(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 718 805 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
26.06.1996 Bulletin 1996/26

(51) Int. Cl.[6]: **G07C 9/00**

(21) Application number: **95101162.6**

(22) Date of filing: **27.01.1995**

(84) Designated Contracting States:
AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE

(30) Priority: **25.12.1994 IL 11213994**

(71) Applicant: **NEWS DATACOM LTD.**
London E1 9XY (GB)

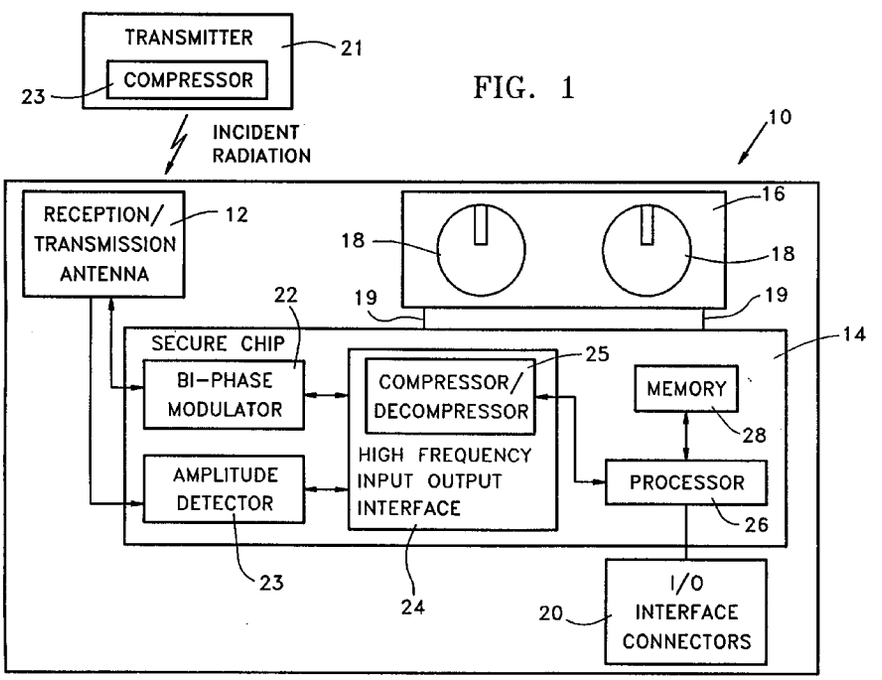
(72) Inventor: **Bogat, Carmi**
Maale Adumim 98420 (IL)

(74) Representative: **Modiano, Guido, Dr.-Ing. et al**
Modiano, Josif, Pisanty & Staub,
Baaderstrasse 3
D-80469 München (DE)

(54) Secure remote access systems

(57) A secure remote access system including a transmitter for transmitting RF signals which include information, and a secure access card, wherein the secure access card includes a receive and transmit antenna receiving the RF signals and a secure chip device for extracting the information from the RF signals, for processing the information and for converting the processed information into a format suitable for transmission via the receive and transmit antenna, whereby the receive and transmit antenna is operable to transmit the processed information to a remote site.

FIG. 1



EP 0 718 805 A2

Description

FIELD OF THE INVENTION

The present invention relates generally to secure remote access systems.

BACKGROUND OF THE INVENTION

There are known in the art radio frequency (RF) tags which provide object identification and access to restricted areas and services without physical contact between the tag and an object.

U.S. Patent 5,058,161 describes a method and apparatus for performing identification and/or verification at predetermined checkpoints.

U.S. Patent 5,204,675 describes a system for collecting a toll for a vehicle, on which a vehicle number plate is mounted.

SUMMARY OF THE INVENTION

The present invention seeks to provide secure remote access systems in which access to restricted areas is provided by RF signals.

Such a secure remote access system may include an access card with a secure chip and RF communication modules. Data is communicated between the access card and remote stations. Tampering with the access card is difficult because a secure chip is employed.

There is thus provided in accordance with a preferred embodiment of the present invention a secure remote access system including a transmitter for transmitting RF signals which include information, and a secure access card, wherein the secure access card includes a receive and transmit antenna receiving the RF signals and a secure chip device for extracting the information from the RF signals, for processing the information and for converting the processed information into a format suitable for transmission via the receive and transmit antenna, whereby the receive and transmit antenna is operable to transmit the processed information to a remote site.

Additionally, the secure remote access system includes a compressor for compressing the information prior to transmitting thereof.

Preferably, the secure access card also includes a decompressor for decompressing compressed information and a compressor for compressing information prior to transmitting the information to a remote site.

Preferably, the information is transmitted in a HDLC communication format.

In accordance with a preferred embodiment of the invention the secure chip device may be an EEPROM chip device.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawing in which Fig. 1 is a generalized illustration of an access card forming part of a secure remote access system constructed and operative in accordance with a preferred embodiment of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Reference is now made to Fig. 1 which is a generalized illustration of an access card forming part of a secure remote access system constructed and operative in accordance with a preferred embodiment of the present invention.

