Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2617901 A1 2007/02/15

(21) 2 617 901

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2006/07/19
(87) Date publication PCT/PCT Publication Date: 2007/02/15
(85) Entrée phase nationale/National Entry: 2008/02/04
(86) N° demande PCT/PCT Application No.: US 2006/027952
(87) N° publication PCT/PCT Publication No.: 2007/018987
(30) Priorité/Priority: 2005/08/04 (US11/197,220)

(51) Cl.Int./Int.Cl. *G07F 7/10* (2006.01)

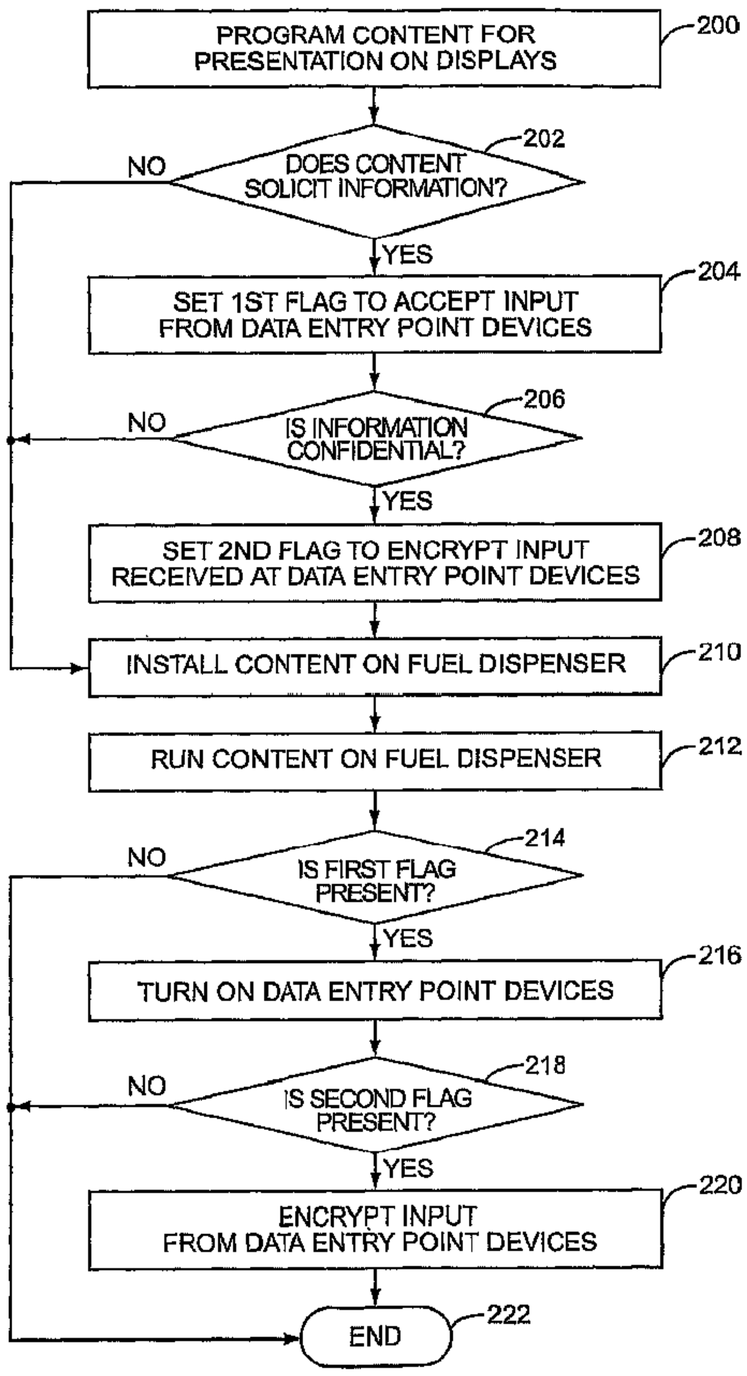
(71) Demandeur/Applicant:
GILBARCO INC., US

(72) Inventeurs/Inventors:
ROBERTSON, PHILIP A., US;
WILLIAMS, RODGER, US;
WESTON, TIMOTHY M., US

(74) Agent: OGILVY RENAULT LLP/S.E.N.C.R.L.,S.R.L.

(54) Titre : SYSTEME ET PROCEDE POUR LE CHIFFREMENT SELECTIF DE DONNEES ENTREES PENDANT UNE TRANSACTION DE DETAIL

(54) Title: SYSTEM AND METHOD FOR SELECTIVE ENCRYPTION OF INPUT DATA DURING A RETAIL TRANSACTION



(57) Abrégé/Abstract:
A retail environment having retail terminals with data entry point devices selectively encrypts input received by the data entry point devices and passes the encrypted data to a security module. The selective encryption is based on whether or not sensitive or

CA 2617901 A1 2007/02/15

(21) 2 617 901

(13) A1

(57) Abrégé(suite)/Abstract(continued):
confidential information, such as a personal identification number (PIN) associated with a debit card, is being input. To prevent hacking of the software of the retail terminal, content destined for display on the retail terminal is authenticated prior to display. In this manner, the retail terminal may be assured that confidential information is input only when desired, and thus may be encrypted only as needed.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 February 2007 (15.02.2007)

PCT

(10) International Publication Number
WO 2007/018987 A3

(51) International Patent Classification:
G07F 7/10 (2006.01)

(21) International Application Number:
PCT/US2006/027952

(22) International Filing Date: 19 July 2006 (19.07.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/197,220 4 August 2005 (04.08.2005) US

(71) Applicant *(for all designated States except US)*: **GILBARCO INC.** [US/US]; 7300 West Friendly Avenue, Greensboro, NC 27410 (US).

(72) Inventors: **ROBERTSON, Philip, A.**; 1501 Bearhollow Road, Greensboro, NC 27410 (US). **WILLIAMS, Rodger**; 9743 Silk Hope Liberty Road, Siler City, NC 27344 (US). **WESTON, Timothy, M.**; 20 Downing Ridge Court, Greensboro, NC 27407 (US).

(74) Agent: **TERRANOVA, Steven, N.**; Withrow & Terranova, PLLC, P.O. Box 1287, Cary, NC 27512 (US).

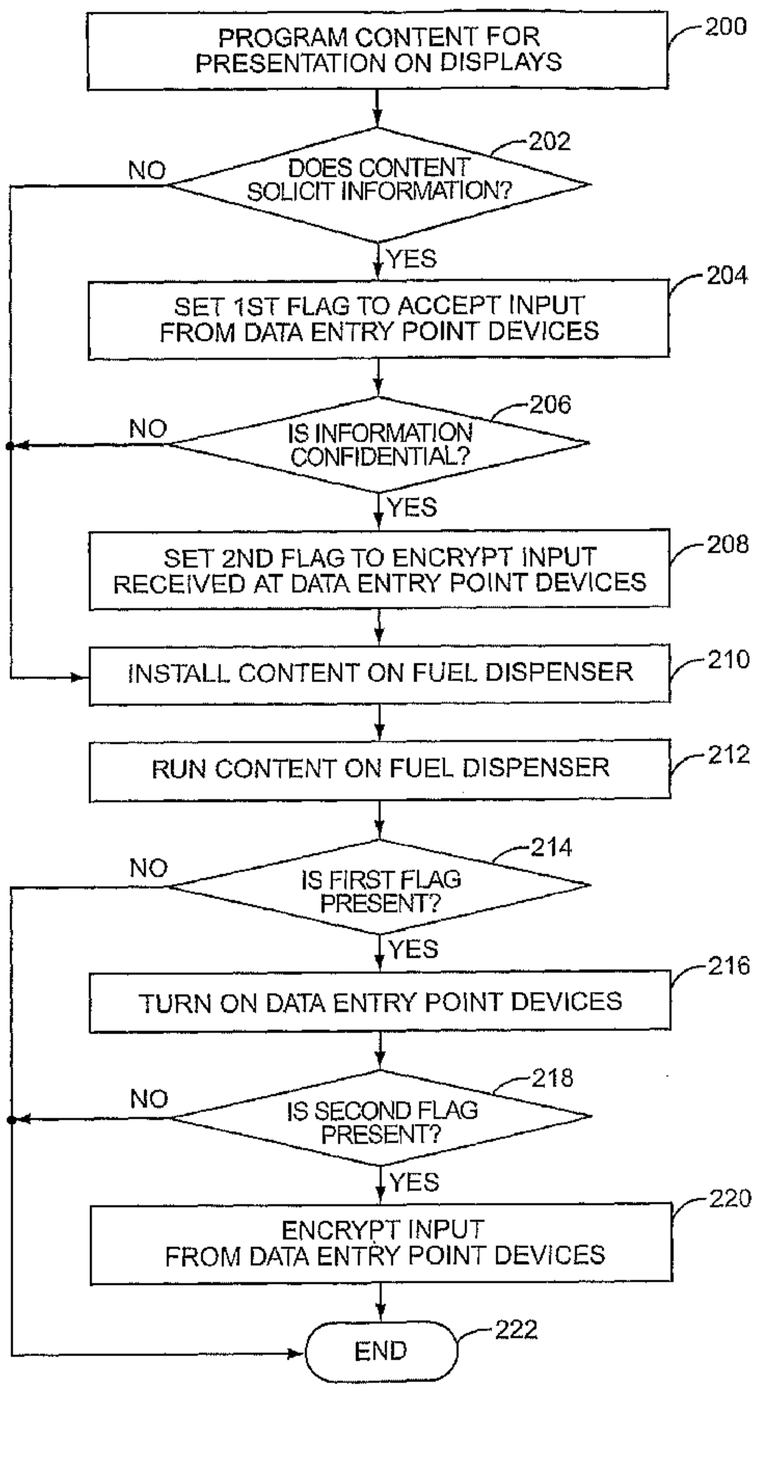
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR SELECTIVE ENCRYPTION OF INPUT DATA DURING A RETAIL TRANSACTION



(57) Abstract: A retail environment having retail terminals with data entry point devices selectively encrypts input received by the data entry point devices and passes the encrypted data to a security module. The selective encryption is based on whether or not sensitive or confidential information, such as a personal identification number (PIN) associated with a debit card, is being input. To prevent hacking of the software of the retail terminal, content destined for display on the retail terminal is authenticated prior to display. In this manner, the retail terminal may be assured that confidential information is input only when desired, and thus may be encrypted only as needed.

