AN ELECTRONIC PAYMENT SYSTEM AND METHOD OF PAYMENT

Field of Invention

The invention relates to a system for making prepaid, credit or debit payment transaction among the online community (mobile user, online retailer, games hub and etc.), and also for transactions in the traditional contactless payment and transport environment.

Background

Electronic payments are increasingly popular more so with the increasing use of electronic mobile devices. Electronic wallets have been proposed. However ensuring the electronic payments and details such as Bank accounts, Payment transaction details and payee details are secured is still a major concern.

WO 2013029095 describes an electronic payment method where user payment request data is transmitted from a mobile device, the user payment request data comprising a payment amount and a merchant identifier; checking a user record corresponding to the mobile device to determine based on at least one payment rule whether to generate merchant payment data corresponding to the payment amount of the user payment request data.

WO 2012 166790 describes a method for receiving a request to process, against an electronic wallet, a portion of a transaction, an electronic wallet optionally comprising a sub-wallet, the transaction processed against the wallet and/or sub-wallet.

WO 2012 154189 describes the use of Mobile payments and processing data related to electronic transactions using a near field communication connection. Authorization data is shared between the mobile communication device and the electronic payment device without providing electronic payment instrument (e.g. credit card) data to the merchant. Authorization data is transmitted from the mobile communication device to a cloud computer or resource that serves as a cloud wallet and hosts respective data of respective electronic payment instruments of respective consumers, and from the electronic payment device a payment processor computer.

Summary of Invention

In the invention, mobile user shall use any of the existing standard payment top up methodology to purchase the prepaid value, if platform configured as prepaid payment solution. Approved credit shall be given to online community service provider merchant bank account. Online community service provider shall then prompt the respective user on the approval credit via the existing data exchange flow mechanism. A host terminal emulator platform been introduced in this invention, as mechanism to load the approved credit amount into the handset's digital wallet.

In the invention, mobile user allow to transfer funds in their prepaid, credit or debit application to other mobile user within the online community. The introduced host terminal emulator platform shall provide the mechanism to transfer money out from the user digital wallet, and to load the transferred and approved money into the digital wallet of the other user of a second electronic mobile device. Alternatively the recipient could be a merchant using a POS. Data exchange flow between 2 mobile users shall use the existing mechanism.

In the invention, the electronic mobile device shall able to carry out a transaction at any POS in the existing contactless payment environment.

Summary of Claims

A first object of the invention is an electronic payment system for processing an electronic transaction involving a consumer using a mobile electronic device and a merchant, wherein the mobile electronic device and an electronic payment device of the merchant are used for making a transaction including transfer of a pre-paid, credit or debit money of the consumer using the mobile electronic device as payment for the transaction , said mobile electronic device having a Mobile Application (MA) and a Payment Application residing in a Card Emulator (CE) Application, or secure element, or embedded secure element including

a Host Terminal Emulator Platform (HTE) which acts as an interface medium between MA processing the transaction requests to a Card Emulator Application, or secure element, or embedded secure element.

Preferably, the HTE has a HTE Driver and an Interrupt Service Handler which periodically receives data from the OS and checks if there is any new set of data be loaded into a shared memory area [F] in a MA OS Layer via the HTE Driver.

Preferably, the HTE has a set of software API for payment request activation and payment data exchange between MA and HTE.

In addition, the HTE comprises the following:-

- A module to interface MA with payment application reside in CE, Se or ESE.
- A module to manage the secure channel processes for entire transaction by using secure entity of SecretKeys which can be formatted in symmetric or asymmetric key, and generating the Payment Security Session Keys, Security Session Tokens and encrypted data component.
- A module to preform debit and credit to payment application.
- A module to translate the mobile application's payment enquiry input data to a set of transaction commands.

A second object of the invention is a method of payment using the HTE as claimed in Claim 1, wherein the MA shall trigger a payment request according to one of the proposed data path [B] [Terminal API →B1 → B2 → B1 → Terminal API] and where upon, the MA shall initiate *Secure Session (1), which* request the HTE via defined API and sends *Session Key Token (1), SKT (1),* account UID to HTE.

