State of Israel
Patent Office

מדינת ישראל
רשות הפטנטים

Patent Specification פירוט פטנט

[11] Application No:	133584	מספר בקשה:
[22] Date of application:	19/12/1999	תאריך הבקשה:

[54] METHOD FOR THE ACOUSTIC ENCODIFICATION
OF DYNAMIC IDENTIFICATION CODES

שיטה לקידוד אקוסטי של סיסמאות זיהוי דינמיות

[71] **Patentee (s):**
ENCOTONE LTD.
Customer No: 374611
P.O. BOX 8446
RAMAT GAN 52813
Israel

בעל (י) הפטנט:
אנקוטון בע"מ
קוד לקוח: 374611
ת.ד. 8446

Address for service:

[74] JMB, FACTOR & CO. LTD.
HAR HOTZVIM HI-TECH PARK,
P.O.B. 45087,
JERUSALEM 91450

המען למסירת הודעות:

ג'יי אמ בי, פקטור אנד קו בע"מ
רחוב המרפא, הר חוצבים
ת.ד. 45087
ירושלים 91450

Reference:	ENCO 720/10.1	סימוכין:
[48] Date of Publication:	17/02/2010	תאריך פרסום:

ארגז 453299 | תיק 133584

בקשה לפטנט

שיטה לקידוד אקוסטי של סיסמאות זיהוי דינמיות

A method for the acoustic encodification of dynamic identification codes

A method for the acoustic encodification of dynamic identification codes

Isaac J. Labaton

Technical Field

The present invention relates, generally, to the identification of persons which sustain transactions through devices which are not necessarily phones, like personal computers, organizers, or the like.

Background Art and Technical Problems

The Wireless Telephony Industry is developing the capability to compute secure identification and authentication codes using the cellular phones Central Processor (CPU) units capability and/ or the CPU in a chip card or smart card inserted in the cellular phone. This secure Identification and authentication codes can be computed according different standards and methods , including such methods for computing Identification/authentication strings, being such strings dynamics or variables, totally or partially, in order to avoid the fraudulent re-use of the said string. This industry trend includes the use of the cellular phone to digitally sign documents, according to well known standards or newly developed standards and protocols.

Most of the industry leaders plan to use the capabilities of the cellular phones as an instrument to completing the so called e-commerce transactions, whereas the authorized owner of the cellular phone , can be identified or authenticated by means of the strings computed as mentioned above, and , whereas certain transaction data is securely transmitted, using encryption methods and/ or Hash functions.

Most of such solutions generate, in order to identify the cellular phone owner and certify transaction data, a string of digits or bits which includes, amongst others data and parameters , the data associated to the identity of such cellular devices, or such chip card inserted in the cellular device, being such data encrypted totally or partially. The said identification data is sometimes associated with the cellular phone owner, or with an anonymous debit account.

Now, the string is transmitted preferentially as an electromagnetic wave, according with one or several cellular phone technologies methodology for transmission.

The problem with the said solutions for securing transactions though the Internet, is that the transaction must be carried at some instance through the cellular phone, meaning through a cellular phone call.

As an example lets take first an e-commerce transaction initiated and completed through the said cellular phone, whereas at a particular moment the cellular phone generates the said string and send it electromagnetically. This is atypical case when, by means of the cellular phone, the holder place a phone call.
Now, as another example that better shows the necessity of the invention presented here, lets take another e-commerce transaction, this time the transaction initiated through other than such cellular phone device , such a PC.

At some instance, the owner of the cellular phone, due to the need to certify his acceptation of the transaction need to use such cellular device to generate the identification /certification string. But he is communicating with the e-merchant by means of , say, his PC, therefore, in some cases the said owner is called back by the merchant, in other cases the owner place a call to the merchant or other entity with such cellular phone , but as, a result the owner ever sent the said string through his cellular phone, as an electromagnetic wave.

Therefore, there is a need for a new methodology, which will enable the Identification and Certification for the remote transactions in general , including Telephone orders, and the e-commerce transaction in particular , which are made though PC, or any other devices like regular wired phones, organizers, Palm computers or others devices, without the necessity of placing a call with the cellular phone in which the capability to compute identification /certification strings have been installed.

