

A METHOD AND SYSTEM FOR SECURING DATA ON A FINANCIAL TRANSACTION INSTRUMENT

FIELD OF THE INVENTION

The present invention relates generally to the data security of a multi-functional personal data security device. In particular, the present invention relates to a method and system for securing data of multiple applications associated with multiple entities on a single financial transaction instrument by a dynamic key generation mechanism.

BACKGROUND

A financial transaction instrument can alternatively be termed as a smart card, a memory card, an integrated circuit card, a memory card, a processor card or typically any plastic card that includes one or more semiconductor integrated circuits. Issuance of a smart card requires an initialization process followed by a personalization process. During the initialization process data and data structures that are common to a batch of smart cards are burned into the cards by a card manufacturer such as Gemalto, Oberthur, Philips, Samsung and the like. Instances of such data or data structures can include the serial number of the smart card, a master key of the smart card, currency of the applications to be hosted by the smart card and the like. After initialization, the personalization process follows, which includes, loading the smart card with user data that uniquely identifies the card as belonging to a particular user. The personalization process can be performed in a manufacturing unit using specialized personalization equipment, alternatively known as a field device. Finally the smart card is issued to the user by mail or in person.

Several methods of issuing of smart cards are existing in the prior art, as discussed below. In certain instances, the personalization process takes place as an offline process in the manufacturing unit. In the offline process, a delay is created in the issuance of the smart card, which is a deterrent to the user for applying for the smart card. In another existing method of issuance of smart cards, specialized personalization equipment is deployed, at a Point of Transaction (POT) terminal or at a customer touch-point that can inject user data into the smart

card for instant issuance of the smart card to the user. The specialized personalization equipments being expensive are a deterrent for wide spread deployment thereby raising the entry barrier for the users. Further, for the issuance of multi-application smart cards that can be used across various entities such as banks, hospitals, travel agencies, educational institutions and the like that offer multiple services to the users, the specialized equipment would have to be altered for the different types of smart cards issued and for the various services being offered. Alteration of the specialized equipment for issuance of multi-application smart cards is a known to be a cumbersome, incompatible and expensive process. Hence there is a need for an inexpensive method of instant issuance of multi-application smart cards that can bring down the entry barrier for the users.

Further, the existing smart card models use firmware security tokens for securing data and transactions occurring through the smart card. The firmware security tokens required for controlling access to the various applications and files on the smart card are stored on the network devices available for transaction with the smart cards; such as a card reader, a point of sale terminal or any other computing device, hereinafter referred to as a network device. The firmware security tokens are known to be difficult to deploy and manage for reasons as stated herein. Firstly, though the firmware security tokens are stored in a cryptographic format on the network device, this layer of security has been known to be breached by brute-force methods, data-sniffing techniques, keyboard hooks, magnetic card duplicators, smart card emulators and so forth. Secondly as the entire set of firmware security tokens are stored on the network device, the network device represents a single point of attack for hackers to emulate the functionality of the network device during the authentication phase of the smart card. This poses a severe threat for financial transactions processed through such a fraudulent network device. Thirdly, due to memory limitation of the network device, the permutations of unique firmware security tokens that can be deployed are reduced, thereby limiting the number of smart cards that can be supported. Alternatively if each unique combination of the firmware security tokens is repeated for a bunch of smart cards the security of data on the smart cards gets compromised. The essential drawback of the existing systems concerning the security on the smart cards is due to the use of static data which if obtained, can be used to commit fraud. The industry has focused mainly on preventing the use of this static data, rather than on developing a method of introducing dynamic security tokens on smart cards. Accordingly, a need exists for a system

and method that can use dynamic security tokens on the network devices that can afford a layer of security that is higher than the systems and methods currently in use.

The proposed method describes a method and system wherein the user data is made dynamic in nature and can be instantly loaded on the smart card using a software application. As the user data can be written on the smart card at the customer touch-point or at the POT terminal, the smart card can be issued instantly. Further, the system deploys an inexpensive smart card read and write device thereby lowering the cost of issuance of the smart card and the entry barrier for the users. As a result of using dynamic security tokens, the security issues prevalent earlier at the network devices get resolved.

SUMMARY

The present invention alleviates the above mentioned drawbacks of the existing prior art by providing a method and system for securing the data on a financial transaction instrument by generating a set of keys dynamically on a transaction terminal and loading the set of keys on the financial transaction instrument where the set of keys refer to a set of authorized keys when a user is an authorized user of the financial transaction instrument.

To achieve the aforementioned objective the instant invention provides a method for accessing a user identifier by a transaction terminal where the user identifier is associated with an authorized user and is stored on a financial transaction instrument, generating a set of authorized keys at the transaction terminal using the user identifier where the user identifier is commonly accessed by one or more entities that process transactions through the financial transaction instrument, partitioning the memory of the financial transaction instrument into a set of storage areas by the transaction terminal where each storage area is associated with one of the entities, and allocating the set of authorized keys to the set of storage areas where the set of authorized keys are adapted to perform operations on the data stored in the memory of the financial transaction instrument.