Preferably, the method of payment using the HTE wherein the user also can trigger the payment request according to one of the proposed data path [D] [Terminal API →D1 → D2 → D2 → D1 → Terminal API] and where upon, the MA shall initiate *Secure Session (1), which* request the HTE via defined API and sends *Session Key Token (1), SKT (1),* account UID to HTE.

Preferably, the method of payment using the HTE comprises a step to transfer prepaid, credit or debit mobile money out from a digital wallet 's card emulator, or secure element or embedded secure element. *SKT (1)*, wherein MA shall send SKT (1) request to MA backend provider. The requests shall include data such as Account UID and dynamical seed component (e.g. occurrence event's date time). MA backend provider shall use Secret Key 0 and MA requests data to generate *SKT (1).*

Preferably, the method of payment using the HTE further comprises loading transferred approved credit money to a digital wallet' card emulator, secure element, or embedded secure element. *SKT (1)* wherein MA shall send SKT (1) request to MA backend provider. The requests shall include data such as Account UID, dynamical seed component (e.g. occurrence event's date time) and approved transfer amount. MA backend provider shall use Secret Key 0 and MA requests data to generate *SKT (1).*

Preferably, the method of payment using the HTE further generating and storing the Random Seed in [G, G'', G'''] which is initiated by HTE.

Preferably, the method of payment the HTE validates the MA's *SKT (1),* if *SKT (1)* credential requirement satisfied, HTE activate Secret Key [1]'s access condition, and proceed to generate *Payment Session Key (1).* PSK (1), is then shared with MA via defined API.

Preferably, in the method of payment using the HTE, the PSK (1) shall be generated from *STK (1)*, account UID, Random Seed *and* Secret Key [1].

Preferably, the method of payment using the HTE includes use of a *Payment Session Security Token (1), PSST (1)* is generated by the MA wherein said PSST (1) is derived from data [Format B'] and *PSK (1).*

Preferably, the method of payment using the HTE wherein the Data [Format B'] and *SKT' (1)* shall be encrypted by using PSK (1), *SKT' (1)* shall be 1st order derivation from *SKT (1).*

Preferably, the method of payment using the HTE includes the step of the HTE

validating the PSST *(1)* upon receiving an encrypted [Format B'] || *PSST (1)* via defined API from MA.

Preferably, in the method of payment using the HTE, whereupon the validation of PSST (1), the Format B' is converted to Format B" [n], which contain set of payment transaction command (e.g. Select, GPO, read record, PIN verification and Generic Application Cryptogram [TC/ARQC], update record) and activates a SecrectKey2 and other payment Secret Keys access condition; If *PSST (1)* credential requirement satisfied, said, PSST (1) Validation, Secret Keys activation, and encrypted Data Format B' decryption being performed in [G, G' G"'] environment.

Preferably, in the method of payment using the HTE, further includes producing a *Payment Session Security Token (2), PSST (2),* which is derived from Data Format B" [n], the Random Seed and SecretKey2.

Preferably, in the method of payment using the HTE, the Data [Format B"] and *SKT" (1)* shall be encrypted by using SecretKey2, and *SKT" (1)* shall be 2nd order derivation from *SKT (1).*

Preferably, the method of payment using the HTE includes storing the SecretKey2 inside [G, G' G"'], and wherein the *PSST (2)* calculation, *SKT (1)* 2nd order transformation and data [Format B"] encryption is performed in [G, G', G"'].

Preferably, in the method of payment using the HTE, encrypted Data Format B" [n] || *PSST (2),* is loaded into the shared memory area, [F].

Preferably, in the method of payment using the HTE, encrypted Data Format B" [n] || *PSST (2),* is send to secure element, or embedded secure element via existing smartcard ISO standard communication protocol.

Preferably, in the method of payment using the HTE, encrypted Data Format B" [n] || *PSST (2),* is picked up by CE application when Interrupt Service Routine been serviced.

