication process from the server or locally
Digital Keys	All protected Digital Objects like Documents will be encrypted with a digital key and Readers require these keys to gain access
Notification	Any notifications sent or required by subscriber Notifications are either in Email, SMS message etc
Email Plug In	This is the plug in used to activate the Document preparation process
Manage Customer details	Manage all the Address, and contact details
Account Details	A tool to enable the end user to mange their Accounts Name Address Payments How many documents have I used Upgrading my service level
Document Management	What documents have I prepared How many have been sent WHO have I sent them to How many have been opened
Version Control	Provides all of the Version Control Functionality
Document Commentary	Provides all the Document Commentary functionality
Communication	This component manages the communication and messaging between the Authors, Readers Apps and the Ostiary Key servers etc

TABLE 8-continued

Components	Brief Description of Components Service
Virus Scanner	This is the component that simply scans the document and says if there is a virus or not It does not remove the virus

The Readers Client Side Components

[0379] The Readers have to install some application and components to enable the system to work.

[0390] Uses the key to open the document within an IE browser

[0391] provides the Comments functionality

TABLE 9

Local Authentication	This is a component that sits on the Readers PC. Its main task is to gather the PC hardware profile to generate the Unique PC ID and or to communicate this information to the Ostiary Server and Local Decryptor Container
Local De-Cryptor	The Local DeCryptor Component manages the following the local document keys the decryption of the keys communicates to BPI Stores the Readers Password in secure format Stores the Local PCID
Browser Plug In (app)	This is the application that is installed by the Reader on their PC device The component is evoked when a Reader wants to read an Ostiary document, It communicates with the Ostiary Server to determine if the User is Authorized. This can be expressed as a desktop stand alone application or as a browser based application
The Local Application	The Local Application is different to the BPI This is a full featured Light Weight Application that provides a higher grade of protection than the BPI does This component also enables the Author and Reader to manage all the Ostiary related documents

Detailed description of the Components

The Reader Components

[0380] There are two ways a Reader can Read a document

[0381] e. Using the Browser Plug In component

[0382] f. Using a desktop Application

The Browser Plug In Component (BPIC)

Description

[0383] The BPI is a component that is installed by a Reader to enable them to view and comment on a document while using Internet Explorer, Firefox, other browsers, etc When the BPI gets registered it is associated with the document type that Ostiary creates (after encryption)

[0384] So when an Author sends an Ostiary prepared document to a Reader the act of trying to open the document invokes the BPI

[0385] The BPI

[0386] Is invoked when a user tries to open an Ostiary prepared Document

[0387] Communicates with the Ostiary authentication servers to

[0388] request the Document keys

[0389] Pass any cookie information

[0392] NOTE : The BPI is ideal for and used primarily where the Reader only requires Read functionality and not Author functionality. If the Reader is also an Author then the OLA would become the client they would use to read and comments on documents.

WHERE can a Reader get the BPI:

[0393] The BPI is a component that can be downloaded from any participating Site. Most likely the primary site will be the Ostiary site. But companies that subscribe to the service can have the BPI downloaded from their site or have a link from their site to the Ostiary download site.

The Ostiary Local App (OLA)

[0394] The OLA is a application that is used by Authors who are also Readers. As such they perform all the functions of the BPI Component plus have all the functionality required by the Author. The app is installed by the Reader when they register. Like the BPI it also is associated with the Ostiary document type. The act of trying to open an Ostiary file will invoke the OLA.

[0395] The OLA however has a built in Browser view component so the document is viewed in this browser component and not IE.

[0396] The OLA provides all the local functionality for

[0397] a. Selecting files for Publishing

[0398] b. Submitting files

[0399] c. Viewing files

Additional Functionality

[0400] In addition to the functionality of the BPIC the OLA has a management component. NOTE: In the ASP environment most of the management functionality will be provided from the server side. But in large corporate environments the OLA would replace this but still have communication to the server to send and receive data.

Digital Keys:

[0401] Digital keys will be used to ensure that encrypted information can only be opened by authorized users.

[0402] The system uses digital key Pairs in a number of areas.

[0403] a. Key pairs for Every Document

[0404] b. Key Pairs for Every Reader

Digital Keys for Documents

[0405] While Every Document has a Unique ID, they also have a set of unique key pairs. These key pairs are used to encrypt and decrypt a document. These unique key pairs are generated at the Ostiary Server at the time of preparing the document for FYEO publishing. An Enterprise deployment might have the Digital Key generation performed at their site.

[0406] The two key pairs for every document are

[0407] a. The Encryptor key

[0408] b. The De-Cryptor Key

[0409] The Encryptor Key encrypts the document prior to being published and sent to Readers.

[0410] The De-Cryptor key is:

[0411] a. Sent WITH the document to the Readers and stored on the Readers Local PC for de-crypting OR

[0412] b. Stored on the server and used ONLY when the Reader is on line

[0413] NOTE: The system will enable an Author to set the rule

[0414] a. Let the Reader open the document Off line or On Line

[0415] b. The Reader can ONLY read this when On line

[0416] The decrypting key is activated when the accessor has been correctly authenticated

Associating Documents with Keys

[0417] When a document is readied for publishing the document and its associated details (Author ID, Document ID, Document Key etc) are registered at the Ostiary server. So EVERY Document ID is associated with the Documents Keys. When the document is sent to the Readers or when Readers pick up the documents the keys MAY also be registered on the Readers Local PC in the Ostiary Encryptor/Decryptor component on the Local PC.

[0418] Therefore, this local component knows which documents are associated with which keys. Local keys are temporary keys for temporary Off Line Access

Rotating Document Keys

[0419] The document ID is always unique. Associated with that Doc ID are the keys that are generated to enable a Reader to open the document.

[0420] An author can set the system such that every time a Reader access and reads a document the Server sends the Next key pair. In this way the keys used can be on a one time only basis.

[0421] The purpose of this feature is to provide a higher grade of security for users that need this.

Alternative Method

[0422] The key that finally opens the document is fixed and once generated is for that document. However, the key generated to gain ACCESS to the document key can be rotated.

Where are the Keys Stored

[0423] Document Keys are stored on the Ostiary Server on a company's server or locally in a container on the Readers PC. Readers don't have access to these keys so keys cannot be copied or sent to another Reader. These keys are only accessed by parts of the application and under certain conditions.

[0424] The keys are stored in the applications directory in the Document and User Key container.

Access to the Keys

[0425] A key is accessed when a Reader tries to open a document.

[0426] The client asks the question "Can I have the key to open this document"

[0427] The PC ID Requestor starts the process by getting the PC Hardware profile.

[0428] It gives this to the Authenticator.

[0429] The authenticator generates the hash ID for the device and sends it to the Ostiary server or compares it locally.

[0430] IF the PC ID is correct the Authenticator lets the Decryptor Component know.

[0431] The Decryptor then unlocks the document key and provides the key to the BPI.

Digital Keys for Users

[0432] Every user that registers has a unique key that is stored on the server and or their local PC and which is associated and is part of their digital identity.

[0433] This key is used as one of the means to authenticate the users and to open the documents.

Users Password

[0434] When a Reader registers on the Ostiary server their user name and password is stored on their Local PC in encrypted format. This is used ONLY when the user is off line.

The Distributed Nature of the Document Key and Authentication server

[0435] Because the user community will be a mixture of small to large companies there will be need to cater to these groups. There are 3 key components:

TABLE 10

Components	The enterprise Secure Environment	Ostuary Secure Environment
The Authors Document	Fortune 1000 Mid Sized	SME and Mid Sized
The Document Key	Fortune 1000	Some Fortune 1000 Small and Mid Sized
The Reader Registration Data		Fortune 1000 Small to Mid Sized

[0436] As the user base spreads outside of the US then there will likely be a need to distribute the “key” servers to accommodate the markets need.

Knowing WHICH servers to get the Key from

[0437] A typical Reader is likely to get Documents from a variety of Authors who potentially can have their documents

[0440] When a document is prepared and published part of the data that is associated with the document is WHERE the authentication and Document Key servers are located.

Document Policy Component

[0441] When an Author publishes a document they may want to specify HOW that document is used by the Readers i.e. What constraints they want to place on the document for the Readers i.e. what rights and privileges they grant for the reader

What Document Constraints and Rights and Privileges are Possible

[0442] Every document has none or some restrictions that can be imposed such as

[0443] Who can access or view the digital objects contents

[0444] What functions are available

[0445] How long can it be viewed for

[0446] Below is a list of possible but not exhaustive list of rights and privileges Table 11:

TABLE 11

Object	Constraints	Description of Constraints and Example
People	Access	Who can View the documents
Digital	Disable	
Object	Print	Disables the Print function within the document
	Copy	Disables the Copy function within the document
	Save	Disables the Copy function within the document
	Screen Capture	Prevents Screen capture to be used
	Access	Disable Users access After
Object Viewing	Number of viewings allowed	Set a documents Viewing life to
	Life of Document	Number of views allowed = Once only or 5 times
		Document exists from This Date to This Date
		For a Period on 2 months from this date etc
Access	From a Particular Geo location	Only people accessing from New York State
	From a particular Domain	Exclude any viewing from certain countries
	From a particular Post Code	Only allow viewing from employees of Proctor and Gamble
Document	Access at a page or section level	Enable access only for pages 1, 5, 9 and 10
		Disable access to this section on this page

registered in a variety different authentication servers located anywhere in the world there will be a need at the Readers end to know WHICH Ostuary server to communicate with to get the particular key to open the particular document.

