SYSTEM AND METHOD FOR AUTHENTICATING PAPER DOCUMENTS OVER A NETWORK

The present invention relates to a possible system and method of paper-document authentication via a server-sided application.

Every day, thousands of paper documents including letters, certificates, bills, degrees, bank statements, etc. are issued by various organizations and authorities all over the world. The present methods of authenticating such paper documents include use of embossed seals, rubber stamps or signatures of the document issuer on the document. Irrespective of the type of the document being issued and the type of the conventional authentication method being used, all paper documents can easily be forged in one way or another leading to fraud.

The present invention eliminates chances of fraud by adopting a different approach for verification of paper documents. A central server running over a computer network (Internet, LAN, WAN, etc.) acts as a document repository where digital copies of all paper documents are uploaded by the document issuer, saved along with the verification information of the document issuer and available for later retrieval for verification purposes. Conventional stamps, seals or signatures are replaced by the server-generated URL or the barcode storing the URL that leads to the original stored document on the server along with the document verification information.

Any deliberate or accidental changes made to the paper copy of the document would not affect the stored, digital copy of the document on the server in any way leading to a visible mismatch between the digital copy stored on the server and the tampered paper copy of the document. Additionally, it would be ensured that the paper copy of the document was issued by the document issuer claiming to be the original issuer of the document.

The method can either be used independently or in addition to the conventional seals, stamps and signatures to authenticate paper documents in a rapid, fool-proof way.

An example of the invention will now be described by referring to the accompanying drawings:

Figure 1 shows a server 1 running software-as-a-service which stores, protects, authenticates and helps in retrieval of stored documents. The document issuer uploads a valid digital copy of the paper document (either a scanned image of the original paper document or a digitally rendered document which is to be printed) on server 1 using computer 3 and over network connection 2. Server 1 stores the document and generates corresponding unique URL and/or a barcode containing at least the URL at which the document can be accessed and verified by the document recipient (verifier). The digital copy of the document is returned to the document issuer on computer 3 with the URL and/or barcode embedded on the digital copy of the document in lieu of a conventional seal, stamp or signature over network connection 2. The paper copy 5 of the digital document containing the embedded URL and/or barcode can be printed by the document issuer using printer 4 connected to computer 3. Paper copy 5, which is the hard copy of the digital copy returned by server 1 may now be sent to the recipient via any means including postal mail or handing in person.

Figure 2 shows a method that the document recipient (verifier) can now follow to verify the authenticity of the paper document 1. The URL printed on the paper document 1 can be accessed using a web-browser on recipient's computer 2 or digital device 7 (which could be a mobile phone, Smartphone, PDA, tablet PC etc.). Alternatively, if the paper document 1 contains a printed barcode can be scanned by a camera of digital device 7 and depending on the capability of digital device 7, a web-browser or a similar application is launched navigating to the URL contained in the barcode.

The URL retrieves the stored digital copy 3 or 8 of the document (depending on whether computer 2 is used or device 7 respectively) from server 5 over a network connection (preferably the Internet) 4 or network connection 6 (depending on whether computer 2 is used or device 7 respectively) along with an assertion statement that the document as displayed on computer 2 or device 7 was issued by the document issuer claiming to be the sender and/or issuer of the document. Preferably, the details of the document issuer are also displayed.

Claims

1. A server at least capable of receiving and storing digital copy of one or more document(s) and being able to generate a corresponding URL and/or barcode containing at least the corresponding URL pointing to the document(s) stored on the server, upon accessing which the stored digital copy of the document(s) is retrieved and displayed along with the verification statement on the digital device of the document recipient.

2. Server according to claim 1, in which document issuer refers to an individual, organization or institution claiming to be the original issuer of the paper document.

3. Server according to claim 1, in which the digital device refers to a computer, tablet computer, mobile phone, Smartphone, PDA or a device at least capable of accessing a computer network.

4. Server of according to claim 1, in which the document recipient or verifier refers to the individual, organization or institution receiving the paper copy of the document containing the unique URL and/or the generated barcode.

5. Server according to claim 1, in which verification statement refers to a statement which includes or excludes the details of the document issuer but asserts that the document was issued by the document issuer claiming to be the original issuer of the paper document.

Abstract

Server 1 running software-as-a-service stores and helps in retrieval of stored documents. The document issuer uploads a valid digital copy of the paper document (either a scanned image of the original paper document or a digitally rendered document which is to be printed) on server 1 using computer 3 and over network connection 2. Server 1 stores the document securely and generates corresponding unique URL and/or a barcode containing at least the URL at which the document can be accessed and verified by the document recipient (verifier). The document recipient or verifier can access the URL to retrieve an exact copy of the stored document on the server along with the verification information of the document issuer.

Use figure 1.