Preferably, the method of payment using the HTE the PSST (2) is validated by CE Application, secure element, or embedded secure element.

Preferably, in the method of payment using the HTE, the CE application, secure element, or embedded secure element only make transaction approval decision by processing Data Format B" [n], if *PSST (2)* credential requirement satisfied.

Preferably, in the method of payment using HTE, the CE application, secure element, or embedded secure element produces Response B"' [n] (e.g. electronic payment receipt) and *Payment Secure Session Token Response, PSST (2R).*

Preferably, in the method of payment using the HTE, the Response B"' [n] and SKT"' (1) shall be encrypted by SecretKey2, and SKT"' (1) shall be 3rd order

derivation from SKT(1).

Preferably, in the method of payment using the HTE, the PSST (2R) is derived from Data Response B''' [n], Random Seed and SecretKey2.

Preferably, in the method of payment using the HTE, the CE application loads encrypted Response B''' [n] || *PSST (2R),* into the shared memory area, [F] which is then picked up by HTE when Interrupt Service Routine been serviced.

Preferably, in the method of payment using the HTE, the secure element, or embedded secure element send the encrypted Response B''' [n] || PSST (2R) to HTE via existing smartcard ISO standard communication protocol.

Preferably, the method of payment using the HTE includes the step of validation of *PSST (2R),* and conversion of Response B''' [n] to Response B'' [n] and inactivation of SecretKey2 and other payment secret keys access condition, if the credential is satisfied and said PSST (2R) validation, inactivate Secret Keys and Response B''' [n] decryption shall performed in [G, G' G''] environment.

Preferably, in the method of payment using the HTE, the HTE calculates the *Session Key Token (1R), SKT (1R)* and invalidates Random Seed at this point and *SKT (1R) shall be generated* from SKT''' (1) and Secret Key 0 under [G, G' G''] environment.

Preferably, in the method of payment using the HTE, the HTE sends Response B'' [n] and *SKT (1R)* back to MA, which then uploads Response B'' [n] and *SKT (1R)* to MA provider's backend via existing communication protocol to validate *SKT (1R) and* update the MA mobile GUI to show payment transaction completed, if *SKT (1R)* credential requirement satisfied.

A third object is an electronic payment system for processing an electronic transaction involving a consumer using a mobile electronic device and a merchant, wherein the mobile electronic device and an electronic payment device of the merchant are used for making a transaction including transfer of a pre-paid credit of the consumer using the mobile electronic device as payment for the transaction , said mobile electronic device having a Mobile Application (MA) and a Payment Application residing in a Card Emulator (CE) Application, including

a Host Terminal Emulator Platform (HTE) which acts as an interface medium between Mobile Application processing the transaction requests to a Card Emulator Application, or secure element, or embedded secure element; and

a Mobile Payment Toolbox (MPT) which stores all payment related icons, wherein the MPT is used by the MA to activate payment transaction.

Preferably, the MPT has an icon for activating a step to Debit, to Credit, to Top Up, to disclose Transaction History and a step to check Pre paid Credit Balance.

Brief Description of the Drawings

For a better understanding of the present invention, and to show more clearly how it may be carried into effect, reference is now made, by way of illustration, to the accompanying drawings, in which:-

Fig 1 is a system overview of the parties who form the online community and are possibly involved in existing online payment gateway wherein users can carry out electronic payments and money transfer using an electronic mobile device. A host terminal emulator platform which forms the basis of this invention, is the mechanism to load the approved money amount into a digital wallet in the electronic mobile device of an user.

Fig 2 is a flow chart showing the steps taken by a user of an electronic mobile device to carry out payment transaction. The corresponding process where another user of an electronic mobile device, who could possibly be downloading the data to receive the funds from the user making the payment transaction is similarly illustrated.