WO 2007/018987 A3

WO 2007/018987 A3

(88) Date of publication of the international search report:
21 June 2007

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR SELECTIVE ENCRYPTION OF INPUT DATA DURING A RETAIL TRANSACTION

Field of the Invention

[0001] The present invention is designed to prevent theft of sensitive and/or confidential information, such as personal identification numbers (PINs), during a retail transaction, particularly at a fuel dispenser retail device.

Background of the Invention

[0002] Credit card companies such as VISA® and MASTERCARD® have been very successful in persuading customers that credit cards should be used to complete any and all commercial transactions in place of cash. As a result of the success of the credit card, almost every retail establishment now has a magnetic card stripe reader to accept credit cards for payment. Concurrent with the proliferation of the magnetic stripe card readers used to process credit cards, many financial institutions have authorized the issuance of debit cards that are interoperable with the magnetic card readers.

[0003] Typically, a credit card is swiped through the magnetic card reader, and the credit card owner does not have to take further steps to complete the authorization of the transaction, although some establishments require a signature to complete the transaction. In contrast, a debit card typically requires the card owner to enter, via a keypad, a personal identification number (PIN) to complete customer authorization of the transaction, since funds are transferred directly from the customer's bank account for payment. The PIN, if present, is typically encrypted at the point of entry and then sent in an encrypted format over open communication links, such as a telephone line, to a host computer for transaction authorization. The encryption is used to protect the PIN from disclosure so that unauthorized persons may not obtain the PIN in clear form to defraud the legitimate card holder, the vendor, or an authorizing institution or card issuer.

[0004] Commonly owned U.S. Patent No. 5,228,084, which is hereby incorporated by reference in its entirety, describes an encryption process for confidential information in the context of a fueling environment. Specifically, fueling environments include a plurality of fuel dispensers that accept debit cards and have a keypad for PIN entry. The '084 patent further describes that the fueling

environment is divided into two zones. The first zone is a local zone within the fueling environment. The local zone extends from the data entry point to a security module associated with a site controller. The second zone is the host zone and extends from the security module to the host computer that authorizes the transaction. The PIN is encrypted by the data entry point device (a keypad, a card reader, or the like) using a local encryption algorithm, and is sent to the security module, which is tamper resistant. The security module decrypts the information from the data entry point device using the local encryption scheme and re-encrypts the information according to a host encryption algorithm used by the host computer. After re-encryption, the information is sent to the host computer for transaction authorization. Thus, the PIN is never present in an unencrypted format on the communication links.

[0005] While the '084 patent has been particularly efficacious at preventing fraud, the fueling environment has not remained static since its introduction. Specifically, the fuel dispenser has evolved to include a large display that may include a touch screen. Even if the display does not include a touch screen, the fuel dispenser has numerous keypads that are used to interact with the customer. The customer may respond to queries presented on the display by pressing one or more keys on the keypad or the touch screen. Not all of these queries solicit sensitive or confidential information like a PIN. For example, the response to a query about whether a customer wants a receipt is not necessarily confidential. The dual nature of the queries to the customer generates a quandary about what to do with the non-confidential information.

[0006] The obvious solution is to encrypt all data received from the customer and pass the encrypted information in the local zone to the security module for decryption so that the security module and the site controller can determine if the data needs re-encryption in the host zone or otherwise needs to be processed. However, this solution imposes a large processing burden on the security module and the site controller. Additionally, the constant communication from the fuel dispenser data entry point device and the security module for all input data, both confidential and non-confidential, burdens the internal communication network of the fueling environment, which in turn may delay the authorization of fueling or raise similar concerns. Thus, there needs to be a better way to encrypt confidential data at the data entry point device.

Summary of the Invention

[0007] The present invention provides two techniques for encrypting data at the data entry point device to prevent fraud in a retail transaction. The first technique involves selectively encrypting only the confidential data at the data entry point device and sending this selectively encrypted data to a security module. In this technique, a system controller associated with the data entry point device knows what queries are posed and what queries generate entry of confidential information. Only the responses to the queries that solicit confidential information are encrypted. The encrypted information is processed normally by the security module. The responses that do not contain confidential information are processed normally by the system controller as needed or desired.

[0008] Unfortunately, the first technique has a potential security vulnerability. Specifically, the selective encryption of certain responses and the lack of encryption on other responses create windows of opportunity during which a thief could attempt to steal confidential information. A thief could hack or reprogram the software controlling the data entry point device and the display such that the display prompts the user to enter confidential information at a time during which the normal software does not expect entry of confidential information. The modified software could then record the key strokes of the customer and capture confidential information such as a personal identification number (PIN). As a result of this vulnerability, the selective encryption approach alone is not preferred, although it forms part of the present invention.

[0009] The second technique also involves the selective encryption of confidential information, as discussed above, but adds a layer of complexity to the software to enhance the security vulnerability of the first technique. Specifically, the second technique, before any content is presented on the display, causes the system controller to verify the content. Once the content has been verified, the content is displayed. In this manner, no fraudulent content is presented on the display and there is no opportunity for a hacker to control the display in an unauthorized manner to request that the user enter confidential information at a time during which the data will not be encrypted. Since the selective encryption of data is used, the security module and the internal network for the retail establishment are not overburdened. Alternatively, if the content is not authenticated, the content may still be displayed,

but the data entry point devices may be disabled such that no input from the customer is accepted.

[0010] The content is verified through an authentication process in which indicia associated with the content is compared to a secure copy of the indicia. If the indicia match, then the content is verified. In an exemplary embodiment, the indicia comprise a digital signature and the secure copy of the indicia is passed to the retail establishment through an encrypted communication. Other forms of verification are also possible.

[0011] Those skilled in the art will appreciate the scope of the present invention and realize additional aspects thereof after reading the following detailed description of the preferred embodiments in association with the accompanying drawing figures.

Brief Description of the Drawing Figures

[0012] The accompanying drawing figures incorporated in and forming a part of this specification illustrate several aspects of the invention, and together with the description serve to explain the principles of the invention.

[0013] Figure 1 illustrates a fuel dispenser in a fueling environment;

[0014] Figure 2 illustrates schematically the elements of the fuel dispenser and the fueling environment connected to a host computer;

[0015] Figure 3 illustrates in a flow chart the steps of passing the encryption keys to the fuel dispenser for transactional use;

[0016] Figure 4 illustrates in a flow chart the steps of a first exemplary methodology of the present invention;

[0017] Figures 5A and 5B illustrate in a flow chart the steps of a second exemplary methodology of the present invention; and

[0018] Figures 6 and 7 illustrate in a flow chart the steps of authenticating content provided by a manufacturer.

Detailed Description of the Preferred Embodiments

[0019] The embodiments set forth below represent the necessary information to enable those skilled in the art to practice the invention and illustrate the best mode of practicing the invention. Upon reading the following description in light of the accompanying drawing figures, those skilled in the art will understand the concepts

of the invention and will recognize applications of these concepts not particularly addressed herein. It should be understood that these concepts and applications fall within the scope of the disclosure and the accompanying claims.

[0020] The present invention is directed to providing selective encryption of data at a retail terminal. In a particularly contemplated embodiment, the retail terminal is a fuel dispenser in a fueling environment. Sensitive or confidential information, such as a credit card account number or personal identification number (PIN), is solicited from a customer at predetermined times during the course of a transaction. The customer then enters the confidential information through a data entry point device such as a keypad. The fuel dispenser's controller knows that the data entry point device is receiving confidential information, and the controller causes the confidential information to be encrypted and passed to a security module. When non-confidential information is being entered by the customer, the fuel dispenser's controller knows that the data entry point device is receiving non-confidential information, and causes the input to be processed normally without encryption.

[0021] In an improved embodiment, the content of the display associated with the retail terminal is verified so that fraudulent content that solicits confidential information when the controller is expecting non-confidential data can not be displayed. Verification of the content of the display helps insure that someone has not reprogrammed the content in an unauthorized manner. Since the content of the display is known and verified, the fuel dispenser's control system knows when confidential information is being solicited, and thus knows when to encrypt information received at the data entry point devices. Likewise, the fuel dispenser's control system knows when the information being received at the data entry point devices is not confidential and thus does not need to be encrypted. While the present invention is optimized for use on a fuel dispenser in a fueling environment, the invention is not so limited and may be used with other retail terminals or kiosks in other retail settings.

[0022] Because the present invention is optimized for use in a fueling environment, the present disclosure starts with an overview of a fueling environment 10 in Figure 1 and its supporting hardware and software. The methodology of the present invention is illustrated in Figures 4-5B below, but the fueling environment 10

is explained initially so that the reader has a thorough understanding of the context of the present invention.

[0023] The fueling environment 10 includes one or more fuel dispensers 12 (only one illustrated) in a forecourt of the fueling environment. The fuel dispensers 12 communicate with a site controller (SC) 14 in a central building of the fueling environment. Note that the central building is not necessarily central to the physical layout of the fueling environment 10, but typically serves as the central focus of the fueling environment 10 and may include a convenience store, a quick serve restaurant, a service bay, or the like as is well understood. The site controller 14 may be associated with a counter top retail terminal 12a if needed or desired.

[0024] The connection between the fuel dispensers 12 and the site controller 14 may be facilitated through an optional translator 16. In an exemplary embodiment, the fuel dispensers 12 may be the ENCORE® or ECLIPSE® fuel dispensers sold by the assignee of the present invention, Gilbarco Inc., of 7300 W. Friendly Avenue, Greensboro, North Carolina 22087. Other fuel dispensers could also be used if needed or desired. The site controller 14 may be the G-SITE® also sold by the assignee of the present invention, Gilbarco Inc. Other site controllers could also be used if needed or desired. Sometimes the site controller 14 may not be made by the same manufacturer as the fuel dispensers 12, in which case certain proprietary protocols may not be fully compatible. The optional translator 16 may be used to make the elements compatible, as is well known.