Summary of the Invention

The method of this invention is designed for solving the identification problems of persons which use other than cellular phone devices in order to perform remote transactions.
The method consists in the encodification of the said identification/ authentication/ certification string, computed in the cellular phone, as said above, to acoustic waves, in a way that such acoustic waves will carry the information encoded in the said string to a external to the cellular phone microphone, like a PC microphone, or an regular, wired phone set microphone.
Once the said sound wave reaches the said external microphone is converted to an electrical signal, which can be digitized and lately decodified into the original string.

Now this string can be transmitted through the telephone lines ,data lines, Internet lines or any other technology for transmission.
As a result, the owner of the cellular phone in which the method of this invention has been installed, can complete a secure remote transaction from any PC, by using such PC in a conventional way to process an e-commerce transaction, and when the time have come to send the cellular phone computed identification string, he will attach the said cellular phone in which method of this invention has been installed, to the PC microphone, and them he will activate the computation of the identification string and the said cellular phone in which the method of this invention has been installed, will compute the identification string and then encode it to sound. This acoustic message will reach the PC microphone, and eventually will be converted to an electrical signal (analog signal), which can be digitized and lately decodified into the original string.

This string can be transmitted to remote computer means for deciphering , and eventually , identification or / and authentication. This remote computer means can , in turn send a certificate to the pertinent entity, like the merchant, authentication server or the like.

Detailed Description of Preferred Exemplary implementations of the method of this invention

There is a need for a new methodology, which will enable the Identification of a remote person and / or the Certification of certain transactions data using a cellular phone in which capabilities of computing identification strings has been installed, but not necessarily through the use of such cellular phone as a phone, instead, by separating or dissociating the function of the cellular phone as a phone from the function of the said cellular phone as a certification/ identification. This dissociation can be accomplished according to the method presented here.
The importance of such dissociation becomes evident when there is a need to certify a remote transaction through another phone , like a regular wired phone, of through a PC, or through any other than the said cellular phone device for cases like e-commerce transaction, telephone orders or access to remote databases .

The method of this invention consists in the encodification of the said identification/ authentication/ certification string, computed in the said cellular phone into acoustic waves using the cellular phone speakers , in a way that such acoustic waves will carry the information encoded in the said string to a external to the cellular phone microphone, like a PC microphone, or an regular, wired phone set microphone , a POS microphone or other external-to –the cellular microphone .

Once the said sound wave reaches the said external wired phone microphone, or the microphone attached to the PC, according to the case, the acoustic message is converted into an electrical signal, which can be digitized and lately decodified into the original string.

Now this string can be transmitted through the telephone lines ,data lines, Internet lines or any other technology for transmission to remote computer means which will in turn decrypt or interpret or decipher the said recuperated string and, as a consequence will identify and / or certify the transaction data.

As a result, the owner of the cellular phone in which the method of this invention has been installed, can complete a secure remote transaction from any , say, PC, by using such PC in a conventional way to process an e-commerce transaction, and when the time have come to send the cellular phone computed identification string, he will attach or affix the said cellular phone in which method of this invention has been installed, to the PC microphone, and them he will activate the computation of the identification string by entering a secret PIN into such cellular phone , in order to avoid unauthorized use of such identification capabilities, and the said cellular phone in which the method of this invention has been installed, will compute the identification string and then will encode it to sound. This acoustic message will reach the PC microphone, and eventually will be converted to an electrical signal (analog signal), which can be digitized and lately decodified into the original string in order to identify the sender and certify the entered transaction data. As a result of this method , the cellular phone was not necessarily used as a phone at all.

The potential applications of the method presented here are more extended that the cases used above as examples, and as a matter of illustration we can bring here the possibility to use a cellular phone in which the method of this invention has been installed as an instrument for certification of certain sensible transaction data , like the transaction amount , whereas such data can be keyed-in in the cellular phone in which the method of this invention has been installed and there, such data will be encrypted according to specific standards, and the final string converted to sound to be inputted in an external microphone.

