A COMPUTER SYSTEM FOR AUTOMATING THE CONTROLLED DISTRIBUTION OF DOCUMENTS

FIELD OF THE INVENTION

This invention relates to a computer system for automating the distribution of documents requiring control of the parties who can view and print the documents.

SUMMARY OF THE PRIOR ART

In the prior art when a party wished to limit who could print a document the party would restrict printing of the document by printing the document themselves and physically delivering a printed copy to the party requesting the document. As an example while an exporter can currently in some jurisdictions file an application for a certificate of origin electronically there is still the requirement to physically collect or have delivered the certificate once the certificate has been processed and printed.

US 2001/0013025 describes a method of controlling the printing process by having specialised software print directly to a printer. This method requires that the computer that is to be used for printing have the specialised software installed.

Other software such as Adobe Acrobat allows the creation of files that can be protected by limit printing but because the user has a copy of the file the there is a security risk that the protection can be overridden.

SUMMARY OF THE INVENTION

The present invention may broadly be said to consist in a computer system for allowing the secure creation of documents requiring certification or authentication from a certifying or authenticating authority in electronic form upon application therefor by subscribers and for controllably releasing such documents in copy-protected paper form to third parties comprising:

means for assembling the text of said documents;

such documents in the description is for illustrative purposes only. The generic trusted document repository is also suitable for distribution of other certified or secure documents where it is desirable to restrict the number of printed copies made by a recipient.

A Certificate of Origin (CO) is a document, required by foreign governments, declaring that goods in a particular international shipment are of a certain country of origin.

Referring to Figure 1 the secure document repository 101 has an interface for communicating with an exporter or agent 102, an interface for communicating with an authorising authority 103, an interface for communicating with a document receiving party 104 and a data store 105. Communication between the document repository and the exporter/agent 102, the authorising authority 103, and the document receiving party 104, is made using secure communication methods such as public key encryption infrastructure to ensure that all communications are secure and trusted. In addition to interfaces to communicate with the parties, the secure document repository has a document assembly engine 106 for assembling the documents and a work flow engine 107 for ensuring the progress of the document and communication with the various parties follows a work flow agreed to by the authorising authority. The repository has a data store to store information on the various parties.

In the preferred embodiment the communication interface is provided by a web server. The web server provides the communication channel between the parties and the repository. The web server has an interface to enable applicants/agents to register with the repository. In alternative forms the repository would communicate with some of the parties using other known secure electronic data interchange methods such as MIME based secure EDI.

identification code and security code in association with the data collected from the application form.

To request electronic certification of documents from a particular certifying authority a user will apply to the authority via an online form served by the repository web server. The repository will process the user's request and forward the user's request and details of the user to the identified certifying authority for approval. In the preferred embodiment the repository would via electronic mail notify the certifying authority that a user had requested to be allowed to apply for certification online, the authority would then log onto the repository via the web server and authorise the user or reject the application as the case may be.

In an alternative embodiment the repository would communicate with the certifying authority using electronic data interchange methods and the repository would receive the approval back in the same manner. Once approval has been granted the repository will record that the user is allowed to apply for certified documents from the certifying authority that has approved the user so to do in it's data store in association with the user identification code. The user will need to apply using the repository web server for approval for every authority the user seeks certified documents from.

Via online forms the repository web server will allow users to delegate authority to agents to enable agents to apply for certified documents on their behalf. The agent to whom the delegation is made must also be an authorised user and authorised by the relevant certifying authority. The repository web server will store the delegation information in association with information kept on the exporters/agents and certifying authority in the repository data store.

A user may limit an agent's delegation to a applying for certification from particular certifying authorities. This is done via an online form served by the

If the repository web server identifies that it is an agent applying then, having authenticated the agent, the repository will present from its data store a list of users the agent is authorised to apply on behalf of, and require a selection from this list before providing the agent with a choice of certifications to apply for.

When an application is made the repository notifies the issuing authority 202 via electronic mail that an application has been made and the issuing authority will approve or reject the application using an online web interface or using secure electronic data interchange methods. Issuing authorities may delegate the approval of certification to the repository. The approval of the repository may be limited to, for example, certifications below a certain threshold value or a particular type of certification. For quality control delegation may require that a proportion of applications is sent to the authority for checking before approval.

When the issuing authority has approved the application the document assembly engine will create a two certificates using the data provided by the applicant, the certifying authority business rules. After the documents are created the repository will store in the documents in its data store. The stored certificates will be in a form approved by the issuing authority. One version of the document is created without an official indicia and one version is created incorporating the official indicia, repository document number and repository security code.

