US 20030217268A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2003/0217268 A1**

Gantman (43) **Pub. Date: Nov. 20, 2003**

(54) **SYSTEM AND METHOD FOR USING ACOUSTIC DIGITAL SIGNATURE GENERATOR AS ORACLE**

(76) Inventor: **Alexander Gantman**, San Diego, CA (US)

Correspondence Address:
Qualcomm Incorporated
Patents Department
5775 Morehouse Drive
San Diego, CA 92121-1714 (US)

(21) Appl. No.: **10/171,960**

(22) Filed: **Jun. 13, 2002**

Related U.S. Application Data

(60) Provisional application No. 60/380,652, filed on May 15, 2002.

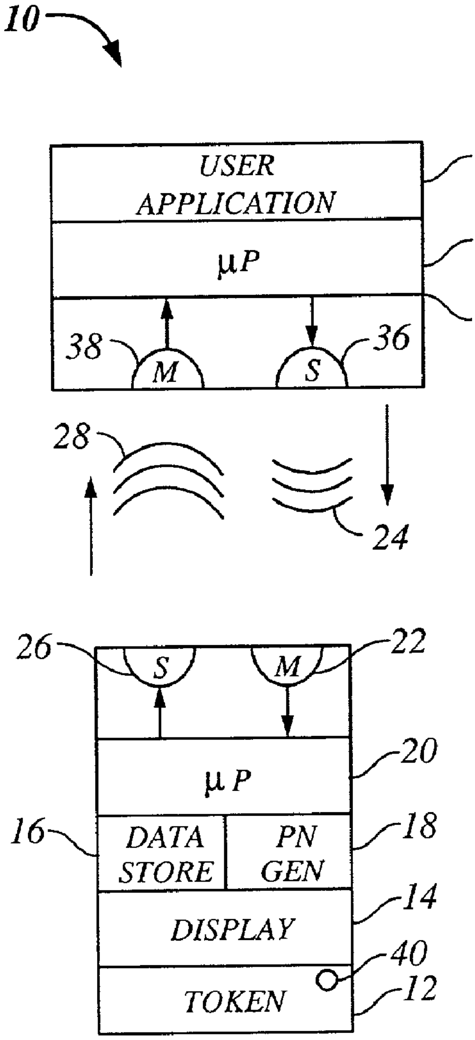
Publication Classification

(51) **Int. Cl.^{7}** **H04L 9/00**

(52) **U.S. Cl.** **713/172**

(57) **ABSTRACT**

A hand-held sonic token can be used as a pseudorandom oracle for a requesting application, which can generate a challenge that is sent to the token. The user of the token decides whether to allow the token to function as an oracle, and if so, the user causes the token to digitally sign the challenge and send it back to the requesting application, for use of the digitally signed challenge as an encryption key. After encryption the requesting application deletes the signed challenge, with subsequent decryption essentially following the encryption process.