The instant invention also provides a system for securing data on a financial transaction instrument. The system comprises a financial transaction instrument, comprising; a personal file section configured to store a user identifier associated with an authorized user; a key file section

configured to store a master key and a set of authorized keys; and a transaction file section configured to store the data, and a transaction terminal associated with at least an entity that communicates with the financial transaction instrument for processing a transaction. The transaction terminal comprises an interface module configured to provide access to the financial transaction instrument, a repository configured to store a list of instrument identifiers, a set of master keys and an entity identification data of the at least one entity, a key generation module configured to generate a set of keys, a personalization module configured to partition the transaction file section into a set of storage areas and allocate the set of authorized keys to each element of the set of storage areas, and a validation module configured to authenticate any user purporting to process the transaction using the financial transaction instrument.

These and other features, aspects, and advantages of the present invention will become better understood with reference to the following description and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a flowchart illustrating a method of securing data on a financial transaction instrument.

FIG. 2 is a flowchart illustrating a preferred embodiment of a method of securing data on the financial transaction instrument.

FIG. 3 is a flowchart illustrating a method of validating a user of the financial transaction instrument.

FIG. 4 is a flowchart illustrating a preferred embodiment of a method of validating a user of the financial transaction instrument.

FIG. 5 illustrates an exemplary system environment in which features of the present invention can be practiced.

DETAILED DESCRIPTION

In the following detailed description, examples are provided only for a thorough understanding of the present invention, the examples in no way limit the scope of the invention. The present invention may be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. In other embodiments, well known methods, procedures, components and circuitry have been described at a relatively high-level, without detail, in order to prevent unnecessary obscuring the aspects of the present invention. The word 'or' as used is in hereinafter is to be interpreted as an inclusive or.

The present invention is applicable to financial transaction instruments 502(refer FIG. 5), also termed as but not limited to smart cards, chip cards, integrated circuit cards, memory cards, or processor cards. A method and system for instant issuance of smart cards using an inexpensive read or write transaction terminal for bringing down the entry barrier for users is illustrated herein below. The system includes software driven security infrastructure management system to provide a transaction terminal 512(ref FIG. 5) that can issue the smart cards instantly in an inexpensive manner. Further, the software driven security infrastructure management system, provides a dynamic key generation process for validating a user purporting to perform a transaction through the smart card.

Basic components of the system that are preferably required for practicing an embodiment of the present invention are a card manufacturer, a card issuer that undertakes the functionality of issuing the smart card instantly at the transaction terminal 512, and the transaction terminal 512 that is preferably the point of contact for the user on the field and the financial transaction instrument 512. The transaction terminal 512 can be any suitable terminal such as are known in the art for reading from and writing to, financial transaction instrument, smart cards, integrated circuit cards, chip cards and the like. The transaction terminal 512 can be any suitable interface device that can transfer information and commands between the financial transaction instrument 512 and the user or a computing device. Further, the transaction terminal 512 can include a processor, application software, and the ability to communicate over a network. The transaction terminal 512 can take a variety of physical forms such as; a standalone unit integrated with a computer and a keyboard of the computer or it can be built into a memory disk that is capable of being read from; a disk drive of a computer; or a portable device such as a laptop, a cellular

phone or a personal digital assistant (PDA). The transaction terminal 512 are alternatively also termed as but not limited to an interface device (IFD), a chip-accepting device (CAD), a chip card reader (CCR), a smart card adapter and a card reader device.

The card manufacturer is responsible for manufacturing the financial transaction instrument 502. Instances of card manufacturers are Gemalto, Oberthur, Philips, Samsung and the like. The card issuer may be an entity such as a bank, a financial institution, a service association, a merchant, or any other organization or agent acting on behalf of such organization. The card issuer, hereinafter referred to as the entity, deploys the transaction terminal 512 in a field for interacting with the users and for issuing the financial transaction instruments to the users. An entity identification data is usually stored on the transaction terminal 512. The entity identification data is used during processing of the transactions initiated by the financial transaction instrument 502. In an embodiment of the invention the entity identification data can be a bank identification number or a bank code when the entity is preferably a bank. The smart card can be a blank card such as a Smart Card Operating System for Transport Application (SCOSTA), a MiFare card or a DESFire8 card. An open platform smart card is recommended for performing the present invention, as applications can be added to such a smart card post-issuance for making the smart card multi-purpose in nature. The Open Platform smart card is capable of including multiple ownership by various entities and running the various applications offered by each such entity.