[0025] Each fuel dispenser 12 may have a user interface 18 (illustrated schematically in Figure 2). Each user interface 18 may include one or more displays 20, which may optionally be a touch screen display, a smart pad 22 (Figure 2 only), a keypad 24 and a card reader 26. The smart pad 22 may be the Smart Pad ™ sold by Gilbarco Inc. For more information about the Smart Pad™, the interested reader is referred to commonly owned U.S. Patent No. 6,736,313, which is hereby incorporated by reference in its entirety. In use, the customer may swipe her debit card (or other payment mechanism) in the card reader 26 and enter her PIN through either the smart pad 22 or the keypad 24. Collectively, the display 20 (if equipped with a touch pad), smart pad 22, the keypad 24, and the card reader 26 are referred to as data entry point devices. The term "data entry point devices" is also herein defined to include contactless card readers and interrogators that interoperate with smart cards, transponders, and other contactless or wireless payment mechanisms

that allow the transfer of information from an item controlled by a customer to the fuel dispenser 12 or other retail terminal.

[0026] The user interface 18 and/or the data entry point devices (20, 22, 24) encrypts the card number and the PIN according to a local encryption scheme and sends the encrypted information to a security module (SM) 28 through the site controller 14. The previously incorporated '084 and '313 patents both discuss how the card number and PIN are encrypted, and the interested reader is referred to those disclosures for a better comprehension of this process. Encryption of the information reduces concerns about sending the information over communication media on which the information may be intercepted.

[0027] The encrypted information is decrypted by the security module 28 using the local encryption scheme and re-encrypted using a host encryption scheme. The security module 28 then sends the re-encrypted information to a host computer 30. The transmission to the host computer 30 may be over a telephone line, a packet network, or the like as needed or desired. Even if the re-encrypted information is intercepted, the host encryption scheme reduces the likelihood of a malefactor gaining access to the card number or PIN. In an exemplary embodiment, the host computer 30 may be a front end merchant processor such as BUYPASS™, PAYMENTECH™, VITAL™, HEARTLAND EXCHANGE™, or the like. Front end merchant processors act as an interface to companies such as SUN TRUST™, BANK OF AMERICA™, WELLS FARGO™, CONCORD EFS™, and the like. Such arrangements are well known in the industry.

[0028] In practice, the fueling environment 10 purchases a security module 28 from a manufacturer such as Gilbarco Inc., and has the manufacturer's authorized representatives install the security module 28 at the fueling environment 10. Once the security module 28 is installed, cryptographic keys may be exchanged between the data entry point devices (20, 22, 24) and the security module 28 for local and host zone encryption.

[0029] In an exemplary embodiment, the site controller 14 is in overall charge of the operation of the fueling environment 10, including the sequence of events between the security module 28 and the fuel dispensers 12. The site controller 14, which is in communication with the fuel dispensers 12, determines that one or more of the fuel dispensers 12 requires a cryptographic key. To initiate the process, the site controller 14 requests key generation for a specific fuel dispenser 12 from the

security module 28. The following process is known as exponential key exchange, and is presented in a flow chart format in Figure 3 as an example. The security module 28 and the fuel dispenser 12 (or other remote unit as needed or desired) are both initially loaded with several values in common, namely the values A, Q, a test message, and a default master key (DMK) (blocks 100). The values A and Q are large prime numbers. None of these values need to be stored on a secure basis, since even knowledge of all four will not assist a malefactor in determining the actual encryption keys which will be used to encrypt the PINs.

[0030] The security module 28 selects a large random number R and calculates the value $X = Mod\ Q\ (A^R)$ (block 102), where the Mod function returns the integer remainder after long division. That is, X = the remainder when A to the R power is divided by Q. The value of X is then encrypted by the security module 28 using the default master key (block 104). The encrypted value of X is then sent to the site controller 14 and the site controller 14 sends it to the correct fuel dispenser 12. The fuel dispenser 12 decrypts X with the default master key (block 106). Then the fuel dispenser 12 selects a random number S and calculates $Y = (A^S)\ Mod\ Q$ and $KD = (X^S)\ Mod\ Q$ (block 108).

[0031] The fuel dispenser 12 then calculates a Key Exchange Key (KEK) from the value KD (block 110). This calculation may involve any desired suitable function f(KD) so as to produce KEK as a 64 bit DES key. Several methods can be used in f(KD), including truncation and exclusive ORing parts of KD together.

[0032] The fuel dispenser 12 then encrypts Y with the default key (block 112), and encrypts the test message using the DES algorithm with KEK used as the encryption key (block 114). Both the encrypted Y and the encrypted test message are returned to the site controller 14, which in turn sends this data to the security module 28.

[0033] The security module 28 decrypts Y with the default key (block 116) and then calculates $KD = (Y^R)\ Mod\ Q$ (block 118). The security module 28 then calculates KEK from the value KD, using the same function f(KD) previously used by the fuel dispenser 12 (block 120). Using the value KEK, the security module 28 then decrypts the test message which was encrypted by the fuel dispenser 12 with the KEK (block 122).

[0034] The security module 28 compares the stored test message to the decrypted test message (block 124). If the test message does not match the stored

value (block 126), the security module 28 selects a new random number R, and calculates a new $X = (A^R)\ Mod\ Q$ to start the process over again (block 102). If the decrypted test message matches the test message stored within the security module 28 (block 128), then the security module 28 continues with the setup process, because the fuel dispenser 12 and the security module 28 have calculated the same KEK. The KEK values in the fuel dispenser 12 and the security module 28 are equal, not only as confirmed by identity in the test messages, but also because the values of KEK calculated are mathematically equivalent.

[0035] The security module 28 then selects a randomly or pseudorandomly generated working key, WK (block 130), encrypts it with the KEK (block 132), and sends it to the site controller 14, which then sends it to the correct fuel dispenser 12. The fuel dispenser 12 decrypts the working key with the KEK (block 134). Depending on the desired mode of operation, the dispenser may use WK as an encrypting key in any of the various encryption methods whenever a PIN or card number is to be encrypted (block 136).

[0036] In a particularly contemplated embodiment, the fuel dispensers 12 use WK as a generating key for Unique Key Per Transaction (UKPT) (block 138). As long as the fuel dispenser 12 and the security module 28 retain the KEK, it is not changed, but the working keys between the security module 28 and the fuel dispensers 12 are preferably changed regularly in response to specific system events or on a timed basis. The KEKs may change for various reasons: cold starting a fuel dispenser 12 (clearing all its memory data storage); replacing a fuel dispenser 12 or a security module 28; or replacing a site controller 14 (either hardware or software). The generation of the KEKs may also be accomplished by algorithms other than exponential key exchange if needed or desired.

[0037] As noted above, not every input received by the data entry point devices (20, 22, 24) contains confidential information. As further noted above, if every input received by the data entry point devices (20, 22, 24) is encrypted and sent to the security module 28, such activity unnecessarily taxes the security module 28, and may clutter the internal communication network of the fueling environment 10. The present invention solves this problem by providing software embodied on a computer readable medium (such as FLASH memory, EEPROM, a hard drive, or the like) that knows when confidential and non-confidential information is being solicited at the data entry point devices (20, 22, 24) and selectively encrypts only the

confidential information. While software is preferred, it is possible that the present invention could also be implemented in hardware, such as an Application Specific Integrated Circuit (ASIC), that effectuates the same result. A flowchart of a first exemplary embodiment of the present invention is presented in Figure 4.

[0038] Initially, the content for presentation on the displays 20 is programmed (block 200). Programming of the content may be done through any conventional manner such as in a conventional programming language as C, C++, JAVA, or the like. Content can be divided into two sorts of content: the first type does not solicit information from the customer and the second type does solicit information from the customer. A determination is made as to whether the content solicits information (block 202). If the answer to block 202 is yes, then a first flag is set for the content to accept input from the data entry point devices (20, 22, 24) (block 204). If the answer to block 202 is no, the content does not solicit information, the process proceeds to block 210, explained below.

[0039] A second determination is made as to whether the information that is solicited is confidential (block 206). If the answer to block 206 is no, the information is not confidential, the process proceeds to block 210, explained below. If the answer to block 206 is yes, then a second flag is set for the fuel dispenser 12 to encrypt input received at the data entry point devices (20, 22, 24) (block 208).

[0040] The content is then installed on the fuel dispenser 12 (block 210). The content may be installed on the fuel dispenser 12 in any conventional manner such as through downloading from a remote source; uploading from a computer readable medium such as a floppy disk, compact disc, or optical disc; insertion of a memory device such as an EEPROM; programming the fuel dispenser 12 directly; or any other technique that allows the fuel dispenser 12 to have access to the content. After installation, the content runs on the fuel dispenser 12 (block 212). The content may provide advertising to the customers, instruct the customers on how to use the fuel dispenser 12, or provide responses to customer input, as is well understood. As the content is run on the fuel dispenser 12, the fuel dispenser control system (↘P) 32 (see Figure 2) checks to see if the first flag is present (block 214). If the answer to block 214 is yes, then the fuel dispenser control system 32 turns on the data entry point devices (20, 22, 24) such that they will accept input from the customer (block 216). The fuel dispenser control system 32 then checks to see if the second flag is present (block 218). If the answer to block 218 is yes, the second flag is present, the fuel

dispenser control system 32 instructs the data entry point devices (20, 22, 24) to encrypt input received by the data entry point devices (20, 22, 24) (block 220). If the answer to either block 214 or 218 is no, or after block 220, then the process ends (block 222).

[0041] While it is illustrated that the process ends at block 222, the more probable practical implementation is that the process will repeat as additional content is presented on the display 20 and the fuel dispenser control system 32 checks for the presence of the flags. Further, while the process described above presents the decision making as being within the fuel dispenser control system 32, it is possible that the decision making could be within the data entry point devices (20, 22, 24) or other processor that operates the data entry point devices (20, 22, 24). Still further, while the process describes a particular sequence of checking for flags and may potentially imply that there is an order in which the flags are checked, it should be appreciated that the flags can be checked concurrently or in reverse order. Even further, while the use of flags is a particularly contemplated way to implement the present invention, other programming techniques could be used to effectuate the same functionality without departing from the scope of the present invention.

