METHOD FOR CERTIFYING LOCATION STAMPING FOR WIRELESS TRANSACTIONS

Field of the Invention

The present invention relates to the stamping of a transaction conducted over a wireless medium with geographic position information specific to the wireless device engaged in the transaction. Specifically, the invention relates to a method for establishing the credibility of geographic location information associated with information transmitted from a wireless device for non-repudiation purposes.

Background of the invention

Wireless devices, such as mobile phones, PDAs, laptop computers, etc, are used to conduct a variety of transactions over wireless media. The geographic position of such wireless devices can be determined by a variety of methods and technologies known to persons of ordinary skill in the art. Information concerning the geographic position of a wireless device can be used to increase the security of transactions conducted over wireless media. Specifically, attaching information about the geographic position of a wireless device with a message or information transmitted from the device is called "location stamping" and is analogous to more widely known time stamping of documents. However, ways of altering the location information associated with a message or information transmitted from a wireless device are also known. Accordingly, there exists a need for a way to validate and certify location stamping of digital documents and information transmitted from wireless devices.

Brief Description of the Invention

The present invention provides a method for certifying location information with respect to a specific wireless device, and associating the certified location information with data, information, documents, and/or transactions originating from the device. According to the invention, a wireless device may be any device that can transmit and receive information over a wireless medium. In addition, the invention may be used in connection with hard-wired devices that are location aware, or the location of which may be determined by virtue of it's connection to a network. The

availability of position information enhances the value of the data, information, documents and/or transactions originating from the device and hence adds a level of convenience to the user of the wireless device, allowing him or her to conduct a wider range of transactions. When messages originating from a wireless device are accompanied by certified and non-repudiable location information, the value of the device may be substantially increased to the extent that location information may be required for security purposes in certain wireless transactions.

Accordingly, the present invention provides methods of certifying location (geographic position) information associated with wireless devices, whether the location information is computed by the wireless service provider that provides wireless service for the subject wireless device, whether it is computed by some other trusted service that has the capability of computing the location of a wireless device, or whether it is computed by the wireless device itself.

In the instances where location information is computed by a wireless service provider, a wireless device user may transmit a message to a location certification server and request a certified location stamp. According to the present invention, a location certification server may be any computer that can prepare and verify digital signatures. Optionally, a location certification server may have the processing power and software necessary to encrypt and decrypt messages. According to a further option, a location certification server may have the ability to maintain secure connections with wireless devices and/or other computers, in which case it need not use digital signatures for authenticating between parties. The location certification server may optionally add its digital signature to the request, and forward it to a location determination server where the geographic position of the device is computed according to methods known in the art.

According to the present invention, a location determination server may be any computer that can compute the geographic position of a wireless device and prepare digital signatures. Optionally, a location determination server may have the processing power and software necessary to maintain secure connections with other computers, for example, location certification servers. The location determination server then adds the location information to the request, certifies it with its digital signature and sends the signed request back to the location certification server which

then verifies the digital signature of the location determination server, adds its own digital signature and then sends the authenticated location information back to the wireless device.

Alternatively, a wireless device user may conduct a transaction with a third party, for example, an e-commerce vendor, and during the transaction or following the conclusion of the transaction, the e-commerce vendor may transmit a request to a location certification server for determination and/or certification of location information particular to the wireless device on which the transaction was or is being conducted. According to one embodiment of the invention, the third party requestor sends a document representing the transaction to the location certification server and the location certification server forwards the document to a location determination server for determination of the geographic position of the subject wireless device. The location determination server then appends location information to the transaction document together with a digital signature and returns it to the location certification server. The location certification server then verifies the location determination server's digital signature, appends it's own digital signature and returns the transaction document to the third party requestor with the location information and the two digital signatures.