The issuance of the smart card undergoes certain basic steps such as initialization, personalization and loading of application codes required for running applications provided by the entities. The initialization process is usually carried out by the card manufacturer. During the initialization process data and data structures that are common to a set of smart cards are installed on the financial transaction instrument 502. An instance of the data that can be common to a set of smart cards is a master key. Post initialization a set of master keys associated with the set of smart cards generated by each card manufacturer are distributed by an authentic Key Management Authority (KMA) to the various entities that seek to transact with the financial transaction instrument 502. The KMA can be a special kind of Certification Authority that controls the distribution of the set of master keys amongst the entities that intend to be associated with the financial transaction instrument 502. The entities can retrieve and verify an

authenticity certificate of an individual financial transaction instrument card, and encrypt their proprietary application code and confidential personalization data using that financial transaction instrument's master key. The set of master keys distributed to one entity are kept confidential with the KMA. After the initialization process, a personalization process follows, which may be performed by the card manufacturer for the set of smart cards that are to be used for a specific purpose, or individually by the entity. During the personalization process, the smart card is preferably loaded with data that uniquely identifies the user of the financial transaction instrument 502. For example, the personalization data can include a user identifier, a personal identification number of the user, a social security number of the user and a biometric identification data of the user and a set of authorized keys. In a preferred embodiment the user identifier can be a unique identification code that uniquely identifies the user. The user identifier can be utilized by the transaction terminal 512 to generate the set of authorized keys. In an embodiment of the invention the biometric identification data can include the fingerprint details of the user, the iris scan details, the blood identification data and the like. A personalization equipment, alternatively referred to as a personalization module 520 (refer FIG. 5), is disposed at the transaction terminal 512 for the personalization process. After the personalization process, entity identification data and application codes associated with applications required by the entity for processing transactions on the smart card are loaded on the smart card by the personalization module 520. The entity identification data can be a unique entity identification code associated with the entity. Post loading of the personalization data and the application codes on the smart card, the smart card is issued to the user or distributed to the user.

FIG. 1 illustrates the basic steps performed by the system for securing data on the financial transaction instrument during the personalization process. At step 102, the transaction terminal 512 accesses the user identifier stored on the financial transaction instrument 502. The user identifier is usually associated with an authorized user of the financial transaction instrument 502. The authorized user is basically the user in whose name the financial transaction instrument has been issued. In step 104, the transaction terminal 512 uses the user identifier to generate the set of authorized keys. The user identifier is usually a data that can be commonly accessed by all the entities that communicate with the financial transaction instrument 502. The user identifier signifies the access point or the entry point to the data that is stored on the financial transaction instrument 502. The user identifier can be accessed only when the authorized user purports to

use the financial transaction instrument for the transaction. Further, at step 106, a memory structure on the financial transaction instrument is partitioned into separate storage areas or memory cells, each storage area being associated with one of the entities that can communicate with the financial transaction instrument 502. For instance, if the entity is a bank, the transaction terminal 512 associated with the bank shall make a partition from the memory structure to store the data associated with the transaction to be carried out in association with the bank. The data can include the personalization data, customer personal details of the user required for registration with the bank, the entity identification data of the bank such as the bank code, and data associated with the transaction. In an embodiment of the invention the personalization data can be stored in a personal file section 504 (refer FIG. 5) of the financial transaction instrument 502 (refer FIG. 5). In an embodiment of the invention the customer personal details can include customer name as it appears on bank records, customer address, customer city, customer state, customer country, status, customer date of birth, ration card number, driver's license number, voter ID number, national ID, account number, account name, account type, product type, account currency, account balance, account status, and any other customer update data. Further, the entity identification code, the customer details and the data associated with the transaction can be stored in the transaction file section 508 (refer FIG. 5) of the financial transaction instrument 502. The set of authorized keys are stored in an area allocated for the entity in the key file section 506 (refer FIG. 5) of the financial transaction instrument 502. Finally, at step 108, the set of authorized keys are allocated to the storage area partitioned by the transaction terminal 512 for the entity. The set of authorized keys are configured to perform a plurality of operations on the data stored in the transaction file section 508 such as delete, read, write, modify, update and the like.

FIG. 2 illustrates a preferred embodiment of securing data on the financial transaction instrument during the personalization process. The financial transaction instrument bears a instrument identifier which is read by a card reader interface of the transaction terminal 512 at step 202. The card reader interface includes any of the conventionally known software and hardware, necessary for communication with devices external to the transaction terminal 512. In a preferred embodiment the transaction identifier can be a serial identification number of the smart card, the serial identification number being hardware encoded into the smart card during manufacturing process of the card. At step 204, the instrument identifier read from the financial transaction