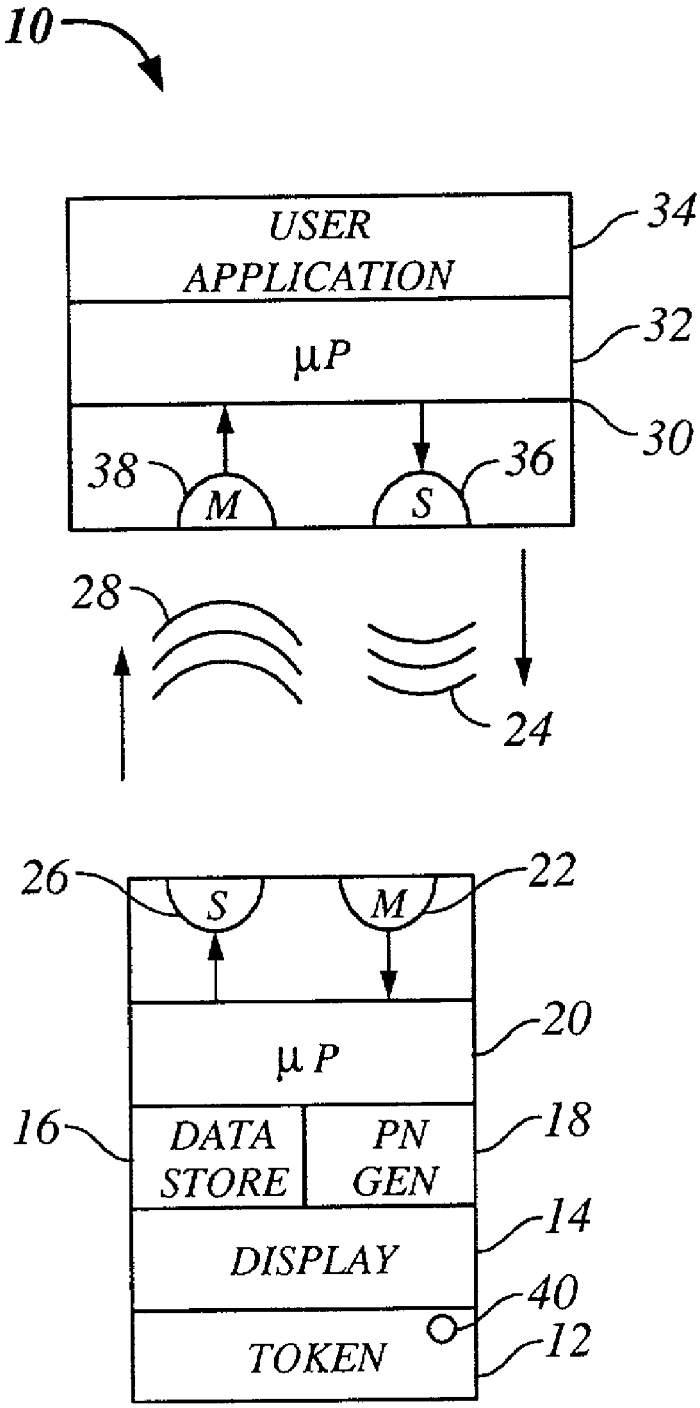

10
USER APPLICATION
34
μP
32
30
38
M
S
36
28
24
26
S
M
22
μ P
20
16
DATA STORE
PN GEN
18
DISPLAY
14
40
TOKEN
12

FIG. 1

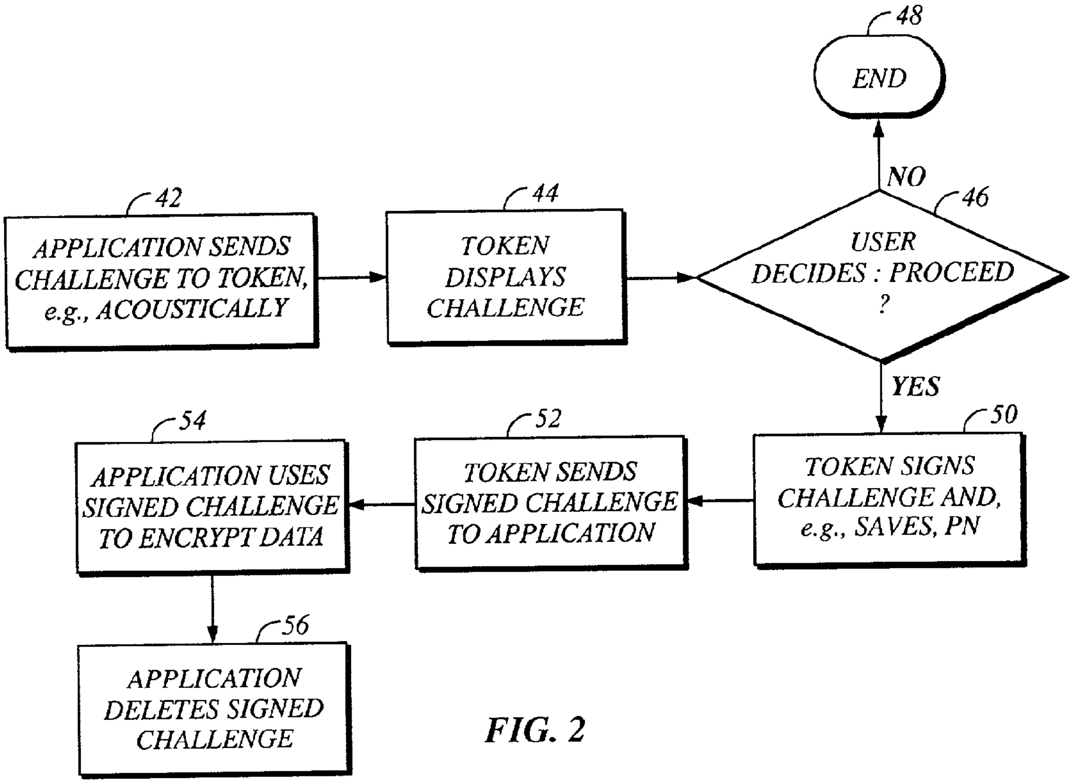

48
END
NO
46
USER DECIDES : PROCEED ?
42
APPLICATION SENDS CHALLENGE TO TOKEN, e.g., ACOUSTICALLY
44
TOKEN DISPLAYS CHALLENGE
YES
54
APPLICATION USES SIGNED CHALLENGE TO ENCRYPT DATA
52
TOKEN SENDS SIGNED CHALLENGE TO APPLICATION
50
TOKEN SIGNS CHALLENGE AND, e.g., SAVES, PN
56
APPLICATION DELETES SIGNED CHALLENGE