Knowing WHICH Servers to get the Readers Authentication Processed from

[0438] ALL Reader registration and Digital IDs can be stored on a central Ostuary managed servers or on servers owned and managed by organizations who may want their own Reader Authentication servers.

[0439] When Readers are registered in a different servers to where the document keys are, the local components will be able to find out WHICH server to talk to for Reader PCID validation.

[0447] The digital object Policy component therefore enables an Author to set these restrictions or constraints.

A Process View of the System

[0448] Authors and Readers of the system have to be registered in the Authentication system first to be able to use the security service. They also have to install the Client application that renders the secured object.

[0449] Once registered and installation is done then Authors can start to secure objects and invite participants to view the objects

[0450] Secured digital objects are made available to Readers by sending it as a file attachment on an email or making it available on a FTP server.

[0451] The reader opens the digital object in the installed client using standard Windows OS methods to open the

[0452] The secure Object Process

[0453] To secure a Object the Author

[0454] opens the client app

[0455] selects the object to be secured

[0456] adds one or more Readers to the authorized list

[0457] sets their rights and privileges and constraints

[0458] Optionally apply keywords

[0459] Optionally apply notifications to the events of the object

[0460] When Author submits the object to the securing process the system then

[0461] Scans the object for potential viruses

[0462] Generates the Document unique ID

[0463] Encrypts the Documents

[0464] Captures relevant Author details such as Authors email address, PCID et

[0465] Creates the Private decrypt key for the document

[0466] Registers the authorized list of Readers for that document key

[0467] Set the versioning attributes of the object

[0468] Send the Secured object to the authorized reader list

[0469] The view, read and comment process

[0470] Once an Author secure a document the Readers will be notified that they have been invited to view and or comment on the object

[0471] To view an object the Reader does the following

[0472] a. Registers with the system

[0473] b. Installs the client Viewer

[0474] c. Opens the Secured object

[0475] d. Gets authenticated

[0476] e. If the Readers is authorized to read the Object then system provides the access and decryption key

[0477] f. and sets their Rights , privileges and constraints

Reading Off Line or On Line

[0478] An Author can enable the Reader to read a document

[0479] a. On Line ONLY

[0480] b. Off Line ONLY

[0481] c. Combination based on Readers situation

The Digital Object Rights and Privileges

[0482] The Author can control two broad aspects of the Objects attributes

[0483] The functions available with the object e.g. Print, , Open, copy, paste

[0484] The Life of the document (the time period a user has access to the digital object)

[0485] The Frequency of access (the number of times a user can access the object twice, 5 times etc)

Functions of a Document

[0486] With any document the system can determine what functions are available or denied.

[0487] Some examples are

[0488] a. Document can have its Print function disabled

[0489] b. Document can disable its copy and Paste function

[0490] c. System can disable Screen Print feature

Life of Documents

[0491] The document can be viewed only once and then dies for that user

[0492] Document has a life of only n days

[0493] Documents used in Web Conferences.

[0494] Often a user can do screen shots and take copies.

The Document Tracking Number

[0495] Every email that is sent from the system with or without a secure object as an attachment but with a Protection request will get a tracking number

[0496] This will be the key number that is assigned to the original email thread

[0497] Any subsequent event e.g. if the email is forwarded or replied will generate an extension

Tracking Number Composition

[0498] The tracking number will be a 16 digit number in the form 4545.6552.5298,9987

[0499] Allowing for a large number of tracked events

Tracking Number Extension

[0500] When an email is forwarded etc then number generated will be of the form 4545.6552.5298,9987.1 4545.6552.5298,9987.2 4545.6552.5298,9987.3

[0501] Etc

[0502] The tracking number is like the Fedex tracking number in that it binds the following

[0503] Sender

[0504] Recipients

[0505] Date and time of email

[0506] Document name

[0507] Document size

[0508] NDA Registry number

The Life Of A Document

Purpose:

[0509] If a Author has a need to establish the life span of a document for Readers For example

[0510] a. For 10 days from date of publishing

[0511] b. From Feb. 20, 2004 to Mar 12, 2004

[0512] c. For 5 days AFTER a recipient has first opened document

[0513] Then this functionality should enable the Author to so

[0514] General Principles:

Life Span is an Attribute of

[0515] a. CASE 1. The digital object or

[0516] b. CASE 2: A digital object AND a USER

[0526] A document is not KNOWN to the system until it has been published. This differentiates all Authors documents from Published and un-published

[0527] Only a registered user who is also an Author can publish a document.

[0528] Document Rights, Policy, Usage

TABLE 15

Right	Description
Full control	In this case the Author has conferred equal rights to the Reader as the Author has
Change	This right enables the Reader to read, edit, and save changes to a protected document (but not print).
Read	This right enables the consumer to read a protected document but not print, edit, save, or copy or forward.
Document expiration	Once set it restricts the viewing window of the document from the date sent to the date of expiry A document Expiry can be for ALL Readers or Expiry can be on a Per Reader basis
Print content	This right denies the consumer the ability to print protected content.
Allow users with read access to copy content	This right enables the consumer to read and copy content of a protected document to the clipboard but not print, edit, or save.
Access content programmatically	This right enables protected content to be accessed by another application programmatically.
Users can request additional permissions	This right enables the consumer to contact the publisher at a specified e-mail address to request an upgrade in the rights assigned.
Allow users with earlier versions of Office to read with browsers supporting Information Rights Management	This right enables protected content to be read in Microsoft Internet Explorer through RMA.
Require a connection to verify a user's permission	This right sets the use license to expire immediately after the protected content has been accessed. As a result, the consumer must have online access to the RMS server to get another use license every time the document is opened.

[0517] Case 1 can accommodate some of the needs of Case 2

[0518] If user needs TWO version of a doc with two different life spans they can create TWO versions and place different Life Span for each

When does the Life Span Start:

[0519] The user will specify WHEN the Life Span rule starts

[0520] The life of the document can start from

[0521] a. Date of Publishing Document (regardless if it has been sent)

[0522] b. Date of 1st sending Document to a Reader

[0523] c. Date of Reader 1st Opening a document

[0524] d. Other

Publishing a Document or Digital Object

[0525] What does it mean to Publish a Document or digital Object

[0529] The Players and Roles Played in the Document Processes

TABLE 16

Type	Description
Admin	Account Admins have total control of ALL keys associated with an Account. Since all Authors belong to an account the Admin can remove, assign delete an Authors access to objects keys
Authors	They originate a document and OWN the document There can be more than One author for a document There is generally a Lead Author of author list is >1 An Author can be a Reader and a Sender
Readers	Authorized Readers receive documents from Authors for the purpose of reading, making some comments or editing documents Readers rights range from Read Only Read and make some Comments but not edit a document Read and Edit text in the body of the document
Senders	Senders are not Readers or Authors but on occasion need to have access to the document to Send the document to others. Examples are the Personal Assistants of CEO, executives etc Senders may need reading rights to ensure they are sending the right document

[0530] A document can be prepared by an Author but Sent by a Sender

[0531] A Document can be Prepared by a Sender and Sent by a Sender or Author

[0532] System provides a setting that enables

[0533] Senders cannot open and view a document

[0534] Senders can view a document but once only

[0535] Readers have to be registered and they have to be validated to gain access.

Version Control of FYEO Docs

[0536] Often a user sends a document that over time gets revised and updated. The user then sends the revised document out to the group. There are many instances when members of the group use the older version of the document not realizing that the version they are using is one or more versions behind documents are new versions of the prior. The versioning functionality for the system is designed to solve this problem.

How will it Work?

[0537] When a user selects a document to protect they prepare that document in the usual way.

[0538] One additional function they set is "versioning"

[0539] When the user sets this the system will ask the user the following

[0540] Who is allowed to change the version of the document? The response will be simply an email address.

[0541] Once this is done the user sends the document

[0542] Every time there is a new version the sender prepares the document and tells the system that the NEW document is superseding a prior document. In this way the system keeps a trail of all prior versions and a chain.

[0543] When a user with an old version clicks the document to view it the agent sends the server the document details e.g. Name of document, Original sender,

[0544] The system looks to see if there are any documents succeeding it. If Yes, it sends the user a Web notification:

[0545] "The document you are trying to view has been superseded, click here to get the latest version"

[0546] In this way the system maintains a thread of the document like a threaded email.

What is the "Authorized Recipients" List

[0547] Whenever a sender sends a document there is always zero or many recipients in the list.

[0548] If list is zero then the ONLY person that has access is the Author

How does the System know that the user is Authorized to get the Latest?

[0549] The system keeps track of ALL the recipients associated with a document

[0550] So whenever it tries to enable the viewing of a document it always uses the authorized recipient list.

