Innovation, Sciences et Développement économique Canada
Office de la Propriété Intellectuelle du Canada

Innovation, Science and Economic Development Canada
Canadian Intellectual Property Office

CA 2683190 C 2019/07/16

(11)(21) 2 683 190

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(22) Date de dépôt/Filing Date: 2009/10/16

(41) Mise à la disp. pub./Open to Public Insp.: 2010/04/17

(45) Date de délivrance/Issue Date: 2019/07/16

(30) Priorité/Priority: 2008/10/17 (US61/106,338)

(51) Cl.Int./Int.Cl. *H04L 9/32* (2006.01), *H04L 12/24* (2006.01), *H04L 29/12* (2006.01), *H04N 21/441* (2011.01)

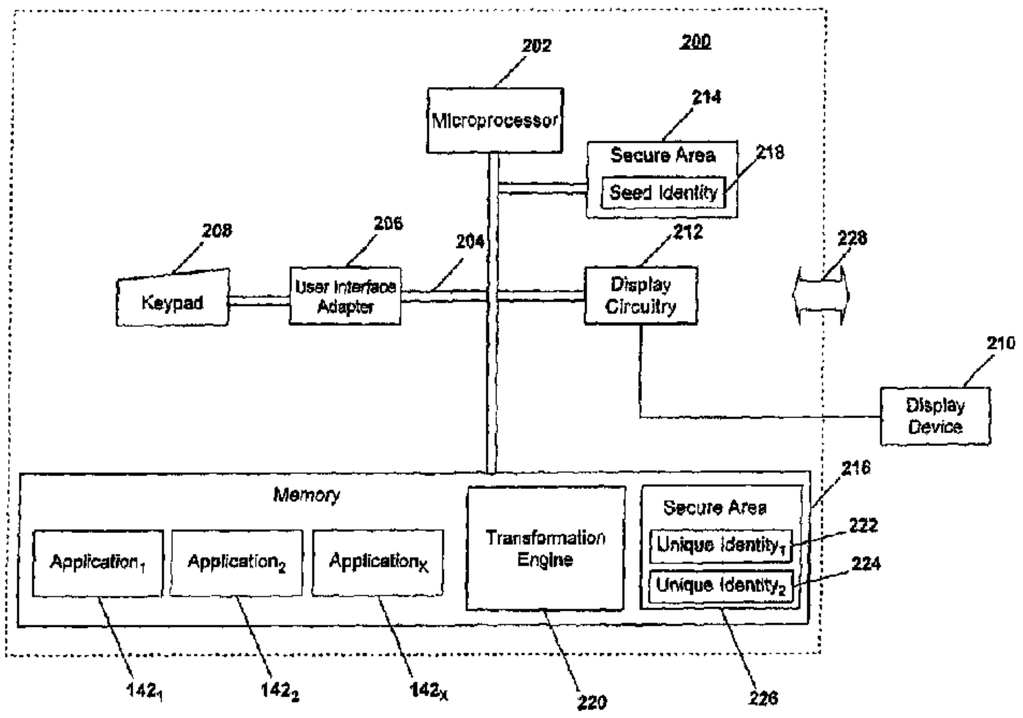
(72) Inventeur/Inventor:
REYNOLDS, STEVEN J., US

(73) Propriétaire/Owner:
COMCAST CABLE COMMUNICATIONS, LLC, US

(74) Agent: MACRAE & CO.

(54) Titre : SYSTEME ET METHODE DE PRISE EN CHARGE D'IDENTITES MULTIPLES POUR DISPOSITIF D'IDENTITE SECURISE

(54) Title: SYSTEM AND METHOD FOR SUPPORTING MULTIPLE IDENTITIES FOR A SECURE IDENTITY DEVICE



(57) Abrégé/Abstract:
A multiple-identity secure device (MISD) persistently stores a single identification code (a "seed identity"). The seed identity need not be a network address, and may be stored in an integral memory of the device, or on an interchangeable card received in a physical interface of the MISD. The MISD is provided with a transformation engine, in hardware or software form, that is subsequently used to generate one or more unique identities (e.g., network addresses) from the stored seed identity using predefined logic. The generated identities may be dynamically generated, e.g., in real-time as needed after deployment of a device into possession of a subscriber/customer/user, etc., or may be securely stored in the MISD for subsequent retrieval. The transformation engine may generate a unique identity in accordance with an addressing scheme identified as a default setting, a global/network setting, or as determined from a received data transmission.

ABSTRACT

[0063] A multiple-identity secure device (MISD) persistently stores a single identification code (a "seed identity"). The seed identity need not be a network address, and may be stored in an integral memory of the device, or on an interchangeable card received in a physical interface of the MISD. The MISD is provided with a transformation engine, in hardware or software form, that is subsequently used to generate one or more unique identities (e.g., network addresses) from the stored seed identity using predefined logic. The generated identities may be dynamically generated, e.g., in real-time as needed after deployment of a device into possession of a subscriber/customer/user, etc., or may be securely stored in the MISD for subsequent retrieval. The transformation engine may generate a unique identity in accordance with an addressing scheme identified as a default setting, a global/network setting, or as determined from a received data transmission.

SYSTEM AND METHOD FOR SUPPORTING MULTIPLE IDENTITIES FOR A SECURE IDENTITY DEVICE

FIELD OF THE INVENTION

[0001] The present invention relates generally to secure communications between devices in an information network. More particularly, the present invention relates to a system and method for supporting multiple identities for a secure identity device by dynamic generation of device identities from a persistently-stored seed identity.

DISCUSSION OF THE RELATED ART

[0002] An "information network" refers to a collection of elements or devices, collectively "devices", having a transport mechanism for exchanging information or content between the devices. Such networks may have any suitable architecture, including, for example, client-server architecture, 3-tier architecture, N-tier architecture, distributed objects, loose coupling, or tight coupling.

[0003] One example of an information network is a subscriber-based cable or satellite system, such as the exemplary system shown in Figure 1. This exemplary information network is typical of many different types of information networks in that it involves data transmissions between devices in the network, and that it is often advantageous or necessary that a particular device be uniquely identifiable and/or

addressable on the network, and/or that transmissions be made in a secure manner with specific devices.

[0004] By way of further example, with reference to Figure 1, the exemplary subscriber-based television system, that propagates content (e.g., entertainment and commercials information such as movies, sports, television programming and the like), information (e.g., video on demand, Interactive Program Guide (IPG) services and the like) and applications (e.g., billing and other services) to client devices or set top boxes associated with subscribers/users.

[0005] "Set top box" or STB refers to a device that connects to a monitor and an external source of signal, converting the signal into content for display/transmission over the monitor. The signal source might be an Ethernet cable, a satellite dish, a coaxial cable, a fiber optic cable, a telephone line (including DSL connections), Broadband over Power Line, or even an ordinary antenna. The STB may have several different embodiments. For example, it may be a special digital STB for delivering digital content on TV sets that do not have a built in digital tuner. The STB may also descramble premium channels. An STB may be a cable converter box to receive digital cable TV channels and convert them to analog for non-digital TVs. In the case of direct broadcast satellite (mini-dish) systems such as SES Astra, Dish Network, or DirecTV, the STB is an integrated receiver/decoder (or IRD). In internet packet (IP) TV networks, the STB is a small computer providing two-way transmissions on an IP network, and decoding the video streaming media which eliminates the need for any

coaxial cabling. The STB may be a discrete unit or its functionality may be incorporated into other components of the user's system such as the monitor, TV, DVR, residential gateway, or personal computer. For example, the STB may be a portable, modular unit (i.e., a personal STB) or it may be integrated into a stationary TV system. The STB may contain one or more digital processors or may use the processing capabilities of the other system components (e.g., TV, DVR, personal computer). Additionally, rather than having its own tuner, the STB may use the tuner of a television (or DVR).

[0006] A "digital video recorder" (DVR) refers to a device or system that records video in a digital format to a digital storage medium such as a disk drive or solid state memory for future playback. DVRs have different configurations. For example, a DVR may be a stand-alone, modular unit (such as those sold by TiVo), it may be a portable personal device, or it may be incorporated into other audiovisual components such as a set-top box or the TV itself. It may even be software for a personal computer (PC) that enables the PC to capture video for playback using the digital storage medium of the PC.

[0007] The system of Figure 1 transmits various data signals constituting various content, which signals may be scrambled, encrypted or otherwise secured, to the different STBs 142 in the system. Operation and interconnection of the similar devices in a similar system are described in detail in U.S. Patent No. 5,787,172. The term "transmitted" or "transmits" refers broadly to sending a signal from a transmitting device

to a receiving device. The signal may be transmitted wirelessly or over a solid medium such as wire or fiber.

[0008] The exemplary system 100 of Figure 1 comprises a head-end 120, a network 130 and a plurality of set-top boxes STBs 140_1 through 140_N (collectively STBs 140), as is typical of such systems. The head-end 120 typically also comprises an application server 122 and operates in part to transmit information to, and receive information from, the STBs 140 via network 130. The head-end 120 also comprises a server 110 which receives data from a data provider 106 through a network 107 such as, for example, the Internet. The server 110 may be accessed using an operator GUI 112 for adding and monitoring data.

[0009] The head-end 120 is associated with a neighborhood of STBs 140_1-$_N$. The head-end 120 communicates with the STBs 140 within its neighborhood via a downstream transmissions channel (DOWN) and an upstream transmissions channel (UP). These channels are supported by a network topology 130, such as a hybrid fiber-coax cable television distribution system, a satellite distribution system (e.g., using a telephone network or reverse satellite link for upstream transmissions) and the like.

[0010] The head-end 120 interacts with the STBs 140 to enable the delivery of content, etc. provided by the server, as well as to return STB messages, etc. to the server 120. Each STB is typically associated with a respective display device

150, such as a television or other video display device, and a user input device 160 such as a remote control, etc.