instrument is matched to a instrument identifier that is preferably stored in a card manufacturer record 516a (refer FIG. 5) of a repository 516 (refer FIG. 5) on the transaction terminal 512. The card manufacturer record 516a may include the instrument identifier of the financial transaction instrument and the master key associated with the financial transaction instrument, the master key required for gaining access to the financial transaction instrument 502. The master key stored across the instrument identifier that matches to the instrument identifier of the financial transaction instrument 502, in the card manufacturer record 516a, is retrieved by an interface module 514 (refer FIG. 5), disposed within the transaction terminal 512. The master key is used by the interface module 514 to gain access to the user identifier 504a (refer FIG. 5) of the financial transaction instrument 502 at step 206. The user identifier 504a is used by the transaction terminal 512 to read the personal identification data of the user stored in the personal file section 504 (refer FIG. 5) of the financial transaction instrument 502. The personal identification data of the user can include, a personal identification number (PIN), a social security number such as a National ID, and a biometric identification data. The biometric identification data can include fingerprint data, iris scan data, blood group, and the like. Further, the transaction terminal 512 retrieves the entity identification data stored at a storage area 532 in the repository 516 of the transaction terminal 512 at step 208. At step 210, the entity identification data, the personal identification data and the user identifier are used as inputs to a unique function, provided by the entity, for computing the set of authorized keys for the user. The unique function could be a random function logic that can be determined by the entity and stored fed into the memory of the key generation module 518 (refer FIG. 5) of the transaction terminal 512. For example, a key K1, for reading data stored in the transaction file section 508 can be computed by the random function logic such as $K1 = \sum(\text{the user identifier, the PIN, numeral 5})$, where, $\sum$ stands for summation of parameters following, K1 stands for the key to be used for reading data. As a result hypothetically if the user identifier is 5678, the PIN is 5028, then K1 shall equate to $5678 + 5028 + 5 = 11711$. Consequently the value 11711 is the authorized value of K1 required for reading data from the transaction file section 508 for the entity. At step 212, the memory structure in the key file section 506 is partitioned by the transaction terminal 512 to store the set of authorized keys (step 214) and the memory area of the transaction file section 508 is further partitioned to secure one or more storage area for storing the data associated with the transaction, and details of the user in specific relationship with the entity

(step 220). The set of authorized keys are allocated to the one or more storage areas at step 218. The set of authorized keys are configured to perform a plurality of operations on the data stored in the transaction file section 508 such as delete, read, write, modify, update and the like. As the personalization process is conducted by the generation of keys dynamically at the transaction terminal 512, the financial transaction instrument 502 can be issued instantly by the transaction terminal itself. The authentication of the personal details of the user as required for populating the transaction file section 508 can be processed by any of the conventionally known methods and processes. As a result, the use of software-driven logic for generating the set of authorized keys aids in the instant issuance of the financial transaction instrument 502 instantly. Consequently, the entry barrier for the users, that otherwise existed in the prior systems of issuing financial transaction instruments, is minimized to a considerable extent.

FIG. 3 illustrates the essential steps required in the method for validating a user of the financial transaction instrument, the user being any user purporting to use the financial transaction instrument for the transaction. In the event the user is the authorized user of the financial transaction instrument, access to perform the transaction shall be given to the user, however, in the event the user is a fraudulent user the access shall be denied. At step 302, the user identifier 504a, stored in the personal file section 504 of the financial transaction instrument 502 is accessed by the transaction terminal 512 when the financial transaction instrument 502 is brought in connection to the card reader interface of the transaction terminal 512. The user identifier is explained to be associated with the authorized user of the financial transaction instrument. At step 304, a set of keys, are generated using the user identifier 504a, personal details of the user and entity identification data stored in 532 of the repository 516 of the transaction terminal. The set of keys, are generated by the unique function fed into the key generation module 518, by the entity. As the unique function used to generate the set of keys is the same as used to generate the set of authorized keys during the personalization process, the set of keys generated must match the set of authorized keys for a valid user. At step 306, the transaction terminal reads the set of authorized keys associated with the authorized user, from the key file section 506, of the financial transaction instrument 502. Finally at step 308, the set of keys, are compared to the set of authorized keys to conclude if the user is the authorized user. In the event the set of keys differ from the set of authorized keys, the user is denied access to perform the transaction through the financial transaction instrument. However, in the event the

set of keys match the set of authorized keys the user is authenticated as the authorized user and is given access to perform the transaction.