How is this Created?

[0551] Whenever a user sends a protected file the system grabs the following details during the Secure process

[0552] Name of Object

[0553] The name of the document being secured

[0554] WHO it was secured for (the Reader list)

[0555] Size of document

[0556] PC ID of each recipient (this occurs only when the user registers)

[0557] Keywords

[0558] Rights and Privileges

[0559] Notifications

[0560] How it was sent

[0561] When the system gets this data it associates this with the particular document key

Document Versioning

[0562] This feature enables an Author to ensure that everyone with authorized access will see only the MOST current version.

The Problem Definition

[0563] A writer has multiple versions of a document in circulation and wants to centrally and automatically control WHICH document the recipients will read without the need to inform the readers.

Use Case Scenario

[0564] Writer Joe sends a draft agreement called "draft proposal 1.doc". He sends the doc to 10 people via email.

[0565] 5 open the doc and read it and 5 don't

[0566] In 5 days the Writer Joe sends a new version called "draft proposal 1a.doc" to the same 10 people.

[0567] In this way Writer Joe could over time publish many versions of the document So as versions of a document proliferate what writer Joe wishes to avoid is a reader opening an older document accidentally and comment on this older document.

Design Concept

Purpose

[0568] To build a feature that would enable a writer or sender to centrally manage which versions of a document a reader is able to read and open.

[0569] When Writer Joe sends a document as an attachment via email the system registers the document. Every subsequent version is recorded. If the naming convention is such as in the above case then the system would cluster the document together as being part of the same with the user being able to override this.

[0570] Say Writer Joe has sent 3 versions (The original and two updates) and now wants to ensure that the right version is opened.

[0571] Writer Joe would log into the system

[0572] System would display Writer Joes list of protected documents (and associated versions) by some category. Below are examples

[0573] By Date (Most recent to old)

[0574] By Group

[0575] By Recipient

[0576] Etc

[0577] Joe would select the document and all its versions
When a user logs on to the system they will get the following:

[0586] To download the current version click on this link www.company.com/securedocs/Proposal2.doc

[0587] If a file upload area was used a URL link would be generated for such location and be used to enable users to download from.

TABLE 17

Document Name	Version	Date sent	Description	Current	Recipients	status
Proposal 1.doc	Original	Aug 3 rd 04	Blah blah	☐	John Adams	Opened
					Abraham Lincoln	Not Opened
					Charles Darwin	Opened
Proposal 1a.doc	Ver 1	Aug 6 th 04	Blah blah	☐	John Adams	Opened
					Abraham Lincoln	Not Opened
					Charles Darwin	Opened
Proposal 1b.doc	Ver 2	Aug 11 th 04	Blah blah	☐	John Adams	Opened
					Abraham Lincoln	Not Opened
					Charles Darwin	Opened
Proposal 2.doc	Ver 3	Aug 15 th 04	Blah blah	☒	John Adams	Opened
					Abraham Lincoln	Opened
					Charles Darwin	Opened

[0578] Writer Joe would scroll to the version they deem to be current and mark it

[0579] The system would then block all prior versions and provide a message to the user.

What Happens when a User tries to Read an OLD Version:

[0580] User will get a message displayed

[0581] Message

[0582] The Document Proposal 1a.doc you are trying to open is an older version

[0583] The current version is Proposal 2. doc

[0584] Sender was Graeme Marsh

[0585] Date sent was Aug. 15, 2004

Process

Background

[0588] Reader A receives 4 emails from Writer Joe over a 15 day period with the following docs attached.

TABLE 18

Doc Name	Date Sent
Proposal 1.doc	Aug 3 rd 04
Proposal 1a.doc	Aug 6 th 04
Proposal 1b.doc	Aug 11 th 04
Proposal 2.doc	Aug 15 th 04

[0589]

TABLE 19

CASE 1. Reader A tries to open the attachment Proposal 2.doc sent by Writer Joe	STEPS: The system agent is invoked Agent ALWAYS goes to server to check the following a. IS this the current authorized version b. IS the user registered c. Is the user Authorized to read this (i.e. definition of authorized is that the user is listed as a recipient) IF User is Registered AND Authorized Then Agent opens the document in the Browser The system agent is invoked Agent ALWAYS goes to server to check the following d. IS this the current authorized version e. IS the user registered
CASE 2 Reader A tries to open the attachment Proposal 1a.doc or Proposal 1b.doc sent by Writer Joe	

TABLE 19-continued

	f. Is the user Authorized to read this (i.e. definition of authorized is that the user is listed as a recipient)
IF	
User is Registered AND	
Authorized	
Then	
Agent opens the document in the Browser	

The Document Verification Feature

[0590] We send documents on many occasion to people who don't know who we are. An example is sending a resume to a recruiter. When the recruiter receives the document they are not certain as to the authenticity of the doc or whether the document contains any viruses etc, so they are reluctant to open it. Furthermore there is no registry that tells them anything about the recipient.

[0591] There is no sense as to HOW SAFE is this document

[0592] The intention of this feature is to

[0593] a. enable he sender to resister with the registry who they are and the document they are sending

[0594] b. enable the receiver to verify that the sender is safe

[0595] When a user registers with the service they are authenticated by the round robin email process that ensures that the sender is indeed from the email address they are registering in the system. Because the user also pays for the service using credit card there is a notion that their billing address has been verified by the credit card company.

[0596] When the receiver goes to open the document the document agent

[0597] a. invokes browser or the client application

[0598] b. goes to the server to get senders details

[0599] c. displays data to receiver

Sample Display for the Recipient

[0600] Details of Document

[0601] Sent by: Clive Flory

[0602] Sent From: Arlington Va.

[0603] Date sent: Nov. 22, 2004

[0604] Name of Document: "My Current Resume"

[0605] Date of Document: Oct. 12, 2004

[0606] Number of pages: 12

[0607] Size: 54 K

[0608] Intended Recipient: bob@gorur.net

[0609] Click here if you wish to open the document

[0610] This is a paid service from XXX

Document Commenting and Annotation Feature

Problem Definition

[0611] When a reader gets a protected document from a writer there maybe a need for the reader to provide feedback and comments to the writer.

[0612] If the document is protected then the writer will NOT be able to save the document and provide inline commentary. The only option available will be as text within an email.

[0613] But this method means that the text of the comments is disassociated from the original document. So creating the comments and reading the comments outside the context of the source document could be a problem.

Use Case Scenario

[0614] Writer Joe sends a document as an email attachment to 5 people. Writer Joe wants their feedback but also wants to ensure the safety of the document.

Design Concept

[0615] Purpose

[0616] The purpose of this feature is to enable a reader to comment or the writer to read comments while having the original text alongside the comments. The KEY design element s to

[0617] a. enable the commenter to be able to comment while having THAT part that is being commented on visible.

[0618] b. enable the writer to READ the comment alongside the section that is being commented on

[0619] c. enable participants to add new comments or responses

The Design

[0620] When a Reader tries to open a protected document they will only be able to open the document within a browser tool or a client application. These tools will have a Comment Function.

[0621] When the user selects this function the browser displays TWO panes.

[0622] The left Pane will have the document and the right pane will have the comment section Both panes will operate in their own window and will have their own independent scroll bars

[0623] There are two ways to make a comment

[0624] Text only Comment

[0625] Comment with Draw element (line, circle, square, highlight etc.)

[0626] Text only comment

[0627] In THIS method the text is associated with the page of the document currently being viewed. A page can have one or MORE comments

[0628] Comments with Draw Elements

[0629] In this method user can markup a section of a document using a draw tool (square, circle, and highlight) then they write their comment that is associated with the marked up section

Can a user Make a Response to a Comment

[0630] Authorized participants can make one or more Responses to a comment

Can a User Make a Response to a Response

[0631] Authorized participants can make one or more Responses to a Response

The Authentication Process

Method of Authenticating

[0632] first time opening will require a query to the server to verify the user authentication and to retrieve the decryption key and a hashed number from PCID. The hashed number ties the PC to the doc (the Ostiary Client code enforces this). then we have options:

[0633] mode 1—every access requires a query to the server

[0634] mode 2—allows offline access, after first authentication

[0635] mode 3—offline access times out after N days, etc.

Section on Devices

Defining Devices

Shared PCs

[0636] The system caters for shared PCs. In today's world MOST work PCS are allocated to a person and there is no sharing However SOME Employees do have to share e.g. in customer care shift workers. The system will cater to this need and request MIINOR authentication process.

The Device ID and Device Fingerprint

[0637] Every Device has a fingerprint that is made up of the following:

[0638] Device ID

[0639] Intel Chip version

[0640] Intel chip ID

[0641] OS and OS version

[0642] IP Address Range of that Device

[0643] Location—Home, Work

[0644] Type—Fixed, Laptop

[0645] This information is converted to a Device ID code generated by the system. When a Device tries to access a document the IP address is recorded and associated with the Location.

