Title

An Interactive Television System

Technical Field

The invention concerns an interactive television system for providing secure interactive services to consumers via broadcast infrastructure operated by a broadcaster.

Background of the Invention

Integrated circuit cards or smart cards are increasingly used for many different purposes in the world today. A smart card typically contains read-only-memory (ROM), electrically erasable programmable read-only-memory (EEPROM), and an output/input (IO) mechanism. These smart cards either require contact or are contactless. A smart card may also contain a microprocessor and other circuitry to support the microprocessor in its operations. A smart card may contain a single application or may contain multiple independent applications in its memory. Its memory may be secured or unsecured.

The present invention seeks to overcome the limitations posed by broadcast infrastructure and set-top boxes in order to provide secure smart card transactions.

Summary of the Invention

In a first preferred aspect, there is provided an interactive television system for providing secure interactive services to consumers via broadcast infrastructure operated by a broadcaster, the system comprising:

a digital receiving device to receive broadcast data and data relating to the secure interactive service via the broadcast infrastructure, the digital receiving device receiving a mobile device of the consumer; and

a return-path host server to provide return path connectivity from the digital receiving device to the broadcaster;

wherein interaction with the secure interactive service is secured by checking whether the consumer has physical access to use the digital receiving device, checking whether the consumer has been granted access to use the secure interactive service, and authenticating the return-path host server and the digital receiving device.

Interaction with the secure interactive service may be further secured by using key pairs and application protocol data unit (APDU) commands of the mobile device to communicate with any one of the group consisting of: the broadcast infrastructure, the digital receiving device and the return-path host server.

Interaction with the secure interactive service may be further secured by verifying the identity of the consumer according to stored data on the mobile device, for communication between the digital receiving device and the return-path host server.

Interaction with the secure interactive service may be further secured by verifying the identity of the consumer before access to the secure interactive service is permitted.

The authentication may be decentralised and key pairs are transmitted from the return-path host server to the digital receiving device, and the key pairs are processed by the set-top box.

The authentication may be centralised and the key pairs are transmitted from the digital receiving device to the return-path host server, and the key pairs are processed by the return-path host server.

The identity of the consumer or the digital receiving device may be verified against a central database. The verification may be performed by entering a personal identification number (PIN), password, or a biometric scan of the consumer.

The digital receiving device may be verified by authenticating the conditional access identification of the digital receiving device.

The broadcast infrastructure may be satellite television infrastructure. The broadcast infrastructure may include infrastructure capable of carrying digital or analogue signals via terrestrial signals, cables, or wireless systems.

The digital receiving device may be set-top box, personal video recorder (PVR), or personal digital assistant (PDA).

The third parties may include financial institutions, government agencies, or merchants.

The secure interactive service may be selected from the group consisting of: TV-Coupons, TV-Pre-Paid, TV-Mobile Downloads, TV-Government, TV-Payment Transactions, TV-Banking, TV-Commerce, TV-Shopping, TV-Card Management, and TV-Tokens.

The return-path host server may be in communication with a third party host server.

For each session of the secure interactive service, a session key may be used to encrypt communication between the broadcast infrastructure and digital receiving device and between the digital receiving device and return-path host server. The session key may be first transmitted by either the broadcast infrastructure to the digital receiving device, mobile device to the digital receiving device, digital receiving device to the return-path host server, return-path host server to the digital receiving device, or between the return-path host server and a third party host server.

Messages transmitted from the digital receiving device to the return-path host server may be digitally signed to ensure message integrity. Digital signatures may be authenticated with a trusted party.

At least one interactive application may be stored on the mobile device to process and transmit data to the secure interactive service.

The mobile device may be personalized with information relating to the consumer, and may be activated for use by a process that uses an activation key.

The digital receiving device and the smart card may authenticate each other according to a mutually agreed authentication procedure in order to securely communicate with each other.

The mobile device of the consumer may be connectable to or is embedded into the digital receiving device. The mobile device may wirelessly communicate with the digital receiving device. The mobile device may be a chip-based card such as a smart card. The mobile device may be a mobile computing device such as a

Personal Device Assistant (PDA), a palm machine, a notebook, a removable hard disk, a thumb drive, or a mobile phone.

The system may further comprise a key and certificate management module and broadcast infrastructure's secure key module to manage and distribute keys or certificates used to encrypt/decrypt communication, messages, application and data between the broadcast infrastructure and the digital receiving device, the mobile device and digital receiving device, the digital receiving device and the return-path host server, and the return-path host server and a third party host server.

The key may be any one in the group consisting of: an activation key, payment keys, post-issuance key, transfer key, terminal key, verification key, host key, and loyalty key.

The system may further comprise a copy protection module to grant the consumer rights to record content broadcast via the broadcast infrastructure.

The system may further comprise a security domain to establish a unique cryptographic key to ensure secure communication between the mobile device and the digital receiving device, between the digital receiving device and return-path host server, and the return-path host server and a third party host server.

The unique cryptographic key may use only a single key, symmetric cryptographic service.

The consumer may enter a password of personal identification number (PIN) to enable access to the secure interactive service and information stored on the mobile device.

A biometric system may be provided to enable access the secure interactive service and information stored on the mobile device if the consumer's scanned biometric data is matched to their record stored in a biometric database.

Brief Description of the Drawings

An example of the invention will now be described with reference to the accompanying drawings, in which:

Figure 1 is a block diagram of the broadcast system; and

Figure 2 is a table illustrating a secure access matrix of security layers of the interactive television system and its system components.

Detailed Description of the Drawings

Figure 1 and the following discussion are intended to provide a brief, general description of a suitable computing environment in which the present invention may be implemented. Although not required, the invention will be described in the general context of computer-executable instructions, such as program modules, being executed by a personal computer. Generally, program modules include routines, programs, characters, components, data structures, that perform particular tasks or implement particular abstract data types. As those skilled in the art will appreciate, the invention may be practiced with other computer system configurations, including hand-held devices, multiprocessor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, and the like. The invention may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

Referring to Figure 1, an interactive television system 100 for providing secure interactive services to cardholders 5 via broadcast infrastructure 50 operated by a broadcaster is provided. The system 100 generally comprises: a set-top box 10 and a return-path host server 60. The set-top box 10 receives broadcast data and data relating to the secure interactive service via the broadcast infrastructure 50. The set-top box 10 also receives and reads data that is stored on a smart card 20 of the cardholder 5. The return-path host server 60 provides return path connectivity from the set-top box 10 to the broadcaster. Interaction with the secure interactive service is secured by checking whether the cardholder 5 has physical access to use the set-top box 10. Another security check is performed by checking whether the cardholder 5 has been granted access to use the secure interactive service. A further security check is performed by authenticating the return-path host server 60 and the set-top box 10.