In instances where the location (geographic position) information is computed by the wireless device itself, the wireless device may add the location information to a document and self-certify the location information by adding a digital signature. If the wireless device does not have sufficient computational power to generate a digital signature in a commercially reasonable period of time (in the context of wireless transactions), the wireless device may encrypt the document and the geographic location information using any known encryption system, and may transmit the encrypted document and geographic location information to a location certification server which decrypts the document and geographic location information and adds a digital signature. Then, depending on the configuration of the system and/or the wishes of the wireless device user, the location certification server may return the document bearing the geographic location information and the digital signature to the wireless device, forward to an intended recipient identified by the user of the wireless device, and/or archive it. In both of the instances where the location information is

computed by the wireless device itself, the software for location determination, for encryption and/or for generating a digital signature, may be saved in the device in a tamper-resistant fashion, that is, in such a way that if these features of the device are tampered with, the device may be disabled, or the location determination and certification features may be disabled. In addition, the computation of location information, the encryption of the information, and transmission to the service provider for certification may optionally be completely transparent to the user.

According to another embodiment of the self-certifying embodiment of the invention, a wireless device engaged in a transaction with a third party may determine it's own position, append the location information to a document representative of the transaction, optionally encrypt the location information, optionally certify the location information with a digital signature, and transmit the location certified document to the third party. If the third party cannot decrypt the encrypted location information or verify/validate the digital signature, the third party may optionally forward the location stamped transaction document to a location certification server for decryption of the location information or verification/validation of the digital signature and for verification and certification of the location information appended to the transaction document.

According to a further optional feature of the invention, a secure connection may exist between any two or more of the relevant actors. That is, a secure connection may exist between the wireless device and the location certification server, or between the location certification server and the location determination server, or between the wireless device and the location determination server. According to this optional feature of the invention, the digital signatures may be dispensed with whenever there is a secure connection between two parties, except that a digital signature is always appended to the document, together with the location information, by the location certification server when the location stamp is prepared.

The foregoing aspects of the invention may be summarized as follows:

i) A request for certified location information originates from the device
    a) the device calculates its own geographic position;
    b) an LDS calculates the device's geographic position;
ii) A request originates from a party to a transaction with the device
    a) the device calculates its own geographic position;
    b) an LDS calculates the device's geographic position.

Each of these scenarios will be described in more detail below with reference to the drawings.

Brief Description of the Drawings

Figure 1 is a block diagram illustrating the relationship between entities that perform operations according to the present invention.

Figure 2 is a flowchart showing steps performed by a location certification server according to one embodiment of the invention.

Figure 3 is a flowchart showing steps performed by a location determination server according to one embodiment of the invention.

Figure 4 is a flowchart showing steps performed by a wireless device or a third party requestor according to one embodiment of the invention.

Figure 5 illustrates the steps according to one embodiment of the self-locating wireless device aspect of the invention.

Figure 6 illustrates the steps according to another embodiment of the self-locating wireless device aspect of the invention.

Detailed Description of the Preferred Embodiments of the Invention

Figure 1 presents a general overview of the processes and relationships of the invention. According to a first aspect of the invention, a wireless device 10 or a third party requestor 11 sends a request to a location certification server 16, over a network 14. The location server 16 signs and forwards the request to a location determination server 18 for determination of the geographic position of the wireless device. The location information is then sent back to the location certification server 16 and the location certification server 16 sends the location information back to the requestor, which may be either the wireless device 10 itself or a third party requestor 11 that is conducting or has conducted a transaction with the wireless device. Information Importer 22 checks whether the information sent to the location certification server is valid and optionally converts it to a standard format, if necessary. It may also perform pre-processing of the data (information) received. Information Processor 24 performs the processing for location information stamping and related processes, e.g., digital signing. External Interface 20 interacts with external entities such as the

location determination server, and certificate authorities. It may also be responsible for optional secure session management. Information management 26 manages the flow of information to and from the location determination server 16, to and from third party requestor 11, and to and from wireless device 10, and is also responsible of archival of transactions.