Fig 3 shows the interface between the OS Layer of an electronic mobile device and the APP Layer of the same device. The various components of the electronic mobile device are labelled Fig 3 -A1, Fig 3 -A2, Fig 3 -A21 Fig 3 -A22, Fig 3 -A23, Fig 3 –Format B'/B", Fig 3 - Response B"'/B"/B', Fig 3 - Session Key Token (1), Fig 3 - Account UID, Fig 3 – F, Fig 3 - G/G"/G"', Fig 3 - Secure Element and Fig 3 – CLF.

Fig 4A to 4E are Graphic User Interface ("GUI") of the electronic mobile device of the user (making the payment using the invention) and the GUI of the electronic mobile device of the beneficiary of the electronic funds payment made by the user. The GUIs are numbered as Fig 4 - GUI1, Fig 4 - GUI2, Fig 4 - GUI2 – Input Box [A], Fig 4 - GUI3, Fig 4 - GUI4, Fig 4- GUI4 – Input Box [B] and Fig 4 - GUI5.

Detailed Description of the Invention

Fig 1 is a system overview of the parties who form the online community and are possibly involved in existing online payment gateway wherein electronic funds transfer and payments are made by an user using a electronic mobile device. The electronic mobile device can be a tablet, notebook, smartphone or any electronic hand held communication or computing device.

The online community could include users who want to carry out electronic payments either to a merchant or other persons in the on line community who could also be selling an article through the on line community. Such electronic payments could include payment for goods and services or even as a friendly personal loan.

Existing on-line funds transfer or electronic payments offer various methods of authentication of such transactions. As increasing use is made of electronic mobile

devices to make such electronic payments, there is a need for a secured method of authenticating and verifying the electronic payment.

A host terminal emulator platform which forms the basis of this invention, is the mechanism to load the approved credit amount into a digital wallet in the electronic mobile device of an user. The Host Terminal Emulator ("HTE") serves to securely process, authenticate and verify the details of the transaction, the details of the user and the details of the recipient including use of passwords.

Fig 2 is a flow chart showing the steps taken by a user of an electronic mobile device to carry out payment transaction. The corresponding process where another user of an electronic mobile device, who could possibly be downloading the data to receive the funds from the user making the payment transaction is similarly illustrated.

Currently, electronic mobile devices would have installed in them a Mobile Application and a Payment Application in a Card Emulator, Secure Element, or Embedded Secure Element, Fig 3 - A1 illustrates a typical mobile operating system (IOS, Android and proprietary multi-Application native OS), which handles all real time hardware/software requests, dispatch data between kernel and application layer, and to schedule all mobile's hard / soft driver event. Fig 3 - A2, illustrates a typical mobile application layer which acts as a platform to house electronic mobile application and services.

Fig 3 - A21, illustrates a typical electronic mobile application program (social network app, instance messaging, online retailer app and etc.), which contains basic graphic user interface and man machine interface.

The inventive feature is a HTE which is shown in Fig 3 - A22. The HTE acts as software interface medium between electronic mobile application to card emulator or secure element (e.g. smart card). The HTE emulates a terminal command which following respective scheme (e.g. international / national payment scheme, or international / national transport scheme, or close loop scheme) required format and structure.

Fig 3 - A23, illustrates a Card Emulator application, which to emulate card behavior according to respective scheme requirement.

HTE API is a software API set to allow electronic mobile application to exchange data with host terminal emulator platform.

HTE driver is a software driver to trigger interrupt service routine, in order to dispatch and exchange data between HTE' platform and Card Emulator, Secure Element, or Embedded Secure Element .

Fig 3 - Format B'/B" are the input data format structure and data content to each module in the chain process. Format B' shall content amount, currency, user UID and occurrence data time. Format B" shall content transaction send command set

which based on respective payment/transport scheme.

Fig 3 - Response B'''/B''/B' are the output data format structure and data content after each module processed the input data in this chain process. Response B''' shall content transaction response command set which based on respective payment/transport scheme. Response B'' shall content approved or declined transaction electronic receipt. B' shall content graphical icon encapsulate with hidden transaction electronic receipt.