Once the document is assembled the repository electronically notifies the applicant 203 (and if requested the third party 204 requiring the document) via electronic mail that the document is available for electronic collection. The notification will include a web page address based on the repository document number and an appropriate security code so that the party is able to view a copy of the digital document via the Internet. A third party such as a bank my forward the information to an overseas bank or customs office 205 that requires the document.

Parties who desire to be able to print certified copies may need to register with the repository and be authorised by the certifying authority who certified documents they wish to print depending on the requirements of the certifying authority. The application can be made online via the repository web interface and is processed and the information stored in the same manner as if the party who wishes to print was a party who wished to apply online.

In order to print the documents in a secure and controlled manner, the repository forwards a data stream in a print control language directly to a printer. The data stream corresponds with the fully certified document including certifications (seals, stamps, signatures etc). Examples of such printer control languages include pcl and postscript.

In the preferred embodiment Sun Microsystems Java Print Service API via a java applet is used to print a data stream in a printer control language directly to a printer without permitting user intervention. Because the Java Virtual Machine is usually installed on a computer with a web browser it is only necessary to download the Java Runtime Environment. Such a download need only be done once and is available at no charge. In addition the security model built into Java means that the receiving party can be sure that the applet was created by a trusted party, in this case the repository.

CLAIMS

1. A computer system for controllably releasing certified or authenticated documents in copy-protected paper form to third parties comprising:

an approval interface for enabling a certifying authority to approve a certified or authenticated document for release;

third party display means for allowing a third party to view a said document approved for release without certification or authentication indicia inserted; and

third party print means which allows said third party to request a print of a limited number of copies only of said document including certification or authentication indicia on a printer local to that third party.

2. A computer system as claimed in claim 1 including:

a repository for storing documents and associated indicia;

said approval interface includes means for a certifying or authenticating authority to cause documents with and without inserted indicia to be stored in said repository;

said third party display means is programmed to retrieve a said document without indicia for viewing by a third party; and

said third party print means is programmed to retrieve a said document with indicia for printing on said printer local to said third party.

3. A computer system as claimed in claim 1 for allowing the secure creation of documents requiring certification or authentication from a certifying or authenticating authority in electronic form including:

means for assembling the text of a said document;

a repository for storing assembled documents and certification or authentication indicia appropriate to selected classes of documents.

4. A computer system as claimed in claim 1 for allowing the secure creation of documents requiring certification or authentication from a certifying or authenticating authority in electronic form upon application therefor by subscribers and for controllably releasing such documents in copy-protected paper form to third parties comprising:

a subscriber interface for requesting the assembly of a specific document and for supplying data specific to each request for assembly into that document;

means for assembling the text of a said document;

a repository for storing assembled documents and certification or authentication indicia appropriate to selected classes of documents;

means for notifying the appropriate certifying or authenticating authority of a request for a document requiring certification or authentication by that authority.

assembling said document with certification or authentication indicia for said printing.

11. A method for controllably releasing certified or authenticated documents in copy-protected paper form as claimed in claim 10 including the steps of:
verifying that said document can be certified or authenticated; and
certifying or authenticating said document.

12. A method for controllably releasing certified or authenticated documents in copy-protected paper form as claimed in claim 10 including the steps of:
notifying an appropriate certifying or authenticating authority of a request for a document requiring certification or authentication by that authority;
receiving from said authority approval to certify said document; and
certifying or authenticating a said document.

13. A method for controllably releasing certified or authenticated documents in copy-protected paper form as claimed in claims 10 to 12 including the step of notifying said subscriber that an authenticated document is available.

14. A method for controllably releasing certified or authenticated documents in copy-protected paper form as claimed in any of claims 10 to 13 including the step of notifying at least one third party that an authenticated document is available.

15. A method for controllably releasing certified or authenticated documents in copy-protected paper form comprising the steps of:
receiving subscriber data and request for the assembly of a specific document from a subscriber;
verifying that said document can be certified or authenticated;
certifying or authenticating said document; and
notifying a third party indicated by said subscriber data that an authenticated document is available.

16. A method for controllably releasing certified or authenticated documents in copy-protected paper form as claimed in claim 15 including the step of notifying said subscriber that the authenticated document is available.

17. A method for controllably releasing certified or authenticated documents in copy-protected paper form as claimed in claim 15 or 16 wherein said step of verifying that said document can be certified or authenticated comprises:
notifying an appropriate certifying or authenticating authority of a request for a document requiring certification or authentication by that authority; and
receiving from said authority approval to certify said document.