FIG. 2

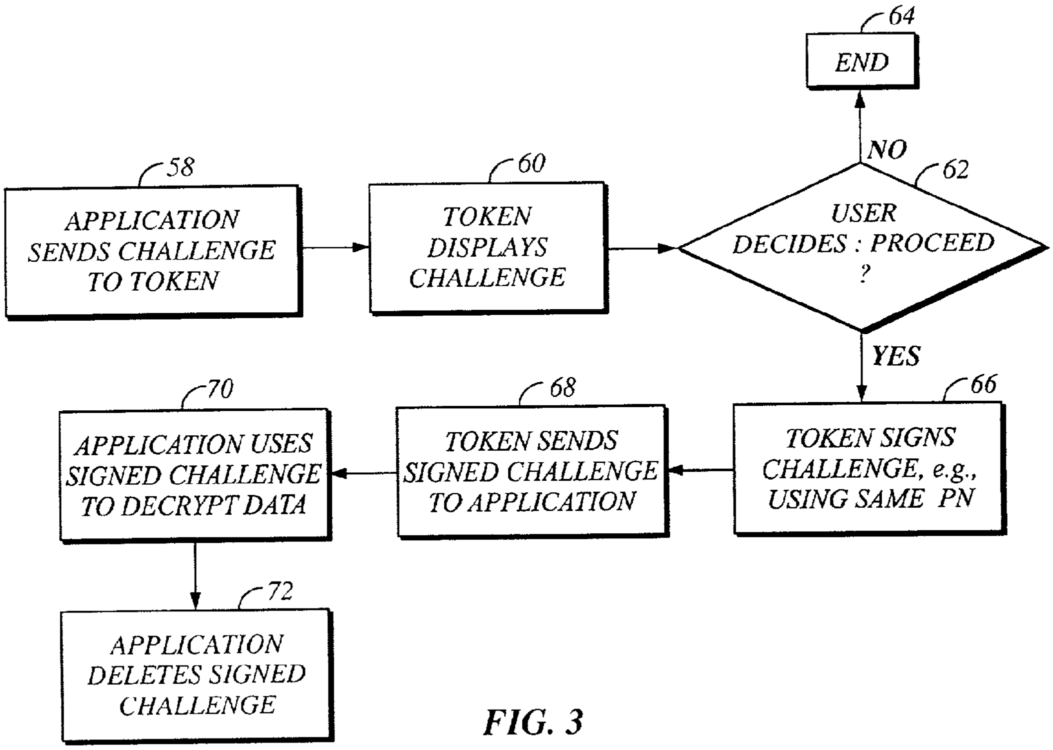

64
END
NO
62
USER DECIDES : PROCEED ?
58
APPLICATION SENDS CHALLENGE TO TOKEN
60
TOKEN DISPLAYS CHALLENGE
YES
70
APPLICATION USES SIGNED CHALLENGE TO DECRYPT DATA
68
TOKEN SENDS SIGNED CHALLENGE TO APPLICATION
66
TOKEN SIGNS CHALLENGE, e.g., USING SAME PN
72
APPLICATION DELETES SIGNED CHALLENGE

FIG. 3

SYSTEM AND METHOD FOR USING ACOUSTIC DIGITAL SIGNATURE GENERATOR AS ORACLE

RELATED APPLICATIONS

[0001] This application is related to co-pending U.S. patent application Ser. No. 10/077,365, filed Feb. 15, 2002, for an invention entitled "Method and Apparatus for Simplified Audio Authentication", is related to co-pending U.S. patent application Ser. No. 09/611,569, filed Jul. 7, 2000, for an invention entitled "Method and Apparatus for Simplified Audio Authentication", and is related to co-pending U.S. provisional patent application serial No. 60/380,652, filed May 15, 2002, for an invention entitled "System and Method for Using Acoustic Digital Signature Generator as Oracle", all of which are incorporated herein by reference.

I. FIELD OF THE INVENTION

[0002] The present invention relates generally to pseudorandom oracles.

II. BACKGROUND OF THE INVENTION

[0003] The above-identified patent applications disclose hand-held sonic-based "tokens" that a person can manipulate to transmit an acoustic signal representing secret information to a device, referred to as an "authenticator", "verifier", or "receiver", to authenticate the person based on the signal. As recognized in those applications, the advantage of sonic-based tokens is that a large installed infrastructure already exists to receive and transmit sound and electronic signals derived from sound. Specifically, the global telephone system exists to transmit data representative of acoustic information, and apart from telephones many computing devices that are now linked by this same system (as embodied in the Internet) have microphones and speakers (or can easily be modified to have them).

[0004] As recognized herein, sonic tokens have the advantage of transmitting the private information on the token in a fashion that prevents the receiver from knowing the private information without a confidential key. Specifically, the above-referenced applications disclose sonic tokens that digitally sign a message using private key/public principles. More specifically, the sonic tokens digitally sign a message by combining the message with secret information (a private key) and with a pseudorandom number (PN) to render a signed message that can be verified as authentic only by an entity possessing the public key that corresponds to the private key.

[0005] As further recognized herein, the above-discussed properties of sonic tokens render them suitable for use as pseudorandom oracles for encryption purposes. More particularly, the present invention recognizes that if an application requires a relatively strong encryption key, it selectively can be granted access to the token by a user of the token to obtain, for use as an encryption key, the product of the secret information in the token, but not the secret information itself, thereby keeping it secure.

SUMMARY OF THE INVENTION

[0006] A method is disclosed for essentially converting an easy to remember challenge to a pseudorandom encryption key using a hand-held sonic token as a pseudorandom oracle. The pseudorandom encryption key that is generated by the sonic token is a relatively strong key that is difficult for unauthorized parties to violate.

[0007] Accordingly, a method for encryption includes generating a challenge, and acoustically sending the challenge to a portable token. The method further includes deciding whether to allow the token to function as a pseudorandom oracle, and if so, causing the token to digitally sign the challenge to render a signed challenge. The signed challenge is acoustically transmitted for use thereof to encrypt data.

[0008] In a preferred, non-limiting embodiment, the challenge is generated by a requesting application which encrypts data using the signed challenge. If desired, the challenge may be displayed in human readable form to help a user decide whether to allow the token to be used as a pseudorandom oracle.

[0009] In exemplary non-limiting embodiments, the token digitally signs the challenge at least in part by combining the challenge with a private key. The private key can be a secret and can have a corresponding public key.