A consumer interface device 40 is used by the cardholder 5 to interface with and control the set-top box 10. Consumer interface devices 40 include any one of the group consisting of: set-top box remote controller, wireless devices/keyboard, infrared devices, mobile phone, PDA or computer. The output of the set-top box 10 is displayed on a presentation device 30 such as a television screen or computer monitor. The secure set-top box application is triggered when the cardholder 5 navigates the set-top box 10 using the consumer interface device 40; or by using their smart card 20 with the set-top box 10.

Smart Card

The smart card 20 includes credit cards, bankcards, charge cards, loyalty cards, pre-paid cash cards, gift cards, entertainment cards, driver's license, and national registration identification cards (NRICs) that have an integrated circuit in the form of a microprocessor or memory chip. The smart card 20 is contact or contactless.

Before the smart card 20 is issued to the cardholder 5, the smart card 20 is initialised with some card data (which uniquely identifies the card). After a personalisation data structure is loaded and stored in the smart card 20, the smart card 20 is identifiable by the card issuer 85, product class, data and identification number. The smart card 20 cannot change its identity once it is personalised.

The smart card 20 is loaded with at least one application, such as credit or stored cash value, a card file structure initialised with default values, and/or keys for transport security.

The smart card 20 does not necessarily have to be activated during the personalisation stage. The set-top box 10 is used to activate the smart card 20 through an authentication process with the return path host server 60 containing the smart card details to be activated.

After issuance of the smart card 20, the smart card 20 needs to be activated using an activation key; or post-issued with new/updated card application; or deleting existing applications on the smart card 20. The post-issuance process also involves both information and data. It involves using a post-issuance key. The set-top box 10 is used to load/write, read and/or delete static cardholder 5 data

including the cardholder's 5 name, address, and preferences in the smart card 20. Therefore, the set-top box 10 is also used for card management processes.

Based on the smart card type data, the set-top box 10 determines whether the smart card 20 is suitable to be personalised and/or post-issued. If the smart card 20 is not the correct type, the process terminates and the cardholder 5 is informed via the presentation device 30.

The set-top box 10 is able to activate the cardholder's 5 smart card 20. Typically, the smart card 20 is issued to the cardholder 5 by a card issuer/manufacturer 85. Adding, deleting or updating smart card applications and file structures in the smart card 20 is also performed by the set top box 10. The set-top box 10 is able to perform cardholder 5 data management. Cardholder 5 data such as the cardholder's 5 name, address, and preferences, is read by the set-top box 10.

A smart card interaction process between the smart card 20 and set-top box 10 occurs when the smart card 20 is connected with the set top box 10. The smart card 20 stores a secret key and public key pair. Generally, the process includes retrieving the public key from the smart card 20, encrypting at least a portion of the data to be transported using the public key, transmitting the encrypted data to the smart card 20, and decrypting the encrypted data using the smart card's secret key.

The smart card's key pairs interact with key pairs that are broadcast to the set-top box 10 through the broadcast infrastructure 50. Alternatively, key pairs are loaded onto the set-top box 10 from the return-path host server 60 or third party smart card system through a secure communications infrastructure. Alternatively, centralised key pairs are located at the return-path host server 60 or third party smart card system and is not transmitted to the set-top box 10.

The types of keys include an activation key, payment keys, post-issuance key, transfer key, terminal key, verification key, host keys, and loyalty keys.

Return-path host server

The broadcaster's return-path host server 60 is connected to other third party host servers 70 to provide other secure interactive services not available with the broadcaster. Authentication/verification with the third party host servers 70 is also

performed. These third party host servers 70 belong to financial institutions, loyalty providers, content providers, and government agencies. The return-path host server 60 enables return-path connectivity. The return-path host server 60 includes a modem pool or a plurality of telecommunication devices and communications infrastructure to receive data from set-top boxes 10 within the system 100. These devices are managed by the broadcaster.

For a secure set-top box transaction, dedicated connectivity from the set-top box 10 to the return-path host server 60 is required as part of the data transmission process. This connectivity is via a secure communication infrastructure using accepted cryptographic systems. The return-path host server 60 is in turn connected to other host servers 70 to perform other secure set-top box transactions.

- For TV-Payment transactions, the return-path host server 60 is connected to a payment gateway's host server 70 to settle any payments transacted by the cardholder 5 using the set-top box 10. Payments are made to utility companies, on-line merchants, government agencies, content providers and loyalty providers. The cardholder 5 is authenticated with the information contained in a payment gateway's host server 70 in addition to data stored on the smart card 20.
- For TV-Banking transactions, the return-path host server 60 is connected to a financial institution's host server 70 to provide specific cardholder's 5 account details, like account balances and mortgage details. The cardholder 5 is authenticated with the information contained in a financial institution's host server 70 in addition to data stored on the smart card 20.
- For TV-Commerce/TV-Shopping transactions, the return-path host server 60 is connected to a "shopping mall" merchant's host server 70 that manages a list of goods and/or services that are purchased by the cardholder 5 using the set-top box 10. The merchant's host server 70 manages the fulfilment and the billing portion of the purchase. The cardholder 5 is authenticated with the information contained in a merchant's host server 70 in addition to data stored on the smart card 20. Specifically, if there is a cardholder 5 pre-registration process where the cardholder's 5 details are stored in the merchant's host server 70. A list of goods and/or services are also transmitted to the broadcast infrastructure 50 for immediate broadcast.