FIG. 4 illustrates a preferred embodiment of a method for validating a user of the financial transaction instrument 502. At step 402, the transaction terminal 512 reads the instrument identifier of the financial transaction instrument 502. At step 404, the instrument identifier read from the financial transaction instrument 502 is preferably matched to an instrument identifier that may be stored in a card manufacturer record 516a of the repository 516 on the transaction terminal 512. The card manufacturer record 516a may include the instrument identifier of the financial transaction instrument and the master key associated with the financial transaction instrument, the master key required for gaining access to the financial transaction instrument 502. The master key stored across the instrument identifier that matches to the instrument identifier of the financial transaction instrument 502, in the card manufacturer record 516a, is retrieved by the interface module 514, disposed within the transaction terminal 512. The master key is used by the interface module 514 to gain access to the user identifier 504a of the financial transaction instrument 502 at step 406. At step 408, personal identification data of the user is captured by an input module 524 (refer FIG. 5) at the transaction terminal 512. The input module can comprise of a standard keyboard, a scanning machine, a camera and other devices that can capture data of the user. The personal identification data of the user can include, a personal identification number (PIN), a social security number such as a National ID, and a biometric identification data. The biometric identification data can include fingerprint data, iris scan data, blood group, and the like. Nature of the personal identification data captured by the user shall be similar to that as captured of the authorized user during the personalization process for generation of the set of authorized keys. Next, the transaction terminal 512 retrieves the entity identification data stored at 532 in the repository 516 of the transaction terminal 512 at step 410. Further at step 412, the entity identification data, the personal identification data of the user and the user identifier are used as inputs to the set of unique function for generating the set of keys. The unique function used to generate the set of keys is the same function as used to generate the authorized set of keys. The set of unique functions is stored in the key generation module 518 of the transaction terminal 512. The set of keys generated at the transaction terminal 512, are compared to the set of authorized keys read from the key file section 506, at step 414. In the event the set of keys match the set of authorized keys, the user is authenticated as the authorized

user of the financial transaction instrument 502, at step 418, and is provided access to perform one or more transactions, step 420. However, in the event the set of keys generated do not match the set of authorized keys the user is denied access to the financial transaction instrument, step 416. As a result the security of the financial transaction instrument is protected from being breached by a fraudulent user whose personal identification data do not match with those of the authorized user as stored in the personal file section 504.

As only the set of unique functions for generation of the set of keys is stored on the transaction terminal 512, the need for storing the set of authorized keys on the transaction terminal is eliminated. Dynamic generation of keys at the time of validation of the user provides the essential security required for financial transaction instruments. Further the only data that needs to be stored on the transaction terminal is the master key associated to the financial transaction instrument. A single master key can be used to generate a large number of keys using different set of unique functions. As a result, a large number of financial transaction instruments, each having a unique set of keys, can be supported by the same master key. The necessary consequence of using the unique set of functions to generate the set of keys dynamically is the memory limitation of the transaction terminals is overcome as a large number of financial transaction instruments having a unique set of keys can be processed through the same transaction terminal using the same master key.

Fig. 5 illustrates an environment in which various embodiments of invention can be practiced. The environment 500 includes the user 528, the financial transaction instrument 502, and the transaction terminal 512. The financial transaction instrument 502 includes a memory structure 530, which further includes a personal file section 504, a key file section 506 and a transaction file section 508. The personal file section is configured to store the user identifier 504a and the personal identification data of the authorized user. The key file section 506 comprises a set of separate storage areas for storing the set of authorized keys of the authorized user. For instance, the set of authorized keys in association with the entity can be stored in a separate storage area 506a. The transaction file section 508 stores the data associated with the transaction carried out by the financial transaction instrument 502 in communication with the transaction terminal 512. The data includes the user personal details as required by the transaction terminal 512 for

processing the transaction, the entity identification data of the entity associated with the transaction terminal 512 and other transaction details.

The transaction terminal 512 includes the repository 516, the interface module 514, a personalization module 520, a validation module 522, the key generation module 518, the input module 524 and an output module 526. The repository 516 can be a suitable database file as known in the art for containing a set of card manufacturer records. A card manufacturer record 516a can include the instrument identifier of the financial transaction instrument 502 and the master key used to access the financial transaction instrument 502. Further, the repository can be configured to store a set of entity identification data at a storage area 531 of the repository 516, each entity identification data shall be associated with the entity that can communicate with the financial transaction instrument 502 through the transaction terminal 512. The interface module 514 provides the necessary interface required for initiating communication with the financial transaction instrument 502. The interface module can include a card reader interface for reading the instrument identifier stored on the financial transaction instrument 502, when the financial transaction instrument 502 is brought in contact with the transaction terminal for the purpose of processing the transaction. A wide variety of card reader interfaces as conventionally known can be employed within the interface module 514 for communication with the financial transaction instrument 502. By way of example, the interface may provide a contact interface, a remote-coupled interface, or a variety of other interfaces. In a contact interface, signals from an integrated circuit disposed at the financial transaction instrument 502 are routed via metal contacts to the outside of the financial transaction instrument 502, which then come in contact with similar contacts present on the card reader interface. Other interfaces include wireless transmission of signals from the financial transaction instrument 502 to the card reader interface of the interface module 514. In an embodiment of the invention, the interface module can use electrical connections embedded within the transaction terminal 512, to read a set of card manufacturer records 516a, 516b up to 516n, from the repository 514. Subsequently, the interface module 514 shall use comparison logic to search the instrument identifier read from the financial transaction instrument 502 within the list of instrument identifiers existing in the set of card manufacturer records, 516a, 516b up to 516n read from the repository 514. In the event the instrument identifier is found in the set of card manufacturer records, 516a, 516b up to 516n, it signifies that the transaction terminal 512 is equipped with the necessary application required for