According to another aspect of the invention, a wireless device 12 computes its own geographic position. Where the device has the computational power to generate a digital signature, the location information is appended to the message, the message is digitally signed by the wireless device 12, and it is delivered to its intended recipient. For example, wireless device 12 can determine its own geographical position, generate its own digital signature, and transmit the digitally signed message to third party requestor 11, over a network 14, without the need for transmitting information to a location certification server.

Alternatively, a wireless device 12, capable of computing its own geographical position can transmit a digitally signed message over wireless network 14, to a location certification server 16. The location certification server 16, can further verify and certify the location information. For example, location certification server 16 can request that location determination server 18, separately determine the location of wireless device 12. If the location determined by the wireless device 12 matches the location determined by location determination server 18, the location certification server 16 may then forward the twice certified message to the intended recipient. For example, location certification server 16 can forward the twice certified message to third party requestor 11 over a network 14. A copy of the twice certified message can also be sent back to wireless device 12 over a network 14.

Preferably, when a wireless device 12 capable of computing its own geographical position is utilized the software for location determination and generating the digital signature is stored in the device in a tamper-resistant fashion. That is, if an attempt is made to tamper with the mechanism for determining location or for generating a digital signature, these mechanisms, or optionally the entire device, can be disabled.

In another embodiment, a wireless device 12 is capable of computing its own geographical location, however, the wireless device 12, lacks the computational

power to quickly generate a digital signature. In this embodiment, wireless device 12 forwards a message and location information, either encrypted with a secret key, or accompanied by a secure hash, to location certification server 16 over a network 14. The location certification server 16, then decrypts the location information, generates a digital signature and forwards the message to an intended recipient, for example a third party requestor 11, returns the location certified document back to the wireless device 12, or archives the location certified document.

In another embodiment that includes a wireless device 12 capable of determining its own geographical location but incapable of producing a digital signature, a message bearing encrypted location information is sent directly from the wireless device 12 to the intended recipient. For example, wireless device 12 sends a message bearing encrypted location information to a third party requestor 11, over a network 14. The third party requestor 11, or other intended recipient, can then forward the message to the location certification server 16, for decryption, verification, and certification of the location information. As with the devices capable of generating digital signatures, preferably the software for location determination and for encrypting the location information is stored in wireless device 12 in a tamper-resistant fashion.

As previously stated, the request for location information verification can come from a third party requestor, which is an entity, other than the wireless device, that seeks location information certification. For example, if the wireless device user is conducting a wireless transaction using his or her wireless device, the party on the other side of the transaction, for example, an e-commerce vendor, may desire to verify location information provided by the wireless device user as part of its e-commerce security measures. In such circumstances, the third party, having received a document containing a location stamp from the wireless device, can forward it to a location certification server for verification and certification of the location information.

The location certification server can then verify whether the wireless device identified by the document has subscribed to location verification services, and whether the user of the subject wireless device has authorized the server to provide location verification to the third party. The location certification server can then sign

the document and forward it to the location determination server for determination of the wireless device's geographic position and/or verification of the location information provided on the document. The location determination server then signs the document and returns the signed document back to the location certification server. The location certification server then provides the information to the third party or to the wireless device for forwarding to the third party.

Alternatively, the third party may have received a document from a wireless device that contains encrypted location information or a digital signature. According to one aspect of this embodiment, the third party may not have the capability to decrypt the information or verify/validate the digital signature. In this case, the third party can forward the document to a location certification server for decryption of the location information or decoding of the digital signature and/or verification of the location information and/or digital signature. The location certification server may then certify the location information with its own digital signature.

Even if the third party has the capability to decrypt the location information or verify/validate the digital signature, the third party can provide additional security by having the location certification server certify the location information and/or digital signature received from the wireless device.

The more detailed aspects and optional features of the invention will be described with reference to Figures 2-4.

Figure 2, shows a preferred flow diagram of the operations of a location certification server. The location certification server can be any computer that has the capability of preparing and verifying digital signatures. In figure 2, the location certification server receives a set of digital information 200, for example, an on-line purchase order, and a request for a certified location stamp from a wireless device or a third party requestor. The location certification then prepares a request to an appropriate location determination server 202. Such preparation can include adding a digital signature certifying the request.