[0011] The STBs 140 operate to receive signal transmissions from the head-ends 120 via the network 130 using the downstream transmissions channel DOWN (or an out-of-band channel). The transmissions may be broadcast, multicast/narrowcast, or unicast. Broadcasting refers to the transmission of content to an audience at large. The audience may be the general public, or a sub-audience. Switched digital video is a type of broadcast that is initiated in response to a client request and is terminated when no more clients are tuned to it. Multicasting refers to the simultaneous transmission of content to a plurality of specific and known destinations or addresses in a network or between networks. Multicast is often used for streaming media and Internet television applications, Ethernet multicast addressing, ATM point-to-multipoint VCs and Infiniband multicast. Unicasting refers to the transmission of a signal to a single destination or address in a network. Unicast is used, for example, in Video-On-Demand applications.

[0012] To enable such transmissions to the STBs, it is important that each STB is uniquely identifiable within the network. By way of example, the identity of a device must be reliably determinable and authenticatable to preserve the integrity of the information network, e.g. to validate data intended for receipt by a specific device in a data distribution system, prevent digital piracy, theft of content, or unauthorized access

to content in a digital data distribution system. Systems and methods of such validation are well-known in the art and thus are not described in detail herein.

[0013] To ensure that each STB is uniquely identifiable, each STB is assigned a unique network address that permits the head-end to communicate with the STB to, for example, establish in the STB an authorization code that determines which pay programs that STB will be able to receive. In many systems, the STB is also able to communicate with the head-end in a two-way transmission link, so as to permit each STB to be interrogated or addressed from the head-end. Such two-way transmission also requires that each STB be assigned a unique network address.

[0014] In order to ensure the uniqueness and authenticity of the devices, it is common practice to encode each device's network address (e.g. in bits) in a memory of the device at a time of manufacture of the device or one of its components. The address/memory is secured, in part, by rendering the associated memory location read-only after initial programming. Furthermore, the address value itself is typically made available to application level software via a secure API to prevent "hacking" or "spoofing" of the identity. By way of example, the STB address is conventionally stored in ROM or one-time-programming (OTP) memory during manufacture of the device. Alternatively, the address may be stored in a programmable read-only-memory (PROM) at or prior to the time the STB is installed at a subscriber's home. This is done in the field by a professional installer, using a PROM programmer. The installer typically

programs the PROM with the preassigned address for that STB and installs the PROM into a socket provided for the PROM in the subscriber's STB.

[0015] These procedures are typically time-consuming, costly and inefficient, and must be repeated in the field each time a new STB is installed at a subscriber's home.

[0016] Further, as information networks have evolved, it has become apparent that there is sometimes a need for a single device, such as a wireless telephone/PDA handset or DVB-Simulcrypt device, to present one of several different identities over its lifetime. Typically, this is done by configuring the device with a physical interface configured to accept a secure identity card, such as a SIM module or SmartCard, and allowing exchange of the identity by physically replacing one secure identity card with another. However, the configuration of devices with such physical interfaces has been found to be undesirable as they provide an interface that can be used by pirates, hackers, etc. to gain unauthorized access to secure information networks.

[0017] Further still, there is sometimes a need for a single device to present, essentially concurrently, several different identities, e.g. to support a conditional access system in which different permissions, rights, entitlement, content, etc. are provided according to a profile for each identity. In circumstances in which an interchangeable card is not intended to be employed, a single device may be initially

programmed to include multiple unique identities. However, programming multiple, unique identities is disadvantageous in that it requires incrementally more space in the secure memory area of the device. This space is often limited and adding space is expensive, as it often requires new revisions of the device or system-on-a-chip elements of the device.

[0018] What is needed is a system and method that addresses the disadvantages of physical interface and multiple identity programming discussed above, and that is capable of providing multiple identities in the event that a physical interface will not be included in a device ,and in the event that the intended identity needed for deployment is not yet known at time of manufacture.

SUMMARY OF THE INVENTION

[0019] The present invention provides a multiple-identity secure device having a single persistently-stored identification code (a "seed identity"), and a transformation engine that is subsequently used to generate one or more unique identities (e.g., network addresses) for the device from the stored seed identity. The seed identity is an identification code, which may be unique, may be a network address, and may be a code other than a network address, such as a serial number or other identification code. The transformation engine includes computer-readable instructions executable by a microprocessor to receive the seed identity as input, and to generate as output at least one unique identity as a function of predefined logic. The transformation engine may receive input identifying and addressing scheme, and may be configured to

correspondingly generate unique identity that is compliant with the identified addressing scheme. The predefined logic may include conditional logic requiring generation of a unique identity by a first method for a first condition and by a second method for a second condition.

[0019.1] In accordance with one aspect of the present invention, there is provided one or more non-transitory computer-readable medium storing computer-readable instructions that, when executed by a processor, cause the processor to receive a data transmission comprising recipient identity data, determine an addressing scheme used to direct the data transmission, retrieve a seed identity comprising an identification code, generate a unique identity based on the seed identity and the determined addressing scheme, extract the recipient identity data from the received data transmission, and determine whether the generated unique identity corresponds to the recipient identity data.

[0019.2] In accordance with another aspect of the present invention, there is provided a device comprising a microprocessor, and memory storing computer-readable instructions that, when executed by the microprocessor, cause the device to receive a data transmission comprising recipient identity data, determine an addressing scheme used to direct the data transmission, retrieve a seed identity comprising an identification code, generate a unique identity based on the seed identity and the determined addressing scheme, extract the recipient identity data from the received data transmission, and determine whether the generated unique identity corresponds to the recipient identity data.

[0019.3] In accordance with a further aspect of the present invention, there is provided a method comprising receiving, at a secure identity device, a data transmission comprising recipient identity data, determining an addressing scheme used to direct the data transmission, retrieving a seed identity from a secure memory, generating, at the secure identity device, a unique identity based on the seed identity and the determined addressing scheme, extracting the recipient identity data from the received data transmission, and determining whether the generated unique identity corresponds to the recipient identity data.

[0019.4] In accordance with yet a further aspect of the present invention, there is provided a method comprising receiving, at a secure device, identity data, obtaining, from a secure memory area of the secure device, a unique identity for the secure device, wherein the unique identity is based on a seed identity stored in the secure device, predefined logic stored in the secure device, and an addressing scheme used to direct the identity data, determining, at the secure device, whether the unique identity corresponds to the identity data, if the unique identity does not correspond to the identity data, discarding the identity data, and if the unique identity corresponds to the identity data, using data from the identity data.

[0019.5] In accordance with another aspect of the present invention, there is provided a system comprising a first device comprising a first microprocessor, first predefined logic, and first memory storing computer-readable instructions that, when executed by the first microprocessor, cause the first device to receive a data transmission comprising recipient identity data, determine an addressing scheme used to direct the data transmission, retrieve a first seed identity comprising an identification

code, generate a unique identity based on the first seed identity and the determined addressing scheme, extract the recipient identity data from the received data transmission, and determine whether the generated unique identity corresponds to the recipient identity data, and a second device comprising a second microprocessor, and second memory storing computer-readable instructions that, when executed by the second microprocessor, cause the second device to store a second seed identity and a second predefined logic, wherein the second seed identity is different from the first seed identity, and wherein the second predefined logic is the same as the first predefined logic.

[0019.6] In accordance with yet another aspect of the present invention, there is provided a system comprising a first device comprising a first microprocessor, first predefined logic, and first memory storing computer-readable instructions that, when executed by the first microprocessor, cause the first device to receive a data transmission comprising recipient identity data, determine an addressing scheme used to direct the data transmission, retrieve a first seed identity comprising an identification code, generate a unique identity based on the first seed identity and the determined addressing scheme, extract the recipient identity data from the received data transmission, and determine whether the generated unique identity corresponds to the recipient identity data, and a second device comprising a second microprocessor, and second memory storing computer-readable instructions that, when executed by the second microprocessor, cause the second device to store a second seed identity and a second predefined logic, wherein the second seed identity is the same as the first seed

identity, and wherein the second predefined logic is different from the first predefined logic.

[0019.7] In accordance with a further aspect of the present invention, there is provided a method comprising determining, by a device, an addressing scheme used to direct a data transmission to the device, wherein the data transmission comprises a recipient identifier, based on the determined addressing scheme, obtaining a unique identity, wherein the unique identity is based on a seed identity of the device, comparing the recipient identifier with the unique identity, and determining whether to keep or to discard the data transmission based on the comparing.

[0019.8] In accordance with a still further aspect of the present invention, there is provided a method comprising generating, using a seed identity of a device, a plurality of unique identities, wherein each unique identity of the plurality of unique identities corresponds to a different addressing scheme, storing, at the device, the plurality of unique identities, determining a first addressing scheme used to direct a data transmission to the device, and retrieving a first unique identity of the plurality of unique identities that corresponds to the determined first addressing scheme used to direct the data transmission to the device.

[0019.9] In accordance with another aspect of the present invention, there is provided a method comprising storing a first unique identity, wherein the first unique identity is based on a seed identity of a device, and wherein the first unique identity corresponds to a first addressing scheme, receiving a data transmission at the device, and responsive to a determination that a second addressing scheme used to direct the

data transmission is different from the first addressing scheme, generating a second unique identity based on the seed identity and the second addressing scheme.

BRIEF DESCRIPTION OF THE DRAWINGS

[0020] The present invention will now be described by way of example with reference to the following drawings in which:

[0021] Figure 1 is a block diagram of an exemplary prior art information network into which multiple-identity secure devices in accordance with the present invention may be deployed;

[0022] Figure 2 is a block diagram of an exemplary multiple-identity secure device in accordance with the present invention;

[0023] Figure 3 is a flow diagram of an exemplary method for supporting multiple identities for a secure identity device in accordance with the present invention; and

[0024] Figure 4 is a flow diagram of an exemplary method for processing data using a multiple-identity secure device in accordance with the present invention.

DETAILED DESCRIPTION

[0025] In contrast to conventional secure identity devices, each of which stores a single network address for use to direct data transmissions to each specific device, the present invention provides a multiple-identity secure device having a single persistently-stored identification code (a "seed identity"), and a transformation engine that is subsequently used to generate, in an automated fashion, one or more unique identities (e.g., network addresses) for the device from the stored seed identity.

[0026] The seed identity is an identification code, and may or may not be unique among identification devices within a network. Unlike conventional storage of network addresses, the seed identity stored in accordance with the present invention may be a something other than a network address. Although the seed identity may be a network address, it may also be another code completely unrelated to a network address, such as a serial number or other alphanumeric string. By way of example, the seed identity may comprise a simple numeric sequence, such as a 32-bit number, or it may be more sophisticated, such as a MAC address.