[0042] While the embodiment presented in Figure 4 is helpful to reduce demands on the security module 28 and the internal communication network of the fueling environment 10 by only encrypting confidential solicited data, the embodiment of Figure 4 is potentially vulnerable. In particular, the fuel dispenser control system 32 could be programmed to display unauthorized content on the display 20 that requests confidential information when such is not expected, or the content could be reprogrammed to remove the second flag or new content could be provided which does not have the second flag. The present invention's second and preferred embodiment addresses this vulnerability, and is presented with reference to Figures 5A and 5B.

[0043] The second embodiment builds on the first embodiment and relies on the concept of authenticating the content before it is displayed on the retail device. If the content is not authenticated, then the data entry point devices (20, 22, 24) may remain inoperative or the fuel dispenser control system 32 may preclude the content from being presented on the display 20. The process of authentication is described in detail below with references to Figures 6 and 7, and in commonly owned U.S. Patent Application Serial No. 09/798,411, filed March 2, 2001, which is hereby

incorporated by reference in its entirety and is now published as U.S. Patent Publication No. 2002/0124170. While the '411 application is a particularly contemplated method of performing an authentication process, any form or method of content authentication is within the scope of the present invention.

[0044] The second embodiment begins much as the first embodiment, wherein content is programmed for presentation on the displays 20 of the fuel dispensers 12 (block 250, Figure 5A). After the content is programmed, appropriate authentication indicia are appended to the content (block 252). A determination is made as to whether the content solicits information (block 254). If the answer to block 254 is yes, then a first flag is set for the content to accept input from the data entry point devices (block 256). If the answer to block 254 is no, the content does not solicit information, the process proceeds to block 262, explained below.

[0045] A second determination is made as to whether the information that is solicited is confidential (block 258). If the answer to block 258 is no, the information is not confidential, the process proceeds to block 262, explained below. If the answer to block 258 is yes, then a second flag is set for the fuel dispenser 12 to encrypt input received at the data entry point devices (block 260).

[0046] The content is then installed on the fuel dispenser 12 and the fuel dispenser 12 runs (block 262). The content may be installed on the fuel dispenser 12 in any conventional manner. After installation, the fuel dispenser control system 32 of the fuel dispenser 12 determines if the authentication indicia on the content is proper (block 264). As noted above, the process by which content is authenticated is explained in greater detail below. If the answer to block 264 is no, the authentication indicia is missing or otherwise improper, the fuel dispenser 12 may lock or otherwise disable the data entry point devices such that no input therefrom is accepted and end the process (block 266). Additionally (or alternatively), the fuel dispenser 12 may preclude the content from being presented on display or take other steps (such as generating an alarm) to prevent the customer from inputting data in response to the unauthenticated content.

[0047] If the answer to block 264 is yes, the authentication indicia is proper, then the fuel dispenser 12 presents the content on the display 20 (block 268). The content may provide advertising to the customers, instruct the customers on how to use the fuel dispenser 12, or provide responses to customer input as is well understood. As the content is run on the fuel dispenser 12, the fuel dispenser control

system 32 checks to see if the first flag is present (block 270, Figure 5B). If the answer to block 270 is yes, then the fuel dispenser control system 32 turns on the data entry point devices such that they will accept input from the customer (block 272). The fuel dispenser control system 32 then checks to see if the second flag is present (block 274). If the answer to block 274 is yes, the second flag is present, the fuel dispenser control system 32 instructs the data entry point devices (20, 22, 24) to encrypt input received by the data entry point devices (20, 22, 24) (block 276). If the answer to either block 270 or 274 is no, or after block 276, then the process ends (block 278).

[0048] As noted above, while it is illustrated that the process ends at block 278, the more probable practical implementation is that the process will repeat as additional content is presented on the display 20 and the fuel dispenser control system 32 checks for the presence of the flags. Further, while the process described above presents the decision making as being within the fuel dispenser control system 32, it is possible that the decision making could be within the data entry point devices (20, 22, 24) or other processor that operates the data entry point devices (20, 22, 24). Still further, while the process describes a particular sequence of checking for flags and may potentially imply that there is an order in which the flags are checked, it should be appreciated that the flags can be checked concurrently or in reverse order. Even further, while the use of flags is a particularly contemplated way to implement the present invention, other programming techniques could be used to effectuate the same functionality without departing from the scope of the present invention.

[0049] The process of authenticating content is explored in the previously incorporated '411 application. Portions of that disclosure are set forth herein for convenience. In essence, a digital signature is appended to the file for authentication. In it's basic definition, a digital signature says "I wrote this page and I signed it", where "I" represents the person or entity that is able to create the digital signature. A digital signature is most usually appended to the end of the data being signed, but it could be embedded within the data in some circumstances. The digital signature scheme may use public and private keys akin to those described above. Where such a scheme is used, the "I" is the person or entity that owns the private key. With the private key, the key owner is able to create the digital signatures. The owner of the private key keeps the private key secret.

[0050] The public key can either be published or stored in a non-secure manner since it does not have to be kept secret. The public key is used to verify that the digital signature is authentic. The public key cannot be used to generate a valid digital signature. An example of a digital signature system that uses private and public keys is the one defined in Federal Information Processing Standard (FIPS) publications 180 and 186. This version of a digital signature is referred to as the Digital Signature Standard (DSS).

[0051] Figure 6 illustrates a situation wherein the digital signature of the content is provided by the Original Equipment Manufacturer (OEM). That is, the content is created by the manufacturer of the fuel dispenser 12. This content file is transferred to the fuel dispenser 12 after operating software has been downloaded and is operational in the fuel dispenser 12.

[0052] The process starts (block 300), and the OEM appends its signature, also known as DSS, to the content file, using the OEM's private key (block 302). The content file is delivered to the site controller 14 either by electronic communication or by a downloading device directly connected to site controller 14 (block 304). The content file is sent from site controller 14 to the fuel dispenser 12 when desired (block 308). The content file may be a particular web page application that is only to be presented on fuel dispenser 12 for a particular option selected by the customer. The application software or boot software, depending on the configuration of the system, uses the public key to authenticate the signature with the file contents (block 308), and the fuel dispenser 12 decides if the signature is authentic (decision 310). If the signature is not authentic, the fuel dispenser 12 performs alternative handling on the content file (block 312). If the content file is authenticated, the content file is executed by fuel dispenser control system 32 of the fuel dispenser 12 (block 314), and the process ends (block 316).

[0053] If the content file was not authenticated (decision 310), alternative handling is performed on the content file (block 312) as illustrated in the flowchart in Figure 6. The alternative handling process is illustrated in Figure 7. The fuel dispenser control system 32 first determines if execution of the content file should be aborted by determining the configuration information concerning alternative handling of content files stored in memory of the fuel dispenser 12 (decision 350). If the content file execution is to be aborted, the process ends (block 316 from Figure 6). If the content file is to be executed, but in a special manner, the special handling

data for non-authenticated content files is checked in memory of the fuel dispenser 12 (block 352). If the special handling data requires that data entry input devices at the fuel dispenser 12 be disabled (decision 354), the fuel dispenser control system 32 causes the data entry input devices to be disabled (block 356), and the content file is executed if desired (block 314 from Figure 6). In this manner, the content file is still executed on the fuel dispenser 12 but the customer cannot interact with the data entry input devices since they are disabled. If the data entry input devices are not to be disabled, any other alternative handling is performed as dictated by the special handling data in memory of the fuel dispenser 12 (block 358), and the content file is executed (block 314 from Figure 6) if desired.

[0054] If the content is derived from a third party other than the OEM, the previously incorporated '411 application describes how to authenticate such content as well. The '411 application also describes how content may be delivered to the fuel dispenser 12 in a secure manner. The interested reader is referred to the '411 application for a more thorough understanding of authentication and content delivery. Other techniques for authenticating data are also within the scope of the present invention.

[0055] Those skilled in the art will recognize improvements and modifications to the preferred embodiments of the present invention. All such improvements and modifications are considered within the scope of the concepts disclosed herein and the claims that follow.

Claims

What is claimed is:

1. A method of collecting information at a retail terminal, comprising:

determining whether content to be presented on a display of the retail terminal requests information;

if the content to be presented on the display requests information, determining whether the content requests sensitive information;

authenticating the content to be presented on the display;

presenting the content on the display if the content is authenticated; and

if the content requests sensitive information, encrypting data received from one or more data entry point devices for transmission to a location removed from the retail terminal.

2. The method of claim 1, further comprising, not encrypting data received from said one or more data entry point devices if the information requested is not sensitive information.

3. The method of claim 1, wherein determining whether content requests sensitive information comprises determining whether the content requests a personal identification number (PIN).

4. The method of claim 1, wherein collecting information at the retail terminal comprises collecting information at a fuel dispenser.

5. The method of claim 1, wherein authenticating the content comprises checking a digital signature.

6. The method of claim 1, further comprising disabling said one or more data entry point devices associated with the retail terminal when the content cannot be authenticated.

7. The method of claim 1, further comprising enabling said one or more data entry point devices associated with the retail terminal when the content is authenticated.

8. The method of claim 2, further comprising receiving the non-sensitive information at the one or more data entry point devices.

9. A fuel dispenser, comprising:

a user interface comprising one or more data entry point devices adapted to receive information from a user and a display; and

a control system adapted to:

determine whether content to be presented on the display of the fuel dispenser requests information;

if the content to be presented on the display requests information, determine whether the content requests sensitive information;

authenticate the content to be presented on the display;

present the content on the display if the content is authenticated; and

if the content requests sensitive information, encrypting data received from one or more data entry point devices for transmission to a location removed from the fuel dispenser.

10. The fuel dispenser of claim 9, wherein the control system is further adapted to present content on the display if the content is not authenticated and concurrently disable the one or more data entry point devices.

11. The fuel dispenser of claim 9, further comprising fuel delivery components and wherein the control system is further adapted to control delivery of fuel to the user through the fuel delivery components.

