CLAIMS

What is claimed is:

1. A multi-purpose smart card in a dynamic environment, the dynamic environment comprising:

an operative field from one of a data connection system, a GPS or normal telecommunication network, a local wireless network, and the smart card comprising:

a top layer with a cover printed and glued to a bottom layer, the cover including identity elements, an activation symbol, a code display window for allowing illustration of a One Time Password Generator (OTP);

the bottom base layer on which is a microprocessor for running in a memory and connected to a power source a software for operation of the smart card in the dynamic environment, and a mass storage memory for storing biometric information of a user and private data;

the microprocessor connected to a one-time password generator (OTP), a biometric reader, an UHF RFID tag for long-range, in-faculty detection, a multi-protocol contactless access control interface with low power Bluetooth connector, and at least one sensor; wherein, the smart card is configured to enable an upload into the memory of a user biometric data, and enabled to allow the user having the user biometric data into the memory to perform an operation of pairing in which the user authenticates himself to the smart card by providing biometric information to the smart card at the biometric reader, wherein the smart card is further configured to enable at least a portion of the dynamic environment from (a) the data connection system, (b) the GPS or normal telecommunication network, or (c) the local wireless network, to interact with one of (i) the

UHF RFID tag for long-range, in-facility detection, (ii) the multi-protocol contactless access control interface with low power Bluetooth connector, or (iii) the at least one sensor for the management (establishing or losing) of trust between the smart card and the user, and wherein the smart card is further configured as part of the management of trust between the smart card and the user to allow for the programming of at least one trust verification parameter (TVP) to be tested and confirmed before the card releases data to help as part of a secured digital transaction.

2. The multi-purpose smart card in a dynamic environment of Claim 1, wherein the smart card is further configured as part of the management of trust between the smart card and the user to allow for the programming of more than one trust verification parameter (TVP) to each be tested serially, randomly or sequentially before the card releases data to help as part of a secured digital transaction.

3. The multi-purpose smart card in a dynamic environment of Claim 1, wherein the data released to help as part of the secured digital transaction includes a security token (HOTP or TOTP systems).

4. A multi-purpose smart card in a dynamic environment, the dynamic environment comprising:

an operative field from one of a data connection system, a GPS or normal telecommunication network, a local wireless network, and the smart card comprising:

a top layer with a cover printed and glued to a bottom layer, the cover including identity elements, an activation symbol, a code display window for allowing illustration of a One Time Password Generator (OTP);

the bottom base layer on which is a microprocessor for running in a memory and connected to a power source a software for operation of the smart card in the dynamic environment, and a mass storage memory for storing biometric information of a user and private data;

the microprocessor connected to a one-time password generator (OTP), a biometric reader, an UHF RFID tag for long-range, in-faculty detection, a multi-protocol contactless access control interface with low power Bluetooth connector, and at least one sensor; and wherein, the smart card is configured to enable an upload into the memory of a user biometric data, and enabled to allow the user having the user biometric data into the memory to perform an operation of pairing in which the user authenticates himself to the smart card by providing biometric information to the smart card at the biometric reader wherein the at least one sensor is selected from the group of: (a) temperature sensors including infrared sensors, IC sensors, Thermistors, resistor temperature detectors, and thermocouples, (b) pressure sensors, (c) infrared sensors, [(d) image sensors such as charge-coupled device or complementary metal-oxide semiconductor imagers, (e) motion detection sensors, (f) accelerometer sensors, (g) gyroscopic sensors such as rotary, vibrating, or optical / MEMS sensors,(h) optical sensors such as photodetector, fiber optic detector, pyrometer, or proximity detectors;

wherein the smart card is further configured to enable at least a portion of the dynamic environment from (a) the data connection system, (b) the GPS or normal telecommunication network, or (c) the local wireless network, to interact with one of (i) the UHR RFID tag for long-range, in-facility detection, (ii) the multi-protocol contactless access control interface with low power Bluetooth connector, or (iii) the at least one sensor

for the management (establishing or losing) of trust between the smart card and the user; and

wherein the smart card is further configured as part of the management of trust between the smart card and the user to allow for the programming of at least one trust verification parameter (TVP) to be tested and confirmed before the card releases data to help as part of a secured digital transaction.