An access card, generally denoted by reference numeral 10, includes a reception/transmission antenna 12, a secure chip 14, a battery compartment 16 including batteries 18, and input/output interface connectors 20.

Reception/transmission antenna 12 receives and transmits RF signals. It is to be appreciated that antenna 12 may be a set of two separate antennas, one for reception and one for transmission.

Access card 10 receives RF signals from a remote transmitter 21. Preferably, the RF signals include data for at least one of identification, verification and validation of the card owner or a combination thereof. Such identification, verification and validation may be carried out in accordance with any suitable algorithm, such as those described in either of U.S. Patents 4,748,668 and 4,932,056. The RF signals also may include monetary data which is employed to credit or debit the card owner with value tokens.

RF signals received at antenna 12 are provided to a bi-phase modulator 22 and an amplitude detector 23, both embedded in the secure chip 14. Bi-phase modulator 22 is employed to modulate the incoming signal and to re-transmit a portion of the incident radiation in a modulated manner. Preferably, the re-transmitted signal is modulated with response data generated in the secure chip.

Bi-phase modulator 22 and amplitude detector 23 are coupled to a high frequency input/output interface 24 which is operable to detect data signals contained in the RF signals, reformat the data signals in a format which is suitable for processing by a processor and provide the reformatted data signals to a processor 26. Processor 26 is coupled to a memory 28 for storing and retrieving of data.

Communication between access card 10 and a remote station in which transmitter 21 is located may be in a compressed digital form. In such a case, transmitter 21 includes a data compressor 23 and high frequency input/output interface 24 includes a data compressor/decompressor 25 which decompresses the informa-

tion transmitted in compressed form and provides it to processor 26.

Processor 26 is operable to control the operation of the card, to provide responses to interrogation by a remote station, to generate messages and to control monetary transactions. Responses to interrogation generated by processor 26 may contain identification codes, verification data, authentication data, general data and any combination thereof. To provide these responses, processor 26 is operable to run secure algorithms for identification, verification and authentication. The algorithms may be stored in memory 28 or provided to processor 26 over-the-air or from an external unit, such as a computer (not shown), via input/output interface connectors 20.

In a preferred embodiment of the present invention monetary data processed by processor 26 may include transactions of value tokens and calculations of debits and credits. Preferably, part of the data received at the card may contain credits or value tokens. Debits for operations in which payment is demanded are deducted by a debit signal, which is received and processed at the card when the card is accessed.

Data generated by processor 26 is provided to high frequency input/output interface 24 which converts the data to signals which are modulated in bi-phase modulator 22 with a portion of the incident radiation and transmitted, over-the-air, to a remote station (not shown). It is to be appreciated that bi-phase modulator 22, amplitude detector 23, high frequency input/output interface 24, processor 26 and memory 28 are all embedded in a secure chip of which tapping is difficult.

In the case that communication between access card 10 and the remote station is in a compressed digital form, compressor/decompressor 25, integrated in high frequency input/output interface 24, compresses the data prior to transmission to the remote station.

Batteries 18 may be employed to provide electrical power for backup. It is to be appreciated that in most applications the incident radiation provides enough power for transmission of the response signals. Batteries 18 are coupled to the secure chip 14 by connectors 19 in the battery compartment 16.

The secure chip 14 may be an Electronically Erasable Programmable Read Only Memory (EEPROM) in which data may be written on or read from. In such a device, data is stored even when the card 10 is not electrically powered. It is to be appreciated that the direct coupling of the secure chip to RF transmitting and receiving modules may result in fast communication protocols such a HDLC communication protocol or any other packet based communication protocol.

The system of Fig. 1 may be employed in various applications, all of which employ transfer of information to and from the access card. Such applications may include a toll road application, a pass entitlement application and an entrance to restricted area application.

It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the present invention is defined only by the claims which follow.

Where technical features mentioned in any claim are followed by reference signs, those reference signs have been included for the sole purpose of increasing the intelligibility of the claims and accordingly, such reference signs do not have any limiting effect on the scope of each element identified by way of example by such reference signs.

Claims

1. A secure remote access system comprising:

   a transmitter for transmitting RF signals which include information; and

   a secure access card including:

   a receive and transmit antenna receiving said RF signals; and

   a secure chip device operative to extract said information from said RF signals, to process said information, to convert the processed information into a format suitable for transmission and to transmit the processed information to a remote site via said receive and transmit antenna.

2. A wireless communicating smart card comprising:

   at least one antenna providing RF reception and transmission of at least partially encrypted information; and

   a secure chip device having an information input and an information output coupled to said at least one antenna and being operative to extract information from RF signals received thereby, to process said information, to convert the processed information into a format suitable for transmission and to transmit the processed information to a remote site via said receive and transmit antenna.

3. Apparatus according to claim 1 wherein said transmitter comprises a compressor for compressing said information prior to transmitting thereof.

