21. The User-Terminal terminal as claimed in any of the previous claims, wherein the Security Box checks the status of the operation system before booting,
preferably in a first step a program is booted that has access to information which are stored in the Security Box, to verify the operating system, and the operating system is started if the status of the operating system passes the verification.

22. A User-Terminal for entering secure user information, comprising:
- a processor for running an operating system, with applications;
- a touch screen for displaying information and receiving user inputs and also to receive the secure information from the user;
- a Security-Box being connected between the touch screen and the processor, to control the user input on the touch screen to the processor, wherein the Security-Box and the processor are connected via a serial interface configured to provide a first and a second logical connection,
wherein the Security-Box is being configured to run in two modes "Secure Mode" using the first logical connection and "Clear Text Mode" using the second logical connection, wherein when running in "Secure Mode" the user input is not forwarded as touch coordinates to the processor via the second logical connection and when running in "Clear Text Mode" the touch coordinates are transmitted to the processor via the second logical connection.

23. The User-Terminal according to claim 22, wherein the touch screen is connected to the Security-Box via a serial peripheral interface and the serial interface is a USB-Channel.

24. The User-Terminal according to claim 23, wherein in the "Secure Mode" crypto commands are transmitted over the first logical connection.

25. The User-Terminal according to claim 24, wherein the USB-Channel is configured as USB Composite Device Class implementing the first logical connection as a COM USB interface and the second logical connection as a HID interface.

26. The User-Terminal according to one or more of the claims 22 to 25, wherein the secure user information is PIN or a Password to have access to personal account information and/or physical items, and wherein the "Secure Mode" is a "PIN Entry Mode".

27. The User-Terminal according to one or more of the claims 22 to 26, wherein the User-Terminal is a Point-of-sale (POS) terminal for entering a PIN to enable a financial transaction, additionally comprising:
- a card reader for reading information from a credit card.

28. The User-Terminal according to claim 27, wherein the card reader is a chip card reader that is integrated into the Security-Box, wherein the Security-Box is configured to perform all necessary steps to process a financial transaction based on the PIN and the information of the chip card.

29. The User-Terminal according to claim 27 or 28, wherein when a virtual pin-pad is displayed on the touch screen the Security-Box switches to "PIN-Entry-Mode" and is configured to interpret the user touch as PIN, and to encrypt the PIN to forward the information together with credit card information to an associate service center/bank over a network controller.

~~30. The User-Terminal according to claim 29, wherein an payment application is running on the operating system switching the Security-Box into "Secure Mode" and displaying the virtual PIN-pad, and/or wherein the payment application forwards the card information from the card reader to the Security-Box, wherein the payment application can also be responsible to forward the encrypted PIN from the Security-Box to the service center/bank.~~

31. The User-Terminal according to one or more of the claims 22 to 30, configured to shift the PIN Pad randomly on the touch screen for every transaction and/or wherein the Security-Box is informed about the coordinates of the PIN Pad, to be able to interpret the touch input.

32. The User-Terminal according to one or more of the claims 22 to 31, configure to submit in "Secure Mode" only replacement information, via the first logical channel, to the operating system in case of touch events.

33. The User-Terminal according to one or more of the claims 22 to 32, wherein the Security-Box is connected to an optical indictor indicating when being in "Security mode".

34. The User-Terminal according to one or more of the claims 22 to 33, wherein the Security-Box and the display are connected with each other, and sensors indicate when a disconnection is performed, which leads to a deletion of keys in the Security-Box.

35. The User-Terminal according to claim 33, wherein the Security-Box is physically attached to the display and protected by a cover.

36. The User-Terminal according to one or more of the claims 30 to 35, wherein the Payment Application which starts the Secure PIN Mode needs to authenticate with the Security-Box using a cryptographic key which is generated by the Security-Box and transferred to the payment application during registration.

37. The User-Terminal terminal according to one or more of the claims 22 to 36, wherein the Security-Box checks the status of the operation system before booting.

38. The User-Terminal terminal according to claim 37, wherein when booting, in a first step a program is booted that has access to information which are stored in the Security-Box, to verify the operating system, and the operating system is started if the status of the operating system passes the verification.

39. The User-Terminal according to one or more of the claims 22 to 38, wherein after a power on of the User-Terminal the Security-Box is configured to start in the "Secure Mode" and after a secure boot with successful verification of the operating system the Security-Box is configured to transfer to the "Clear Text Mode".

40. The User-Terminal according to one or more of the claims 22 to 39 is configured to run at least two types of applications displaying information on the touch screen and allowing an interaction with the user, the first of the applications is interacting with the Security-Box to perform security relevant financial transactions;
and the other application, Add-on applications, interacting in "Clear Text Mode" with the touch-screen,
wherein the application interacting with the Security-Box and switching the Security-Box into "Secure Mode" needs to be authenticated ~~with the Security-Box using one or more security keys.~~

~~41. The User-Terminal according to claim 40, wherein the application interacting with the Security-Box using a signature or cryptogram to authenticated with the Security-Box.~~

42. The User-Terminal according to claim 41, wherein the Security-Box is configured to verify the signature or cryptogram of the application interacting with the Security-Box before allowing switching into "Secure Mode".

43. The User-Terminal according to one or more of the claims 22 to 42, being a mobile device, like a mobile pad, without any physical keyboard, allowing interaction via the touch screen.

~~44. The User-Terminal according to one or more of the claims 22 to 43, wherein the operating system is an Android operating system.~~