A request is then made to an appropriate location determination server 204. The location determination server computes the location of the wireless device and transmits the document back to the location certification server together with the certified location information. The operations performed by the location

determination server will be described in more detail below. Once the location certification server receives a response from the location determination server, it verifies the location determination server's signature 206. If the signature of the information determination server proves invalid, the system is intimated 214, and the process is terminated 216. If the signature of the information determination server is valid, the location certification server digitally signs the document and the information submitted for certified location information, now containing two signatures, the signature of the location determination server and the signature of the location certification server, is forwarded to the wireless device as a confirmation query 208.

If the request for a certified location stamp is made by a wireless device, the confirmation query can take the form, for example, of "A request was made by you for your location. Your location has been certified by the location determination server as follows: Pennsylvania Ave., N.W., Washington, D.C. Is this information correct?" If the request for a certified location stamp is made by a third party requestor, the confirmation query can take the form, for example, of "A request was made by (third party e-commerce vendor) for your location. Your location has been certified by the location determination server as follows: Pennsylvania Ave., N.W., Washington, D.C. Is this information correct? Do you wish to provide (third party e-commerce vendor) with certified location information?"

If the location certification server receives from the wireless device a signed response to the confirmation query, the location certification server optionally validates the device's signature and analyses the response, for example, to see if the user of the wireless device has confirmed the location computed by the location determination server, or to confirm that user of the wireless device wants the location certification to proceed 210. If there are any errors in the submitted information, the system is intimated 214, and the process is terminated 216. If there are no errors, the data structure for the stamp is prepared, attached to the document and the resulting certified location stamped information sent to the device or archived if requested by the device 212.

In an alternative preferred embodiment, the location certification server may receive a document from a wireless device to which location information has already

been appended by the wireless device. The location information may be encrypted. According to this embodiment, the location certification server may decrypt the location information, add a digital signature, and return the document to the wireless device, forward the document to a third party e-commerce vendor at the request of the user of the wireless device, and/or archive the document with the certified location information. Alternatively, the wireless device may have digitally signed the document. In this instance, the location certification server may verify the digital signature, certify the document by adding its own digital signature and return the certified document to the wireless device, forward the document to a third party at the request of the user, and/or archive the document.

The data structure of the certified location stamp can take many forms. The location stamp can include identity information, location information, payload information, archival information and/or cryptographic information. Identity information can include information identifying, for example, the wireless device, the user, or information concerning a transaction.

Location information can include any position identifying information, for example, longitude and latitude or position with respect to a fixed landmark. Preferably, the location information includes the time that the position was determined.

Payload information can include information relating to the content of a document, a transaction or other data. For example, the payload may contain the content of the content itself. If the content is included in the payload, preferably, the content is encrypted. The encryption algorithm and scheme can then also be included as part of the payload information. Alternatively, a cryptographic hash of the content can be included as part of the payload information, in which case the cryptographic hashing algorithm is preferably included.

Archival information can be included if the location stamp is to be archived. Archival information can include archival period, location of archive, and/or access permissions, for example, login/password or SSL with client authentication OR some other scheme.

If a secure connection exists between the location certification server and the wireless device or between the location certification server and the location

determination server, all digital signatures and verification thereof may optionally be dispensed with, provided that at least one of the location certification server or the location determination server digitally sign the location information to certify the location information.

The location determination server is any computer that can compute the location of a wireless device. Preferably the location determination server is operated by the wireless service provider for the subject wireless device. According to this embodiment, there may be one or more location determination servers for each wireless service provider. Alternatively, there may be a centralized location determination server for more than one wireless service provider. According to a further alternative embodiment, the location determination server may be owned and/or operated by the same entity that operates the location certification server. According to yet a further embodiment, the location certification server and the location determination server may be the same computer.