- For TV-Loyalty and TV-Reward transactions, the return-path host server 60 is connected to loyalty-provider's host server 70 to provide specific cardholder 5 with loyalty details, such as points balance, redemption status and special offers. The cardholder 5 is authenticated with the information contained in a loyalty provider's host server 70 in addition to data stored on the smart card 20.
- For TV-Tokens transactions, the return-path host server 60 is connected to a third party smart card system's host server 70 to manage/update information pertaining to the third party smart card system via the set-top box 10 through the communication infrastructure and the return-path host server 60. The cardholder 5 is authenticated with the information contained in a third party smart card system's host server 70 in addition to data stored on the smart card 20. Specifically, if there is a cardholder 5 pre-registration process where the cardholder's 5 details are stored in the third party's host server 70.
- For TV-Coupon transactions, the return-path host server 60 is connected to loyalty providers/merchant's host server 70 to securely download the latest promotional discount offers onto their smart card 20 for redemption at the participating merchant outlet upon check-out. Redemption is instant in some cases. The cardholder 5 is authenticated with the information contained in the loyalty providers/merchant's host servers 70 in addition to data stored on the smart card 20.
- For TV-Pre-Paid transactions, the return-path host server 60 is connected to third party host servers 70 operated by pre-paid service provider like telecommunications companies so that the stored-value on the smart card 20 is increased or topped-up. The cardholder 5 elects to pay for the top-up value through the TV-Payment service.
- For TV-Mobile Download transactions, the return-path host server 60 is connected to third party host servers 70 operated by ring-tone and/or wall-paper mobile download content providers, where cardholder 5 can pay for the mobile downloads through the TV-Payment service.
- For TV-Government, the return-path host server 60 is connected to government agency's host servers 70 like road transport and immigration departments for on-line enquiries/payment on government related matters like driving license renewals and payment of fines through the TV-Payment services. The cardholder 5 is authenticated with the information contained in the government agency's host server 70 in addition to data stored on the smart card 20. Information on the National Registration Identification Card (NRIC) smart card 20 is authenticated with the government agency's database through

the set-top box 10 and return-path connectivity over a secured communications infrastructure.

- For TV-Card Management, the return-path host server 60 is connected to card issuer/manufacturer's host servers 70 for card management services like post-issuance and smart card activation.

A secure environment is created by establishing a unique cryptographic key (first key component) in a first cryptographic device, for example the set-top box 10. The same unique cryptographic key is securely established in the second cryptographic device, such as a return-path host server 60. The unique cryptographic key ensures a secure communications infrastructure between the set-top box 10 and return-path host server 60. For example, the unique cryptographic key uses only a single key, symmetric cryptographic service.

The first key component is loaded onto the set-top box 10 through the broadcast infrastructure 50; through an onboard smart card system; through the return-path host server 60 using a secure communication infrastructure, using centralised or distributed methods; or downloaded from a third party smart card system, independently from the first key component.

Secure interactive services

The secure interactive services provided by the system 100 include:

- TV-Payment (debit, credit and stored value) – Cardholders 5 insert their payment smart card 20 into the set-top box 10 for debit, credit and stored value financial transactions. Payments through the set-top box 10 include bill payments, TV-Commerce, TV-Pre-paid, TV-Mobile Downloads, and TV-Government as secured set-top box applications through a secure communications infrastructure, connected to a payment provider's return-path host server 70.
- TV-Banking – Smart cards 20 interfacing with the set-top box 10 enable access to a financial institution and provide the cardholder 5 with an array of financial information. The cardholder 5 is able to perform financial transactions including a review of balances in different accounts, review of transaction journals for various accounts; funds transfer, mortgage account information, cheque book request, and bill/utility payment. All these transactions are made through a secure communications infrastructure connected to a financial institution's return-path host server 70.

- TV-Commerce, TV-Shopping - Cardholders 5 insert their payment smart card 20 into the set-top box 10 to pay for goods and/or services ordered using the set-top box 10 through a secure communications infrastructure, connected to a merchants' return-path host server 70.
- TV-Loyalty – Set-top box 10 can add/delete/update loyalty information and/or reward points onto the smart card 20 or "TV Loyalty Card" through a secure communications infrastructure, connected to a loyalty provider's return-path host server 70. This includes TV-Gift Cards that contain information about a particular people, place, and item and loyalty information is only read by the set-top box 10 and displayed on the presentation device 30.
- TV-Rewards – Set-top box 10 accumulates and downloads reward points on the smart card 20 for every secure set-top box transaction made or for interactive television navigation using the consumer interface device 40. This is to increase participation and cardholder 5 "stickiness" to the set-top box 10 and to the services offered.
- TV-Tokens - Cardholders 5 use their smart card 20 as an off-line physical conduit to transfer utility/payment information and/or data between the set-top box 10 and a third party smart card system (for example, pre-paid smart card meters and computers fitted with a smart card reader). The smart card 20 is inserted into a pre-paid utility meter, installed with a smart card reader and enabled with a cryptographic system, to physically transfer the utility usage data from the pre-paid utility meter to the utility company through the set-top box 10 and return-path connectivity, secure communications infrastructure and the utility provider's return-path host server 70. Upon updating the utility usage data, the cardholder 5 pays for any utility top-up. The top-up utility data is subsequently transferred to the pre-paid utility meter through the set-top box 10 using the same smart card 20, as the physical conduit.
- TV-Coupons – Cardholders 5 download electronic promotional discount vouchers onto their smart card 20 and enjoy the downloaded promotional discounts when making payment for the goods/services purchased with the same smart card 20 during the redemption process at the check-out counter of the participating merchant. The set-top box 10 can perform either downloading and redemption processes. When connected to a return-path host server 60, complex and secure promotional discount vouchers are downloaded into the smart card 20. Downloaded secure TV-Coupons are redeemable using the set-top box 10.

- TV-Pre-Paid – Cardholders 5 use the set-top box 10 to top-up the monetary value on their pre-paid smart card 20 (for example, entertainment card or telecommunication services like pre-paid mobile) and make the required payment using the TV-Payment services through a secure communications infrastructure, connected to a return-path host server 60.
- TV-Mobile Downloads – Cardholders 5 can request for ring-tone and/or wall-paper mobile downloads through the set-top box 10 and make the required payment using the TV-Payment services through a secure communications infrastructure, connected to a content provider's return-path host server 70.
- TV-Government – Cardholders 5 having a national identification smart card 20 (like Malaysian Government's National Registration Identification Card (NRIC) smart card 20 called "MyKad"), can make on-line enquiries on government related matters like status of an application and/or make necessary government payments like driving license renewals and payment of fines using the TV-Payment services through a secure communications infrastructure, connected to a government agency's return-path host server 70.
- TV-Card Management – Card issuer/manufacturer can assist the cardholder to perform card management services like post-issuance of new/updated application into their smart cards and smart card activation of newly issued smart cards to cardholders.

Data is transmitted throughout the system 100 between: the set-top box 10, smart card 20; return-path host server 60, third party host servers 70 and third party smart card systems.