processing the transaction. However, in the event the instrument identifier is not found in the set of card manufacturer records, 516a, 516b up to 516n, the financial transaction instrument shall be denied access to perform the transaction through the transaction terminal and the transaction terminal shall be denied access to the financial transaction instrument. In the event the instrument identifier is found in the list of instrument identifiers, the master key stored against the instrument identifier in the list of instrument identifiers is retrieved. The master key is the access code to the financial transaction instrument 512. In an embodiment of the invention the master key can be provided to the operating system of the financial transaction instrument 502 to retrieve the user identifier of the authorized user. In an embodiment of the invention the user identifier can be stored in a storage area 514a of the personal file section 504. The user identifier can include a personal identification data or a unique identification number of the authorized user. Hence to gain access into the financial transaction instrument 502, the interface module 514, provides the master key to the operating system of the financial transaction instrument 502, and receives the user identifier in response.

Further, the personalization module 520 uses the retrieved user identifier for the personalization process of the financial transaction instrument. In an embodiment of the invention, the personalization process involves, generating the set of authorized keys and storing the personal identification data of the authorized user in the personal file section. In an embodiment of the invention the personalization module 520 reads the key inputs required for generation of the set of authorized keys. In an embodiment of the invention, the key inputs can include the user identifier as read from the interface module 514, the entity identification data read from the storage area 532 of the repository 516, and the personal identification data of the authorized user as received by the input module 524. The input module 524 can be any device suitable for receiving data that is inserted or provided by the user. Instances of the input module 524 can include a keyboard, a touch screen, a scanning machine, or any other data sensing device. The input module 524 can be enabled with bio-metric authentication for benefitting the illiterate. The bio-metric authentication can also be used for authenticating a field agent who operates the transaction terminal thereby improving the security of the financial transaction instrument transactions.

Further, the key generation module 518 is designed computes the value of the set of unique functions when the key inputs are provided. The set of unique functions are defined by the entity. Value of the set of unique functions comprises the set of authorized keys which are stored by the personalization module 520 into a key storage area 506a of the key file section 506. The key storage area 506a represents the area where the set of authorized keys associated with the particular entity are stored. The set of authorized keys of different entities shall be stored in separate storage areas such as 506a, 506b, 506c, up to 506n. Each key of the set of authorized keys are configured by the key generation module 518 to perform various operations such as add, modify, delete, read, write, and update data in the personal file section 504 and the transaction file section 508 of the financial transaction instrument 512. In an embodiment of the invention, the personalization module 520 is designed to partition the transaction file section into one or more storage areas. Each of the storage area can store the data associated with the transactions associated with various entities and applications. The criteria of partitioning the transaction file and the manner in which data would be stored in the transaction file section can be set as per techniques conventionally known. On partitioning the transaction file, the personalization module 520 defines which of the set of authorized keys shall hold the access and modification permissions to the partitioned storage area.

In an embodiment of the present invention authorizing the user for performing the transaction using the financial transaction instrument 502 is carried out by the validation module 522. The validation module 522, receives the key inputs such as the personal identification data of the user from the input module 524, the entity identification data as stored in 532 and the user identifier from the interface module 514. Further the validation module provides the key inputs to the key generation module 518. The key generation module 518 generates the set of keys in response to the key inputs provided. The set of keys are generated using the same set of unique functions as used during the personalization process, and hence if the user is the authorized user the set of keys ought to match with the set of keys stored in the personal file section 506. In order to compare the set of keys to the set of authorized keys the validation module reads the set of authorized keys from the key storage area 506a of the personal file section 506 and provides the set of keys and the set of authorized keys to a comparator function logic. In the event the set of keys are similar to the set of authorized keys, the comparator function logic outputs a positive response signifying that the user is the authorized user. On receiving the positive response the

validation module 522, provides access to the user for performing the transaction. However, in the event the set of keys differ from the set of authorized keys, the comparator function logic outputs a negative response, indicating that the user is a fraudulent user and ought not to be given access to perform the transaction. In response to the negative response of the comparator function logic, an authentication failure message is composed by the validation module 522 and sent to the output module 526 for displaying it to the user. The output module 526 can include any suitable device that can display messages such as a computer screen, an LED display, a LCD or any display of the portable device.

While the foregoing has described certain embodiments and the best mode of practicing the invention, it is understood that various implementations, modifications and examples of the subject matter disclosed herein may be made. It is intended by the following claims to cover the various implementations, modifications, and variations that may fall within the scope of the subject matter described.