12. The fuel dispenser of claim 9, wherein the control system is adapted to not encrypt data received from the one or more data entry point devices if the information requested is not sensitive information.

13. The fuel dispenser of claim 9, wherein the control system is adapted to determine whether the content requests a personal identification number (PIN).

14. The fuel dispenser of claim 9, wherein the control system is adapted to check a digital signature when authenticating the content.

15. The fuel dispenser of claim 9, wherein the control system is adapted to disable the one or more data entry point devices when the content cannot be authenticated.

16. The fuel dispenser of claim 9, wherein the control system enables at least one of the one or more data entry point devices when the content is authenticated.

17. A fueling system comprising:
a site controller;
a security module;
a fuel dispenser comprising:
a user interface comprising one or more data entry point devices and a display;
a control system adapted to:
determine whether content requests sensitive information;
authenticate the content;
if the content is authenticated, present the content on the display such that the content prompts the user for sensitive information;
receive the sensitive information through the user interface; and
encrypt the sensitive information for transmission to the security module through the site controller.

18. The fueling system of claim 17, wherein other content prompts the user for non-sensitive information.

19. The fueling system of claim 18, wherein the control system does not encrypt the non-sensitive information.

20. The fueling system of claim 17, wherein the transmission of encrypted sensitive information from the fuel dispenser to the security module occurs using a local encryption scheme.

21. The fueling system of claim 20, wherein the security module decrypts the local encryption scheme and re-encrypts the sensitive information with a host encryption scheme for transmission to a host.