[0646] Product Activation identifies a computer by considering nine characteristics, e.g. the make and model, of a variety of hardware components contained in the computer and constructs a Hardware Hash—the identifier for a computer—from the gathered information. A Hardware Hash thus represents the hardware configuration of a computer. Note that the term hardware configuration comprises, in the context of this manual, only some selected hardware components and not the full hardware configuration of the computer.

[0647] As computers typically differ in many hardware components, chances that any two computers yield the same Hardware Hash are slim. In addition, copying hardware components from one computer to another is not possible. So, Hardware Hashes meet the two conditions described above.

[0648] Hardware Hashes are sequences of 12 characters, e.g. LNKJ-BLR7-7TNZ Like Serial Numbers, Hardware Hashes are case-insensitive. Each of the characters is selected from the set of 26 letters and digits that we also use for Serial Numbers. The hardware components represented by the Hardware Hash and their considered characteristics are

[0649] one of the installed hard drives—make and model

[0650] one of the installed CD-ROM drives—make and model

[0651] one of the installed SCSI host adapters or IDE controllers—make and model

[0652] one of the installed graphics boards—make and model

[0653] The first CPU in the computer—make and model, serial number

[0654] the installed RAM—size

[0655] one of the available disk volumes—volume serial number

[0656] one of the installed Ethernet adapters—Ethernet address

[0657] Typically, the end-user may not specify of which hard drive, CD-ROM drive, etc., the characteristic is included in the Hardware Hash. The hardware components to be used are automatically determined. However, in customized Product Activation, advanced end-users can themselves select the hardware components to be considered.

[0658] From each of the collected characteristics, with the exception of the CPU serial number and the Ethernet address, a numerical value between 0 and 7, i.e. a 3-bit value, is derived. The CPU serial number and the Ethernet address are mapped to numerical values between 0 and 511, i.e. a 9-bit value. A value of 0 indicates that the corresponding characteristic is not available. If a computer, for example, did not have any CD-ROM drive installed, the value representing the make and model of one of the installed CD-ROM drives would be 0. If the installed CPU did not support a CPU serial number, the respective value would be 0. And so on. Any value different from 0 indicates that the corresponding characteristic is available. In this case

the value is the result of passing a text representation of the characteristic through a hash function.

[0659] As $\log_2(26)$ is roughly 4.7, each of the 12 characters of a Hardware Hash represents about 4.7 bits. A complete 12-character Hardware Hash thus represents a 56-bit value. We use big-endian "character ordering," so the first character of a Hardware Hash represents the most significant 4.7 bits. The 40 least significant bits of the 56-bit value represent the hardware configuration. The remaining 16 bits contain a CRC-16 checksum to guard against typographic errors.

ON Line Authenticated Document Signature Method/Process

The Document ID Thumbprint

[0660] Every document can generate a unique Thumbprint based on the contents of the document at a particular time. This thumbprint is some unique digital string generated based on content characters and layout (number of words, characters, spaces, date, etc) If any one of the characters is altered, changed, moved then the document ends up with a NEW thumbprint. If a document remains unchanged then its thumbprint will remain unchanged.

[0661] Furthermore a documents thumbprint can be determined at any time and compared to prior determinations. In this way the system offers users an ability to record events associated with a documents thumbprint and ability to test if there have been changes by testing and comparing two documents thumbprints.

[0662] If the thumbprints are identical then the documents are the same if they are not then the docs are not identical.

[0663] The systems basically tests for

[0664] Question: "Are the two documents being compared identical"

[0665] The answer can only be a Yes or No based on the thumbprint

[0666] The system does not provide information as to HOW much change has occurred in a document if changes have been made or WHERE the changes occurred

[0667] Once this string is generated the system stores this against the document information.

[0668] NOTE the document itself need not be stored in the Ostiary server.

Providing an Electronic Signature Page for a Document (Agreement etc)

[0669] Every agreement or contract has a Signature page

[0670] Ostiary will provide the ability for parties to perform the signature process on line by

[0671] providing an on line Signature page that will be associated with the agreement.

[0672] Note the actual document need not be stored. But at some stage the document has to be analyzed by Ostiary system to generate the thumbprint and to capture the document details.

[0673] During the last stages of negotiations and once the terms and conditions have been captured on the agreement

and agreed to be both sides then the document is submitted to the system for the signature process. Ostiary provides the signors an ability to generate a

[0674] Signature Page and use this as the Record.

[0675] Ostiary maintains the Signature Page.

What Data about the Signors do we Capture

[0676] The Online signature page will need to captured the following details about the signors

TABLE 20

User Entered	
Name of Person	Joe Blow
Company	Verisign (automated when user signs on)
Email address	joe@verisign.com
Position	VP Marketing
System Entered	
Date first registered	
Number of Documents signed	

The Signature Process

[0677] In a legal agreement at some point both parties agree to the terms and conditions captured in the agreement and both claim they are ready to sign the document

[0678] At this point the Originator submits the document to the system and creates the Signature Page

[0679] The user sets up the features of the signature page

[0680] Who and How many from both sides are signing? (name and Email address)

[0681] If there is a need for a Verifier or Witness

[0682] Is there a need for someone to authorize the signors signing capability

[0683] Details of the document (name, date, size)

[0684] All the email address of the signors (they have to know at least ONE email address of the other party)

[0685] The system generates the Thumbprint but does not store the document (this is optional and based on users request)

[0686] This thumbprint is associated with the attributes of the document

[0687] Names of parties in the document

[0688] Signing parties

[0689] Domain names

[0690] etc

[0691] Once the documents thumbprint has been generated and displayed on the Signature Page the originator can go ahead and electronically sign the signature page using their company email address.

[0692] Once the first signatory signs then the system send an email signing request to ALL other parties on the Signature page

[0693] IF the other party wants to ADD additional signatories to the page then they can log in and ADD additional names and email addresses.

What is a Verifier

[0694] A verifier is like a witness to a physical signature and a person that verifies that a signing party is still a valid person and holds a title they claim. They are people nominated by a signor who work in the same organization and who can vouch that the signor is indeed a person that works for the company and has the claimed title.

[0695] When a verifier gets a email verification request the web page they eventually see will say something like:

[0696] You have been asked to verify that it is Friday 23 September 10:40 am (today's date and time)

[0697] Joe Blow still works for Verisign and has the title of VP Marketing

[0698] Your Name:

[0699] Your Title:

[0700] Your Signature:

Can the Ostiary Signature Server act as a Witness

[0701] The Ostiary signature server can also act as a "witness" to the parties digitally signing the documents

Can the Server Act as the Verifier

[0702] The system will also act as a verifier only of a users rights to an email ID

Multiple Signatories

[0703] In some cases the parties may request that there be multiple witnesses and hence multiple verifiers to the parties signing. In most cases ONE Verifier can verify for ALL the other signatories.

[0704] In this case the verifiers email address is entered by the signors and the verifiers also get notified

[0705] When the originator and their parties sign on line they will get an email authentication request and they will go through the round robin process

[0706] If there is a verifier required then the system requests the verifier to go through the same round robin process.

The Round Robin Process

[0707] The round Robin Process is a method that tries to ensure that the email address provided is indeed from the authorized owner and User of that email.

Method

[0708] The system generates an email authentication request and sends a message with a link to that party using the email address provided

[0709] The party opens link in the email and is sent to a web page And clicks on the confirm button

Completing the Online Signing Process

[0710] Once all the signatories and verifies have signed the document a Completion email is sent out the parties

[0711] This completion email will be like a Receipt that they can use as further proof of the process

[0712] The email will have the details:

[0713] Receipt for the Signing of Agreement

[0714] Name of the Agreement: XXXXXXXXXX

[0715] Name of document

[0716] Document Thumbprint ID:

[0717] Date of Agreement

[0718] Date signing was completed:

[0719] Companies: Xyz Inc

[0720] Signatories of XYZ INC

[0721] 1st Signor and Verifier

[0722] 2d Signor and Verifier

[0723] 3rd Signor and Verifier

[0724] Company: ABC Inc

[0725] Signatories of ABC:

[0726] 1st Signor and Verifier

[0727] 2d Signor and Verifier

[0728] 3rd Signor and Verifier

[0729] Once done all parties get an email saying that the agreement has been signed.

[0730] Optionally the parties can store the document on the Ostiary server.

Determining the Validity of the Document

[0731] IF there is a dispute later on as to which version the parties signed then to determine this the parties do the following

[0732] a. Either party submit a document to the system to determine the thumbprint of he document

[0733] b. System determines the thumbprint

[0734] c. System searches for a match

[0735] d. If match is found the details of that agreement are displayed

[0736] e. If no match is found then the system displays a message

Security

Levels of Security

[0737] The system can provide different level of security

[0738] Each level of security will attract a different pricing

[0739] The highest level of security is requiring the user to identify where they are when they are NOT in the two fixed areas e.g.

[0740] Office Location

[0741] Home location

[0742] Temporary Location

[0743] When users register, the system asks them for their office location.

[0744] IF they intend to access from Home they then provide their home location. Both these location are the defaults in the system and these are mapped to known IP address for that area.