5. A process of use of a multi-purpose smart card in a dynamic environment, the dynamic environment comprising one of an operative field from one of a data connection system, a GPS or normal telecommunication network, a local wireless network, and the smart card comprising a top layer with a cover printed and glued to a bottom layer, the cover including identity elements, an activation symbol, the bottom base later on which is a microprocessor for running in a memory and connected to a power source a software for operation of the smart card in the dynamic environment, and a mass storage memory for storing biometric information of a user and private data, the microprocessor connected to a biometric reader, an UHF RFID tag for long-range, in-faculty detection, a multi-protocol contactless access control interface with low power Bluetooth connector, and at least one sensor, and wherein, the smart card is configured to enable an upload into the memory of a user biometric data, and enabled to allow the user having the user biometric data into the memory to perform an operation of pairing in which the user authenticates himself to the smart card by providing biometric information to the smart card at the biometric reader,

the method comprising the steps of:

powering an unpaired card;

providing to a new user the unpaired card;

pairing the card with the user by either one of (a) entry of the user's biometric data, (b) the request of a code, or (c) the entry from a terminal of identification data; and creating a trust by allowing the card further configured to enable at least a portion of the dynamic environment from (a) the data connection system, (b) the GPS or normal telecommunication network, or (c) the local wireless network, to interact with one of (i) the UHF RFID tag for long-range, in-faculty detection, (ii) the multi-protocol contactless access control interface with low power Bluetooth connector, or (iii) the at least one sensor; further including the step of allowing for the management (establishing or losing) of trust between the smart card and the user, and further including the step of allowing for the programming of at least one trust verification parameter (TVP) to be tested and confirmed before the card releases data to help as part of a secured digital transaction.

6. The process of use the multi-purpose smart card in a dynamic environment of claim 5, further including the step of allowing for the programming of more than one trust verification parameter (TVP) to each be tested serially, randomly or sequentially before the card releases data to help as part of a secured digital transaction.

7. A process of use of a multi-purpose smart card in a dynamic environment, the dynamic environment comprising one of an operative field from one of a data connection system, a GPS or normal telecommunication network, a local wireless network, and the smart card comprising a top layer with a cover printed and glued to a bottom layer, the cover including identity elements, an activation symbol, the bottom base later on which is a microprocessor for running in a memory and connected to a power

source a software for operation of the smart card in the dynamic environment, and a mass storage memory for storing biometric information of a user and private data, the microprocessor connected to a biometric reader, an UHF RFID tag for long-range, in-faculty detection, a multi-protocol contactless access control interface with low power Bluetooth connector, and at least one sensor, and wherein, the smart card is configured to enable an upload into the memory of a user biometric data, and enabled to allow the user having the user biometric data into the memory to perform an operation of pairing in which the user authenticates himself to the smart card by providing biometric information to the smart card at the biometric reader,

the method comprising the steps of:

powering an unpaired card;

providing to a new user the unpaired card;

pairing the card with the user by either one of (a) entry of the user's biometric data, (b) the request of a code, or (c) the entry from a terminal of identification data; and

creating a trust by allowing the card further configured to enable at least a portion of the dynamic environment from (a) the data connection system, (b) the GPS or normal telecommunication network, or (c) the local wireless network, to interact with one of (i) the UHF RFID tag for long-range, in-faculty detection, (ii) the multi-protocol contactless access control interface with low power Bluetooth connector, or (iii) the at least one sensor, and wherein the at least one sensor is selected from the group of: (a) temperature sensors including infrared sensors, IC sensors, Thermistors, resistor temperature detectors, and thermocouples, (b) pressure sensors, (c) infrared sensors, (d) image sensors such as charge-coupled device

or complementary metal-oxide semiconductor imagers, (e) motion detection sensors, (f) accelerometer sensors, (g) gyroscopic sensors such as rotary, vibrating, or optical / MEMS sensors, (h) optical sensors such as photodetector, fiber optic detector, pyrometer, or proximity detectors;

wherein the smart card is further configured to enable at least a portion of the dynamic environment from (a) the data connection system, (b) the GPS or normal telecommunication network, or (c) the local wireless network, to interact with one of (i) the UHR RFID tag for long-range, in-facility detection, (ii) the multi-protocol contactless access control interface with low power Bluetooth connector, or (iii) the at least one sensor for the management (establishing or losing) of trust between the smart card and the user; and

wherein the smart card is further configured as part of the management of trust between the smart card and the user to allow for the programming of at least one trust verification parameter (TVP) to be tested and confirmed before the card releases data to help as part of a secured digital transaction.