4. Apparatus according to any of the claims 1 - 3 wherein said card comprises a decompressor for decompressing compressed information.

5. Apparatus according to any of the claims 1 - 4 wherein said card comprises a compressor for compressing information prior to transmission thereof.

6. Apparatus according to claim 1 wherein said information is transmitted in a HDLC communication format.

7. Apparatus according to claim 2 wherein said information is transmitted in a HDLC communication format.

8. Apparatus according to claim 1 wherein said secure chip device is an EEPROM chip device.

9. Apparatus according to claim 2 wherein said secure chip device is an EEPROM chip device.

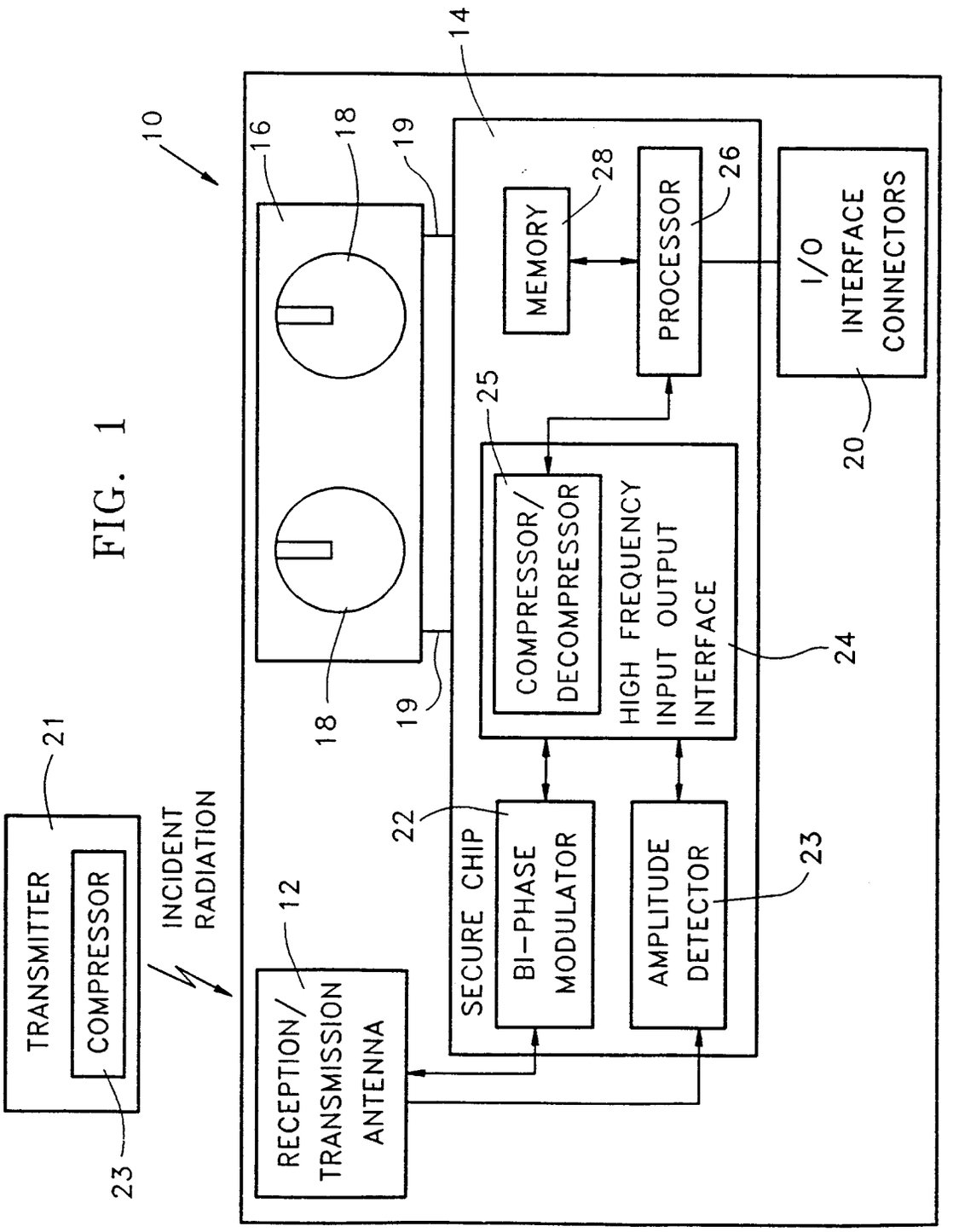

10
14
16
18
19
MEMORY
28
PROCESSOR
26
I/O
INTERFACE
CONNECTORS
20
25
COMPRESSOR/
DECOMPRESSOR
HIGH FREQUENCY
INPUT OUTPUT
INTERFACE
24
18
19
22
SECURE CHIP
BI-PHASE
MODULATOR
AMPLITUDE
DETECTOR
23
RECEPTION/
TRANSMISSION
ANTENNA
12
INCIDENT
RADIATION
TRANSMITTER
COMPRESSOR
21
23

FIG. 1