Broadcast data transmitted from the broadcaster to the set-top box 10 is via the broadcast infrastructure 50. This is considered remote infrastructure. Under this connectivity path, the set-top box 10 is the host system. This is typically a one-way satellite broadcast to the set-top box 10. With return-path connectivity through a secure communications infrastructure between the set-top box 10 and the return-path host server 60, the entire communication loop is completed with the broadcaster. Data transmitted from the set-top box 10 to the return-path host server 60 includes response data for a secure interactive service.

Data transmitted between the set-top box 10 and smart card 20 is via the set-top box's smart card reader 12. Under this connectivity path, the host system is either the set-top box 10 or smart card 20, depending on the application and/or business

logic. It also depends on which system initiates the command sets to the smart card 20 to perform the business process/logic.

Data transmitted from the set-top box 10 to the return-path host server 60 is via communications infrastructure. The communications infrastructure is secured by accepted cryptographic systems. This connectivity, together with the remote infrastructure is collectively referred to as local infrastructure. Under this connectivity path, the host system is the return-path host server 60.

Data transmitted between the set-top box 10 and third party smart card systems uses the smart card 20 as a physical conduit between the set-top box 10 and the third party smart card systems. Under this connectivity path, the host system is the third party smart card system through a communications infrastructure that is secured using accepted cryptographic systems.

Security Layer 1

Referring to Figure 2, the broadcast transmission is encrypted throughout the broadcast infrastructure 50 using widely accepted cryptographic systems. Upon receiving the broadcast transmission to the set-top box 10, the set-top box 10 uses its own conditional access (CA) system 11 to decrypt the received broadcast transmission. This is considered the first security layer 200. Interaction with the set-top box's conditional access system 11 increases security of the secure set-top box transaction. In one example, the broadcaster uses the set-top box's conditional access system 11 to manage physical access to the set-top box 10 by the cardholder 5. Without physical access rights granted through the set-top box's conditional access system 11, the cardholder 5 cannot perform any secure set-top box transactions using the smart card 20 with the set-top box 10.

Security Layer 2

Restrictions are placed on the cardholder 5 to only permit access to selected secure interactive services. This is considered the second security layer 201. For example, restrictions are based on the subscription plan of the cardholder 5, the location of the cardholder 5 or the age of the cardholder 5. The second security layer 201 is enforced by physical access rights used by the first security layer 200.

Security Layer 3

In one example, there are no authentication or encryption/decryption schemes used for the smart card 20. That is, the smart card 20 does not require a key and/or certificate to read/write into a "free-read-write" smart card 20. If no authentication is required, the application, information or data is considered as unregistered. This poses a threat to the security of the smart card 20 and/or set-top box 10, especially if it is hacked or compromised.

If a cryptographic system is required to read/write onto a smart card 20, then this is a "secure-read-write" smart card 20. It is expected in most cases that a "secure-read-write" smart card 20 is used.

Without smart card security, key pairs are transmitted from the return-path host server 60 or third party smart card system to the set-top box 10 through a secure communications infrastructure. Key exchange authenticates the return-path host server 60 and the set-top box 10 with each other. The key pairs are already on the smart card 20 or part of the set-top box's conditional access system 11. This is considered the third security layer 202.

Key management is provided to ensure that key values which are generated have the necessary properties, making the key known in advance to the particular systems through the secure broadcast infrastructure and/or return-path connectivity through a secure communications infrastructure, working together or in isolation of each other. Key management also ensures that the key is protected against disclosure or substitution using combinations of various cryptographic techniques. Key management methods vary substantially depending on whether it uses an asymmetric cryptographic system, or a public key cryptographic system.

For key management, the return-path host server 60 is connected to a host service of a trusted party 80 to manage/distribute the keys and/or certificates, either on an on-line or off-line basis. Trusted parties 80 can use the set-top box 10 for managing their key life cycle. Trusted parties 80 include a certification authority, loyalty provider, banks, and trusted third parties, which provide a trusted service.

Storing multiple secure set-top box applications, information or data (or a message) on a single smart card 20 introduces challenges concerning the authenticity, integrity and security of the message exchanged with the smart card 20, set-top box 10, and return-path host server 60, the broadcast infrastructure 50 and return-

path connectivity. A message includes any one of the following: application, information or data.

The authenticity of a received message is never fully guaranteed since a message may originate from anyone, anywhere at anytime. To increase security protection, a security domain architecture is implemented to limit the number of senders or receivers within a particular security domain or closed environment, using accepted cryptographic systems. Secure domains are also introduced onto the smart card 20.

Security Layer 4

Smart card authentication is used in the fourth security layer 203. The key set on the smart card 20 is made up of three different key items. The smart card's secret key which is known only to the card 20; the smart card's public key, which is stored on the smart card 20; and the smart card's public key certificate, which is the smart card's public key signed by a trusted party 80.

If a combination of keys is used by the set-top box 10, the message is both authenticated and encrypted/decrypted. Encryption techniques are implemented for each data transmission process to maintain confidentiality of sensitive cardholder 5 information and messages. This ensures authenticity and integrity of the systems and host system's data elements and minimise the risk and impact of exposing the key and the certificate.

Encrypted data elements are not presented in clear text or any other form that allows extraction without the knowledge of the appropriate keys or cryptographic systems.

The life cycle of a key typically includes key establishment, key recovery, key replacement/update, key revocation and key termination. The set-top box 10 is enabled to provide key management functionality to the card issuer 85 and/or application provider, through connectivity via the return-path host server 60. The loading of keys or key components incorporates a validation mechanism such that the authenticity of the keys is ensured and it is evident whether they have been tampered with, substituted, or compromised. The key loading process does not disclose any portion of a key component to an unauthorised individual.

Using digital certificates (for authentication) and public key infrastructure, a secure communication session is initiated between host systems for the exchange of digital certificates, whereby digital certificates are authenticated by both systems using a public key of a trusted party 80. Once the digital certificates are exchanged and authenticated, the systems are able to pass encrypted messages between each other.

Another way to initiate a secure communication session is to authenticate digital signatures of a trusted party 80 against the certificates found in host systems like the set-top box 10, return-path host server and the smart card 20. Public keys of trusted party 80 and/or secret keys are also be used to authenticate the digital signature of the trusted party 80 found on the certificates of the host system. The host system validates the certificates of another system using the public keys of the trusted party 80.

The keys which are stored are dedicated keys and are not used for other purposes. For example, it is not possible to use the same key for data encryption and personal identification number (PIN) encryption. Keys stored in host systems are generated through a diversification scheme and are not be exposed in clear text.

The key pairs are broadcast through the broadcast infrastructure 50 to the set-top box 10 through the broadcast infrastructure 50 as temporary session key pairs on the set-top box 10 and/or when interacted with the smart card 20 that has been used with the set-top box 10.