Figure 3, shows a preferred flow diagram of the operations of a location determination server. Location determination servers have the capability of authenticating themselves using digital signatures, for example IETF's PKIX RFCs , or other methods known to those of ordinary skill in the art. When the location determination server receives a certified request from the location certification server 300, the location determination server validates the location certification server's signature 302. The location determination server then verifies the privileges set by the wireless device's owner for location services, against the request by the location certification server 304. That is, the location server may be an optional service available by subscription. If there are any errors or inconsistencies in the operations described above, the system is intimated 310, and the process terminated 312. If there are no errors, the location determination server computes the geographic position of the wireless device 306. The location determination server then attaches the location information to the document, certifies it by adding its digital signature and sends it to the location certification server 308, before terminating 312.

Referring now to Figure 4, the detailed operations of the requestor of certified location stamping will be described. As discussed above, the requestor may be a wireless device or it may be a server at an e-commerce vendor with which the

wireless device is conducting, or has conducted, a transaction. For the sake of clarity, the process will be explained with reference to a wireless device, but this explanation is not intended to limit the invention to requests from wireless devices. The wireless device initiates the process by submitting a set of digital information and a request for certified location stamping to a location certification server 400. For example, the digital information may be an on-line purchase order for products or services from a third party e-commerce vendor. Within a system-defined time frame, if the process has not been terminated at the location certification server or location determination server levels, the wireless device may receive a confirmation query from the location certification server, bearing the digital signatures of both the location certification server and the location determination server 402. If it has digital signature verification capabilities, the wireless device may optionally validate the location certification server's signature 404 and location determination server's signature 406, and if any errors or inconsistencies are detected by the wireless device, the system may be is intimated 412, and the process terminated. In any event, the wireless device may display the confirmation query to the user and wait for the user to input a response. If the user inputs a response to the confirmation query 408, the wireless device may transmit the response to the location certification server 410. If the wireless device has digital signature capability, it may apply a digital signature to its response. The wireless device will then receive a location information stamping acknowledgement response from the location certification server 414, before terminating 416.

Referring to Fig. 5, a block diagram for the operations in the wireless device according to a preferred embodiment in which the wireless device itself computes the location is shown. According to this embodiment, a typical public key solution is employed. The wireless device has a private key 504 embedded in tamper-resistant manner 502 in the wireless device. The device is connected to a network 500, which it uses to compute its location at 506. The information, including the message 508, user/device identification, and location information, is signed and/or encrypted at 510 and sent to the location certification server.

Referring to Fig. 6, a block diagram for the operations in the wireless device according to a preferred embodiment in which the wireless device itself computes the

location, but lacks the computational power to quickly generate a digital signature, is shown. According to this embodiment, a typical secret key solution is employed. The wireless device has a secret key 604 embedded in tamper-resistant manner 602 in the wireless device. The device is connected to a network 600, which it uses to compute its location using 606.

The information, including the message 608, user/device identification, and location information, is used to create an encrypted hash using 604. This is then sent to a trusted agent, for example the location certification server, which verifies the encrypted hash at 616 using 604. It then signs the information at 618 using its own private key 614, and the signed information is sent to the external party, as described above.

Having now fully described this invention, it will be appreciated by those skilled in the art that the invention can be performed within a wide range of parameters within what is claimed, without departing from the spirit and scope of the invention.

We claim:

1. A method for associating information concerning geographic position of a wireless device with data originating from said wireless device, comprising:
receiving data originating from a wireless device having a geographic position;
obtaining information concerning the geographic position of said wireless device;
appending a digital signature to said data originating from said wireless device;
transmitting said data originating from said wireless device, together with said appended digital signature.

2. A method according to claim 1, wherein the data originating from a wireless device is received directly from said wireless device.

3. A method according to claim 2 wherein the data originating from a wireless device is received over a secure connection.

4. A method according to claim 2 wherein the data originating from a wireless device is received together with a digital signature.

5. A method according to claim 1, wherein the data originating from a wireless device is received from a third party.

6. A method according to claim 5 wherein the data originating from a wireless device is received over a secure connection.