[0027] The transformation engine generates identities as a function of the seed identity, using predefined logic. The generated identities may be dynamically generated, e.g., in real-time as needed, after deployment of a device into the field, e.g., into the possession of a subscriber/customer/user. The transformation engine includes computer-readable instructions executable by a microprocessor to receive the seed identity as input, and to generate as output at least one unique identity as a function of

predefined logic accessible to the transformation engine 220. The transformation engine may be implemented as firmware in hardware or as software stored in memory. The predefined logic may be incorporated into the transformation engine, e.g., hard-coded into the transformation engine software, and may include any suitable logic for generating a unique identity, e.g., unique network address, from the seed identity. By way of example, the predefined logic may require generation of a unique identity by adding an offset, bit mask, or bit shift to the seed identity. By way of further example, the predefined logic may include conditional logic requiring generation of a unique identity by a first method for a first specified addressing scheme, and by a second method for a second specified addressing scheme.

[0028] Thus, the present invention provides a system and method that addresses the drawbacks of physical interface and multiple identity programming discussed above, and yet is capable of providing and supporting multiple identities in the event that a physical interface will not be included in a device and that the intended identity needed for deployment is not yet known at time of manufacture.

[0029] Although the prior art discussion above relates to a subscriber-based television system, one of skill in the art will understand that the present disclosure is applicable to a wide variety of information networks that require each device to have a secure identity. For example, the present invention can be employed in a subscriber radio system, a wireless voice or data network. Examples of secure identity devices include an STB in a cable or satellite television system, a wireless

telephone handset or personal digital assistant (PDA) devices in a telecommunications network.

[0030] In addition, one of skill in the art will understand that the present disclosure is applicable to other systems for which communication is not the primary purpose. For example, the present invention can also be applied in an alarm system network involving transmission between different elements of the system. The present invention should not be construed to limit the scope of the invention to an "information network," where the primary objective of the system is to transmit information. The present invention can apply to systems in which the transmission of information is only a minor, or even insignificant, aspect of the overall system. In fact, the present invention can be adapted for use in any system involving secure identity devices.

[0031] As used herein, an identity, memory, etc. is considered "secure" if an encryption/decryption system is used for which determination of encrypted information is computationally or economically infeasible without knowledge of specific decryption information and where the decryption information has not been acquired by outsiders, or if a signature/verification system is used for which unauthorized insertion or modification of signed information is computationally or economically infeasible without knowledge of specific signature information and where the signature information has not been acquired by outsiders, or if data is otherwise protected by security measures. In one embodiment, an encryption/decryption system is used for which determination of encrypted information is computationally infeasible without knowledge

of specific decryption information, and a signature/verification system is used for which unauthorized insertion or modification of signed information is computationally infeasible without knowledge of specific signature information.

[0032] Figure 2 is a high level block diagram of an exemplary multiple-identity secure device (MISD) 200. Each MISD includes conventional hardware and software typical of commercially-available secure identity devices, which may include a variety of client devices and/or network devices.

[0033] The exemplary MISD be a specially-configured set top box (STB) for use in the exemplary network of Figure 1, in accordance with the present invention. Alternatively, the MISD may be configured as a wireless telephone handset, a smartphone, a PDA, or another communications device. The discussion below discusses the MISD 200 in the context of an STB for illustrative purposes only.

[0034] Referring now to Figure 2, the MISD 200 includes a microprocessor 202 and a bus 204 employed to connect and enable communication between the microprocessor 202 and the components of the MISD in accordance with known techniques. The MISD typically includes at least a user interface adapter 206, which connects the microprocessor 202 via the bus 204 to one or more interface devices, such as a keypad 208. The bus 204 also connects a display device 210, such as an external television, LCD screen or monitor, to the microprocessor 202 via a display adapter 212. The bus 204 also connects the microprocessor 202 to non-volatile

memory 216, which can include a hard drive, diskette drive, tape drive, random access memory (RAM), etc.

[0035] In accordance with the present invention, the MISD stores a seed identity 218 in memory. In this example, the MISD stores the seed identity 218 in a read-only memory (ROM) 214 operatively connected to the microprocessor 202. The term ROM is intended herein to be read in a broad, and not limiting, fashion, and includes conventional ROM, PROM and one-time programmable (OTP) memory. For example, the MISD may store the seed identity in a secure storage area of the device. The inclusion of such secure storage areas in such chips and devices, and storing data in such secure storage areas, are well known in the art. In accordance with conventional manufacturing techniques, the ROM is written to at the time of manufactures. In accordance with the present invention, a seed identity is assigned and stored in the ROM at the time of manufacture. The seed identity may be stored in the ROM in a conventional fashion.

[0036] In one embodiment, each MISD is provided with a unique seed identity, so that no two devices are assigned the same seed identity. In such an embodiment, a single predefined logic may be used to generate unique identities from each respective seed identity.

[0037] Alternatively, some secure identity secure cards, and thus some devices, may be provided with identical seed identities. In such a case, different

predefined logic may be used to generate different unique identities for the devices from the same seed identity.

[0038] As discussed above, the MISD further includes a non-volatile storage memory operatively 216 connected to the microprocessor 202. The MISD may store various microprocessor-executable software applications. For example, in the context of an STB, the MISD may store application programs 142_1-142_x (application programs 142), which may include any of the applications used within the context of an STB 140, such as an interactive program guide (IPG) application, a VOD selection/billing application and the like.

[0039] In accordance with the present invention, the MISD further includes a transformation engine 220. The transformation engine 220 includes computer-readable instructions executable by the microprocessor 202 to receive the seed identity 218 as input, and to generate as output at least one unique identity 222, 224 as a function of predefined logic accessible to the transformation engine 220. The unique identity 222, 224 is a code uniquely identifying the MISD, such as a network address.

[0040] In this exemplary embodiment, the transformation engine 220 is implemented as computer software stored in the memory 216. Alternatively, the transformation engine 220 may be implemented as firmware in hardware. In one embodiment, the software program is stored and/or executed in secure code space 226 within the device, such secure code space being well known in the art. The predefined

logic may be incorporated into the transformation engine, e.g., hard-coded into the transformation engine software.

[0041] The predefined logic may include any suitable logic for generating a unique identity, e.g., unique network address, from the seed identity. By way of example, the predefined logic and seed identities are selected such that all generated identities across all devices deployed for use within a network are unique identities. By way of example, the predefined logic may require generation of a unique identity by adding an offset, e.g., 0x8000, to the seed identity. Alternatively, by way of example, the predefined logic may require generation of a unique identity by applying a predetermined bit mask or bit shift to the seed identity.

[0042] By way of further example, the predefined logic may include conditional logic requiring generation of a unique identity by a first method for a first specified addressing scheme, and by a second method for a second specified addressing scheme. For example, such conditional logic may require generation of a unique identity by adding a first offset (e.g., 0x8000) if a first addressing scheme is received as input, and a second offset (e.g., 0x4000) if a second addressing scheme is received as input. It will be appreciated that the fundamental methodologies for generating a unique identity may be entirely different for each addressing scheme (e.g., requiring applying an offset for a first addressing scheme and requiring applying a bit mask for a second addressing scheme).

[0043] In one embodiment, the transformation engine 220 is capable of receiving further input representing a desired addressing scheme with which the generated unique identity must comply. For example, this input may designate a specific addressing scheme and the transformation engine may be capable of generating a single identity in each scheme from the seed identity. In a preferred embodiment, the transformation engine 220 is configured to be capable of generating a plurality of unique identities in at least one addressing scheme from the seed identity. By way of example, the specified addressing scheme may be a conditional access scheme, such as Digicipher or Nagra Aladdin, or a more general addressing scheme, such as a MAC address.

[0044] In other embodiments of the MISD, such as a wireless telephone handset, smartphone, PDA, personal computer, etc., the MISD may further include a mouse, keyboard and/or other interface devices, such as a touch sensitive screen, digitized entry pad, etc., connected to the user interface adapter, and may further include an integral display device. It will be understood by those skilled in the art that the MISD may further include various other components, such as an operating system stored in the memory, various conventional circuitry, various I/O ports and devices, etc., which are well-known in the art. Further, although the MISD is generally depicted as a general purpose computer that is programmed to perform various control functions in accordance with the present invention, the invention can be implemented in hardware as, for example, an application specific integrated circuit (ASIC) or field programmable gate array (FPGA). As such, the process steps described herein are intended to be

broadly interpreted as being equivalently performed by software, hardware or a combination thereof.

[0045] Optionally, the ROM may be part of a secure identity card that is interchangeably connectable to a network device via a suitable physical interface, such as a conventional I/O port. By way of example, a discrete secure identity card may be one of a CableCARD, a PCMCIA card, a SIM card and a Smart Card. In such an embodiment, the MISD includes a data communication physical interface port capable of interchangeably receiving the cards. In a preferred embodiment, the ROM is an integral part of the MISD and is not configured to be interchangeable. It will be appreciated that the secure identity card may be manufactured to include the seed identity apart from any manufacture of the MISD, or alternatively, may be manufactured to include the seed identity as part of the MISD device itself. Further, it will be appreciated that the device may be provided with the transformation engine and predefined logic during manufacture of the device, or after manufacture and deployment of the device within a network. The device and/or secure identity cards may be distributed to end users/consumers and deployed within a network in any suitable manner.

[0046] In the context of Figure 1, the MISDs could be deployed as STBs connected via an information network to, in this example, a head-end of a cable television network. Each of the MISDs is configured to receive data transmissions via the network. The head-end includes, as is conventional, a plurality of content sources

and prepares digital data transmissions directed to specific receiving devices, e.g. STBs. The digital data transmissions are directed to a specific receiving device in that it is prepared include recipient identity data corresponding to the intended recipient device's unique identity, e.g., network address of a specific receiving device. Methods and systems for addressing digital data transmissions intended for specific receiving devices are well-known in the art.