The encrypted private key is embedded into the broadcast infrastructure's secure key module. The secure key module is further encrypted using the broadcaster's conditional access, providing another layer of security by further scrambling of the private key string within the secure key module code. This ensures that the private key is not presented in clear or plain text even within the secure key module code.

The smart card 20 contains either a combination of card domain and secure domain; or a card domain. The card issuer/manufacturer 85 defines the card domain, representing the interest of the card issuer/manufacturer 85. The card domain includes an application protocol interface (API) interface and a command interface, such as application protocol data unit (APDU) interface. The APDU interface facilitates interfacing with the external environment. An application "load"

and "install" option is performed through a set of appropriate APDU commands received by the card domain.

If no card domain is associated with the application that is being loaded, then the cryptographic key and the signature of the card domain, by default, is used, if available..

If the smart card 20 already has an application loaded, then the subsequent smart card application interacts with the first application during the post-issuance process or during a secure set-top box transaction. The second application either uses the first application or the card domain for post-issuance or for a secure set-top box transaction. As such, the cryptographic service of the first application is used to install the second application onto the smart card 20 during post-issuance or during a secure set-top box transaction.

If the smart card has two or more applications already loaded onto the smart card 20, then the subsequent application interacts with the card domain or any other existing secure domain for post-issuance or for a secure set-top box transaction. Thus, installing a second application onto the smart card 20 during the post-issuance process involves downloading the first application into the card domain. The set-top box 10 is used to post-issue an application, information or data onto a valid smart card 20 enabled for post-issuance transactions. The smart card 20 grants the rights to post-issue from the set-top box 10 by way of its key pairs and certificates, working together or separately with the broadcast infrastructure 50 and/or return-path host server 60.

There may be multiple secure domains on a smart card 20, each represented by unique cryptographic relationships or systems. Each secure domain is responsible for the management and sharing of cryptographic keys and its associated cryptographic methods make up the secure domain's cryptographic relationship/service.

Multiple smart card applications are associated with the same secure domain. The secure domain is created by the card issuer/manufacturer 85, or subsequently added by the card issuer/manufacturer 85 or an application provider.

An application, information or data for post-issuance is forwarded for downloading to the smart card 20: either through: the broadcast infrastructure 50 to the set-top box 10; the return-path host server 60; or a third party smart card system. The message is encrypted and pre-signed (for authentication purposes) with a key equivalent to one existing on the smart card 20 so that each application has a unique signature that can be verified or authenticated by the smart card 20.

The card domain uses key services from the smart card's own secure domain for decrypting and checking the signature of the forwarded message with a public key of an asymmetric encryption key pair of the application provider. Alternatively, the card domain uses the key services of the set-top box's conditional access system 11 for decryption and verification. Alternatively, the card domain uses the key services of the smart card 20 which are downloaded through the broadcast infrastructure 50 to the set-top box 10; or transmitted from the return-path host server 60 or third party smart card system.

If the signature associated with the message is not valid, then the application, information or data is not loaded onto the smart card through the set-top box 10, or the secure set-top box transaction is aborted. An error notification appears on the presentation device 30. But if the signature associated with the message is valid, the application, information or data is then loaded onto the smart card 20 or the secure set-top box transaction is activated, in a secure environment.

The interactive application is downloaded to the smart card 20 as a file or an application object.

During the post-issuance process, the set-top box 10 initiates an "open" command which previews the smart card 20 to make sure that the smart card 20 is qualified to accept the loading of a specific application, information or data. The open command provides the smart card 20 with the message's permission data, the message size, and instructs the smart card 20 to determine if the smart card 20 has been personalised; whether the message code and associated data will fit in the existing memory space on the card. It also determines whether the personalisation data assigned by the message to be loaded allows for the loading of the message onto the particular smart card 20. The open command makes additional checks required by the smart card system/card domain/secure domain.

After the open command has been executed, the "application loader" through the set-top box 10 is notified whether the smart card 20 contains proper identification personalisation data and if there is enough room that exist in the memory of the smart card 20 for further download of an application, information or data.

The loading occurs in conjunction with a "create" step that completes the loading process. This step enables the application to execute the smart card 20 after it has been loaded. The combination of "open", "load" and "create" commands are sent by the set-top box 10 to the smart card 20 through the broadcast infrastructure or return-path host server 60 connectivity, using a secure communications infrastructure.

The create command for post-issuance checks if an application load certificate is signed/encrypted by a trusted party 80 and therefore authenticates the application as a proper application for the smart card and set-top box 10; and checks the smart card personalisation data stored in the smart card 20 against the permission profile for the application to be loaded to qualify the smart card 20 for loading. If these checks fail, then a failure response is displayed on the presentation device 30 and the process is aborted. After passing these checks, the application is loaded into the memory of the smart card 20.

In one embodiment, a smart card application provider creates an independent secure domain on the smart card 20, in addition to the card domain. This separates the security protocol/system between the smart card issuer/manufacturer 85 and the application provider. The secure domain contains security keys that are kept confidential from the card issuer/manufacturer 85. The card domain approves commands for smart card initialisation and post-issuance by invoking the secure domain's cryptographic service.

Each domain has its own unique cryptographic service, complete with its own private and/or secret key pair(s), are used for encryption, decrypting, and hashing. Each domain contains its own unique digital certificate(s), digitally signed by a trusted party 80.

The system component transmitting the data to a host system can verify that the trusted party 80 has approved the initiating system by using the host system's signed public key of the trusted party 80. If the verification is successful, the

initiating party has verified that the trusted party 80 has approved the host system, and the secure transaction commences.

The smart card 20 is automatically locked if a breach of security has been detected by the application that is either residing in the set-top box 10 or the return-path host server 60/third party smart card system. The set-top box 10 performs a locking/unlocking function, both at the card and application level, either by way of a key or using the card domain. The locking/unlocking function is performed manually by the cardholder 5 or automatically according to business logic or rules.

Card domain operates in conjunction with a secure domain. The secure domain functions like a logical construct to provide security-related functions to the card domain and to applications, information or data (or message) associated with the secure domain. The card domain decrypts the application, information or data with the card issuer's secret key.

The secure domain assists in the secure post-issuance loading of an application, information or data onto a smart card 20. It provides a secure mechanism that keeps the application provider's information confidential, such as cryptographic keys, and prevents disclosure to the card issuer/manufacturer 85.