Another example can be the use of the cellular phone in which the method of this invention has been installed as an identification/ certification tool for completing bank or brokers remote transaction, by means of PCs or other devices in the above mentioned way.
A further example can be the use of the cellular phone in which the method of this invention has been installed enabling it to be an identification/ certification tool to be used also through other devices microphones, for On-the-Spot

transactions, whereas the holder of the said cellular phone, is physically present of the store or beside an special transaction machine as a vendor machine or an ATM . assuming there is an external-to-the-cellular phone microphone connected to the Point-of-Sale machine or to other store or automatic machine, the holder of the said cellular phone in which the method of this invention has been installed enabling it to be an identification/ certification tool to be used also through other devices microphones, will trigger the computing capabilities as a external-certification tool of the cellular, by entering a PIN on it, and if desired so, enter also, transaction data, and finally approach such cellular phone to the external microphone, and send the computed string encoded to sound an acoustic message for further processing in the machine attached to the external microphone or any other machine connected in one way or other to such machine.
In this way the cellular phone in which the method of this invention has been installed enables it to be an identification/ certification tool to be used also via Point of Sale (POS) or others on-the-spot transactions.
A additional example of the potential applications of such cellular phone in which the method of this invention has been installed enabling it to be an identification/ certification tool to be used also through other devices microphones , the use of such cellular as the instrument to pay for the so referred micro-transactions, or e-purse, e-wallet, debit applications whereas in the act to pay the string computed in the said cellular or in any other place, and transmitted to such cellular, will be converted to acoustic waves by such cellular to be entered into an external to the cellular microphone.

A further application of such cellular phone in which the method of this invention has been installed enabling it to be used also through other devices microphones as an identification/ certification tool is to use such cellular phone as an access instrument gain access to Intra-net, corporations intra-net, corporations databases, web-sites and restricted places in general always using an external to the cellular phone microphone to input the identification/authentication /certification string computed into the cellular and converted to sound by it.

A further embodiment of this invention is this cellular phone in which the method as described above has been installed enabling it to be an identification/ certification tool to be used also through other devices microphones, which is as before but with biometrics ways of identifying or authenticating the holder, such as reading and checking a finger-print or a voice-print or other biometrical parameter of the holder in the way to identify the authorized owner.

A preferred variation of the method of this invention is as follows: a method which by means of a piece of software which can run in cellular phones CPUs, is able to identify/ authentify the authorized owner of the smart card or chip-card inserted in the cellular or the owner of the cellular phone itself, and whereas the said software computes a digital string, preferentially totally variable, or at least partially variable, and whereas this string is further encoded to an analog wave and as a result of that the cellular phone generates as sound by means of a speaker, an acoustic wave, and whereas such acoustic wave is inputted into an external-to-the-cellular phone microphone, and re-converted into an analog wave, which is de-codified into the said original string, and whereas such string is interpreted or decrypted or processed in order to identify the said cellular phone or the said chip-card inserted into the cellular phone or the authorized owner of such cellular phone, and whereas such identification process is accomplished in the device attached to the external-to-the-cellular phone microphone, or, the said string is transmitted by such device to remote means through the Internet , the PSTN or any other media, in order to cause such string to be interpreted or decrypted or processed for completing the identification as above.

Another preferred variation of the method is a method as above whereas the software is able to be download through the Internet.
A preferred variation is a method similar as in the cases referred above whereas the method also allows the entering of data into the cellular phone, by keying-in such data or as a cellular holder utterance, being such utterance converted to text by means of Speech- Recognition- Techniques adopted in the cellular phone , and whereas such data, locally entered in one way or another is referred as a document, and being such document digitally signed in the cellular's CPU according to in use standards or newly developed standards.

Once such document is ready it is a string which is referred heretofore as the digitally signed document, and whereas such digitally signed document is encoded to an analog wave and as a result of that conversion the cellular phone generates as sound by means of a speaker an acoustic wave, and whereas such acoustic wave is inputted into an external-to-the-cellular phone microphone, and re-converted into an analog wave, which is de-codified into the said original digitally signed document , and whereas such digitally signed document is interpreted or decrypted or processed (referred heretofore as decryption process) in order to identify the said cellular phone owner and / or recuperate the said data.
Naturally this decryption process can be accomplished on the device attached to the external-to-the-cellular phone microphone, or, the said digitally signed document is transmitted by such device to remote means through the Internet , the PSTN or any other media, in order to cause such digitally signed document to be interpreted or decrypted or processed for completing the identification as above and the certification of the originally keyed-in or uttered data.