[0047] Figure 3 is a flow diagram illustrating an exemplary method 250 for supporting multiple identities for a secure identity device. Referring now to Figure 3, the method involves preparing an MISD, which includes storing a seed identity in a secure memory, such as ROM, of an MISD, as shown at step 252 of Figure 3. For example, this may involve manufacture of an STB, a wireless telephone, a PDA, a computer, etc. in a substantially conventional manner, but to include the seed identity. Alternatively, this may involve manufacture of a secure identity card in a substantially conventional manner, but to include a seed identity, and later operatively installing the secure identity card in a physical interface of the MISD.

[0048] The method further includes providing a transformation engine in the MISD, as shown at step 254. For example, this may be performed during manufacture of the device by storing a computer program in the non-volatile storage memory of the device. Alternatively, this may be performed post-manufacture by copying software to the device, or by post-installation downloading of software to the device via a network.

[0049] After the MISD has been provided, the transformation engine is run, e.g. the software is executed, to generate a unique device identity as a function of the stored seed identity, as shown at step 256. By way of example, this may be performed responsive to power-up of the MISD, responsive to connection of the MISD to a network, responsive to receipt of a command via a keypad, etc. of the MISD, responsive to receipt of a command via the network, or responsive to receipt of a data transmission via the network, as part of a verification process to ensure that the data transmission is intended for the device, etc.

[0050] In this exemplary embodiment, the generated device identity is stored in secure memory of the device, e.g., in RAM, for subsequent use, as shown at step 258. In an alternative embodiment, the generated identity may not be stored for subsequent retrieval, but rather may be generated for immediate use and then deleted.

[0051] In this exemplary embodiment, it is next determined if another identity is required. If not, then the method ends, as shown at steps 260 and 262. If so, the transformation engine 220 may be rerun to generate a unique identity, as shown at steps 260 and 256. It should be noted that in certain instances, that engine may be run and rerun to repeatedly generate a certain single unique identity, e.g. upon receipt of each transmission, for verification purposes. Alternatively, the engine may be rerun to generate multiple different identities, which may be used concurrently, or successively. Alternatively, the engine may be rerun to generate a new identity in response to a command via the network, e.g. to implement a new identity-generation logic, to create a

new identity in the event of discontinuance of service, to create a new identity in the event of changes in the network, to create a new identity in the event of unauthorized access, for example.

[0052] Figure 4 is a flow diagram of an exemplary method 270 for processing data using an MISD in accordance with the present invention. Referring now to Figure 4, the method begins with deploying an MISD for use in the network, as shown at step 272 in Figure 4. For example, this may involve distributing the MISD, connecting the MISD to the network, configuring the MISD for use in the network, etc.

[0053] Next, the method involves preparing a data transmission for secure delivery to a specific network device having a specific identity, as shown at step 274 in Figure 4. Exemplary data transmissions include transmissions of voice, video and/or data content. Methods and technology for doing so are well-known in the art and therefore not described in detail herein. Next, the method involves transmitting data to one or more network devices via an information network, as shown at step 276. For example, this may be performed by the head-end in a subscriber television network, or by a wireless voice/data carrier in a wireless voice/data network, or by a digital content provider in a digital information network. It should be noted that a data transmission can be addressed to a particular MISD when the MISD's seed identity and the transformation logic are known to the head-end, etc. of the network, because the MISD's unique ID will be/has been generated in a predictable manner known to the head-end, etc.

[0054] Next, the MISD receives the transmitted data, as shown at step 278. Further, the MISD extracts recipient identity data from the transmitted data, as shown at step 280. This may be performed by application software stored in the memory 216 of the MISD 200 and executable by the microprocessor 202. Examples of such application software are well-known in the art.

[0055] In certain embodiments, the application software examines the recipient identity data and determines which of several known addressing schemes are being used to direct the data transmission to the recipient. In such embodiments, the application software provides an indication of the application addressing scheme as input to the transformation engine, and the transformation engine generates a unique identity compliant with the identified addressing scheme.

[0056] The MISD then obtains a generated identity, generated by the transformation engine from the seed identity, as shown at step 282. In one embodiment, this involves referencing a secure storage area 216 of the MISD and retrieving an identity 222 previously-generated by the transformation engine 220. In a preferred embodiment, this involves causing the transformation engine 220 to run to generate a unique identity in response to receipt of a data transmission at the MISD.

[0057] In embodiments in which the MISD determines the addressing scheme used by the data transmission, the MISD retrieves an identity conforming to

that addressing scheme from the memory of the MISD, or alternatively, provides the identity of that addressing scheme as an input to the transformation engine for use to generate an identity compliant with that addressing scheme.

[0058] The MISD then compares the generated identity to the recipient identity data to determine whether they correspond. For example, correspondence may be found when there is an exact match of all or a portion of the recipient identity data to the generated unique identity, as known in the art. In this manner, each MISD may determine whether the received data transmission is intended for that particular MISD, as shown at steps 282 and 284. This may be performed by the application software, as is conventional in secure identity systems.

[0059] If it is determined at step 286 that the generated identity does not correspond to the recipient identity data specified by the data transmission, then the received data transmission was not intended for use by that particular MISD, and the received data transmission is discarded, e.g., deleted or ignored, and the method ends, as shown at steps 288 and 290.

[0060] If it is determined at step 286 that the generated identity does correspond to the recipient identity data specified by the data transmission, then the received data transmission was intended for use by that particular MISD, and the MISD processes the received data transmission in a conventional manner and the method ends, as shown at steps 290 and 292. For example, such processing may include

displaying the data transmission or related content via a display device, such as a television, CRT, LCD or other display screen associated with the MISD.

[0061] The invention may be implemented by a computer program product wherein computer instructions, when processed by a computer, adapt the operation of the computer such that the methods and/or techniques of the present invention are invoked or otherwise provided. Instructions for invoking the inventive methods may be stored in fixed or removable media, transmitted via a data stream in a broadcast media or other signal bearing medium, and/or stored within a working memory within a computing device operating according to the instructions. Thus, the present invention also provides computer readable media storing computer readable code for carrying out the method steps identified above. The computer readable media stores code for carrying out subprocesses for carrying out the methods described above.

[0062] While there have been described herein the principles of the invention, it is to be understood by those skilled in the art that this description is made only by way of example. The scope of the claims should not be limited by the preferred embodiments set forth in the examples, but should be given the broadest interpretation consistent with the description as a whole.

CLAIMS:

1. A method comprising:

receiving, by a secure identity device, a data transmission comprising recipient identity data;

determining an addressing scheme used to direct the data transmission;

retrieving a seed identity from a secure memory;

generating, by the secure identity device, a unique identity based on the seed identity and the determined addressing scheme;

extracting the recipient identity data from the received data transmission; and

determining whether the generated unique identity corresponds to the recipient identity data.

2. The method of claim 1 further comprising:

if the generated unique identity does not correspond to the recipient identity data, discarding the data transmission; and

if the generated unique identity corresponds to the recipient identity data, using data from the data transmission.

3. The method of claim 1 or 2 wherein generating the unique identity comprises generating the unique identity in compliance with the determined addressing scheme.

4. The method of any one of claims 1-3, further comprising:

storing the unique identity in non-volatile storage memory;

receiving a second data transmission directed using the addressing scheme; and

retrieving, from the non-volatile storage memory, the stored unique identity based on a determination that the stored unique identity is compliant with the addressing scheme.

5. The method of any one of claims 1-4, wherein generating the unique identity is performed based on receiving the data transmission.

6. The method of any one of claims 1-5, further comprising:

providing, to a transformation engine, information identifying the addressing scheme, wherein generating the unique identity comprises generating the unique identity in compliance with the addressing scheme.

7. The method of claim 4, further comprising:

storing the unique identity in a secure area of the non-volatile storage memory.

8. The method of claim 7, wherein the non-volatile storage memory stores a plurality of unique identities, and wherein the plurality of unique identities includes the unique identity.

9. The method of any one of claims 1-8, wherein the unique identity comprises a network address.

10. The method of any one of claims 1-9, wherein generating the unique identity comprises applying a predefined bit mask to the seed identity.

11. The method of any one of claims 1-9, wherein generating the unique identity comprises adding a predefined offset to the seed identity.

12. The method of any one of claims 1-9, wherein generating the unique identity comprises generating the unique identity by a first method if a first condition exists and generating the unique identity by a second method if a second condition exists.

13. The method of any one of claims 1-12, wherein the unique identity comprises a first unique identity, the method further comprising:

generating, by the secure identity device, a second unique identity based on the seed identity, wherein the second unique identity is different from the first unique identity.

14. The method of any one of claims 1-13, wherein the secure memory comprises a first secure memory, the method further comprising:

storing the unique identity in a second secure memory of the secure identity device, wherein the second secure memory is different from the first secure memory.

15. The method of any one of claims 1-13, further comprising:

storing the seed identity in a secure identity card having the secure memory; and

receiving the secure identity card in a physical interface of the secure identity device.

16. A device comprising:

one or more processors; and

memory storing computer-readable instructions that, when executed by the one or more processors, cause the device to:

receive a data transmission comprising recipient identity data;

determine an addressing scheme used to direct the data transmission;

retrieve a seed identity comprising an identification code;

generate a unique identity based on the seed identity and the determined addressing scheme;

extract the recipient identity data from the received data transmission; and

determine whether the generated unique identity corresponds to the recipient identity data.

17. The device of claim 16, wherein the instructions, when executed by the one or more processors, further cause the device to:

if the recipient identity data does not correspond to the generated unique identity, discard the data transmission; and

if the recipient identity data corresponds to the generated unique identity, use data from the data transmission.

18. The device of claim 16 or 17 wherein the instructions, when executed by the one or more processors, cause the device to generate the unique identity in compliance with the determined addressing scheme.

19. The device of any one of claims 16-18, wherein the instructions, when executed by the one or more processors, further cause the device to:

store the unique identity in a non-volatile storage memory;

receive a second data transmission directed using the addressing scheme; and

retrieve, from the non-volatile storage memory, the stored unique identity based on a determination that the stored unique identity is compliant with the addressing scheme.

20. The device of any one of claims 16-19, wherein the instructions, when executed by the one or more processors, cause the device to generate the unique identity based on receipt of the data transmission.

21. The device of any one of claims 16-20, wherein the instructions, when executed by the one or more processors, further cause the device to:

provide, to a transformation engine, information identifying the addressing scheme, wherein generating the unique identity comprises generating the unique identity in compliance with the addressing scheme.