[0010] If desired, the signed challenge can be generated using a process that always renders the same signed challenge when presented with the same challenge. For instance, the token can digitally sign the challenge by combining the challenge with the private key and with a pseudorandom number (PN), and when a challenge is signed, the PN can be stored for reuse upon a second receipt of the same challenge for, e.g., decryption purposes.

[0011] In another aspect, a system for encryption includes a requesting application transmitting a challenge to a token using a wireless communication path. A token receives the challenge and digitally signs it with a private key to render a signed challenge. The token then transmits the signed challenge to the requesting application using a wireless communication path, so that the requesting application can use the signed challenge to encrypt data.

[0012] In yet another aspect, an encryption system includes acoustic means for transmitting a challenge from a requesting application, and means for receiving the challenge and generating a signed challenge in response. Acoustic means are provided for transmitting the signed challenge to the requesting application. Means are also provided for encrypting data associated with the requesting application using the signed challenge.

[0013] The details of the present invention, both as to its structure and operation, can best be understood in reference to the accompanying drawings, in which like reference numerals refer to like parts, and in which:

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] **FIG. 1** is a block diagram of the present system;

[0015] **FIG. 2** is a flow chart of the encryption logic; and

[0016] **FIG. 3** is a flow chart of the decryption logic.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0017] Referring initially to **FIG. 1, a** system is shown, generally designated **10**, that includes a portable hand-held token **12** that can be configured as a key fob or other small device. The present invention, however, applies to other token configurations, such as mobile communication stations including laptop computers, wireless handsets or telephones, data transceivers, or paging and position determination receivers that can be hand-held or portable as in vehicle-mounted (including cars, trucks, boats, planes, trains), as desired. Wireless communication devices are also sometimes referred to as user terminals, mobile stations, mobile units, subscriber units, mobile radios or radiotelephones, wireless units, or simply as "users" and "mobiles" in some communication systems.

[0018] In any case, the preferred token **12** includes a visual display **14** and an electronic data store **16**. Also, the token **12** can include a pseudorandom number (PN) generator **18**. A token microprocessor **20** accesses the PN generator **18** and data store **16**, and can cause the display **14** to present alpha-numeric or graphical information that a user can read or hear.

[0019] As shown in **FIG. 1**, the token microprocessor **20** can receive electronic signals from a microphone **22**, which generates the electronic signals by transforming received sound waves **24** received by the microphone **22**. Also, the token microprocessor **20** can send electronic signals to a speaker **26**, which transforms the electronic signals to transmitted sound signals **28**. As disclosed further below, the received sound signals **24** might represent a challenge (e.g., a request for encryption key) from a user component **30**, and the transmitted sound signals **28** might represent a signed challenge (e.g., the requested encryption key). While an acoustic wireless communication is preferred, other wireless paths, e.g., rf paths, might be used.

[0020] The user component **30** can be, e.g., a computer that includes a requesting microprocessor **32** which executes a software-implemented user application **34**. The user application **34** can be, e.g., a word processing application or other document-generating or more generally data-generating application that might wish to encrypt the generated data with a relatively strong encryption key. In any case, the user component **30** can include a speaker **36** for transmitting an acoustic representation of a challenge and a microphone **38** for receiving an acoustic representation of the response. Both the speaker **36** and microphone **38** communicate with the requesting microprocessor **32**.

[0021] In accordance with private key/public key principles known in the art and set forth in, e.g., the National Institute for Standards and Technology (NIST) Federal Information Processing Standards Publication 186-2, January, 2000, the signature algorithm in the token **12** (executed by the token microprocessor **20**) can combine a private key with a message to be signed and with a random number "k" from the PN generator **18** to render a digital signature which is a random pair (r,s). Preferably, the token microprocessor **20** executes the signature algorithm upon receipt of activation signals from, e.g., one or more activation elements **40** such as toggle switches, voice activation devices, or push-buttons. It is to be understood that the token microprocessor **20** can include a digital processor proper as well as necessary clocks, analog to digital conversion circuitry, and digital to analog conversion circuitry known in the art.