The set-top box 10 and smart card 20 authenticate each other via a mutually agreed authentication procedure and cryptographic system, predetermined APDU command sets, and protocol checks for both the smart card 20 and set-top box 10. This is to ensure authenticity, integrity and compatibility with each other. This interaction is used for secure set-top applications including TV-Payment, TV-Banking, and TV-Commerce/TV-Shopping. These protocols also prevent the use of a fraudulently issued smart card 20 with the set-top box 10.

Once authentication is completed, the set-top box 10 and the smart card 20 pass transaction messages and commands between each other in an environment secured by a cryptographic service.

Cryptographic Services

There are two types of cryptographic service that are used for system components to run the secure set-top box application and for data transmission between

systems. These are: symmetric (commonly referred to as private key or secret key systems) and asymmetric (commonly referred to as public key infrastructure).

A secret key system uses a key as part of a mathematical formula that encrypts application, information and data (collectively called messages) by transforming the message using the mathematical formula, certificates and key. After the message is encrypted, another party/recipient can only decrypt the encrypted message using the same secret key with a pre-defined decryption algorithm. Thus, the same secret key is used for both encryption and decryption (hence the technique is termed symmetric). This is secure since there is only one secret key involved throughout the encryption and decryption process. But this increases the risk if that secret key is compromised. If so, the entire encryption and decryption system may also be compromised.

An asymmetric cryptographic service uses two different keys or a key pair for authentication and/or encrypting/decrypting messages. The two keys are typically referred to as a private/secret key and a public key. When the message is encrypted with one key of the pair, the other key is used to decrypt the message. If person A wants to send an encrypted message to person B that no one else is able to read, he encrypts the message with person B's public key and send it to person B. Only the holder of B's secret key is able to decrypt the encrypted message.

There are also different key usage methodologies. In one example, session keys are stored inside a particular system for use in the next transaction only. The system derives session keys from static symmetric master keys for every transaction. These master keys must be generated, distributed, and loaded under greater security control than the normal keys. Alternatively, the system uses only static symmetrical session keys for each transaction.

A master/static key is a cryptographic key that exists in the system prior to, during and after processing or transaction. The master key is typically embedded into the system, for example in a secure module of a host system.

A session key is a cryptographic key that is specifically generated for a particular transaction/session and becomes obsolete once the original transaction has been completed. The session key is transferred between system components to authenticate the transactions and facilitate the encryption/decryption process.

Since the session key is used for only one transaction, the potential for compromise is reduced. The key-encryption key, or master key, however, is used for encrypting a session key that is transmitted over normal communications infrastructure or stored in a host server's (return-path host server 60 included) secure module. These master keys must be generated, distributed, and loaded under greater security control than the normal keys.

The symmetric keys (master and/or session keys) are stored either outside or inside a secure module. If the keys are stored inside the secure module, the symmetric keys never leaves the secure module. Cryptographic calculations are performed inside the secure module through function calls from the system. The secure module resides in a third party host server 70 or broadcaster's return-path host server 60.

Security Layer 5

Another level of security 204 is provided for payment methods like 3D Secure or Verified-by-Visa modified for the set-top box 10 and TV-Commerce. The cardholder 5 needs to pre-register for the service beforehand and supply their username and password to complete the payment transaction. The cardholder's details are stored in a central database, and for each secure transaction with a secure interactive service, the cardholder's details from the smart card 20 are validated against the centrally stored cardholder's details.

Security Layer 6

Another level of security 205, requires the cardholder 5 to enter their personal identification number (PIN) secretly on a consumer interface device 40 and/or through other cardholder 5 authentication steps, as required. Alternatively, a biometric reading device is installed, interfacing with the set-top box 10 or return-path host server 60, to authenticate the cardholder 5.

Example - TV-Banking

In one example, the set-top box 10 is able to function similar to an automated teller machine (ATM). A cardholder 5 transacts with their financial institution to transfer money and make account enquiries by using their smart card 20 issued by their own issuing bank. In a typical ATM transaction, protection is provided to the cardholder's 5 personal identification number (PIN), the cardholder's 5 primary account number (PAN), the cash amount, the date and time of financial

transaction, and the ATM identification number. The transaction information and a personal identification number (PIN) are received from the cardholder 5 at a transaction terminal; in this example, the set-top box 10. A first session key encrypted by a first master key is retrieved from the memory of the set-top box 10 and is decrypted with the first master key that is also stored in the memory of the financial institution's host server 70.

The set-top box 10 is secured using various cryptographic systems for transmission of the data elements on the smart card 20 to the set-top box 10, the return-path host server 60 and the financial institution's host server 70. There are various cryptographic systems in existence that provide the secure means by which these data elements can be protected/secured. Europay-Mastercard-Visa (EMV) payment transactions are initiated via the set-top box 10. The EMV procedures includes requesting the smart card application to verify a cryptographic service; sending transaction-related data to the smart card 20, which computes and returns a cryptographic service; retrieving data that is not encapsulated in a message within the current smart card application; initiating the EMV payment transaction with smart card 20; and performing an "on-card" comparison of a supplied personal identification number (PIN) with the PIN contained within the card application.

Similar to the "load" command for post-issuance, a load command is used to credit value to a stored value smart card 20 via the set-top box 10. In addition, a "payment" command is used to initiate the payment sequence, debit the stored value smart card 20 by the indicated/predetermined amount, and terminate the payment sequence. The "stored value" command causes a balance inquiry transaction to be executed.

Similarly, the "payment" command causes a payment transaction to be executed and are applicable for a wide variety of payment instruments including credit, debit, and stored value smart card based transactions. The payment amount and currency are passed as parameters.

In another example, the transaction terminal is the set-top box 10. The first master key is either resident in the set-top box 10 as contained in a secure module, or is transmitted through the broadcast infrastructure, and working in conjunction with the set-top box's conditional access system 11. The first master key is temporarily

resident in a secured environment in the set-top box 10 until the set-top box 10 is switched-off. The set-top box's conditional access system 11 also decrypts using the master key for broadcast.

The financial institution re-transmits the message to the cardholder 5 with the same session key, but now encrypts it in a second master key. With this return message, a new, or second/subsequent session key, encrypted in the first master key, is appended to the return message. At the conclusion of the first transaction, the second encrypted session key replaces the first session key and is stored for the next transaction. This ensures that all encrypted data and message authentication codes is different even for identical transaction.