22. The device of claim 19, wherein the instructions, when executed by the one or more processors, further cause the device to:

store the unique identity in a secure area of the non-volatile storage memory.

23. The device of claim 22, wherein the non-volatile storage memory stores a plurality of unique identities, and wherein the plurality of unique identities includes the unique identity.

24. The device of any one of claims 16-23, wherein the unique identity comprises a network address.

25. The device of any one of claims 16-24, wherein the instructions, when executed by the one or more processors, cause the device to generate the unique identity through application of a predefined bit mask to the seed identity.

26. The device of any one of claims 16-24, wherein the instructions, when executed by the one or more processors, cause the device to generate the unique identity through addition of a predefined offset to the seed identity.

27. The device of any one of claims 16-24, wherein the instructions, when executed by the one or more processors, cause the device to generate the unique identity by a first method if a first condition exists and generate the unique identity by a second method if a second condition exists.

28. The device of any one of claims 16-27, further comprising:

a first secure memory configured to store the seed identity; and

a second secure memory configured to store the unique identity of the secure identity device, wherein the second secure memory is different from the first secure memory.

29. The device of any one of claims 16-27, further comprising:

a secure identity card comprises a secure memory configured to store the seed identity, wherein the secure identity device comprises a physical interface configured to receive the secure identity card.

30. The device of any one of claims 16-27, wherein the memory comprises:

a read-only memory (ROM) operatively connected to the one or more processors and configured to securely store the seed identity.

31. The device of any one of claims 16-27, further comprising:

a data communication port configured to receive a secure identity card, wherein the secure identity card is configured to store the seed identity.

32. The device of claim 31, wherein the secure identity card comprises one of a CableCARD, a PCMCIA card, a SIM card, or a Smart Card.

33. The device of claim 30 wherein the ROM comprises one of a programmable read only memory (PROM) and a one-time-programmable (OTP) memory.

34. One or more non-transitory computer-readable media storing computer- readable instructions that, when executed by a processor, cause the processor to:

receive a data transmission comprising recipient identity data;

determine an addressing scheme used to direct the data transmission;

retrieve a seed identity comprising an identification code;

generate a unique identity based on the seed identity and the determined addressing scheme;

extract the recipient identity data from the received data transmission; and

determine whether the generated unique identity corresponds to the recipient identity data.

35. The one or more non-transitory computer-readable media storing computer-readable instructions of claim 34 that, when executed by the processor, further cause the processor to:

if the generated unique identity does not correspond to the recipient identity data, discard the data transmission; and

if the generated unique identity corresponds to the recipient identity data, use data from the data transmission.

36. The one or more non-transitory computer-readable media storing computer-readable instructions of claim 34 or 35 that, when executed by the processor, cause the

processor to generate the unique identity in compliance with the determined addressing scheme.

37. The one or more non-transitory computer-readable media storing computer-readable instructions of any one of claims 34-36 that, when executed by the processor, further cause the processor to:

store the unique identity in non-volatile storage memory;

receive a second data transmission directed using the addressing scheme; and

retrieve, from the non-volatile storage memory, the stored unique identity based on a determination that the stored unique identity is compliant with the addressing scheme.

38. The one or more non-transitory computer-readable media storing computer-readable instructions of any one of claims 34-37 that, when executed by the processor, cause the processor to generate the unique identity based on receipt of the data transmission.

39. The one or more non-transitory computer-readable media storing computer-readable instructions of any one of claims 34-38 that, when executed by the processor, further cause the processor to:

provide, to a transformation engine, information identifying the addressing scheme, and generate the unique identity in compliance with the addressing scheme.

40. The one or more non-transitory computer-readable media storing computer-readable instructions of claim 37 that, when executed by the processor, further cause the processor to:

store the unique identity in a secure area of the non-volatile storage memory.

41. The one or more non-transitory computer-readable media storing computer-readable instructions of claim 40, wherein the non-volatile storage memory stores a

plurality of unique identities, and wherein the plurality of unique identities comprises the unique identity.

42. The one or more non-transitory computer-readable media storing computer-readable instructions of any one of claims 34-41, wherein the unique identity comprises a network address.

43. The one or more non-transitory computer-readable media storing computer-readable instructions of any one of claims 34-42 that, when executed by the processor, cause the processor to generate the unique identity through application of a predefined bit mask to the seed identity.

44. The one or more non-transitory computer-readable media storing computer-readable instruction of any one of claims 34-42 that, when executed by the processor, cause the processor to generate the unique identity through addition of a predefined offset to the seed identity.

45. The one or more non-transitory computer-readable media storing computer-readable instructions of any one of claims 34-42 that, when executed by the processor, cause the processor to generate the unique identity by a first method if a first condition exists and generate the unique identity by a second method if a second condition exists.

46. The one or more non-transitory computer-readable media storing computer-readable instructions of any one of claims 34-45, wherein the unique identity comprises a first unique identity, and the computer-readable instructions, when executed by the processor, further cause the processor to:

generate, by the secure identity device, a second unique identity based on the seed identity, wherein the second unique identity is different from the first unique identity.

47. The one or more non-transitory computer-readable media storing computer-readable instructions of any one of claims 34-46, wherein the secure memory comprises a first secure memory, and the computer-readable instructions when executed by the processor, further cause the processor to:

store the unique identity in a second secure memory of the secure identity device, wherein the second secure memory is different from the first secure memory.

48. A system comprising:

an apparatus comprising:

one or more processors; and

memory storing instructions that, when executed by the one or more processors, cause the apparatus to perform the method of any one of claims 1-14;

a secure identity card comprising:

one or more processors; and

memory storing instructions that, when executed by the one or more processors of the at least one interface, cause the secure identity card to store the unique identity.

49. A method comprising:

receiving, by a secure device, identity data;

obtaining, from a secure memory area of the secure device, a unique identity for the secure device, wherein the unique identity is based on a seed identity stored in the secure device, predefined logic stored in the secure device, and an addressing scheme used to direct the identity data;

determining, by the secure device, whether the unique identity corresponds to the identity data;

if the unique identity does not correspond to the identity data, discarding the identity data; and

if the unique identity corresponds to the identity data, using data from the identity data.

50. The method of claim 49, wherein obtaining the unique identity comprises:

based on receiving the identity data, generating, by a transformation engine of the secure device, the unique identity based on the seed identity, the predefined logic, and the addressing scheme.

51. The method of claim 49 or 50, wherein:

obtaining the unique identity comprises:

determining, by the secure device and based on the identity data, the addressing scheme used to direct the identity data; and

receiving, by the transformation engine of the secure device, the determined addressing scheme; and

generating the unique identity comprises generating the unique identity in compliance with the determined addressing scheme.

52. The method of any one of claims 49-51, further comprising:

generating a first unique identity and a second unique identity based on the seed identity and the predefined logic, the first unique identity being compliant with a first addressing scheme and the second unique identity being compliant with a second addressing scheme different from the first addressing scheme, wherein obtaining the unique identity comprises:

determining, by the secure device, the addressing scheme used to direct the identity data; and

based on determining the addressing scheme, selecting, as the unique identity for the secure device, one of the first unique identity and the second unique identity that is compliant with the addressing scheme.

53. One or more non-transitory computer-readable media storing computer- readable instructions that, when executed by a processor, cause the processor to perform the method of any one of claims 49-52.

54. An apparatus comprising:

one or more processors; and

memory storing instructions that, when executed by the one or more processors, cause the apparatus to perform the method of any one of claims 49-52.

55. A system comprising:

an apparatus comprising:

one or more processors; and

memory storing instructions that, when executed by the one or more processors, cause the apparatus to perform the method of any one of claims 49-52;

a secure identity card comprising:

one or more processors; and

memory storing instructions that, when executed by the one or more processors of the at least one interface, cause the secure identity card to store the first unique identity.

56. A system comprising:

a first device comprising:

a first microprocessor;

first predefined logic; and

first memory storing computer-readable instructions that, when executed by the first microprocessor, cause the first device to:

receive a data transmission comprising recipient identity data;

determine an addressing scheme used to direct the data transmission;

retrieve a first seed identity comprising an identification code;

generate a unique identity based on the first seed identity and the determined addressing scheme;

extract the recipient identity data from the received data transmission; and

determine whether the generated unique identity corresponds to the recipient identity data; and

a second device comprising:

a second microprocessor;

second predefined logic; and

second memory storing computer-readable instructions that, when executed by the second microprocessor, cause the second device to:

store a second seed identity, wherein the second seed identity is different from the first seed identity, and wherein the second predefined logic is the same as the first predefined logic.

57. A method comprising:

receiving a data transmission at a first device comprising recipient identity data;

determining an addressing scheme used to direct the data transmission;

retrieving a first seed identity comprising an identification code;

generating a unique identity based on the first seed identity and the determined addressing scheme;

extracting the recipient identity data from the received data transmission; and

determining whether the generated unique identity corresponds to the recipient identity data; and

storing at a second device a second seed identity and second predefined logic, wherein the second seed identity is different from the first seed identity, and wherein the second predefined logic is the same as the first predefined logic.

58. A system comprising:

a first device comprising:

a first microprocessor;

first predefined logic; and

first memory storing computer-readable instructions that, when executed by the first microprocessor, cause the first device to:

receive a data transmission comprising recipient identity data;

determine an addressing scheme used to direct the data transmission;

retrieve a first seed identity comprising an identification code;

generate a unique identity based on the first seed identity and the determined addressing scheme;

extract the recipient identity data from the received data transmission; and

determine whether the generated unique identity corresponds to the recipient identity data; and

a second device comprising:

a second microprocessor;

second predefined logic; and

second memory storing computer-readable instructions that, when executed by the second microprocessor, cause the second device to:

store a second seed identity, wherein the second seed identity is the same as the first seed identity, and wherein the second predefined logic is different from the first predefined logic.

59. A *method comprising*:

receiving at a first device a data transmission comprising recipient identity data;

determining an addressing scheme used to direct the data transmission;

retrieving a first seed identity comprising an identification code;

generating a unique identity based on the first seed identity and the determined addressing scheme;

extracting the recipient identity data from the received data transmission; and

determining whether the generated unique identity corresponds to the recipient identity data; and

storing at a second device second seed identity and a second predefined logic, wherein the second seed identity is the same as the first seed identity, and wherein the second predefined logic is different from the first predefined logic.