CLAIMS

What is claimed is:

1. A method of securing data on a financial transaction instrument comprising:

accessing a user identifier by a transaction terminal, the user identifier being associated with an authorized user and stored in the financial transaction instrument;

generating a set of authorized keys by the transaction terminal using the user identifier, the user identifier being common amongst at least one entity;

partitioning a memory structure on the financial transaction instrument into one or more storage areas by a transaction terminal, whereby the one or more storage areas are configured to store data associated with the at least one entity; and

allocating the set of authorized keys to the one or more storage areas, whereby the set of authorized keys is configured to perform a plurality of operations on the data.

2. The method of claim 1, wherein the step of accessing a user identifier comprises:

reading a instrument identifier of the financial transaction instrument by the transaction terminal;

mapping the instrument identifier to a master key by an application installed at the transaction terminal, whereby the master key is stored on the transaction terminal; and

securing access to the user identifier using the master key;

3. The method of claim 2, wherein the master key is associated with the financial transaction instrument.

4. The method of claim 1, wherein the user identifier comprises a unique identification data of the authorized user.
5. The method of claim 1, wherein the set of authorized keys is associated with the authorized user and the at least one entity.
6. The method of claim 1, wherein the transaction terminal is associated with the at least one entity.
7. The method of claim 1, further comprising:
capturing a personal identification data of the authorized user by the transaction terminal; and
fetching an entity identification data associated with the at least one entity.
8. The method of claim 7, wherein the step of generating a set of authorized keys comprises computing values of a set of unique functions at the transaction terminal.
9. The method of claim 8, wherein inputs to the set of unique functions comprises the user identifier, the entity identification data of the at least one entity and the personal identification data of the authorized user.
10. The method of claim 8, wherein the set of unique functions is provided to the transaction

terminal by the at least one entity.

11. The method of claim 6, wherein the entity identification data comprises a unique identification code associated with the at least one entity.

12. The method of claim 6, wherein the entity identification data is stored in a repository of the transaction terminal.

13. The method of claim 6, wherein the entity identification data is provided to the transaction terminal by the at least one entity.

14. The method of claim 6, wherein the personal identification data of the authorized user comprises at least one of a personal identification number, a social security number, and a biometric identification data.

15. The method of claim 1, wherein the data is associated with one or more transactions carried out by the authorized user of the financial transaction instrument in communication with the transaction terminal.

16. The method of claim 1, further comprising storing the set of authorized keys in the financial transaction instrument.

17. The method of claim 1, wherein the plurality of operations comprises read, write, add, modify, delete and update functions.

18. A method of validating a user of a financial transaction instrument, the method comprising:
accessing a user identifier by a transaction terminal, the user identifier being associated with an authorized user and stored in the financial transaction instrument;
generating a set of keys by the transaction terminal, the transaction terminal being associated with at least one entity;
retrieving a set of authorized keys by the transaction terminal, the set of authorized keys being stored in the financial transaction instrument; and
comparing the set of authorized keys to the set of keys generated by the transaction terminal.

19. The method of claim 18, wherein the step of accessing a user identifier further comprises:
reading a instrument identifier of the financial transaction instrument by the transaction terminal;
mapping the instrument identifier to a master key by an application installed at the transaction terminal, the master key being stored in the transaction terminal; and
securing access to the user identifier using the master key.

20. The method of claim 19, wherein the master key is associated with the financial transaction instrument.

21. The method of claim 18, wherein the user identifier comprises a unique identification data of the authorized user.

22. The method of claim 18, wherein the set of authorized keys is associated with the authorized user and the at least one entity.

23. The method of claim 18, further comprising:
capturing a personal identification data of the user by the transaction terminal; and
fetching an entity identification data associated with the at least one entity.

24. The method of claim 23, wherein the step of generating the set of keys at the transaction terminal comprises computing the value of a set of unique functions at the transaction terminal.

25. The method of claim 24, wherein inputs to the set of unique functions comprises the user identifier, the entity identification data of the at least one entity and the personal identification data of the user.

26. The method of claim 24, wherein the set of unique functions is provided to the transaction terminal by the at least one entity.

27. The method of claim 25, wherein the personal identification data of a user comprises at least

one of a personal identification number, a social security number and a biometric identification data.

28. The method of claim 23, wherein the entity identification data comprises a unique code associated with the at least one entity.

29. The method of claim 23, wherein the entity identification data is stored in a repository of the transaction terminal.

30. The method of claim 23, wherein the entity identification data is provided to the transaction terminal by the at least one entity.

31. The method of claim 18, wherein the step of comparing the set of authorized keys to the set of keys generated at the transaction terminal further comprises:

authenticating the user as the authorized user when the set of keys generated at the transaction terminal match the set of authorized keys; and

denying the user access to the financial transaction instrument when the set of keys generated at the transaction terminal differ from the set of authorized keys.