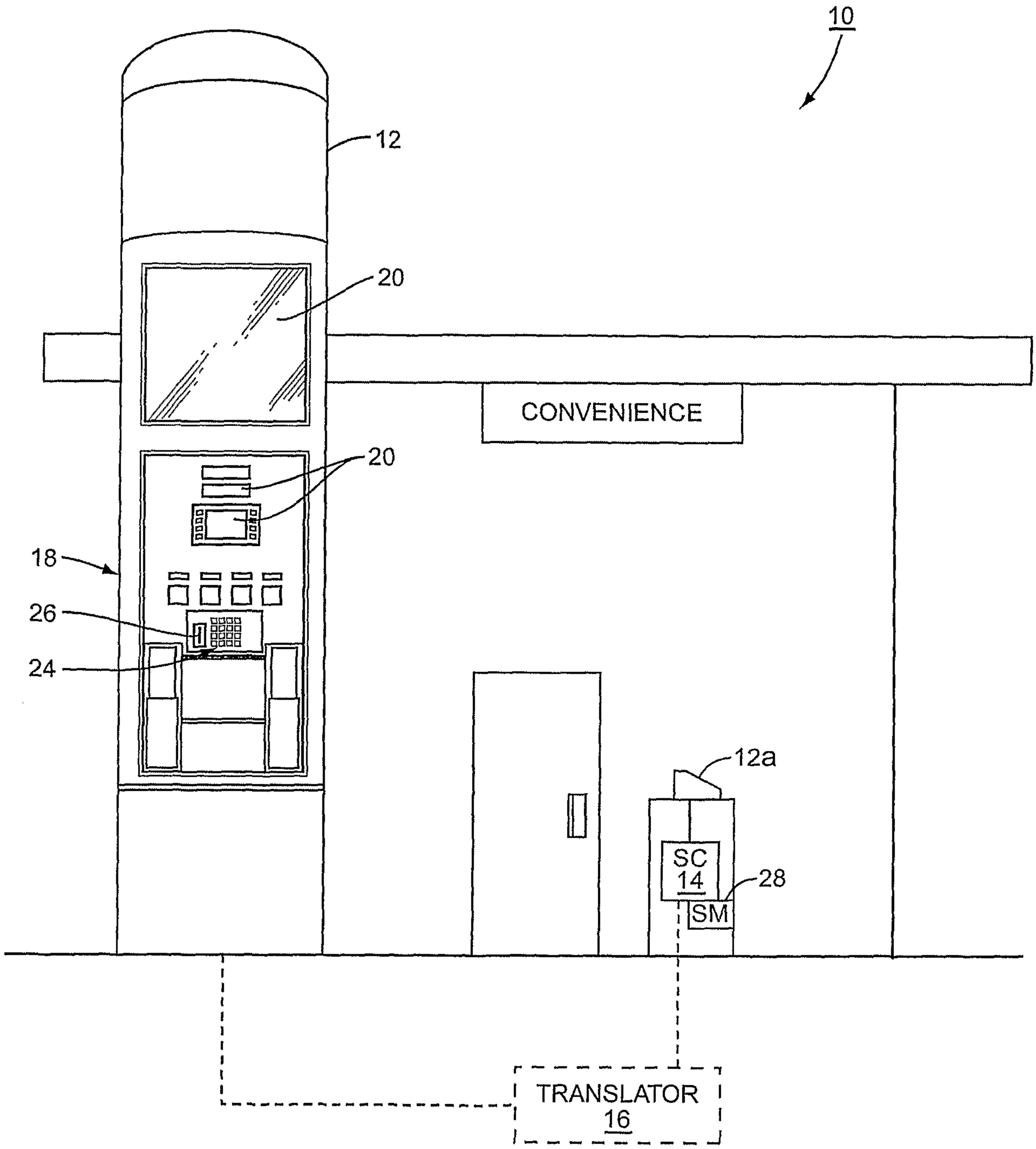


FIG. 1
PRIOR ART

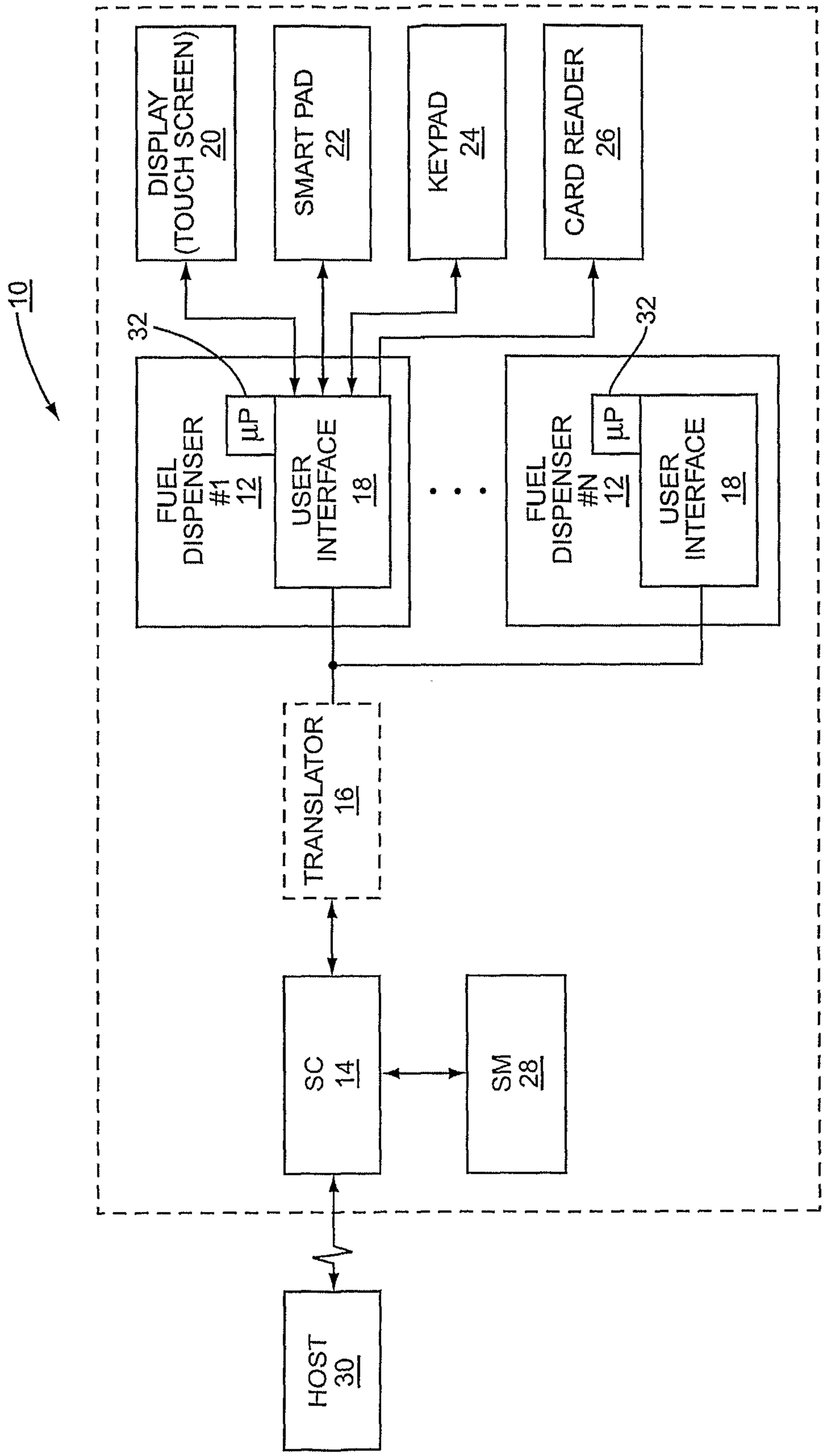


FIG. 2
PRIOR ART

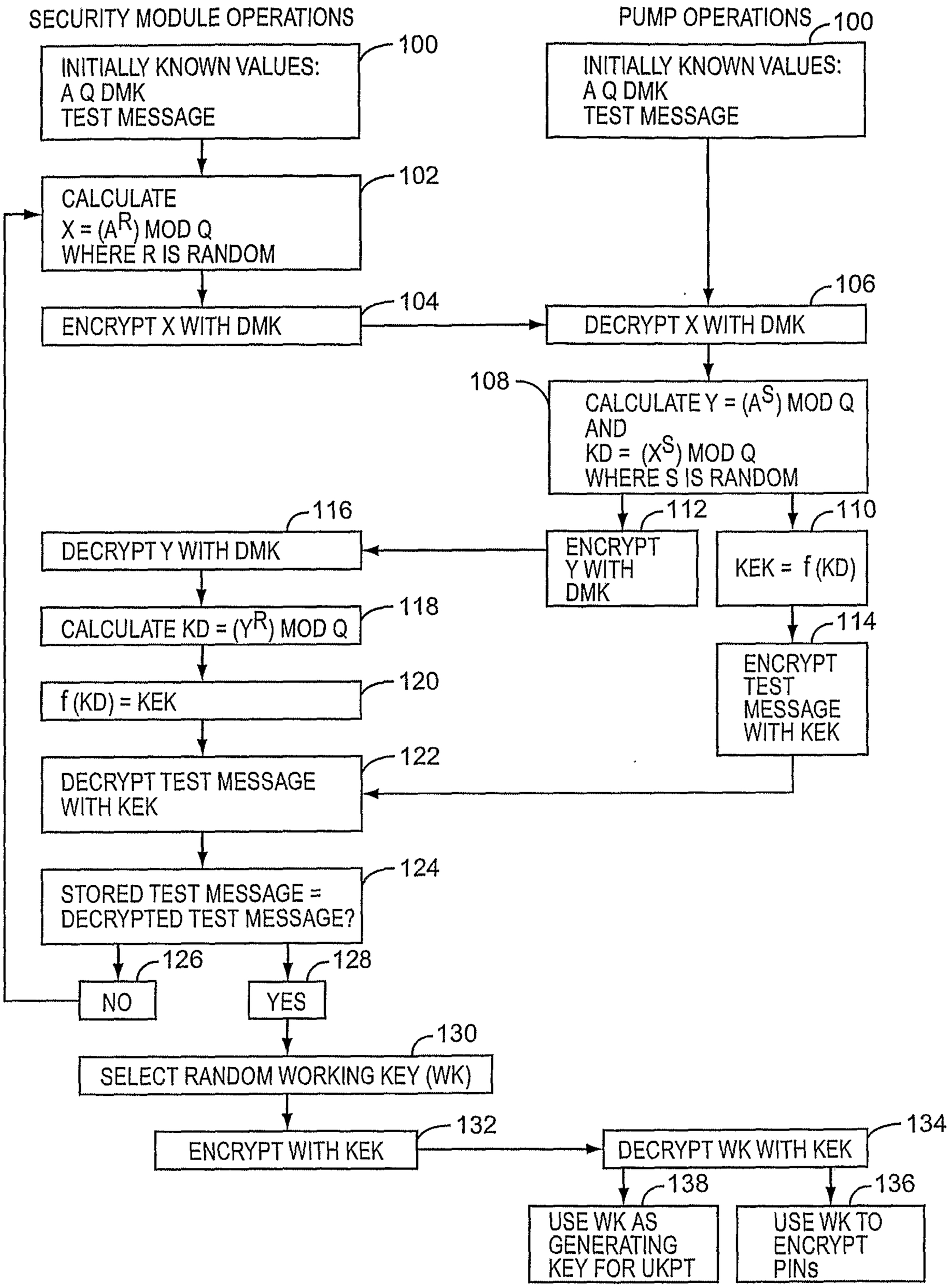


FIG. 3
PRIOR ART

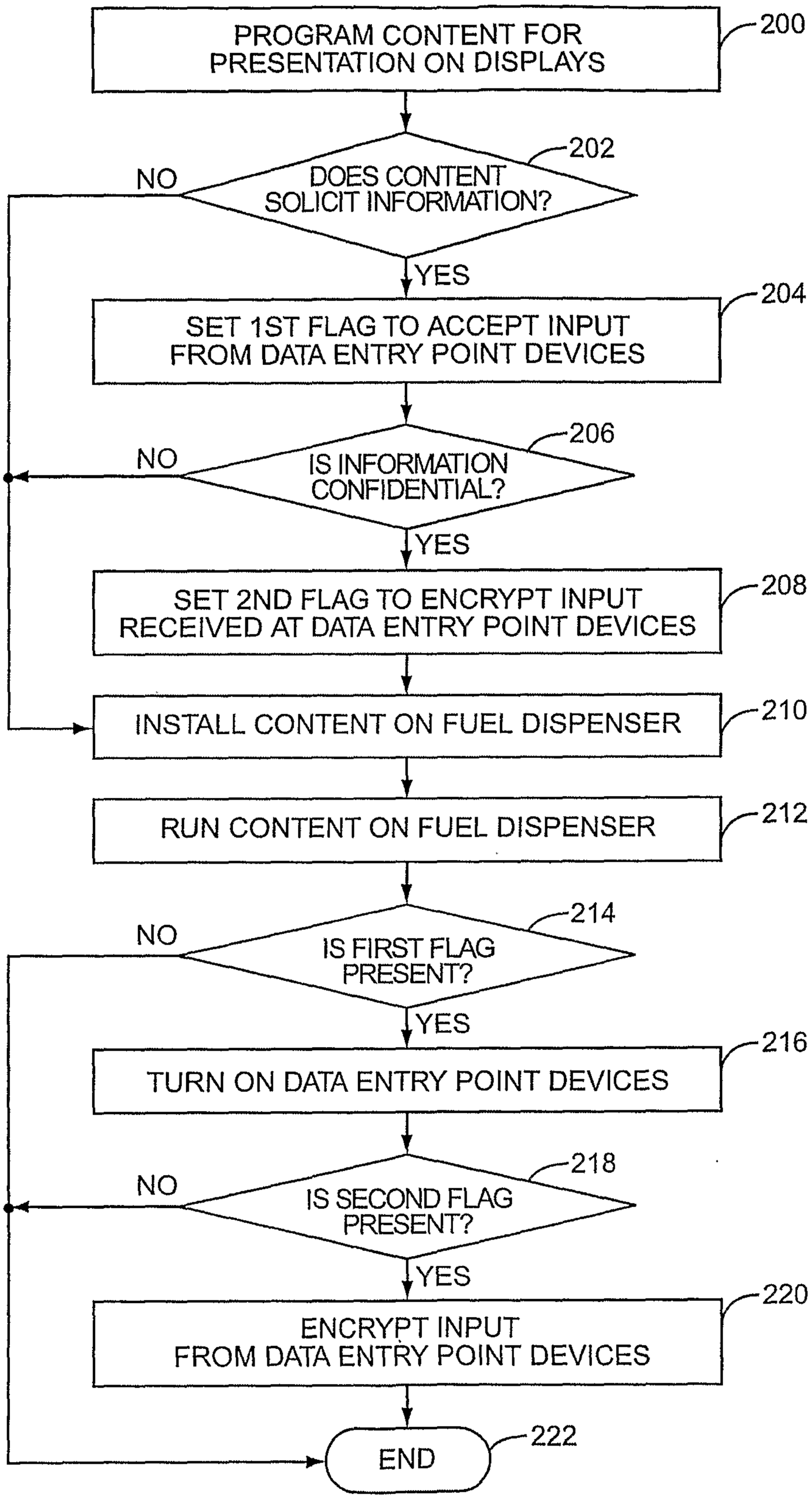

PROGRAM CONTENT FOR PRESENTATION ON DISPLAYS
200
DOES CONTENT SOLICIT INFORMATION?
202
NO
YES
SET 1ST FLAG TO ACCEPT INPUT FROM DATA ENTRY POINT DEVICES
204
IS INFORMATION CONFIDENTIAL?
206
NO
YES
SET 2ND FLAG TO ENCRYPT INPUT RECEIVED AT DATA ENTRY POINT DEVICES
208
INSTALL CONTENT ON FUEL DISPENSER
210
RUN CONTENT ON FUEL DISPENSER
212
IS FIRST FLAG PRESENT?
214
NO
YES
TURN ON DATA ENTRY POINT DEVICES
216
IS SECOND FLAG PRESENT?
218
NO
YES
ENCRYPT INPUT FROM DATA ENTRY POINT DEVICES
220
END
222