[0745] When a user tries to read a doc from any of the two fixed locations the system lets it through

[0746] When a user is traveling and is in another location AND the Author has subscribed to this level of security, the system does the following:

[0747] When system validates the users email and PC ID and finds that the IP address is not in the range of fixed locations registered it takes the user to web page and says:

[0748] We note that you are in a different location form registered please tell us what

[0749] Country

[0750] State and

[0751] City

[0752] Since the system HAS the IP address of the user, it uses the information provided to verify that they are in the same location as what the system has determined.

[0753] Once done the system registers this as the Temporary Location:

[0754] User can at have at least ONE temporary location associated with the email and IP address.

Location and Address of User and Device

[0755] A user can have 3 types of location information associated with them:

[0756] Location and address of where they work

[0757] Location and address of where they live and access work related stuff

[0758] Temporary location—i.e. when they travel

[0759] When a Person (Reader or Author) registers

[0760] They tell us WHERE they are registering from (Home, Work, on the road)

[0761] And we grab the IP address

What Happens when a User Moves from Location to Location

[0762] Some employees do not move from their location of work others such as Sales Reps and

[0763] Business Development people move a lot.

[0764] For those that move a lot and where we intend to use Geo Location for testing validity of user.

[0765] The system should have the notion of users and locations of users.

[0766] A user can have

[0767] One fixed office location

[0768] One fixed Home location

[0769] One temporary location

[0770] The Settings will be as Follows

TABLE 21

My Office Location	Country = USA State = Maryland City = Bethesda Post Code = 20852
My Home Location	Country = USA State = Virginia City = Arlington Post Code = 22201
My current Temporary Location is	Country = USA State = Virginia City = Arlington

Verifying Ownership of Person Email Address

[0771] One of the foundations of the system is the process of a registered Author and Reader to “verify their ownership of their email address”

[0772] The purpose is to ensure that when a user registers on the Web for the service and provides their email address that the email address belongs to the registered owner.

[0773] The secondary and equally important reason is to lick the users email address with the PC that they have sent it from.

[0774] The method for doing this is as follows

[0775] a. User registers as a Author or Reader on the system and provides their email address

[0776] b. The system sends a message to the email address with a URL link that the user is required to click on

[0777] c. The URL link sends the user BACK to the systems web site

[0778] d. When User returns the systems grabs the users PC Thumbprint and, links that to their email address.

[0779] e. The system also checks the DNS records and grabs the MX record as the record for who is the authorized delivery mail server for incoming email

[0780] f. System looks up Digital Envoys IP DB and gets Country, State and Local data

[0781] g. The system notes that it's the nth device that has been registered to the user

[0782] Registration Data for User

TABLE 22

Name of User	Joe blow
Email Address	joe@microsoft.com
Company name	Microsoft
Device Number	The nth device that is being registered There will be a limit 1 st , 2 nd , 3 rd etc Device 67tyw788hhjjh4877 b9899
PC Thumbprint ID	This will be Operating System and version Intel; Chip ID etc The ID is linked to the device number mail-01.name-services.com
Incoming Mail Server address From DNS MX Records	

TABLE 22-continued

Local IP address of POP associated at time of process (From Digital Envoy)	216.168.41.240
Country	USA 100%
State	Virginia 97%
City of Email Address (from Digital envoy)	Arlington 89%

[0783] When the users register on the Web Site they will get a message on the web site similar to this:

[0784] A Verification e-mail message has successfully been sent to your Inbox.

[0785] To better protect your privacy, Ostiary requires that you verify ownership of your e-mail address prior to enabling you view the Document.

[0786] Please follow the steps to verify your e-mail address.

[0787] After you verify your email address, you will be able to view the Secure document

[0788] The email address we have sent the verification to is joe@microsoft.com

[0789] Step 1. Open the email sent from verification@ostiary.com

[0790] Step 2. Click on the verification link

[0791] Step 3: System will take you back to the Verification section of the Ostiary site to verify your address

Sample of the Email Address form Ostiary to Reader or Author

[0792] The user gets this sample email:

Final Step

[0793] To verify that you own this e-mail address, click, <https://verification.ostiary.com/verifyvalidateemail/ProcssEmail.aspx?1cid=1033&Email=joe%40blow.info&eck=w2UTkwbApcMkcpEDJsoq9Q&CP=2&WizID=c0984801-c59c-43fc-a8d6-1>.

[0794] *If clicking the link above does not work:

[0795] Select and copy the entire link.

[0796] Open a browser window and paste the link in the address bar.

[0797] Click Go or, on your keyboard, press Enter or Return.

[0798] You may be asked to sign in with a Microsoft.NET Passport.

[0799] Do not reply to this message. This e-mail message has been sent from an unmonitored e-mail address. We are unable to respond to any replies sent to this e-mail address.

[0800] If you continue to have access problems or want to report other issues, please Contact Us.

[0801] When the user clicks on the URL link in the email they will be taken back to a Verification Page on www.verification.ostiary.com

[0802] On this page they get this message:

Mail Verification Confirmation

[0803] Mr. Joe Blow form Microsoft you have successfully verified your e-mail address joe@microsoft.com with Ostiary Your Can now view all documents protected by Ostiary.

How Many Devices can a User Access Secure Documents from

[0804] A user can access documents from a restricted number of devices

[0805] From Their corporate PC

[0806] Their Laptop

[0807] Their Home PC

[0808] The system will bind a user corporate email to 1 or 3 devices based on the business rules In all cases the email and the PC's ID is bound and in ALL cases the user will have to go through the Email Verification method to bind the PC thumbprint.

What Happens when a user CHANGES their PC?

[0809] They have to go through a Device registration which is registering device ID and associating Email ids to this device

[0810] This is a Device only registration

How Many LOCATIONS can a User Access Sensitive Documents from

[0811] A user can access documents from ANY location in the world

[0812] Provided the Author has not restricted the access to certain locations

[0813] The system could restrict Persons access to few locations with ability to request for

[0814] Location extension to the Author.

The Ostiary Seal—your Email ID

Background

[0815] In many situations we check the credentials of people that we are dealing with—in banks, for building access, employee records, access to systems.

[0816] In the digital world and in particular with regards to email we don't have such an ID that enables someone to know that the sender is authentic. In the physical world, it takes considerable effort to change our physical appearance to assume another individual's identity however this is a simple task for email communications.

[0817] In all cases, a 3rd party provides a person with an ID. This ensures that the 3rd party has verified aspects of that person. In most cases this is done in person and requires that the person bring proof of claim of identity. Proof of claim of identity usually is drivers licence, Passport, Birth certificate, Bills from place of residence

[0818] The Individual Seal

[0819] The Company and Employee Seal

[0820] The Ostiary Seal will be an additional service that an Individual or Employee of a company can opt to get. In doing so there are some conditions and process that the company and employees need to go through to get the seal.

[0821] NOTE: Since employees are given an email address when they join and email addresses are revoked when they leave we can use this condition to control when a users Seal gets revoked without the need of an administrator.

[0822] This would however that the Email Server administrator send updates on current list or those that have been removed

The Basic Design Concept

[0823] The basic design is to

[0824] a. Enable a Company to request the Seal Service

[0825] b. Establish an Administrator or Seal Authoriser within the organisation (unless we create a self serve model)

[0826] c. Enable an Employee to Register for Personal Seal

[0827] d. Enable System to deregister Person form using Company Seal

[0828] Once a user has registered for a Seal they are able to use the seal in an Email.

Sample of Employee Seal

[0829] Ostiary

[0830] Graeme Marsh

[0831] VP Sales and Marketing

[0832] Ostiary ID Seal issued Jul. 23, 2004 3:23:00

[0833] To verify click here

How a Seal is Used

[0834] A user opens an Email and writes the message and maybe attaches a document.

[0835] From the tool bar user clicks the "INSERT SEAL" button

[0836] The agent checks the users email address

[0837] Agent interrogates the Seal Server looks up the seal associated with the email address and places a Generic Ostiary Seal in the email

[0838] (NOTE: At this stage the system does not know if the email address in the From field is actually the one being used)

[0839] Users then clicks SEND

[0840] NOTE: System has to ensure that the email address is legitimate

Opening an Email with a Seal

[0841] When the recipient gets the email and opens the email an agent attached to the email interrogates the seal server

[0842] Looks for the seal associated with the email

[0843] Places the seal in the email.

How to get the Ostiary Seal

[0844] To get the Ostiary seal the requestor also gets verified by Ostiary . The method to verify is however done electronically and with human intervention.

[0845] When a user registers for the Protection service they register as an Individual or as an employee of a company. In either case the process will be different.