Fig 3 - Session Key Token (1) is the initial generated temporary security token by MA backend to initialize a single security session between electronic mobile application and host terminal emulator platform.

Fig 3 - Account UID represents user account unique identity; the ID shall be unique within the respective electronic mobile application user community, as well as unique within respective handset hardware ID.

Fig 3 - F, illustrate the share memory area in the OS kernel which accessed by different software entity, if the access methodology is correct or access condition requirement satisfied.

Fig 3 - G/G''/G''', illustrate the secure container to store cryptogram calculation function, keys (Secret Keys and Session Keys), each key session access condition, generate and store random seed. The secure container shall be located in the mobile processor's secure zone or in the secure element (e.g. Smart card) or in secure server platform (e.g. Cloud).

Fig 3 - Secure Element or Embedded Secure Element represent a secure hardware platform which tamper proof Industry commonly used secure elements or embedded secure element includes Smart Card based product (e.g. NFC SIM and micro SD) to store respective payment scheme and transport scheme, or to store applications to perform cryptograph function.

Fig 3 - CLF represent the contactless front end, which to bridge card emulator application or secure element with the antenna. The CLF shall support international contactless protocol; 1444-3 Type A and B or Type C.

Users of an electronic mobile device shall use any of the existing available payment top up mechanism to purchase the prepaid if the configuration is prepaid digital wallet. Approved credit shall be given to online community service provider merchant bank account. Online community service provider shall then prompt the respective user on the approval credit via the existing data exchange flow mechanism. The HTE acts as the mechanism to load the approved credit amount into the handset's digital wallet.

It is also possible that electronic mobile user wish to transfer theirs prepaid, credit and debit money to other electronic mobile user within the online community. The HTE again is the mechanism which allows the user to transfer prepaid, credit and

debit money out from the user's digital wallet, and to load the transferred approved credit into the digital wallet of another user of another electronic mobile device ("beneficiary"). Data exchange flow between the electronic mobile device of the user and the beneficiary then use the HTE and the existing mechanism for such funds transfer.

It is also possible for the user of an electronic mobile device to use the digital wallet's card emulator, or secure element or embedded secure element to pay for transactions at any POS in the existing contactless payment environment.

Description of the HTE

The HTE acts as software interface medium between electronic mobile application to card emulator or secure element (e.g. smart card). The HTE emulates a terminal command which following a scheme, (e.g. international / national payment scheme, or international / national transport scheme, or close loop scheme) that mandated the required format and structure.

The HTE has a drive, HTE Driver which dispatches and exchanges data between; HTE and Card Emulator application, or HTE and secure element, or HTE and embedded secure element.

The HTE Driver has an Interrupt Service Handler inside the CE application and HTE. The Interrupt Service Handler is be periodically serviced by the OS, and the Interrupt Service Handler checks if there is any new set of data be loaded into the shared memory area [F] via HTE Driver.

A secure container [G, G', G'''] is provided in the electronic Mobile Device OS layer to store all keys, cryptogram function / calculation, and secure object access activation, which is used between Mobile Application ("MA") , HTE and Secured element or Card Emulator.

The HTE provides a set of software API for payment request activation and payment data exchange between MA and HTE.

An user of electronic mobile device shall trigger the payment request according to one of the proposed data path [B] [Terminal API →B1 → B2 → B1 → Terminal API].

The MA then initiates a ***Secure Session (1). SS (1)*** requests HTE via defined API by sending ***Session Key Token (1), SKT (1),*** account UID to HTE.

MA shall sends request to MA backend provider to request *SKT (1)* if need to transfer the prepaid, credit or debit mobile money out from digital wallet' card emulator, or secure element, or embedded secure element of the electronic mobile device. MA requests shall include data such as Account UID, dynamical seed component (e.g. occurrence event's date time). MA backend provider shall use Secret Key 0 and MA requests data to generate *SKT (1)*. MA shared the received SKT (1) with HTE via HTE defined API.