FIG. 4

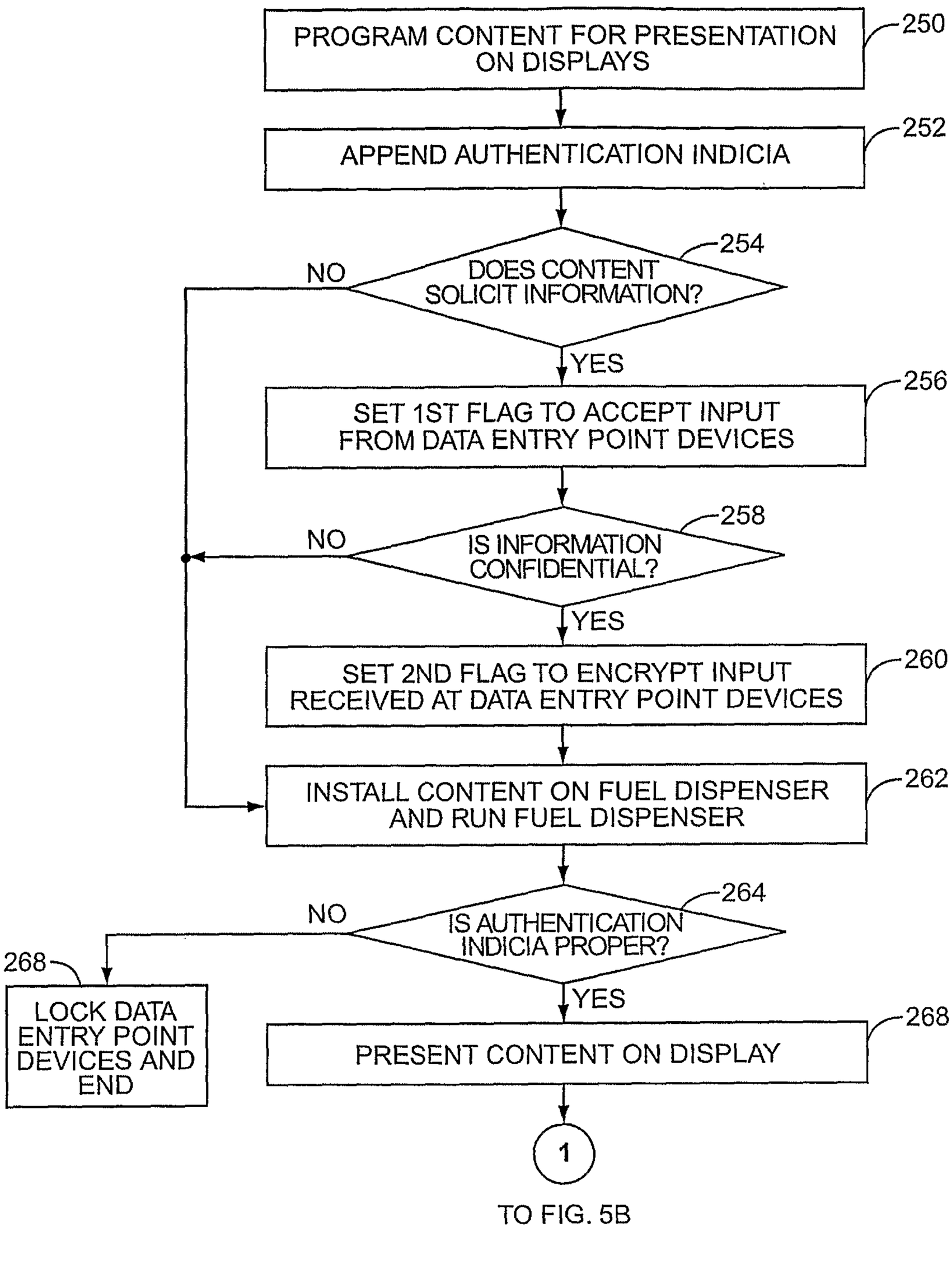

PROGRAM CONTENT FOR PRESENTATION ON DISPLAYS
250
APPEND AUTHENTICATION INDICIA
252
DOES CONTENT SOLICIT INFORMATION?
254
NO
YES
SET 1ST FLAG TO ACCEPT INPUT FROM DATA ENTRY POINT DEVICES
256
IS INFORMATION CONFIDENTIAL?
258
NO
YES
SET 2ND FLAG TO ENCRYPT INPUT RECEIVED AT DATA ENTRY POINT DEVICES
260
INSTALL CONTENT ON FUEL DISPENSER AND RUN FUEL DISPENSER
262
IS AUTHENTICATION INDICIA PROPER?
264
NO
YES
LOCK DATA ENTRY POINT DEVICES AND END
268
PRESENT CONTENT ON DISPLAY
268
1
TO FIG. 5B

FIG. 5A

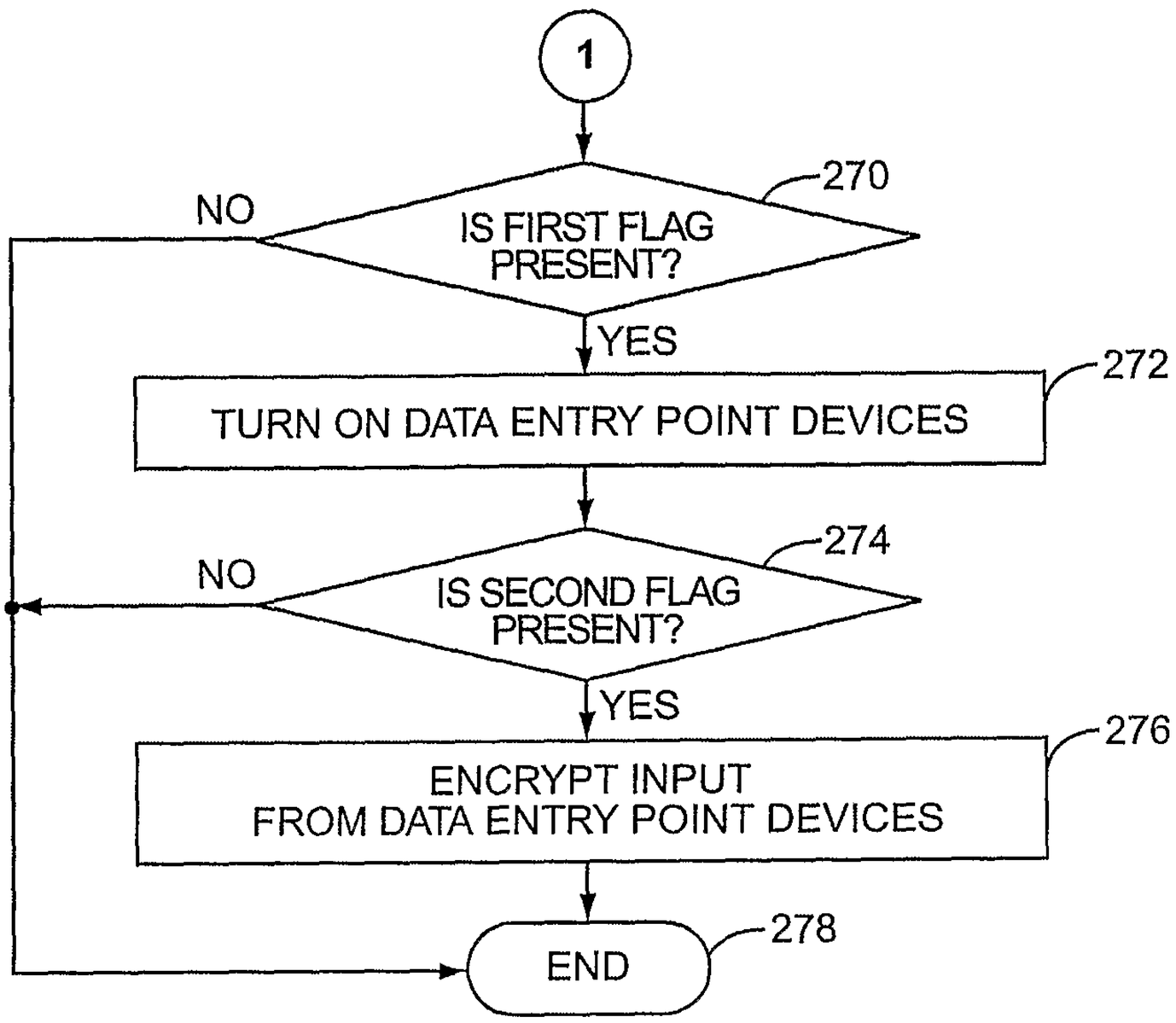

FROM FIG. 5A
1
270
IS FIRST FLAG PRESENT?
NO
YES
272
TURN ON DATA ENTRY POINT DEVICES
274
IS SECOND FLAG PRESENT?
NO
YES
276
ENCRYPT INPUT FROM DATA ENTRY POINT DEVICES
278
END

FIG. 5B

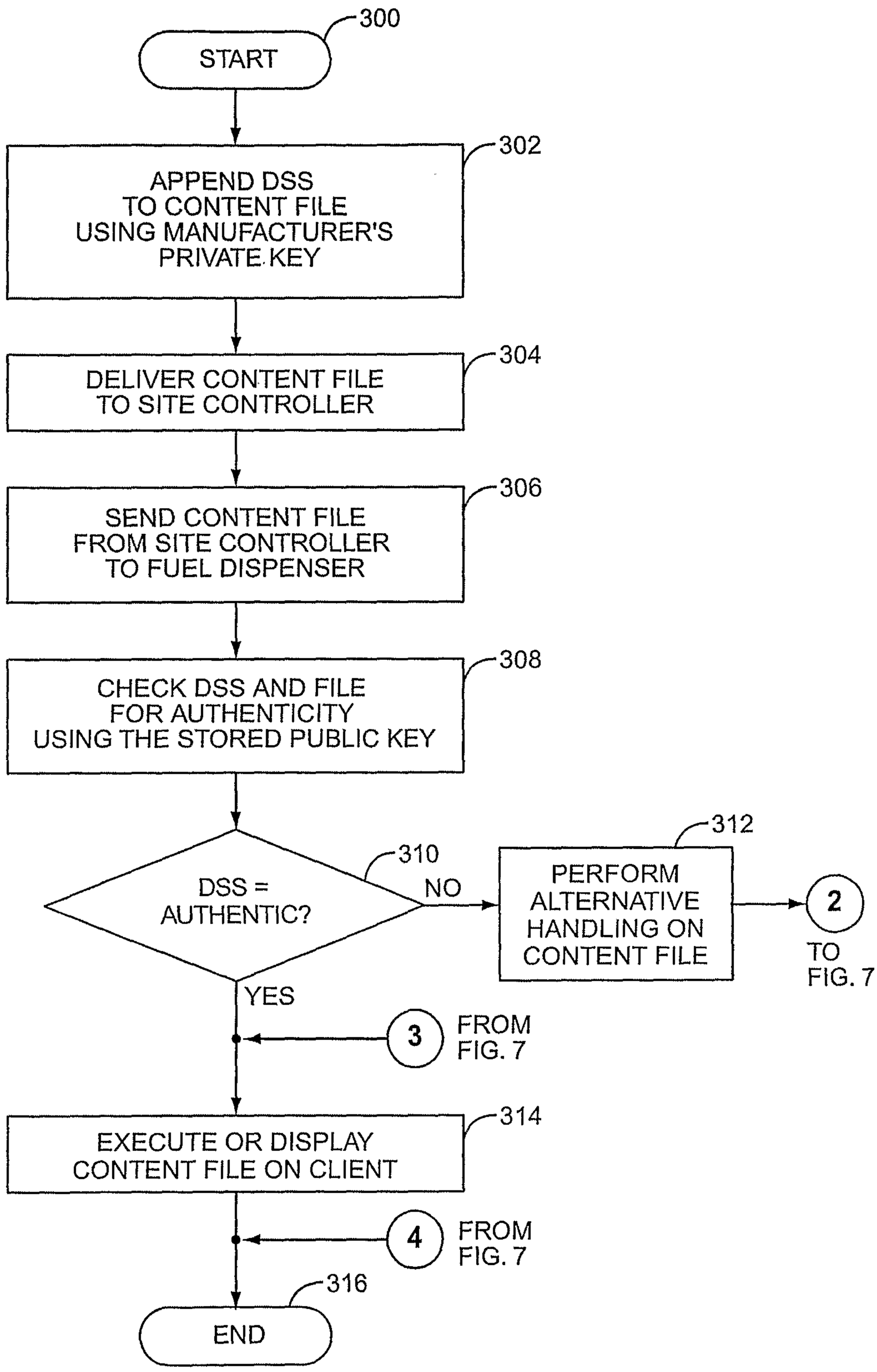

300
START
302
APPEND DSS
TO CONTENT FILE
USING MANUFACTURER'S
PRIVATE KEY
304
DELIVER CONTENT FILE
TO SITE CONTROLLER
306
SEND CONTENT FILE
FROM SITE CONTROLLER
TO FUEL DISPENSER
308
CHECK DSS AND FILE
FOR AUTHENTICITY
USING THE STORED PUBLIC KEY
310
DSS =
AUTHENTIC?
NO
312
PERFORM
ALTERNATIVE
HANDLING ON
CONTENT FILE
2
TO
FIG. 7
YES
3
FROM
FIG. 7
314
EXECUTE OR DISPLAY
CONTENT FILE ON CLIENT
4
FROM
FIG. 7
316
END