60. A method comprising:

determining, by a device, an addressing scheme used to direct a data transmission to the device, wherein the data transmission comprises a recipient identifier;

based on the determined addressing scheme, obtaining a unique identity, wherein the unique identity is based on a seed identity of the device;

comparing the recipient identifier with the unique identity; and

determining whether to keep or to discard the data transmission based on the comparing.

61. The method of claim 60, wherein determining whether to keep or to discard the data transmission based on the comparing comprises:

based on comparing the recipient identifier with the unique identity, discarding the data transmission if the recipient identifier does not correspond to the unique identity.

62. The method of claim 60, wherein determining whether to keep or to discard the data transmission based on the comparing comprises:

based on comparing the recipient identifier with the unique identity, keeping the data transmission if the recipient identifier corresponds to the unique identity.

63. The method of any one of claims 60-62, further comprising:

prior to obtaining the unique identity, generating a plurality of unique identities using the seed identity of the device, wherein:

the unique identity is one of the plurality of unique identities,

each of the plurality of unique identities corresponds to a different addressing scheme, and

the unique identity corresponds to the determined addressing scheme.

64. The method of claim 63, further comprising:

storing the plurality of unique identities at a memory location of the device, wherein obtaining the unique identity comprises retrieving the unique identity from the memory location of the device.

65. The method of any one of claims 63-64, further comprising:

determining a second addressing scheme used to direct a second data transmission to the device; and

based on the determined second addressing scheme, retrieving a second unique identity from the plurality of unique identities.

66. The method of any one of claims 60-65, wherein obtaining the unique identity comprises generating the unique identity based on the seed identity of the device and the determined addressing scheme.

67. The method of claim 66, further comprising:

after comparing the recipient identifier with the unique identity, discarding the generated unique identity.

68. The method of any one of claims 60-67, wherein the device comprises a set top box.

69. The method of any one of claims 60-68, wherein the seed identity comprises a network address, a serial number, an alphanumeric string, or a media access control address.

70. The method of any one of claims 60-69, further comprising:

storing the seed identity at a first memory location of the device; and

storing the unique identity at a second memory location of the device different from the first memory location.

71. A method comprising:

generating, using a seed identity of a device, a plurality of unique identities, wherein each unique identity of the plurality of unique identities corresponds to a different addressing scheme;

storing, by the device, the plurality of unique identities;

determining a first addressing scheme used to direct a data transmission to the device; and

retrieving a first unique identity of the plurality of unique identities that corresponds to the determined first addressing scheme used to direct the data transmission to the device.

72. The method of claim 71, wherein the data transmission comprises a recipient identifier, the method further comprising:

determining whether the first unique identity corresponds to the recipient identifier.

73. The method of claim 72, further comprising:

if the first unique identity corresponds to the recipient identifier, keeping the data transmission; and

if the first unique identity does not correspond to the recipient identifier, discarding the data transmission.

74. The method of any one of claims 71-73, wherein the plurality of unique identities comprises the first unique identity and a second unique identity, and wherein generating the plurality of unique identities comprises:

using a first predefined logic and the first addressing scheme to generate the first unique identity; and

using a second predefined logic and a second addressing scheme to generate the second unique identity, wherein the first addressing scheme is different from the second addressing scheme.

75. A method comprising:

storing a first unique identity, wherein the first unique identity is based on a seed identity of a device, and wherein the first unique identity corresponds to a first addressing scheme;

receiving a data transmission at the device; and

after a determination that a second addressing scheme used to direct the data transmission is different from the first addressing scheme, generating a second unique identity based on the seed identity and the second addressing scheme.

76. The method of claim 75, further comprising:

storing the second unique identity with the first unique identity.

77. The method of claim 75 or 76, wherein the data transmission comprises a recipient identifier, the method further comprising:

extracting the recipient identifier from the data transmission; and

determining whether the recipient identifier corresponds to the second unique identity.

78. The method of claim 77, further comprising:

if the recipient identifier corresponds to the second unique identity, using data from the data transmission; and

if the recipient identifier does not correspond to the second unique identity, discarding the data transmission.

79. The method of any one of claims 75-78, further comprising:

receiving a second data transmission at the device, wherein the second data transmission comprises a recipient identifier; and

after a determination that the first addressing scheme is used to direct the second data transmission to the device, retrieving the first unique identity for comparison with the recipient identifier.

80. A system comprising:

an apparatus comprising:

one or more processors; and

memory storing instructions that, when executed by the one or more processors, cause the apparatus to perform the method of any one of claims 60-70;
a secure identity card comprising:

one or more processors; and

memory storing instructions that, when executed by the one or more processors of the at least one interface, cause the secure identity card to store the unique identity.

81. An apparatus comprising:

one or more processors; and

memory storing instructions that, when executed by the one or more processors, cause the apparatus to perform the method of any one of claims 60-70.

82. A system comprising:

an apparatus comprising:

one or more processors; and

memory storing instructions that, when executed by the one or more processors, cause the apparatus to perform the method of any one of claims 71-74;
a secure identity card comprising:

one or more processors; and

memory storing instructions that, when executed by the one or more processors of the at least one interface, cause the secure identity card to store the first unique identity.

83. An apparatus comprising:

one or more processors; and

memory storing instructions that, when executed by the one or more processors, cause the apparatus to perform the method of any one of claims 71-74.

84. A system comprising:

an apparatus comprising:

one or more processors; and

memory storing instructions that, when executed by the one or more processors, cause the apparatus to perform the method of any one of claims 75-79;

a secure identity card comprising:

one or more processors; and

memory storing instructions that, when executed by the one or more processors of the at least one interface, cause the secure identity card to store the first unique identity.

85. An apparatus comprising:

one or more processors; and

memory storing instructions that, when executed by the one or more processors, cause the apparatus to perform the method of any one of claims 75-79.

86. A method comprising:

receiving, from a server and by a computing device storing a first identifier that identifies the computing device, a data transmission;

extracting, by the computing device and from the data transmission, a second identifier;

determining, by the computing device, an addressing scheme used by the server to direct the data transmission to the computing device;

generating, by the computing device and using the first identifier, an address of the computing device, the address being compliant with the addressing scheme;

comparing, by the computing device, the address to the second identifier; and

either processing, by the computing device, the data transmission after determining that the address corresponds to the second identifier or discarding, by the computing device, the data transmission after determining that the second identifier does not correspond to the address.

87. The method of claim 86, wherein the address is a first address and the addressing scheme is a first addressing scheme, the method further comprising:

generating, by the computing device and using the first identifier, a plurality of unique addresses of the computing device, wherein:

the first address is one of the plurality of unique addresses,

each of the plurality of unique addresses is compliant with a different addressing scheme, and

the first address is compliant with the first addressing scheme.

88. The method of claim 86 or 87, further comprising:

determining, by the computing device, a second addressing scheme used to direct a second data transmission to the computing device; and

retrieving, by the computing device and from among the plurality of unique addresses, a second address that is compliant with the second addressing scheme.

89. The method of any one of claims 86-88, wherein the computing device comprises a set top box.

90. The method of any one of claims 86-89, wherein the first identifier comprises a network address, a serial number, an alphanumeric string, or a media access control address.

91. The method of any one of claims 86-90, further comprising:

storing, by the computing device, the first identifier at a first memory location of the computing device; and

storing, by the computing device, the address at a second memory location of the computing device different from the first memory location.

92. The method of any one of claims 86-91, wherein the computing device uses the second identifier extracted from the data transmission to determine the addressing scheme.

93. The method of any one of claims 86-92, wherein the computing device generates the address after receiving the data transmission.

94. The method of any one of claims 86-93, further comprising:

extracting, by the computing device and from the second data transmission, a third identifier; and

processing, by the computing device, the second data transmission after determining that the third identifier corresponds to the second address.

95. The method of any one of claims 86-94, wherein generating the address by the computing device comprises either:

applying a bit mask to the first identifier after determining that the addressing scheme is a first addressing scheme; or

applying an offset to the first identifier after determining that the addressing scheme is a second addressing scheme different from the first addressing scheme.

96. An apparatus comprising:

one or more processors; and

memory storing instructions that, when executed by the one or more processors, cause the apparatus to perform the method of any one of claims 86-95.

97. A system comprising:

a server comprising:

one or more processors; and

memory storing instructions that, when executed by the one or more processors, cause the server to send the data transmission; and

a computing device configured to receive the data transmission, and the computing device comprising:

one or more processors; and

memory storing instructions that, when executed by the one or more processors, cause the computing device to perform the method of any one of claims 86-95.