32. The method of claim 31, wherein the step of authenticating the user as the authorized user further comprises providing the user access to perform one or more transactions through the financial transaction instrument.

33. A system for securing data on a financial transaction instrument comprising:

a memory structure disposed at the financial transaction instrument, the memory structure comprising:

a personal file section configured to store a user identifier, the user identifier being associated with an authorized user;

a key file section configured to store a master key and a set of authorized keys; and

a transaction file section configured to store the data; and

a transaction terminal associated with at least one entity configured to communicate with the financial transaction instrument, the transaction terminal comprising:

an interface module configured to provide access to the financial transaction instrument;

a repository configured to store a list of instrument identifiers , a set of master keys, and an

entity identification data of the at least one entity;

a key generation module configured to generate a set of keys when key inputs are provided;

a personalization module configured to partition the transaction file section into the one or more storage areas and allocate the set of authorized keys to each of the one or more storage areas ; and

a validation module configured to authenticate a user of the financial transaction instrument.

34. The system of claim 33, further comprising an input module disposed at the transaction terminal configured to accept a personal identification data.

35. The system of claim 33, wherein the set of authorized keys is associated with the authorized user.

36. The system of claim 33, wherein the user identifier comprises a unique identification number of the authorized user.

37. The system of claim 34, wherein the personal file section further comprises the personal identification data of the authorized user.

38. The system of claim 33, wherein one of the instrument identifier from the list of unique identifiers is associated with the financial transaction instrument.

39. The system of claim 33, wherein the entity identification data comprises of a unique code associated with the at least one entity.

40. The system of claim 33, wherein the entity identification data is provided to the transaction terminal by the at least one entity.

41. The system of claim 33, wherein the interface module comprises of:

means for reading a instrument identifier stored on the financial transaction instrument;

means for mapping the instrument identifier to the master key when the instrument identifier matches to an entry in the list of instrument identifiers stored in the repository;

means for capturing the user identifier from the personalization file section using the master key; and

means for denying access to the financial transaction instrument when the instrument identifier does not match to an entry in the list of instrument identifiers.

42. The system of claim 33, wherein the key generation module is further configured to compute

the value of a set of unique functions using the key inputs, the set of unique functions being

provided by the at least one entity.

43. The system of claim 34, wherein the personalization module comprises of:

means for providing the key inputs to the key generation module, wherein the keys inputs comprise the user identifier, the entity identification data of the at least one entity and the personal identification data of the authorized user;

means for storing the set of keys generated by the key generation module as the set of authorized keys in the key file section; and

means for assigning the set of authorized keys to the one or more of the storage areas.

44. The system of claim 43, wherein the personalization module further comprises:

means for receiving the personal identification data of the authorized user from the input module;

means for accessing the user identifier from the interface module;

means for reading the entity identification data of the at least one entity from the repository;

45. The system of claim 44, wherein the personal identification data of the authorized user comprises at least one of personal identification number, social security number and a biometric identification data of the authorized user.

46. The system of claim 33, wherein the each of the one or more storage areas is associated with one or more of the at least one entity.

47. The system of claim 33, wherein the set of authorized keys are configured to perform a plurality of operations on the data stored in each of the one or more storage areas.

48. The system of claim 47, wherein the plurality of operations comprises of read, write, add, modify, delete and update functions.

49. The system of claim 44, wherein the personalization module further comprises of means for storing the personal identification data of the authorized user in the personal file section.

50. The system of claim 34, wherein the validation module comprises of:

means for providing the key inputs to the key generation module, wherein the key inputs comprises the user identifier, the entity identification data of the at least one entity and the personal identification data of the user;

means for accessing the set of authorized keys from the key file; and

means for comparing the set of keys generated by the key generation module to the set of authorized keys.

51. The system of claim 50, wherein the validation module further comprises:

means for receiving the personal identification data of the user from the input module;

means for reading the entity identification data of the at least one entity from the repository; and

means for accessing the user identifier from the interface module;

52. The system of claim 50, wherein the validation module further comprises:

means for authenticating the user as the authorized user when the set of keys generated by the key generation module match the set of authorized keys; and

means for denying the user access to the financial transaction instrument when the set of keys generated by the key generation module differ from the set of authorized keys.

53. The system of claim 52, wherein means for denying access to the financial transaction

instrument comprises of an output module, the output module configured to display the user authentication failure message.

54. The system of claim 53, wherein the output module is further configured to provide the data

to the transaction file section, the data being associated with one or more transactions processed by the transaction terminal and the financial transaction instrument.

55. The system of claim 54, wherein the means for authenticating the user further comprises providing the user access to perform the one or more transactions.

56. The system of claim 51, wherein the personal identification data of the user comprises at least one of a personal identification number, a social security number and a biometric identification data of the user.