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 sending 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 SKR (1R).