TABLE 23

Type	Description
As An employee of a Company	Before an Employee of a company can get a seal the Company itself must subscribe to the service. Someone from the organisation is nominated to "authorise" requests for seals. (See process and UI for being nominated as "Seal Authoriser"
Process	Company Registering for the Ostiary Seal Service To register for the Seal service the company must be already registered for the Document Protection Service Once registered the company can get the Seal service by doing he following a. Log on to web site as Administrator b. Select Seal Service c. Register who in their organization will be the administrator and internal authoriser of seals d. Go through the Ostiary verification process for the proposed administrator Once the Authorised Administrator and Seal Administrator has been setup then the employees can register for their personal seals Revoking a Employees Seal
Process:	When an employee requests a seal steps This assumes that a. The company is already registered for the service b. The employee is already registered as a Reader or Writer c. The registered company has opted to take the Seal Service

TABLE 23-continued

Type	Description
	d. Someone has been appointed as the Companies "Seal" authoriser
	Employee logs onto system using us

The Ostiary Seal Design

[0846] The Seal is a simple object created on the fly that has the following data elements

TABLE 24

Data Element	Example
Name of Company	Ostiary INC
Employee Name	Graeme marsh
Employee Position	EVP Sales and Marketing
Date and Time Seal issued	07-23-04 3:23:00
Colour	Blue = Red = Yellow =

[0847] Ostiary INC

[0848] Graeme Marsh

[0849] VP Sales and Marketing

[0850] Ostiary ID Seal issued Jul. 23, 2004 3:23:00

[0851] To verify click here

Revoking a Seal

[0852] A seal can be revoked for the following reasons and by the following people

[0853] An employer can revoke a seal from an employee for whatever reason

[0854] Ostiary can revoke All seals for a Company but cannot revoke a seal for an individual employee.

[0855] Ostiary seals bring an additional level of trust to emails—in the same way as identity tags provide additional trust in our everyday workplace.

The NDA Registry System

The NDA Register

[0856] In many cases sensitive documents get exchanged AFTER an NDA has been signed between two people or two companies

[0857] The NDA essentially says that any information the company exchanges will be kept private and for the eyes of the company and their employees only.

[0858] The system will provide number of functionality

[0859] a. It will act as a central registry for companies that enter into an NDA relationship thereby enabling them to keep track of which companies they have an NDA with, Who entered the NDA agreement, when it expires, etc

[0860] b. It will attempt to replace the paper based NDA version with an online version using the Document protection Infrastructure

[0861] The intent is to tie the NDA registry to the Document protection system.

The Concept

[0862] The NDA Registry is a central registry enabling a company to keep track of all NDAs that they have entered into

[0863] The Registry can cater for documents that require physical signatures

[0864] But the registry will enable the ability to create NDAs with digitally signed signatures

[0865] The registry will also provide access to a template of standard NDA S that users can use if they don't have their own

[0866] The system can be used in conjunction with the Document Protection system to prevent documents sent from Company A to ONLY go to recipients whose email addresses are that of the signatory Companies

The Registry

[0867] IF Company A has entered the NDA details and Company B joins later then they can see the same NDAs and associate this with their details:

The NDA Data

[0868] Name of your Company

[0869] Name of the other party

[0870] The date of the NDA

[0871] The address details

[0872] The names of the signatory

[0873] The position of the signatory

[0874] The restriction i.e. only for Division

[0875] The domain names of the recipient companies that can use the documents

[0876] (The ability to block a NDA from being sent to or read in countries outside USA, for example)

The Domain Protection

[0877] With NDAs there is the notion that the NDA covers all employees within an organization.

[0878] How will the NDA registry and the document protection system work:

[0879] If two companies are registered in the NDA registry and any employee sends a document to another employee in that organization the system does the following

- [0880] a. Checks the email; address of the sender
- [0881] b. Looks at the Domain element of the email address
- [0882] c. Looks at the recipient email and specifically at the domain element
- [0883] d. Checks to see if the two parties have registered any NDA agreements
- [0884] e. If so it enables members of the companies to exchange documents in a secure manner

Membership Rules

- [0885] An Individual can subscribe for the Services
- [0886] A company can subscribe for the services

General Notes:

The Processes

The Subscription Process

- [0887] User subscribes
- [0888] They register their details
- [0889] They see the service options available
- [0890] They select the service they want
- [0891] The Upgrade Service Process
- [0892] They are able to upgrade the service plan
- [0893] The Document Protection Process
- [0894] The Web Protection Process

- [0895] Using the System to define the community of people that can see your stuff

- [0896] Defining the rules for what people outside of this community can do with your stuff

System Architecture

- [0897] DRM Server can be Centralized or distributed
- [0898] A Server holding the Docs can be as an ASP service and centralized for Small, SOHO and Personalized versions
- [0899] Enterprise markets will probably use their own Servers to hold their own documents but use Ostiary DRM systems to hold the Key infrastructure and the Comments and annotation data
- [0900] The R&P system can be centralized or decentralized and distributed So Enterprise users can host their own R&P servers

- [0901] Billing will be Central for US

Using Unique Values to Create a Protection System

- [0902] The purpose of this section is to describe the method, process and elements involved in constructing a Protection System
- [0903] There are many unique elements in the system that will enable us to use to create a
- [0904] Protection system or Protective Ecosystem
- [0905] The Unique Objects and their Elements

TABLE 25

Object	Uniqueness
Companies Unique Domain Name	Most companies have their own domain names. Every domain name is unique When a company has their own domain names they generally use this to create their employees email address. Example: Your_Company_Name
Readers Authors Unique Email	Every employee is given a email address constructed in the form of employees_name@companies_name.com This email address is unique at the Company AND in the world
Document ID	Every document has a unique ID and based on elements of the document a Unique ID can generated The elements can be Content Author name Date and time of Document etc
Readers PC	Every Readers PC or device has some unique characteristics Examples are make and model of one of the installed hard drives- make and model and model of one of the installed CD-ROM drives- make and model of one of the installed SCSI host adapters or IDE controllers- make and model of one of the installed graphics boards- make and model, serial number of the first CPU in the computer- size of the installed RAM- volume serial number of one of the available disk volumes Ethernet address one of the installed Ethernet adapters - These characteristics can be used to generate ONE hardware Hash Code for that device

TABLE 25-continued

Object	Uniqueness
Readers Access	Generally a Reader access the Internet from a minimum of 2
Location	Key areas Workplace Home In both cases the IP address and the Location of the Access Providers POP for that location can be determined This can lock in the location characteristics of a user

Other Scenarios:

Securing and Trusting the Email Attachments

[0906] Users are afraid of opening email attachments. When a user receives an attachment secured by the system there is a level of trust that they are getting the document from someone they know and that the attachment is secure. How to let users know that the attachment is from a secure environment

[0907] We introduce the concept of the registered user

[0908] When a user wants to secure the doc they register once

[0909] The system adds a logo to the email attachment so when the user receives the email.

[0910] A good example is: Say, Nextel and Wal-Mart have a project where Nextel is launching their products in Wal-Mart stores. Say Joe Blow is the project lead at Wal-Mart and Jenny Craig is the lead at Nextel. Now Joe has NO CLUE who is in Jenny's team and should not know, and Jenny has no clue who is in Joe's team.

[0911] However, the companies have entered into an agreement, and these two are officially the points of contact.

[0912] Say, Joe sends Jenny a doc, and it is protected. Jenny needs to send this Doc to her team.

[0913] How does she do this:

[0914] In this environment there is an implied TRUST between two points of contact between the two companies

[0915] Because of this we introduce the idea of "Forwarding Rights"

[0916] In this scenario Joe prepares the doc to send to jenny and turns on the attribute enable

[0917] Forwarding rights

[0918] When Jenny gets the doc she is able to forward the doc to her team members and JOE is

[0919] NOT involved in this process. But relies on Jenny's sense as to who should get the doc

[0920] On the systems audit trail which shows who DOES get the doc from jenny

[0921] Now Jenny can also send the doc with forwarding rights to the group or can withhold this

[0922] If she has withheld this and someone in her group tries to forward the doc, the unauthorized person is unable to open the message, and Jenny will get a message telling her who in her team tried to forward the doc.

[0923] The system can have say 1 level of forwarding or two levels.

[0924] In this way there won't be a need to have groups and manage this complexity

[0925] And we rely on the fact that the INITIAL two people have a shared and implied trust

[0926] Naturally, if there is no Forwarding Rights on a document, then Jenny would NOT be able to forward.

[0927] The other method was to have a concept called "Request to Open"

[0928] Say Joe sends Jenny a Doc with NO forwarding rights

[0929] Jenny send doc to 5 people who try to open

[0930] The system sends Jenny and Joe with a message saying that there has been a request to open by this list of people

[0931] Joe and Jenny allow or don't allow

[0932] The fact that people WILL know that the original senders will be notified if illegal access is tried will be a HUGE deterrent for people to send documents illegally

[0933] In this way the system self manages and removes the need for the complex issue of Groups

[0934] There are two concepts or objects here

[0935] 1. The trusted registered user

[0936] 2. The Group

[0937] 3. The Document in question

[0938] The system provides some smarts and protection for both objects independently and as a combination.

The Member Object

[0939] Being a member of the trusted group is a bit like signing a CENTRAL NDA with us and allowing everyone to share the benefits of that one time NDA signing. It also means that others can send you stuff, knowing that you are already setup to read their protected documents.

[0940] Since the system can track what a member does with respect to forwarding a protected doc that they were not supposed to forward the system can monitor this and based on rules do something if you transgressed this say 5 times. In other words, you get revoked when a member registers the system gets User Name Password Email Address Users PC fingerprint.