MA shall sends request to MA backend provider to request *SKT (1)* if need to load the transferred approved credit to digital wallet's card emulator, or secure element, or embedded secure element of the electronic mobile device. MA requests shall include data such as Account UID, dynamical seed component (e.g. occurrence event's date time) and approved transfer amount. MA backend provider shall use Secret Key 0 and MA requests data to generate *SKT (1)*. MA shared the received SKT (1) with HTE via HTE defined API.

The HTE shall generate and store Random Seed in [G, G", G"'].

The HTE shall validate the MA's *SKT (1)*, if *SKT (1)* credential requirement satisfied, HTE activate **Secret Key [1]**'s access condition, and proceed to generate ***Payment Session Key (1). PSK (1),*** is then shared with MA via defined API. ***PSK (1)*** shall be generated from ***STK (1),*** account UID, Random Seed and Secret Key [1].

The Secret Key [1] is stored in [G, G', G"']. ***SKT (1)*** validation and ***PSK (1)*** calculation shall be performed in [G, G', G"'].

The MA shall prepare data [Format B'], upon receiving PSK (1). Data [Format B'] is then encapsulated with payment data (e.g. amount, currency, date / time and etc.) and User Account UID. The electronic Mobile Application then produce ***Payment Session Security Token (1).*** The ***PSST (1)*** is generated from data [Format B'] and PSK (1). Data [Format B'] and ***SKT' (1)*** shall be encrypted by using PSK (1), and *SKT' (1)* shall be 1st order derivation from ***SKT (1).*** The electronic Mobile Application then sends encrypted Data [Format B'] and PSST (1) to HTE via defined API.

HTE validates the ***PSST (1)*** upon receiving [Format B'] || ***PSST (1)*** from electronic Mobile Application. The HTE converts the Format B' to Format B" [n], which contain set of payment transaction command (e.g. Select, GPO, read record, PIN verification and Generic Application Cryptogram [TC/ARQC], update record) and activates ***Secret Key2*** and others Payment's Secret Key access condition; If *PSST (1)* credential requirement is satisfied. ***PSST (1)*** Validation is to be performed in [G, G' G"'] environment.

HTE shall then produce ***Payment Session Security Token (2). PSST (2)***, which is generated from Data Format B" [n], Random Seed and SecretKey2. ***SecretKey2*** is stored inside [G, G' G"'], and the ***PSST (2)*** calculation is performed in [G, G', G"']. In the secure area [G, G' G"'], HTE shall encrypt Data Format B" [n] and SKT" (2) by using SecretKey2. SKT" (2) shall be 2nd order derivation from SKT (1). HTE loads encrypted Data Format B" [n] || ***PSST (2),*** into the shared memory area, [F].

Encrypted Data Format B" [n] || ***PSST (2),*** is then picked up by CE application when Interrupt Service Routine been serviced. The Card Emulator application or secure element or embedded secure element then validates ***PSST (2)***. The Card Emulator application or secure element or embedded secure element only makes transaction approval decision by processing Data Format B" [n], if *PSST (2)* credential requirement satisfied.

The Card Emulator application, or secure element or embedded secure element produces Response B''' [n] (e.g. electronic payment receipt) and ***Payment Secure Session Token Response, PSST (2R).*** ***PSST (2R)*** is generated from Data Response B''' [n], Random Seed and SecretKey2. Response B''' [n] and SKT''' (1) shall be encrypted by SecretKey2, and SKT''' (1) shall be 3rd order derivation from SKT(1).

The Card Emulator application, or SE, or ESE loads encrypted Response B''' [n] || ***PSST (2R)***, into the shared memory area, [F]. Response B''' [n] || *PSST (2R),* is picked up by HTE when Interrupt Service Routine been serviced. HTE then validates ***PSST (2R),*** and convert Response B''' [n] to Response B'' [n] and inactivate **Secret Key2** and others payment Secret Keys access condition, if the credential is satisfied. **PSST (2R)** Validation is performed in [G, G' G'''] environment.