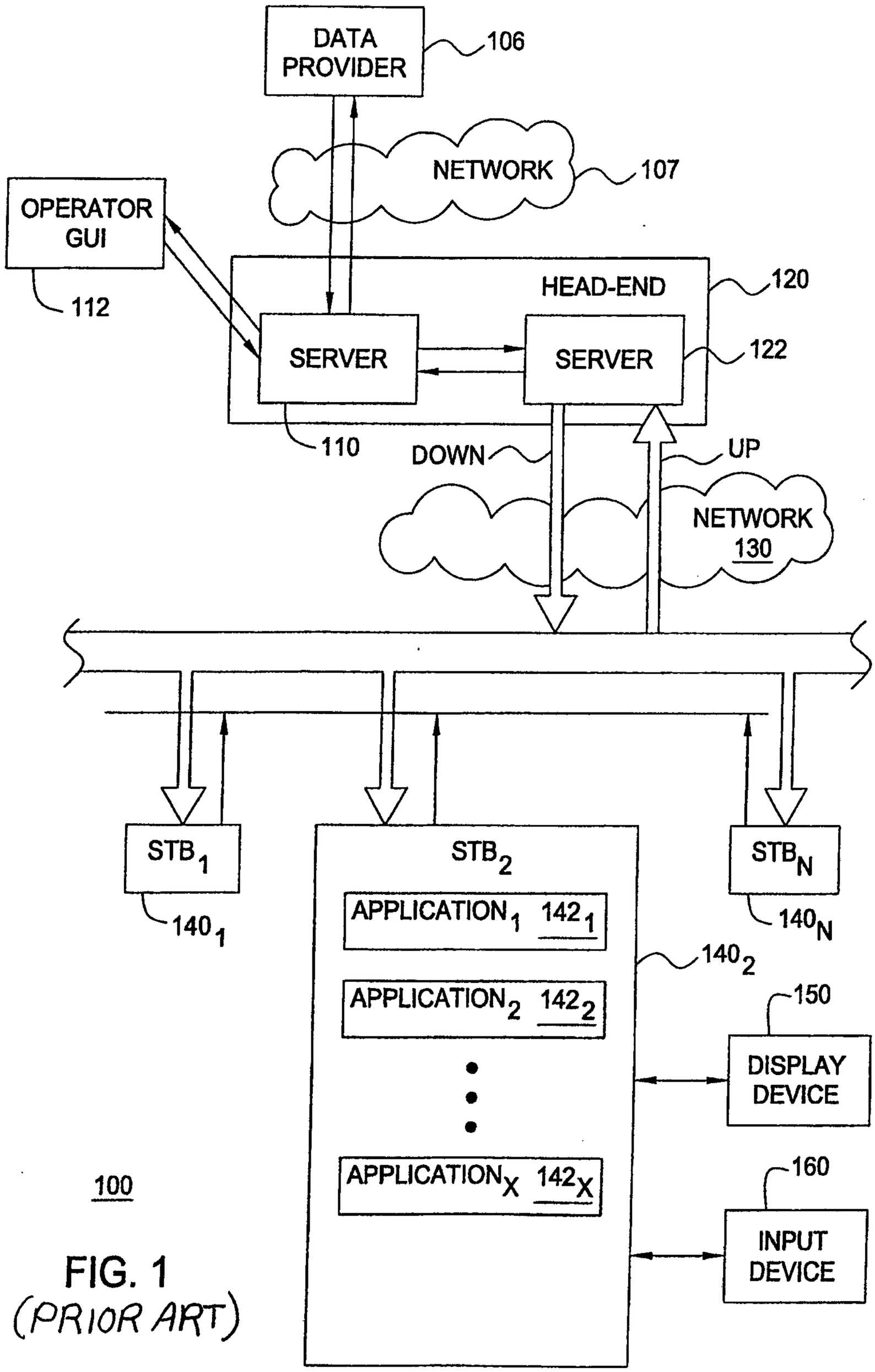


FIG. 1
(PRIOR ART)

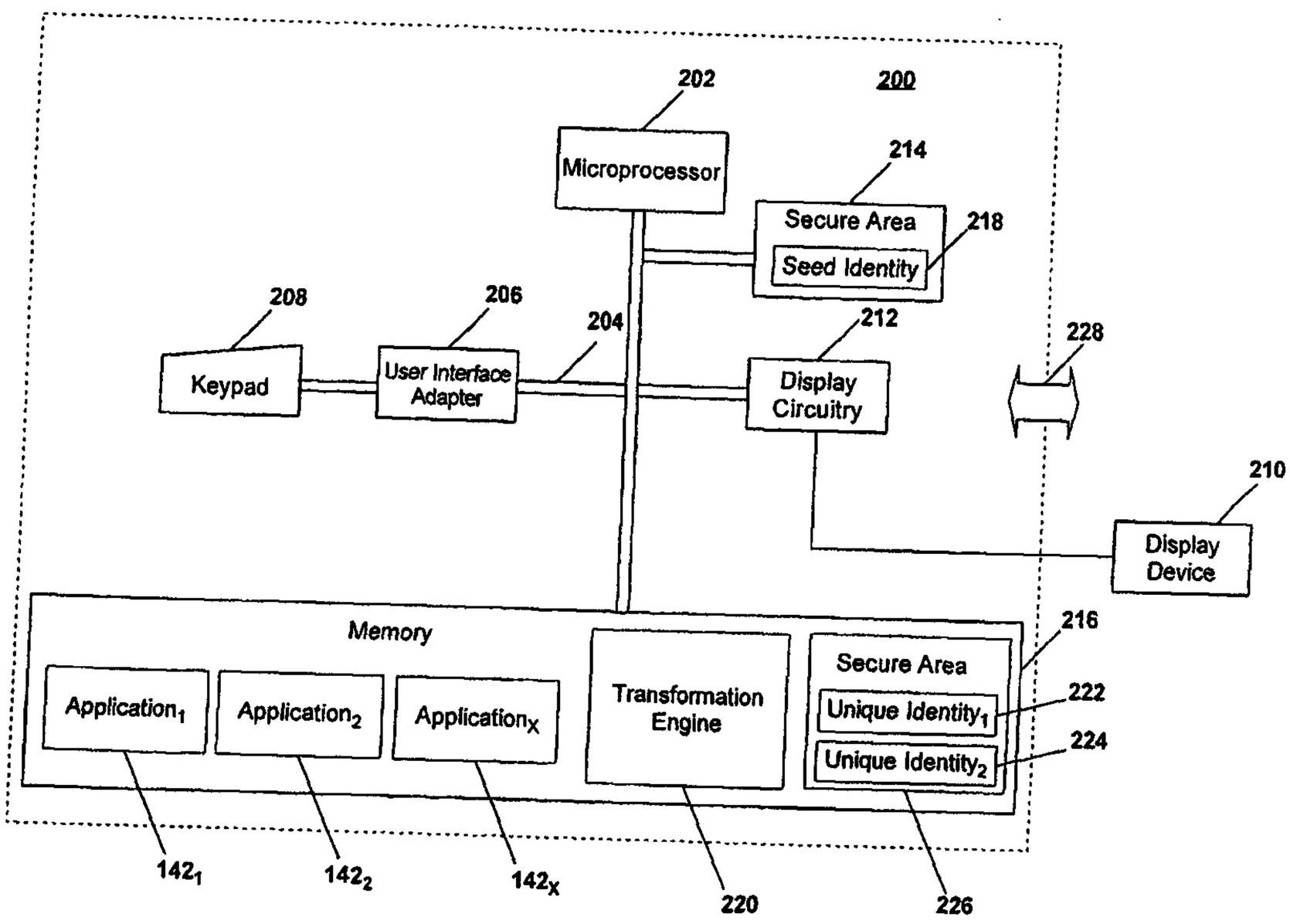

202
200
Microprocessor
214
Secure Area
218
Seed Identity
208
206
204
212
228
Keypad
User Interface Adapter
Display Circuitry
210
Display Device
Memory
216
Application1
Application2
ApplicationX
Transformation Engine
Secure Area
222
Unique Identity1
224
Unique Identity2
142₁
142₂
142X
220
226

Figure 2

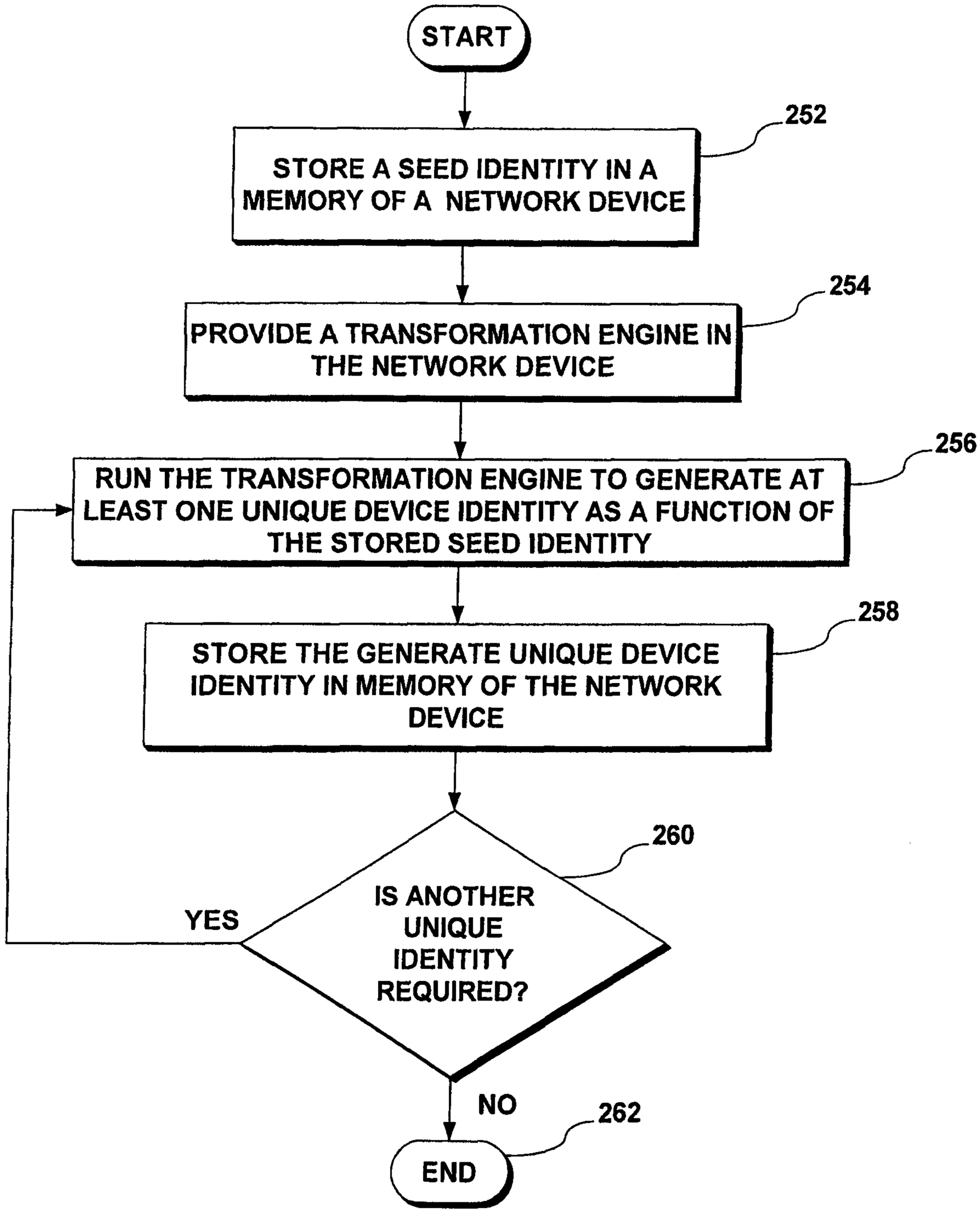

250
START
252
STORE A SEED IDENTITY IN A MEMORY OF A NETWORK DEVICE
254
PROVIDE A TRANSFORMATION ENGINE IN THE NETWORK DEVICE
256
RUN THE TRANSFORMATION ENGINE TO GENERATE AT LEAST ONE UNIQUE DEVICE IDENTITY AS A FUNCTION OF THE STORED SEED IDENTITY
258
STORE THE GENERATE UNIQUE DEVICE IDENTITY IN MEMORY OF THE NETWORK DEVICE
260
IS ANOTHER UNIQUE IDENTITY REQUIRED?
YES
NO
262
END