The Group

[0941] The Group could have its set of rules that govern that group and they could inherit from a Global Group set of rules to classes of groups that we setup, e.g. CFO class, CEO class, VP class.

The Document Object

[0942] The document has its own set of rules that govern behavior Once a Doc is an attachment to an email when its sent the System grabs the email address of the recipients and allows access to the document only from those recipients If a user tries to open it requires not only the recipients user name and password but also checks the PC Fingerprint. If this does not match up then the document just does not open. The system then sends an email to both the original sender and the recipient who forwarded the attachment letting them know that there was an attempt at unauthorized access.

[0943] You've pointed out an interesting thing: the notion of a trusted user based on registration. A trusted user can be sent documents from multiple sources with security ensured.

Tracking Documents Sent

[0944] There is a general need to track documents enabling an Author to see Who sent What to Whom and When

[0945] Some of the areas to track are

[0946] a. What documents did I (Mr. user) send, When did I send and to whom

[0947] b. Was it received and Did they open it

[0948] c. Did any of the recipients forward the document to an unauthorized Reader

[0949] The purpose is to enable Authors to see who is sending what sensitive documents to which unauthorized Readers

Tracking WHO sent WHAT Document to WHOM

[0950] When an Author or Sender attaches an Ostiary prepared document to an email and that email is sent, then the details of that transaction have to be registered with the Ostiary server. Information such as

[0951] Name of Author

[0952] Name of Sender

[0953] Name of Document

[0954] Version of Document

[0955] Date and Time of Document

[0956] Author info of Document

[0957] Recipients of Document Should be captured.

[0958] This method has to be automated unless the Sender is using the Web based method to make a document available.

[0959] Since a Recipient of a document can forward that document to an unauthorized user there is a need for the Author to track this. Not all Authors will want this so there is a need to enable the Author tell the system if they wish to track "Unauthorized forwarded" documents.

[0960] In this way the server maintains a record of ALL Recipients that receive the document.

Notifications

[0961] An Author can request that they be notified whenever a document has been sent to an unauthorized Reader. When this occurs the Author will be sent an email notification of the event (If this is turned On)

[0962] Notification can be done by email, SMS, etc.

[0963] The system has to enable the Author to select this option

[0964] Document History

TABLE 26

Document Name:	The potential merger of Microsoft and IBM .doc
Name of Author:	Bill Gates
Sent By	Sarah McDonald

[0965]

TABLE 27

Doc Ver	Date First Sent by Author	Recipients	Email Address	Location	Company Name	Web Site	Date opened	Date re-sponded
1.0	Aug 12 th 04	Bill Gates	bgates@microsoft.com	Internal	Microsoft	www.microsoft.com	Aug 15 th 04	
	12:16:53	Louis Gerstner	lgerstner@ibm.com	External	IBM	www.ibm.com	12:19:45	
		John Berry	john.berry@morganstanley.com	External	Morgan Stanley	www.morganstanley.com		
		Jenny Brighton	jbrighton@lehmanbros.com	External	Lehman Bros	www.lehmanbros.com		
		Jeremiah Johnson	jjohnson@citiobank.com	External	CitiBank	www.citiobank.com		

[0966] Unauthorized Forwarding

TABLE 28

Sent by	Sent Email	Sent to	Date Sent	Open Attempt
Bill Gates	Larry.ellison@oracle.com	Larry Ellison	Aug 21 st 04	None
	Scott.McNealy@sun.com	Scott McNealy	Aug 21 st 04	Twice
Jenny Brighton	jeff.borland@blrland.com	Jeff Borland	Aug 22 nd 04	Three
	sam.albus@citiobank.com	Sam Aldus	Aug 23 rd 04	None

[0967] Authorized Forwarding

TABLE 29

Sent by	Sent Email	Sent to	Date Sent	Open Attempt
Louis Gerstner	Larry.ellison@oracle.com	Larry Ellison	Aug 21 st 04	None
	Scott.McNealy@sun.com	Scott McNealy	Aug 21 st 04	Twice
Jenny Brighton	jeff.borland@blrland.com	Jeff Borland	Aug 22 nd 04	Three
	sam.aldus@citibank.com	Sam Aldus	Aug 23 rd 04	None

Notes:

when an Author SENDS a document we won't have the name of the recipients but only their Email address. The ONLY way we will get the name is when the Reader registers. If a Reader sends a document to an unauthorized unregistered person then we will only have their email address.

What Happens when a Reader Gives up their Email Address

[0968] Like telephone numbers a reader can cease using their telephone number and someone else can get this.

Re-Authenticating a Reader and their devices

[0969] There are many reasons why there is a need to re-authenticate a Reader

- [0970]** a. When they sell their Device
- [0971]** b. When they give away their device
- [0972]** c. When their device has been repaired

[0973] Methods:

[0974] if a user starts using a new device, he gets re-authenticated.

[0975] as part of the re-authentication process, he can disable the old device(s)

[0976] we may want a provision to disable a device after a long period of no use. The user can always re-register.

[0977] a single password for all Ostiary docs the reader has is required. We may want to use .Net at some point as an option.

TABLE 30

Object	Description	Links
Publisher/ Author	A Publisher or Author Publishes things These are called Protected Published Objects Examples of PPO are Documents Music Video	Protected Published Objects
Protected Published Objects	Either these objects are for FREE access or for authorized access The Publisher grants Authorized Reader Access on the basis of a. Privilege b. Payment c. Other reasons Once access is granted to a Reader the Readers details are entered into an Authorized Access List. Every PPO has a Unique Object ID that identifies that object. The Unique Object ID is potentially generated differently for different Object types	Authorized Access List Unique Object ID
Authorized Access List	This is the DB that contains the list of all Authorized Readers the PPO that they are authorized to access Their Details (name, Internet address etc)	Unique Object ID Readers Digital ID
Object ID	This is the Unique ID(a long string) that is generated for each Object. Part of the ID contains info on the Object Type For example the Doc ID is generated from a. Object Type b. Name of Document c. Date and time d. Content e. Authors name f. etc The ID is encrypted	Current cookie Unique Object Keys
Object Keys	Every Object is encrypted when sent to a Reader The keys used to encrypt and de-crypt the object are central to Access of the Object	

TABLE 30-continued

Object	Description	Links
Readers Digital ID	Every Reader that is registered with the central system is given a Unique Digital ID This ID is generated from a number of data elements including Person e-mail address Their PC Hardware ID elements e.g. CPU number, Mac Address	Device ID Readers Details
Current Cookie	Cookies are generated by the Ostiary server and placed on a Readers Device EVERYTIME a Reader makes a request for access to a document. At the server end Cookies are Associated with a. ALL Object IDS that a Particular Reader is Authorized to access b. ONE of the Readers Digital ID associated with a particular Device Cookies are associated with is used to ensure that a. The Requesting Device is a registered device b. That A cookie is generated at the Ostiary server and associated with A particular Objects ID A particular Readers Device ID When a Reader wants to have access to a Document the Ostiary Server asks the Question "what is the cookie number" The BPI then supplies the cookie and the Document ID to the Ostiary server The Ostiary server then checks if the cookie received, matches the Document ID on the server receiving the cookie it can determine if that cookie should get access to the document being requested. This is the first simple pass MATCHING. It leaves a cookie ID. Every time The cookie ID is associated with The Readers Digital ID. the Object IDs Every time it communicates it leaves a different cookie The cookie is used to determine if the sending Readers Device	
Readers	A Reader can have many devices Each Device has one Device ID A reader has only ONE email from one employer at any one time But a Reader can have more than one employer Example: A consultant working for company x and working for their own company will have two email addresses A reader can use their ISPs email address A reader can have more than one digital ID	
Devices	Each Device has to be able to generate some unique Device ID This is done either form a single data element or From a composite of data elements inherent to that device	
Email	While a Reader may be employed by several companies EACH company will only provide ONE email address But a Reader can have several Emails Example Joe Blogs can have the following Private: joebloggs123@yahoo.com Main Employee: joe.bloggs@greatconsulting.com Company consulting to: jbloggs@microsoft.com Their OWN Company: joe@bloggs.biz But the emails are independent of the devices being used and ALL emails could be used on ALL devices from Outlook or Web Based email	
Readers Digital ID	Each Digital ID is a combination of Email and Device ID The Same device can have two or more Digital IDs operational on that Device ID	

[0978] In general the system associates the Reader with

[0979] the Devices they use

[0980] The Email address they get

[0981] Since a Reader can have one or more of both the result is a matrix

[0982] The result is that the Reader can get as many as 4×3=12 Digital IDs registered in the system. This is like getting 12 Credit cards from 12 different companies.