7. A method according to claim 5 wherein the data originating from a wireless device is received together with a digital signature

8. A method according to claim 1 further comprising computing the geographic position of said wireless device.

9. A method according to claim 8 further comprising appending information concerning said geographic position of said wireless device to said data originating from said wireless device.

10. A method according to claim 1 comprising requesting geographic position information specific to a wireless device from a wireless service provider.

11. A method according to claim 10 wherein said geographic position information is requested over a secure connection.

12. A method according to claim 10 wherein said request for geographic position information contains a digital signature

13. A method according to claim 9 wherein the data originating from the wireless device is transmitted to said wireless service provider.

14. A method according to claim 13 wherein the data originating from a wireless device is transmitted over a secure connection.

15. A method according to claim 13 wherein the data originating from a wireless device is transmitted together with a digital signature

16. A method according to claim 10 comprising receiving back from said service provider the data originating from the wireless device, to which is appended geographic position information for said wireless device.

17. A method according to claim 16 wherein the data originating from a wireless device is received back from said service provider over a secure connection.

18. A method according to claim 16 wherein the data originating from a wireless device is received back from said service provider together with a digital signature.

19. A method according to claim 1 wherein said information concerning the geographic position of said wireless device is obtained from a wireless service provider.

20. A method according to claim 1 wherein said information concerning the geographic position of said wireless device is received from said wireless device.

21. A method according to claim 20 wherein said information concerning geographic position is received over a secure connection.

22. A method according to claim 20 wherein said information concerning the geographic position of said wireless device received from said wireless device includes a digital signature generated by said wireless device.

23. A method according to claim 22 wherein software for computing said geographic position and for generating said digital signature is stored in said wireless device in a tamper-resistant fashion.

24. A method according to claim 22 wherein said information concerning the geographic position of said wireless device received from said wireless device has been encrypted by said wireless device.

25. A method according to claim 20 wherein said information concerning the geographic position of said wireless device received from said wireless device is accompanied by a secure hash.

26. A method according to claim 2 comprising transmitting said data originating from said wireless device, together with said appended digital signature, to said wireless device.

27. A method according to claim 5 comprising transmitting said data originating from said wireless device, together with said appended digital signature, to said third party.

28. A method for associating information concerning geographic position of a wireless device with data originating from said wireless device, comprising:

receiving from a requestor, data originating from a wireless device having a geographic position;

transmitting said data to a service capable of computing the geographic position of said wireless device;

receiving from said service said data, including geographic position information for said wireless device and digital signature of said service;

appending a second digital signature to said data; and

transmitting said data, together with said geographic position information, said digital signature of said service, and said second digital signature, to said requestor.

29. A method according to claim 28, wherein said requestor is said wireless device.

30. A method according to claim 28, wherein said requestor is a third party.

31. A method for associating information concerning geographic position of a wireless device with data originating from said wireless device, comprising:

computing the geographic position of said wireless device;

appending information concerning said geographic position to a set of data;

appending a digital signature to said set of data including said appended information concerning geographic position;

transmitting said set of data, including said digital signature and said information concerning geographic position

32. A method for associating information concerning geographic position of a wireless device with data originating from said wireless device, comprising:

computing the geographic position of said wireless device;

appending information concerning said geographic position to a set of data;

encrypting said set of data and said appended information concerning said geographic position;

transmitting said encrypted set of data and appended information concerning said geographic position.

33. A method for associating information concerning geographic position of a wireless device with data originating from said wireless device, comprising:

receiving from a wireless device an encrypted document comprising a set of data and information concerning the geographic position of said wireless device computed by said wireless device;

decrypting said document;

applying a digital signature to said document; and

transmitting said document bearing said digital signature to a third party.

34. A method according to claim 1, further comprising transmitting to said wireless device a request for authorization to comply with a request for certified location information.

35. A method according to claim 1, further comprising transmitting to said wireless device a request for authorization to comply with a request for certification of location information.

36. A method according to claim 28, further comprising transmitting to said wireless device a request for authorization to comply with a request for certification of location information.