[0022] The token microprocessor **20** accesses the data store **16**, such that when multiple activation elements **40** are used, one or more can be associated with a respective private key in the store **16**. In addition to one or more private keys of private key/public key pairs, the data store **16** may hold public key IDs, and if desired PNs that have already been generated and used to sign challenges, along with a correlation of the PNs to the challenges, in accordance with one non-limiting exemplary embodiment disclosed below.

[0023] **FIG. 2** shows the encryption logic of the present invention. Commencing at block **42**, a challenge (e.g., an easy to remember challenge such as the word "password") is generated by, e.g., the user application **34** and is sent by the user component **30** to the token **12** using the communication pathway discussed above in reference to **FIG. 1**. If desired, at block **44** the token **12** can display the challenge and, if desired, the source of the challenge in human readable form on the display **14**, so that a user may decide, at decision diamond **46**, whether to allow the token **12** to function as a pseudorandom oracle. If the user decides against allowing the application **34** to access the token **12** for oracle purposes, the logic ends at state **48**.

[0024] On the other hand, if the user decides to allow the token **12** to function as an oracle, the user can so indicate by, e.g., manipulating the activation element **40**. The logic then proceeds from decision diamond **46** to block **50**, wherein the token digitally signs the challenge to render a signed challenge. In some preferred, non-limiting embodiments, the token uses a signing process that always renders the same signed challenge when presented with the same challenge. For instance, the token **12** might combine the challenge with a private key in the data store **16** but not with a PN from the PN generator **18**. Or, the conventional private key protocol might be followed, wherein the signed challenge is generated by combining the challenge with both the private key and with a PN, but with the PN subsequently being stored in the data store **16** along with a correlation of the PN to the particular challenge with which it was used, for purposes to be shortly disclosed.

[0025] Moving to block **52**, the token **12** sends the signed challenge to the user component **30** using the communication paths disclosed above for use of the signed challenge as an encryption key by the user application **34** to encrypt data at block **54** using, e.g., DES encryption principles known in the art. Preferably, the application then proceeds to block **56** to delete the signed challenge from its memory and from any peripheral storage devices (e.g., hard disk drives) associated with the user component **30** on which the signed challenge might have been stored.

[0026] When it is desired to decrypt the data, the logic of **FIG. 3** is invoked. Commencing at block **58**, the same challenge that was used in **FIG. 2** is sent by the user component **30** to the token **12**. If desired, at block **60** the token **12** can display the challenge in human readable form on the display **14**, so that a user may decide, at decision diamond **62**, whether to allow the token **12** to function as a pseudorandom oracle for decryption purposes. If the user decides against this, the logic ends at state **64**. Otherwise, the logic proceeds to block **66**, wherein the token digitally signs the challenge to render a signed challenge. In the above-mentioned preferred, non-limiting embodiments wherein it is desired that the token always generates the same signed challenge when presented with the same input challenge, the token can, e.g., regenerate the same signed challenge as was generated for encryption using a signing process that does not require a PN, or it can regenerate the same signed challenge using conventional private key protocol, with the following exception. The PN that was used to generate the signed challenge during encryption and that was subsequently stored in the data store **16** (along with a correlation of the challenge) can be retrieved at block **66** based on the challenge and then combined with the challenge and the private key to render the signed challenge.

[**0027**] Moving to block **68**, the token **12** sends the signed challenge to the user component **30** for use of the signed challenge by the user application **34** to decrypt data at block **70**. Preferably, the application then proceeds to block **72** to delete the signed challenge from its memory and from any peripheral storage devices (e.g., hard disk drives) associated with the user component **30** on which the signed challenge might have been stored.