HTE shall calculate the ***Session Key Token (1R), SKT (1R)*** and invalidate Random Seed at this point. ***SKT (1R)*** *shall be generated* from SKT''' (1) and Secret Key 0 under [G, G' G'''] environment. HTE sends Response B'' [n] and ***SKT (1R)*** back to MA.

The MA uploads Response B'' [n] and ***SKT (1R)*** to MA provider's backend via existing communication protocol. MA provider's backend validates ***SKT (1R),*** *and* updates the electronic MA's GUI to show payment transaction completed, if *SKT (1R)* credential requirement satisfied.

The user also can trigger the payment request according to one of the proposed data path [D] [Terminal API →D1 → D2 → D2 → D1 → Terminal API]. Such transaction based on data path [D] does not need Card Emulator.

Transactions based on data path [D] need secure element on the handset (e.g. NFC SIM, microSD or embedded secure element).

Mobile Payment Toolbox

A Mobile Payment Toolbox (MPT) is proposed to be used with the HTE, electronic Mobile Application and Card Emulator Application. The MBT shall store all payment related icons, which user can see on the display screen of the electronic mobile device to activate payment transaction.

Fig 4 - GUI1 illustrate the common electronic mobile application (instance messaging application) which internally linked to card emulator application or secure element via the host terminal emulator platform.

Fig 4 - GUI2 illustrate the graphic user interface to transfer prepaid, credit, or debit money out from the digital wallet application (international / national payment scheme) in card emulator or secure element. The graphic user interface provides the electronic Mobile Payment Toolbox for user to select type of mobile payment need to be executed. The MPT shall contain icon with featuring; Debit, Top Up,

Transaction History and Purse Balance check:-

GUI2  represent Mobile Payment Toolbox toolbar icon.

GUI2  represent Money Transfer (prepaid, debit or credit) feature.

GUI2  represent Money Top up feature.

GUI2  represent Transaction Historical.

GUI2  represent digital wallet balance.

GUI5  represent approved credit transfer process competed and invalidated.

Fig 4 - GUI2 – Input Box [A] illustrate the graphic man machine interface for Money Transfer Feature. User need to input the money amount to be transferred out from the digital wallet, and PIN code needed for the payment transaction.

To Debit / Transfer Money from Mobile Application, the user of an electronic mobile device shall activate the MPT, and click on the Mobile Money (MM) icon. The Mobile Application shall prompt the Input Box [A] for user to key in total debit amount and PIN code needed for debit transaction. The user (payee) confirms debit payment transaction details by clicking Debit button in Input Box [A].

The Payee's Mobile Application shall start the debit payment transaction as described above.

Fig 4 - GUI3 illustrate the graphic user interface update, upon transfer money completed with approval by the card emulator application / secure element and host terminal emulator platform.

Payee's Mobile Application's GUI is updated.

Fig 4 - GUI4 illustrate the beneficiary's graphic user interface to download the payee Mobile Money to benefactor digital wallet.

Beneficiary shall download transferred prepaid Mobile Money by clicking the MM

icon in the chat box and Input Box [B] shall be prompted to indicate total amount to be credited and PIN code to allow the credit payment transaction. Beneficiary Mobile Application shall confirms credit payment transaction details by clicking credit button in Input Box [B]. Fig 4- GUI4 – Input Box [B] illustrates the graphic man machine interface to download payee.

Beneficiary's Mobile Application shall credit payment transaction as follows:-

Acceptance of Mobile Money into benefactor digital wallet is by clicking , Input Box [B] which is prompted to show total amount to be loaded. Beneficiary shall key in the PIN code to allow the transaction to proceed.

Fig 4 - GUI5 illustrate the graphic user interface update, upon downloading of funds into the beneficiary's digital wallet completed with approval by the card emulator application / secure element and HTE.

While many aspects of the invention have been disclosed and described herein, such disclosure is provided for purposes of illustration only. Where methods and steps described indicate certain events occurring in a certain order, those of ordinary skill in the art having the benefit of this disclosure would have recognize that the ordering of certain steps may be modified and that such modifications are in accordance with variations of the invention. In addition, certain of the steps may be performed concurrently in a parallel process when possible, as well as performed sequentially.