FIG. 6

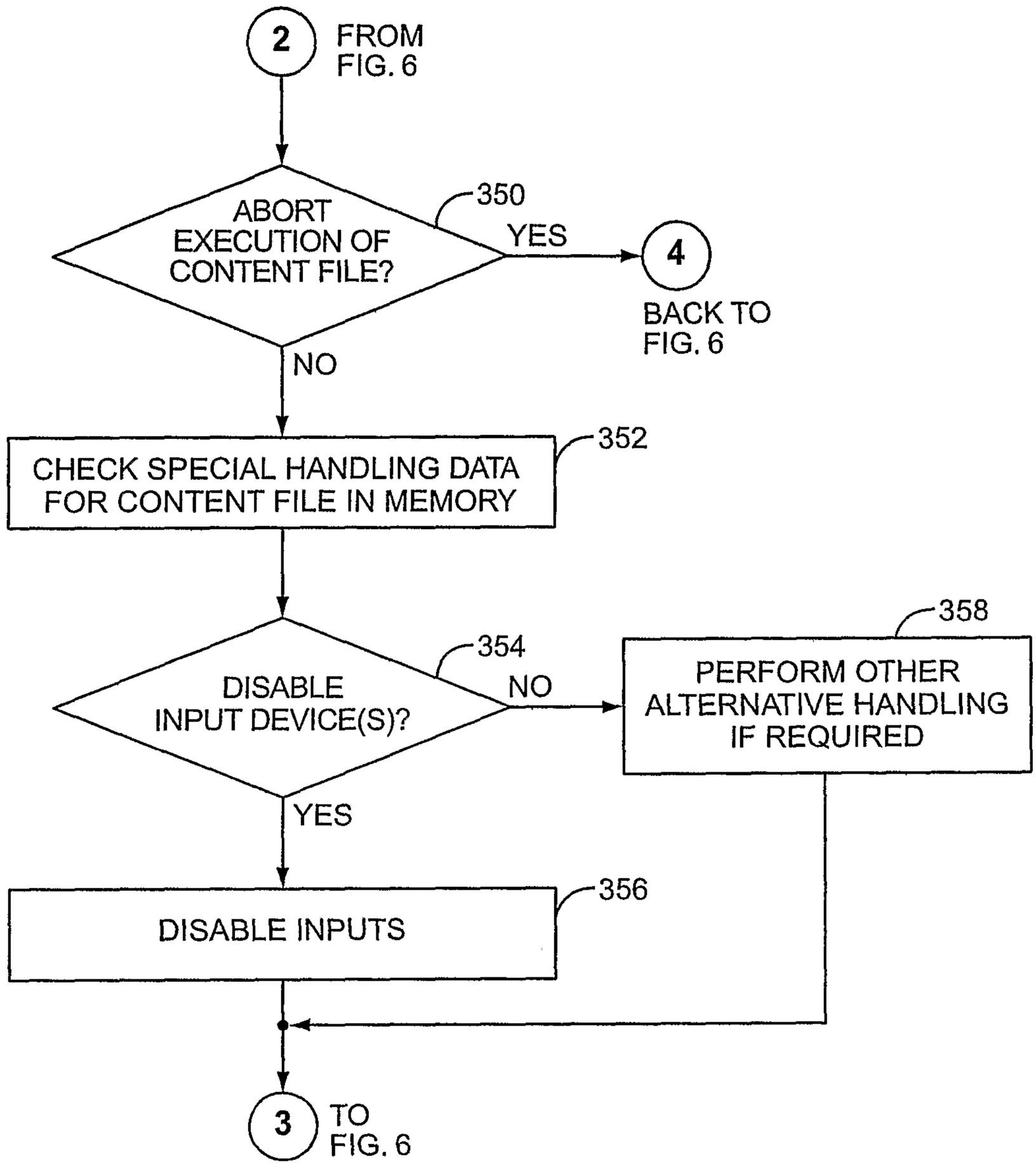
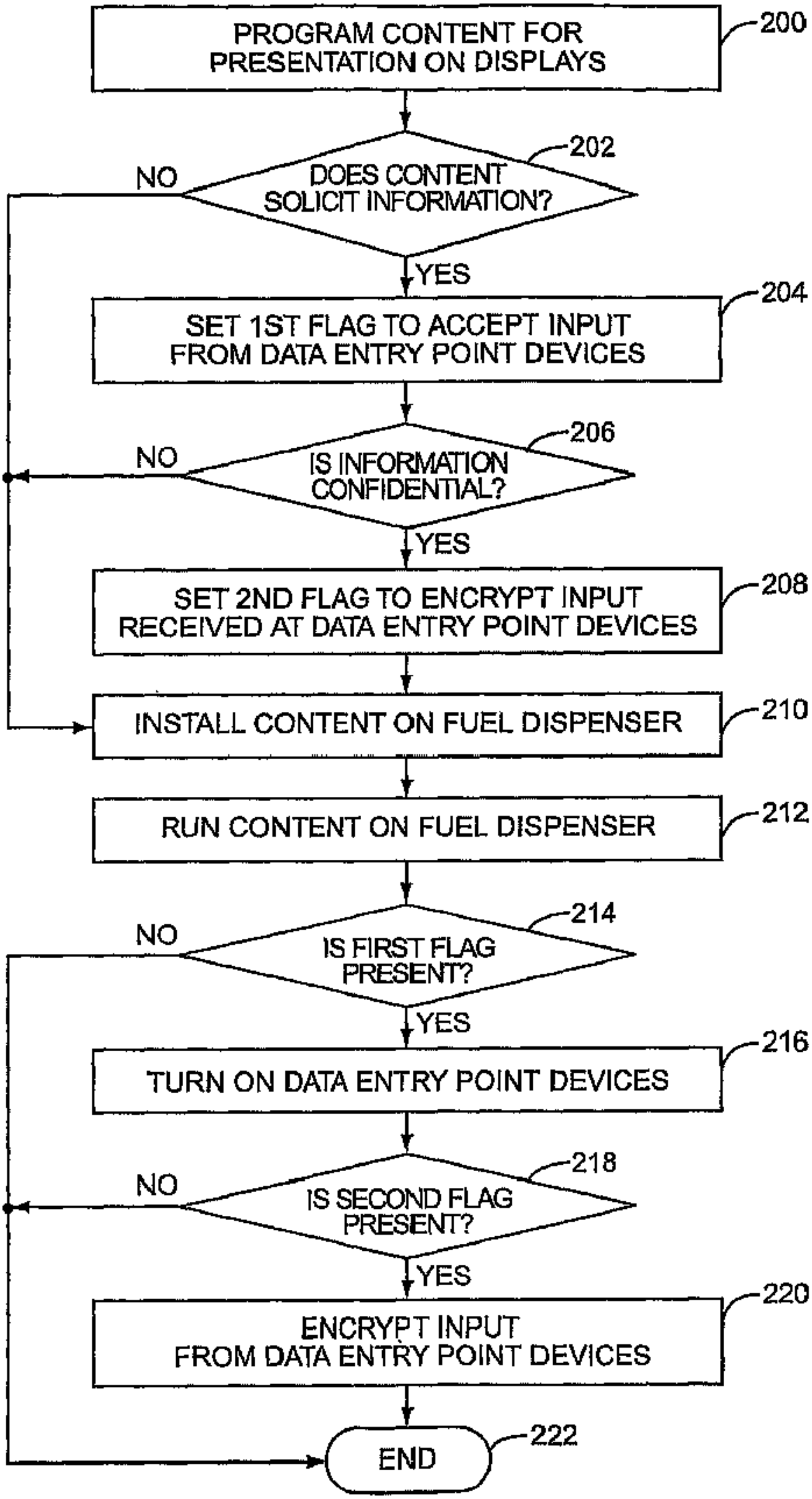

2
FROM FIG. 6
ABORT EXECUTION OF CONTENT FILE?
350
YES
4
BACK TO FIG. 6
NO
CHECK SPECIAL HANDLING DATA FOR CONTENT FILE IN MEMORY
352
DISABLE INPUT DEVICE(S)?
354
NO
PERFORM OTHER ALTERNATIVE HANDLING IF REQUIRED
358
YES
DISABLE INPUTS
356
3
TO FIG. 6

FIG. 7


PROGRAM CONTENT FOR PRESENTATION ON DISPLAYS
200
DOES CONTENT SOLICIT INFORMATION?
202
NO
YES
SET 1ST FLAG TO ACCEPT INPUT FROM DATA ENTRY POINT DEVICES
204
IS INFORMATION CONFIDENTIAL?
206
NO
YES
SET 2ND FLAG TO ENCRYPT INPUT RECEIVED AT DATA ENTRY POINT DEVICES
208
INSTALL CONTENT ON FUEL DISPENSER
210
RUN CONTENT ON FUEL DISPENSER
212
IS FIRST FLAG PRESENT?
214
NO
YES
TURN ON DATA ENTRY POINT DEVICES
216
IS SECOND FLAG PRESENT?
218
NO
YES
ENCRYPT INPUT FROM DATA ENTRY POINT DEVICES
220
END
222