[**0028**] While the particular SYSTEM AND METHOD FOR USING ACOUSTIC DIGITAL SIGNATURE GENERATOR AS ORACLE as herein shown and described in detail is fully capable of attaining the above-described objects of the invention, it is to be understood that it is the presently preferred embodiment of the present invention and is thus representative of the subject matter which is broadly contemplated by the present invention, that the scope of the present invention fully encompasses other embodiments which may become obvious to those skilled in the art, and that the scope of the present invention is accordingly to be limited by nothing other than the appended claims, in which reference to an element in the singular is not intended to mean “one and only one” unless explicitly so stated, but rather “one or more”. All structural and functional equivalents to the elements of the above-described preferred embodiment that are known or later come to be known to those of ordinary skill in the art are expressly incorporated herein by reference and are intended to be encompassed by the present claims. Moreover, it is not necessary for a device or method to address each and every problem sought to be solved by the present invention, for it to be encompassed by the present claims. Furthermore, no element, component, or method step in the present disclosure is intended to be dedicated to the public regardless of whether the element, component, or method step is explicitly recited in the claims. No claim element herein is to be construed under the provisions of 35 U.S.C. §112, sixth paragraph, unless the element is expressly recited using the phrase “means for” or, in the case of a method claim, the element is recited as a “step” instead of an “act”.

What is claimed is:

1. A method for encryption, comprising:

generating a challenge;

acoustically sending the challenge to a portable token;

deciding whether to allow the token to function as a pseudorandom oracle, and if so, causing the token to digitally sign the challenge to render a signed challenge;

acoustically transmitting the signed challenge; and

using the signed challenge to encrypt data.

2. The method of claim 1, wherein the challenge is generated by a requesting application, the requesting application encrypting data using the signed challenge and deleting the signed challenge after use.

3. The method of claim 2, wherein the challenge is displayed in human readable form to facilitate the deciding act.

4. The method of claim 1, wherein the token digitally signs the challenge at least in part by combining the challenge with a private key.

5. The method of claim 4, wherein the private key is a secret and has a corresponding public key.

6. The method of claim 4, wherein the signed challenge is generated using a process that always renders a first signed challenge when presented with a first challenge.

7. The method of claim 6, wherein the token digitally signs the challenge at least in part by combining the challenge with the private key and with a pseudorandom number (PN), and the method further comprises:

storing the PN and reusing the PN upon a second receipt of the challenge to sign the challenge.

8. A system for encryption, comprising:

at least one requesting application transmitting at least one challenge to at least one token using a wireless communication path; and

at least one token receiving the challenge and digitally signing it with at least one private key to render a signed challenge, the token transmitting the signed challenge to the requesting application using a wireless communication path, the requesting application using the signed challenge to encrypt data.

9. The system of claim 8, wherein the requesting application deletes the signed challenge after encrypting data.

10. The system of claim 8, wherein the token displays the challenge to a user to facilitate the user deciding whether to permit the token to sign the challenge and/or to transmit the challenge.

11. The system of claim 8, wherein the wireless communication path is an acoustic path.

12. The system of claim 8, wherein the signed challenge is generated using a process that always renders a first signed challenge when presented with a first challenge.

13. The system of claim 12, wherein the token digitally signs the challenge at least in part by combining the challenge with the private key and with a pseudorandom number (PN), and the token stores the PN after signing the challenge and reuses the PN upon a second receipt of the challenge to sign the challenge.

14. An encryption system, comprising:

acoustic means for transmitting a challenge from a requesting application;

means for receiving the challenge and generating a signed challenge in response;

acoustic means for transmitting the signed challenge to the requesting application; and

means for encrypting data associated with the requesting application using the signed challenge.

15. The system of claim 14, wherein the means for receiving and generating generates the signed challenge only in response to receiving authorization to do so from a user.

16. The system of claim 14, wherein the means for receiving and generating always generates the same signed challenge in response to the challenge.

17. The system of claim 14, wherein the means for receiving and generating includes a hand-held sonic token.

18. The system of claim 15, further comprising means for displaying the challenge.

19. The system of claim 14, wherein the means for receiving and generating digitally signs the challenge at least in part by combining the challenge with a private key and with a pseudorandom number (PN).

20. The system of claim 19, further comprising:

means for, when a challenge is signed, storing the PN and reusing the PN upon a second receipt of the challenge to sign the challenge.

* * * * *