Thus, session keys can be generated by one or more master keys under a symmetric cryptographic service, which provide a more secure alternative to the asymmetric cryptographic service. Similarly for other secure set-top box transactions, specific application protocol data unit (APDU) commands are initiated by the set-top box 10 to the smart card 20 through the broadcast infrastructure or return-path host server connectivity, using a secure communications infrastructure.

For each secure transaction, the set-top box 10 and smart card 20 authenticate each other via a mutually agreed authentication procedure or cryptographic system, which checks the smart card 20 and set-top box 10 authenticity and compatibility with each other. This mutual authentication prevents use of a fraudulently issued smart card 20 to complete the secure set-top box transaction. Once security authentication is completed, the set-top box 10 and the smart card 20 pass transaction messages between each other, to initiate the secure set-top box transaction.

The smart card 20 incorporates digital encryption signatures and encryption algorithms to enable the smart card 20 to be validated from a remote location through either a local infrastructure or remote infrastructure. The local infrastructure includes the connectivity between the broadcast system and set-top box 10, through the broadcast infrastructure 50. In contrast, the remote infrastructure includes the connectivity between the set-top box 10 and return-path host server 60, through a communications infrastructure that is typically secured using accepted cryptographic systems.

Keys and certificates reside in the secure module (not shown) of the return-path host server 60/set-top box 10, or on the smart card 20, or temporarily on the set-top box 10 (for those set-top boxes 10 not fitted with a secure module), which is deleted once power supply to the set-top box 10 is turned-off.

Each of the following transactions are separated using the same or different smart card secure domain or the card domain's cryptographic system:

- For TV-Commerce/TV-Shopping transactions, a "payment" command is used to pay for the selected goods/services ordered using the set-top box 10, either through credit, debit or stored value payment systems. In addition, the "reward" command is initiated to reward the cardholder 5 for performing the secure set-top box transaction (part of TV-Rewards). Reward points earned and accumulated are securely stored either in the smart card 20 or at the return-path host server 60.
- For TV-Loyalty and TV-Reward secure set-top box transactions, a "loyalty" command is initiated to perform the loyalty transaction. A "query" command is used to request loyalty information from the loyalty-provider's host server 70 to provide specific cardholder 5 loyalty details, like points balance, redemption status and special offers. Accumulation of TV-Reward points is managed using the "reward" command.
- For TV-Tokens transactions, the "token" command initiates the transaction. The "token download" command is used to download the TV-Token information from a third party smart card system. The "upload" command is used to upload the information to the third party smart card system's host server 70 through the set-top box 10 and communications infrastructure. The "top-up" command is used to pay for the top-up of monetary credits onto the smart card 20, which is subsequently used for uploading to the third party smart card system. And the "upload" command is used to upload the credit information into the third party smart card system.
- For TV-Coupon transactions, the "coupon" command is used to download the selected TV-Coupons from the set-top box 10 onto the smart card 20. Whereas the "redeem" command is used to redeem the downloaded secure TV-Coupons to the set-top box 10.
- For TV-Pre-Paid transactions, the "top-up" command is used to pay for the top-up of monetary credits onto the smart card 20 (for telecommunication and utilities). This is integrated with the "payment" command to pay for the transaction, either through credit, debit or stored value payment systems.

- For TV-Mobile Download transactions, the "mobile download" command is used for mobile downloads from the content provider's host server 70 into the mobile phone/device 20. This is integrated with the "payment" command to pay for the transaction, either through credit, debit or stored value payment systems.
- For TV-Government, the "query" command is used to request information from the government agency's host server 70 to provide specific cardholder 5 details like driving license renewals. This is integrated with the "payment" command to pay for the transaction, either through credit, debit or stored value payment systems for the payment government levies, fines and licenses.
- For TV-Card Management, the "post-issue" command is used to post-issue a new/updated application into the smart card with connectivity to the card issuer/manufacturer's host servers 70.
- For key management, similar combinations of "open", "load" and "create" commands are used to manage/distribute the keys on the smart card 20 and set-top box 10.

Message Integrity

Encryption is commonly used for authentication/secrecy. But if message integrity also is important, then a cryptographic system is used to seal the message by applying a cryptographic function, sometimes called a hash, checksum, or message authentication code (MAC). This message authentication system protects the message against alteration, thus preserving the message integrity. The checksum value is stored with the message. Each time the message is accessed or used, the checksum is recomputed. If the computed/recomputed checksum matches the stored value, it is likely that the message has not been changed. Thus, a cryptographic checksum is an important measure against message tampering and failures during message transmission along with the broadcast and communications infrastructure.

A public key and the cardholder's 5 identity are bound together in a certificate, which is then digitally signed by a trusted party 80, certifying the accuracy/authenticity of the binding. This digital signature is a protocol that produces the same effect as a real signature. It is a mark that only the sender can make, but other people can easily recognised as belonging to the sender.

Trusted parties 80 provide various security components of the host system, and encrypt or digitally sign a copy of the host server's public key and the signed copy is also stored on the host server/system. A digital signature is a very convenient way for distributing certificates. The signer has a copy of its own certificate and attaches a copy of that certificate to the digital signature. The signer attaches other certificates that might be needed in validating their own certificate. For example, certificates for the signer's trusted party 80 issued by another trusted party 80.

Each system component may have more than one set of certificates: A first set of certificates is associated with a first set of private/secret key pairs that are used for decrypting and encrypting information. A second set of certificates is associated with a second set of private/secret key pairs that are used for signing and verifying digital signatures on information passed between systems. The number of certificates and/or key pairs depends on the security level required to complete the secure set-top box transaction using the smart card 20.

Copy Protection

Copy protection is implemented with a smart card 20 having a unique cryptographic service that is interfaced with the set-top box's conditional access system 11. This enables the cardholder 5 to be granted rights to record movies, pay-per-view (PPV) programmes, or pay-to-tape (PTT) programmes through a "copy-protected" set-top box 10. Access rights are stored on the smart card 20 or downloaded on demand through a secure communications infrastructure, connected to the content provider's return-path host server 70 or return-path host server. The access rights require a fee and the smart card 20 needs to be top-up with some predefined monetary value.

For copy protection, the return-path server connects to a content provider's host service to grant the cardholder 5 access rights to download a particular content. The cardholder 5 is authenticated with the information contained in the content provider's host server 70 in addition to data stored on the smart card 20. Specifically, if there is a cardholder 5 pre-registration process where cardholder 5 details are stored in the content provider's host server 70.

For copy protection, the "approval" command is used to grant the cardholder 5 access rights to download specific content. This is integrated with the "payment"

command to pay for the transaction, either through credit, debit or stored value payment systems.