One possible variation of this method is a method as in the cases referred above whereas the method uses the well known DTMF telephony's standard for encoding and decoding the digital strings into and from sound respectively

Another **possible variation of this method is a** method as in the cases referred above whereas the method uses a chip card or smart card inserted on the cellular phone to keep certain owner's secret key , and every time the cellular need to compute the the said string reads the secret data from the chip-card

A further variation of the method is a method as in the cases above but whereas the cellular uses the chip-card CPU to partially or totally compute the string

An additional variation of this method is a method as in the cases referred above whereas the method uses the biometrics authentication described in Israeli patent application No. 122,023 which is also the PCT/IB98/01835

A further preferred variation of the method presented here is a method as in the cases above whereas the computation of the identification certification strings as well as the decryption or interpretation are performed according to the methodology presented in the Israeli Patent application No. 122,106 which is also the PCT/IB98/01834

An additional variation of this method is a method as in the cases above whereas the encodification into sound as well as the decodification from sound are performed according the Israeli Patent application No. 111,157 which is also the PCT/US9512979

A further additional variation is a method as in the cases above whereas the use of the cellular phone in which the method of this invention has been installed enabling it to be used as an instrument for identification / certification as above but using the methodology described in US patent No. 5,742,684

A most preferred variation of the method of this invention is a method as in the cases above whereas the use of the cellular phone as an identification/ certification tool is made according to the methods described in Israeli Patent application No. 128,720

Although the invention has been described herein in conjunction with the explanation and examples mentioned above, those skilled in the art will appreciate that the scope of the invention is not so limited. Various modifications in the selection and arrangement of the various components and method steps discussed herein may be made without departing from the spirit of the invention as set forth in the appended claims.

משרד המשפטים

מסמך זה הינו העתק שנסרק בשלמותו ביום ובשעה המצוינים ,
בסריקה ממוחשבת מהימנה מהמסמך המצוי בתיק ,
בהתאם לנוהל הבדיקות במשרד המשפטים.

על החתום

משרד המשפטים (חתימה מוסדית).

Claims:

1. A method for digitally signing data comprising the steps of: providing a cellular phone having capabilities to store a private key, to accept locally entered data from a user, to digitally sign the locally entered data using the private key such that one or more digital strings are produced; and to encode the digital strings to sound; directly entering the data, by the user, in the cellular phone; computing, by the cellular phone, a digital signature of the data using the private key; encoding, by the cellular phone, the digitally signed data to sound; and generating, by the cellular phone, the digitally signed data as acoustic sound waves.

2. The method of claim 1 further comprising the step of receiving the acoustic sound waves by an external microphone.

3. The method of claim 1, wherein the cellular phone further has the capability to accept the locally entered data by at least one of a keypad, as sound using speech recognition techniques, and as sound transmitted to and recorded by the cellular phone.

4. The method of claim 1, wherein the cellular phone has a speaker, and further comprising the step of encoding the digitally signed data to sound using the cellular phone speaker.

5. The method of claim 1, wherein the cellular phone further has the capability to generate the private key as well as a corresponding public key.

6. The method of claim 1, wherein the cellular phone uses an inserted chip-card for storing the private key.

7. The method of claim 1, wherein the cellular phone uses an inserted chip-card for computing the digital signature.

8. The method of claim 1 further comprising the steps of identifying the user of the cellular phone; and authorizing the use of the private key by biometrical means.

9. The method of claim 1 further comprising the steps of identifying the user of the cellular phone; and authorizing the use of the private key by requesting a personal identification number (PIN).

10. A method for facilitating a user to digitally sign data, the method comprising the steps of: providing a cellular phone to the user, wherein the cellular phone has the capabilities to store a private key, to accept locally entered data directly from the user, to digitally sign the locally entered data using the private key such that one or more digital strings are produced; and to encode the digital strings to sound; and providing remote access to a processing device, wherein the processing device retrieves and processes the encoded digital strings.

11. The method of claim 10 further comprising the steps of: identifying the user of the cellular phone; and authorizing the use of the private key by biometrical means.

12. The method of claim 10 further comprising the steps of: identifying the user of the cellular phone; and authorizing the use of the private key by requesting a personal identification number (PIN).

For the Applicant,

JMB, Factor & Co.
ENCO 720/10.1

משרד המשפטים
מסמך זה הינו העתק שנסרק בשלמותו ביום ובשעה המצוינים ,
בסריקה ממוחשבת מהימנה מהמסמך המצוי בתיק ,
בהתאם לנוהל הבדיקות במשרד המשפטים.
על החתום

משרד המשפטים (חתימה מוסדית).