[0983] Email to Device Matrix for a Reader

TABLE 31

	Device 1	Device 2	Device 3
Email 1	Email 1. Device ID 1	Email 1. Device ID 2	Email 1. Device ID 3
Email 2	Email 2. Device ID 1	Email 2. Device ID 2	Email 2. Device ID 3
Email 3	Email 3. Device ID 1	Email 3. Device ID 2	Email 3. Device ID 3
Email 4	Email 4. Device ID 1	Email 4. Device ID 2	Email 4. Device ID 3

[0984] Furthermore a Device can have different players from different vendors and a Player can be installed on different devices owned by the Reader

[0985] But each player installed on each device will have a unique serial number Player to Device matrix

TABLE 32

	Device 1	Device 2	Device 3
Player 1 (P1)	P1.SN.x1. Device ID 1	P1.SN.x2. Device ID 2	P1.SN.x3. Device ID 3
Player 2 (P2)	P2.SN.x4. Device ID 1	P2.SN.x5. Device ID 2	P2.SN.x6. Device ID 3
Player 3 (P3)	P3.SN.x7. Device ID 1	P3.SN.x8. Device ID 2	P3.SN.xn. Device ID 3

[0986] Each Device has ONE cookie regardless of the number of 3rd Party Players installed.

[0987] ALL players will use the Ostiary cookie for that Device.

[0988] Cookie to Device Matrix

TABLE 33

	Device 1	Device 2	Device 3
Cookie 1	Cookie 1. Device ID 1		
Cookie 2		Cookie 2. Device ID 2	
Cookie 3			Cookie 3. Device ID 3

[0989] Every Reader registered will have ONE user name and password

[0990] Reader to User Name and Password

TABLE 34

	Device 1	Device 2	Device 3
Cookie 1	Cookie 1. Device ID 1		
Cookie 2		Cookie 2. Device ID 2	
Cookie 3			Cookie 3. Device ID 3

Associating Many Email and Digital IDs under one Reader Name

[0991] A Reader could have many email address and Device resulting in many Digital IDs. The system has to enable a Reader to consolidate all IDS and emails under one roof This means that a Reader can register and get a Normal User account and have this one user account consolidated.

[0992] In principle a Reader can have several Identities based on their association with that entity:

[0993] My Private Identity

[0994] My Id with my Employer

[0995] My ID with the company I consult with

[0996] In all cases, these can be generated independently. At any time, a Reader can consolidate.

[0997] Note: Any variation of the teachings above is also intended to be covered and protected by the current patent application.

1. A system to manage, control, track, or monitor access, usage, view, provide comments, or provide collaboration environment for digital contents or services, said system comprising:

an environment to offer digital contents or services by a provider; and

a network of one or more computers, telephones, communication devices, mobile devices, wireless devices, cellular devices, PDAs, electronic devices, nodes, routers, hubs, optical devices, connection means, or switches,

wherein said provider or another entity assigns one or more rights, constraints, limitations, or privileges to one or more users,

wherein said one or more users operate, access, or use said network, and

wherein said one or more users are controlled, monitored, constrained, or limited by said one or more rights, constraints, limitations, or privileges.

2. A system as recited in claim 1, wherein said system is used in an ASP service.

3. A system as recited in claim 1, wherein said system is used to collaborate on or jointly edit or modify a common document or digital content.

4. A system as recited in claim 1, wherein said system incorporates an encryption and/or electronic signature scheme, method, or module.

5. A system as recited in claim 1, wherein said system incorporates one or more of the following for the authentication process: an e-mail ID, password, biometrics, digital certificate, hardware ID, software ID, cell phone ID, or a random number generator on a USB device.

6. A system as recited in claim 1, wherein said system enables a federated approach to control, monitor, or manage the comments, inputs, or feedbacks, and/or enables a federated or centralized approach to managing the distributed user's authentication and authorization, for all companies in a given country or spread globally.

7. A system as recited in claim 1, wherein said system provides a mechanism to move a threaded conversation, e-mail trail, feedback trail, input, reply trail, response trail, or continuous collaboration from one version to another version.

8. A system as recited in claim 1, wherein said system manages one or more registered users and providers as a part of a community, circle, secured network, private network, virtual trusted network, or closed network.

9. A system as recited in claim 1, wherein said system provides a mechanism to enable users in a circle to inherit items or characteristics supplied or applied by a provider, in addition to the users' own items or characteristics.

10. A system as recited in claim 1, wherein said system provides continuous and persistent protection for said provider.

11. A system as recited in claim 1, wherein said system provides a safe forum for exchanging, sharing, editing, conferencing, or collaboration on sensitive or confidential business information, through one or more documents, one or more web sites, or one or more business blogs.

12. A system as recited in claim 1, wherein said system provides a network-based management of shared electronic files.

13. A system as recited in claim 1, wherein said system is used on the Internet.

14. A system as recited in claim 1, wherein said system is used for one or more of the following applications: information about a merger or acquisition, companies' financial information, proprietary information shared with a corporate partner, information about a new product launch, research information around a proposed new patent, HR or compensation information on employees, or an intranet web site.

15. A system as recited in claim 1, wherein said system enables companies to send documents anywhere in the world, and receive a high level of protection, regardless of the location of users.

16. A system as recited in claim 1, wherein said system provides the foundation for a user, document delivery agent, or digital identity created from a composite of elements.

17. A system as recited in claim 1, wherein said system provides hierarchical structure for the documents or contents.

18. A system as recited in claim 1, wherein said system provides hierarchical structure for the rights.

19. A system as recited in claim 1, wherein said system provides hierarchical structure for the services.

20. A system as recited in claim 1, wherein said system provides composite documents or contents.

21. A system as recited in claim 1, wherein said system provides composite rights.

22. A system as recited in claim 1, wherein said system provides composite service offerings.

23. A system as recited in claim 1, wherein said system provides one or more withdrawn rights or expired rights.

24. A system as recited in claim 1, wherein said system provides executable codes.

25. A system as recited in claim 1, wherein said system provides a central non-disclosure agreement registry for one or more entities or companies.

26. A system as recited in claim 1, wherein said system provides a secure guaranteed on-line signing process for business or non-business contracts and agreements.

27. A system as recited in claim 1, wherein said system provides a method to segregate threaded document messages into two or more message channels.

28. A system as recited in claim 1, wherein said system is used in a court or a legal organization.

29. A system as recited in claim 1, wherein said system provides the view of or access to the content for a selected set of users.

30. A system as recited in claim 1, wherein said system enables multiple users and/or providers manage different versions of the same original digital object.

31. A system as recited in claim 1, wherein said system provides a receipt of delivery and receipt of initial access.

32. A system as recited in claim 1, wherein said system provides alert to said provider.

33. A system as recited in claim 1, wherein said system provides notification of the key events.

34. A system as recited in claim 1, wherein said system is based on a browser-based or a desktop application.

35. A system as recited in claim 1, wherein said system provides link between digital objects.

36. A system as recited in claim 1, wherein said system provides link to one or more databases.

37. A system as recited in claim 1, wherein said system provides means of changing or viewing authorship and/or ownership.

38. A system as recited in claim 1, wherein said system interacts with an address book.

39. A system as recited in claim 1, wherein said system provides a role or context-based right assignment.

40. A system as recited in claim 1, wherein said system provides a usage policy.

41. A system as recited in claim 1, wherein said system uses biometrics, fingerprint, signature, header, hash, or any other unique features for authentication.

42. A system as recited in claim 1, wherein said system provides the document or digital object keyword list.

43. A system as recited in claim 1, wherein said system provides employee registration.

44. A system as recited in claim 1, wherein said system provides audit trails.

45. A system as recited in claim 1, wherein said system provides digital signature and approval for documents, comments, or actions.

46. A system as recited in claim 1, wherein said system provides the delegation of one or more rights to another entity.

47. A system as recited in claim 1, wherein said system provides a digital license or a token.

48. A system as recited in claim 1, wherein said system provides a method to segregate threaded document messages into private and public message channels between two or more companies, and/or within each divisions or functions of a company.

49. A system as recited in claim 1, wherein said system provides a mechanism that enables two or more users to share the simultaneous viewing of a document, wherein one of the users has the control of the document and its changes, actions, or movements.

50. A system as recited in claim 1, wherein said system presents intensity of the relationships as an indication of the frequency of interactions for one or more documents and the users.

51. A system as recited in claim 1, wherein said system presents intensity of the communication relationship as an indication of the frequency of interactions with comments for one specific document or series of documents.

52. A system as recited in claim 1, wherein said system uses the frequency of the usage of the keywords as an indication of the interest level of said provider or user with respect to the subject matter or keywords.

53. A system as recited in claim 1, wherein said system provides classification using keywords.

54. A system as recited in claim 1, wherein said system uses two or more keywords sharing some basic or fundamental concepts, to be able to classify.

55. A system as recited in claim 1, wherein said system stores history and activity.

56. A system as recited in claim 1, wherein said system status, parameters, or appearance is dynamically changing.

57. A system as recited in claim 1, wherein said system interacts with a group of users to expose and analyze the social interactions that arise from the shared objects.

58. A system as recited in claim 1, wherein said system only stores one copy of the e-mail for all the recipients or users.

59. A system as recited in claim 58, wherein said system prevents forwarding the e-mail to a third party.

60. A system as recited in claim 58, wherein said system allows the removal of a non-intended recipient's name from the list of recipients in an e-mail, and wherein said system further allows the removal the right to access or usage associated with said non-intended recipient.

* * * * *