Although the security layers 200, 201, 202, 203, 204, 205 have been described with reference to certain combinations, it is envisaged that any combination of the security layers is possible such that a secure interactive service is provided to the cardholder 5.

It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the invention as shown in the specific embodiments without departing from the scope or spirit of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects illustrative and not restrictive.

WE CLAIM:

1. An interactive television system for providing secure interactive services to consumers via broadcast infrastructure operated by a broadcaster, the system comprising:

a digital receiving device to receive broadcast data and data relating to a secure interactive service via the broadcast infrastructure, the digital receiving device receiving a mobile device of the consumer; and

a return-path host server to provide return path connectivity from the digital receiving device to the broadcaster;

wherein interaction with the secure interactive service is secured by checking whether the consumer has physical access to use the digital receiving device, checking whether the consumer has been granted access to use the secure interactive service, and authenticating the return-path host server and the digital receiving device.

2. The system according to claim 1, wherein interaction with the secure interactive service is further secured by using key pairs and application protocol data unit (APDU) commands of the mobile device to communicate with any one of the group consisting of: the broadcast infrastructure, the digital receiving device and the return-path host server.

3. The system according to claim 1, wherein interaction with the secure interactive service is further secured by verifying the identity of the consumer or the digital receiving device according to stored data on the mobile device, for communication between the digital receiving device and the return-path host server.

4. The system according to claim 1, wherein interaction with the secure interactive service is further secured by verifying the identity of the consumer before access to the secure interactive service is permitted.

5. The system according to claim 1, wherein the authentication is decentralised and key pairs are transmitted from the return-path host server to the digital receiving device, and the key pairs are processed by the set-top box.

6. The system according to claim 1, wherein the authentication is centralised and the key pairs are transmitted from the digital receiving device to the return-path host server, and the key pairs are processed by the return-path host server.

7. The system according to claim 3, wherein the identity of the consumer is verified against a central database.

8. The system according to claim 4, wherein the verification is performed by entering a personal identification number (PIN), password, or a biometric scan of the consumer.

9. The system according to claim 1, wherein the digital receiving device is verified by authenticating conditional access identification of the digital receiving device.

10. The system according to claim 1, wherein at least one interactive application is stored on the mobile device to process the data relating to the secure interactive service and to transmit response data to the secure interactive service.

11. The system according to claim 1, wherein the secure interactive services are provided by the broadcaster or third parties.

12. The system according to claim 11, wherein the third parties include financial institutions, government agencies, or merchants.

13. The system according to claim 1, wherein the return-path host server is in communication with a third party host server.

14. The system according to claim 1, wherein the secure interactive service is selected from the group consisting of: TV-Coupons, TV-Pre-Paid, TV-Mobile Downloads, TV-Government, TV-Payment Transactions, TV-Banking, TV-Commerce, TV-Shopping, TV-Card Management, and TV-Tokens.

15. The system according to claim 1, further comprising a key and certificate management module and broadcast infrastructure's secure key module to manage and distribute keys or certificates used to encrypt/decrypt communication, messages, application and data between the broadcast infrastructure and the

digital receiving device, the mobile device and digital receiving device, the digital receiving device and the return-path host server, and the return-path host server and a third party host server.

16. The system according to claim 15, wherein the key is any one in the group consisting of: an activation key, payment keys, post-issuance key, transfer key, terminal key, verification key, host key, and loyalty key.

17. The system according to claim 1, further comprising a copy protection module to grant the consumer rights to record content broadcast via the broadcast infrastructure and the digital receiving device.

18. The system according to claim 1, further comprising a security domain to establish a unique cryptographic key to ensure secure communication between the mobile device and the digital receiving device, between the digital receiving device and return-path host server, and the return-path host server and a third party host server.

19. The system according to claim 18, wherein the unique cryptographic key uses only a single key, symmetric cryptographic service.

20. The system according to claim 1, wherein for each session of the secure interactive service, a session key is used to encrypt communication between the broadcast infrastructure and digital receiving device and between the digital receiving device and the return-path host server.

21. The system according to claim 20, wherein the session key is first transmitted by either the broadcast infrastructure to the digital receiving device, mobile device to the digital receiving device, digital receiving device to the return-path host server, return-path host server to the digital receiving device, or between the return-path host server and a third party host server.

22. The system according to claim 1, wherein messages transmitted from the digital receiving device to the return-path host server are digitally signed to ensure message integrity.

23. The system according to claim 22, wherein digital signatures are authenticated with a trusted party.

24. The system according to claim 1, wherein the mobile device is personalized with information relating to the consumer, and is activated for use by a process that uses an activation key.

25. The system according to claim 1, wherein the digital receiving device and the smart card authenticate each other according to a mutually agreed authentication procedure in order to securely communicate with each other.

26. The system according to claim 25, wherein the consumer enters a password of personal identification number (PIN) to enable access the secure interactive service and information stored on the mobile device.

27. The system according to claim 25, wherein a biometric system is provided to enable access to the secure interactive service and information stored on the mobile device if the consumer's scanned biometric data is matched to their record stored in a biometric database.

28. The system according to claim 1, wherein the broadcast infrastructure is satellite television infrastructure.

29. The system according to claim 1, wherein the broadcast infrastructure includes infrastructure capable of carrying digital or analogue signals via terrestrial signals, cables, or wireless systems.

30. The system according to claim 1, wherein the broadcast data is a television broadcast.

31. The system according to claim 1, wherein the digital receiving device is a set-top box, personal video recorder (PVR), or personal digital assistant (PDA).

32. The system according to claim 1, wherein the mobile device of the consumer is connectable to or is embedded into the digital receiving device.

33. The system according to claim 1, wherein the mobile device wirelessly communicates with the digital receiving device.

34. The system according to claim 1, wherein the mobile device is a chip-based card such as a smart card.

35. The system according to claim 1, wherein the mobile device is a mobile computing device such as a Personal Device Assistant (PDA), a palm machine, a notebook, a removable hard disk, a thumb drive, or a mobile phone.

36. The system according to claim 1, wherein identification information relating to the consumer is stored on the mobile device and is read by the digital receiving device.

37. The system according to claim 36, wherein at least the identification information is encrypted and transmitted from the digital receiving device to the return-path host server to enable to the consumer to interact with the secure interactive service, and responses from the secure interactive service based on interaction with the consumer are transmitted via the broadcast infrastructure to the digital receiving device.