Figure 3

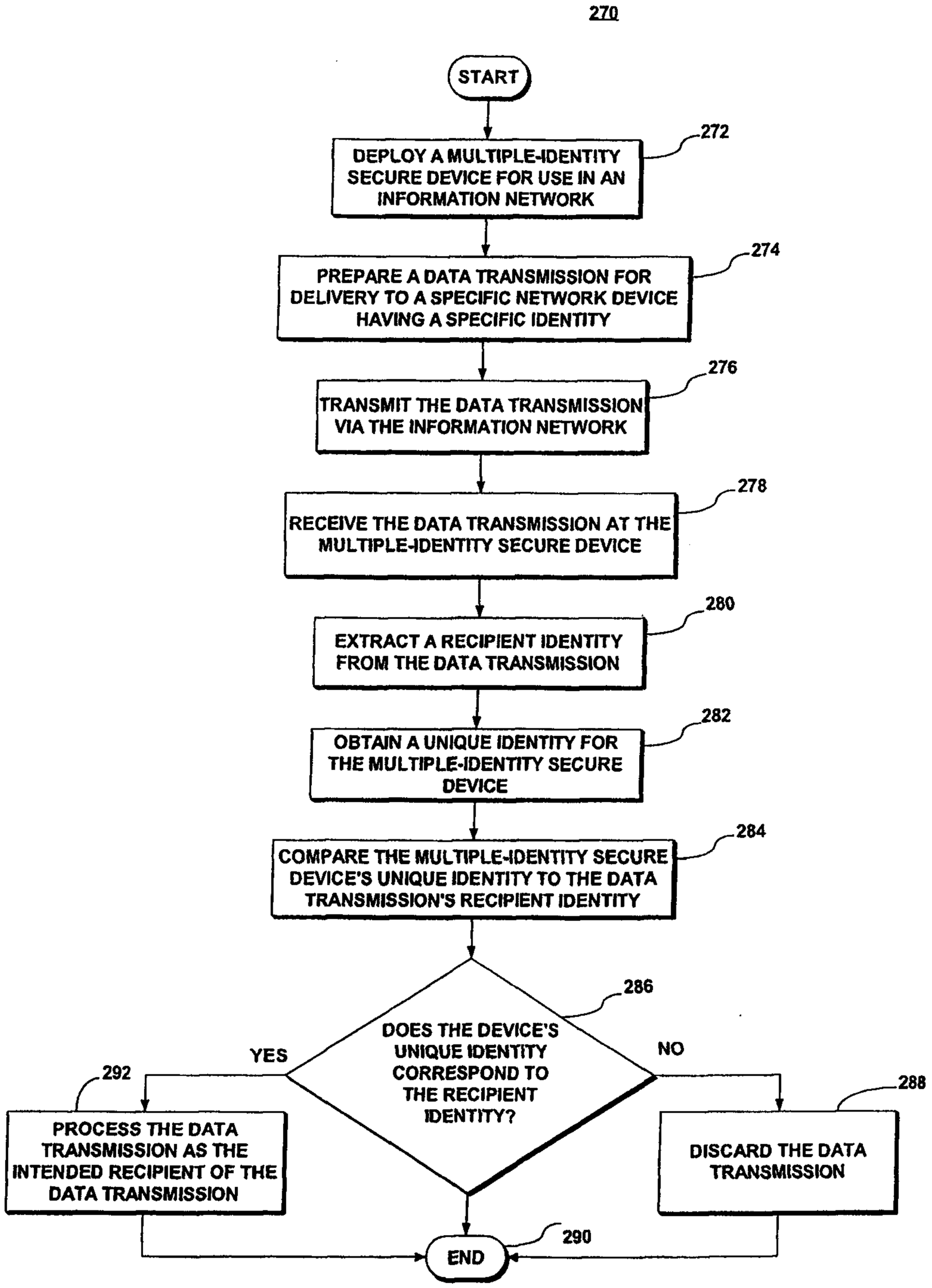
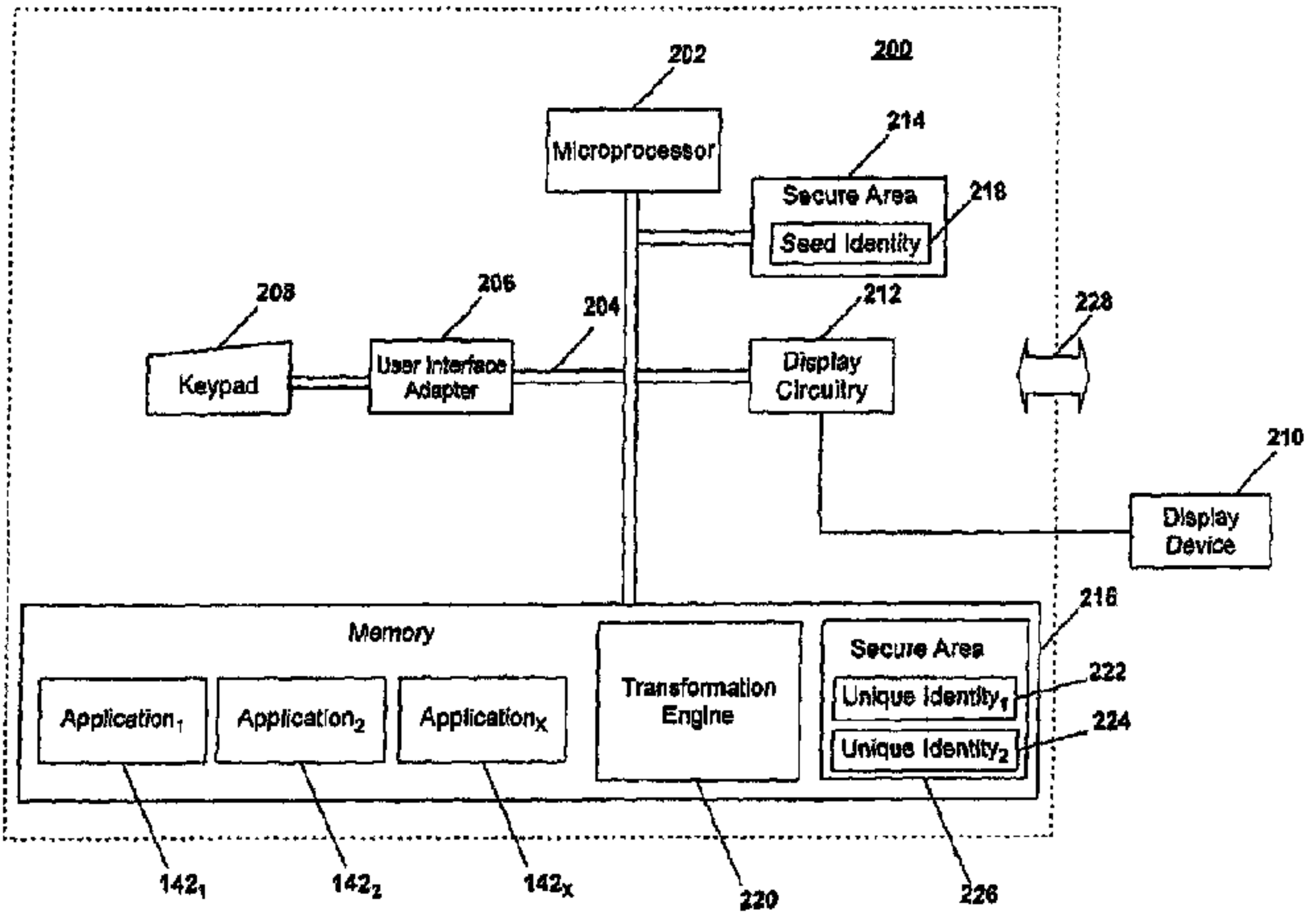

270
START
272
DEPLOY A MULTIPLE-IDENTITY SECURE DEVICE FOR USE IN AN INFORMATION NETWORK
274
PREPARE A DATA TRANSMISSION FOR DELIVERY TO A SPECIFIC NETWORK DEVICE HAVING A SPECIFIC IDENTITY
276
TRANSMIT THE DATA TRANSMISSION VIA THE INFORMATION NETWORK
278
RECEIVE THE DATA TRANSMISSION AT THE MULTIPLE-IDENTITY SECURE DEVICE
280
EXTRACT A RECIPIENT IDENTITY FROM THE DATA TRANSMISSION
282
OBTAIN A UNIQUE IDENTITY FOR THE MULTIPLE-IDENTITY SECURE DEVICE
284
COMPARE THE MULTIPLE-IDENTITY SECURE DEVICE'S UNIQUE IDENTITY TO THE DATA TRANSMISSION'S RECIPIENT IDENTITY
286
DOES THE DEVICE'S UNIQUE IDENTITY CORRESPOND TO THE RECIPIENT IDENTITY?
YES
NO
292
PROCESS THE DATA TRANSMISSION AS THE INTENDED RECIPIENT OF THE DATA TRANSMISSION
288
DISCARD THE DATA TRANSMISSION
290
END

Figure 4


200
202
Microprocessor
214
Secure Area
218
Seed Identity
208
206
204
212
228
Keypad
User Interface Adapter
Display Circuitry
210
Display Device
216
Memory
Application$_1$
Application$_2$
Application$_X$
Transformation Engine
Secure Area
222
Unique Identity$_1$
224
Unique Identity$_2$
142$_1$
142$_2$
142$_X$
220
226