Advantageous Effects of the Invention

The invention allows for safer and more secure method of payment through any electronic mobile device using prepaid, credit or debit payment transaction among the online community (mobile user, online retailer, games hub and etc.), and also for transactions in the traditional contactless payment and transport environment.

The invention also allows for safer and more secure method of payment by the user of an electronic mobile device carrying out electronic transactions with merchant having a POS.

Claims:

1. An electronic payment system for electronic transaction using a mobile electronic apparatus and a merchant having an mobile electronic payment apparatus wherein the electronic payment apparatus of the merchant and the mobile electronic apparatus are used to making online payment transaction including transferring a digital currency of a consumer using the mobile electronic apparatus as payment for the online transaction, said mobile electronic apparatus having a Mobile Application (MA) and a Payment Application residing in a Card Emulator (CE) Application running on a Mobile electronic Operating Software (OS), including

a Host Terminal Emulator Platform (HTE) which is an interface medium for transaction between the Mobile Application (MA) and the Card Emulator (CE) Application; and

a Mobile Payment Toolbox (MPT) including icons for activating a step to Debit, to Credit, to Top Up and to disclose Transaction History, and for activating a step to check Prepaid Credit Balance, and the MPT stores all payment related icons, wherein the MPT icon functions are integrated and used by the MA to activate payment transaction, and wherein the Card Emulator Application emulates card behaviour, and contains payment application, and the MA initiates a request with the HTE via a defined Application Programming Interface (API).

2. The electronic payment system of Claim 1, wherein the Host Terminal Emulator Platform (HTE) comprises a HTE Driver and an Interrupt service Handler which periodically receives data from said Operating System of the Mobile electronic, and checks for new sets of data loaded via the HTE or the Driver.

3. The electronic payment system of Claim 2, wherein the HTE further comprises a set of software API for payment request activation and payment data exchange between the MA and the HTE.

4. The electronic payment system of Claim 1, wherein the HTE further comprises,

a. a module to interface MA with payment application residing in the card Emulator;

b. a module to manage a secure transaction process wherein the secure token validation and generation process shall be performed within a secure container [G,G' or G'']; and

c. a module to perform debit and credit payment by translating the payment enquiry input data to respective payment scheme transaction commands, wherein all commands shall already residing within the HTE.

5. The electronic payment system of Claim 1, wherein a mobile user triggers a payment request through the MPT Icon of said MA by sending Session Key Token (1) (SKT (1)) and relevant Transaction Data to the HTE.

6. The electronic payment system of Claim 5, wherein the MA sends an SKT (1) request to a MA backend provider and forwards the SKT (1) to the HTE.

7. The electronic payment system of Claim 6, wherein upon SKT (1) validation by the HTE, the HTE generates a Payment Session Key (1) (PSK (1)) which is sent to the MA; the MA translates said Transaction Data to data [Format B'] using PSK (1), and uses said data [Format B'] to generate Payment Secure Session Token (1) (PSST (1)); the PSST (1) and the data [Format B'] is sent to the HTE; the HTE validates the PSST (1) and, upon successful validation, converts the data [Format B'] to data [Format B" [n]] which is then used to generate Payment Secure Session Token (2) (PSST (2)).

8. The electronic payment system of Claim 7, wherein the card emulator applications conduct a transaction approval decision by processing said data [Format B" [n]] to generate Response B"' [n] and Payment Secure Session Token Response PSST (2R) (PSST (2R)) as response data set to the HTE upon PSST (2) credential requirement validation satisfied by the card emulator application.

9. The electronic payment system of Claim 8, wherein the HTE sends a Response B" [n] and a Session Key Token (1R) (SKT (1R)) to the MA backend provider through the MA upon PSST (2R) validation.

10. The electronic payment system of Claim 9, wherein the MA backend provider completes the online payment transaction by updating an MA GUI upon validation of the SKT (1R).