8. A method of use of a smart card in a dynamic environment, the dynamic environment, the dynamic environment comprising one of an operative field from one of a data connection system, a GPS or normal telecommunication network, a local wireless network, and the smart card comprising a top layer with a cover printed and glued to a bottom layer, the cover including identity elements, an activation symbol, the bottom base later on which is a microprocessor for running in a memory and connected to a power source a software for operation of the smart card in the dynamic environment, and a mass storage memory for storing biometric information of a user and private data, the

microprocessor connected to a biometric reader, an UHF RFID tag for long-range, in-faculty detection, and at least one sensor, and wherein the smart card is configured to enable an upload into the memory of a user biometric data, and enabled to allow the user having the user biometric data into the memory to perform an operation of pairing in which the user authenticates himself to the smart card by providing biometric information to the smart card at the biometric reader; the method comprising the steps of:

pairing an unpaired card to a user by inserting biometric data in the memory of the card;

creating trust by allowing a user at the biometric reader to validate the paired biometric data in the memory of the card; and

establishing a set of trust verification parameters for testing of trust (established or loss) before any use of the card in a digital transaction,

wherein the smart card is further configured to enable at least a portion of the dynamic environment from (a) the data connection system, (b) the GPS or normal telecommunication network, or (c) the local wireless network, to interact with one of (i) the UHF RFID tag for long-range, in-faculty detection, (ii) the multi-protocol contactless access control interface with low power Bluetooth connector, or (iii) at least one sensor for the management (establishing or losing) of trust between the smart card and the user, wherein the smart card is further configured as part of the management of trust between the smart card and the user to allow for the step of programming of at least one trust verification parameter (TVP) to be tested and confirmed before the card releases data to help as part of a secured digital transaction.

9. The Method of Claim 8, wherein the smart card is further configured as part of the management of trust between the smart card and the user to allow for step of programming of more than one trust verification parameter (TVP) to each be tested serially, randomly or sequentially before the card releases data to help as part of a secured digital transaction.

10. The Method of Claim 9, wherein the method include the additional step of releasing data to help as part of the secured digital transaction includes a security token (HOTP or TOTP systems).

11. A method of use of a smart card in a dynamic environment, the dynamic environment, the dynamic environment comprising one of an operative field from one of a data connection system, a GPS or normal telecommunication network, a local wireless network, and the smart card comprising a top layer with a cover printed and glued to a bottom layer, the cover including identity elements, an activation symbol, the bottom base later on which is a microprocessor for running in a memory and connected to a power source a software for operation of the smart card in the dynamic environment, and a mass storage memory for storing biometric information of a user and private data, the microprocessor connected to a biometric reader, an UHF RFID tag for long-range, in-faculty detection, and at least one sensor, and wherein the smart card is configured to enable an upload into the memory of a user biometric data, and enabled to allow the user having the user biometric data into the memory to perform an operation of pairing in which the user authenticates himself to the smart card by providing biometric information to the smart card at the biometric reader; the method comprising the steps of:

pairing an unpaired card to a user by inserting biometric data in the memory of the card;

creating trust by allowing a user at the biometric reader to validate the paired biometric data in the memory of the card; and establishing a set of trust verification parameters for testing of trust (established or loss) before any use of the card in a digital transaction, wherein at least one sensor of the card is selected from the group of: (a) temperature sensors including infrared sensors, IC sensors, Thermistors, resistor temperature detectors, and thermocouples, (b) pressure sensors, (c) infrared sensors, (d) image sensors such as charge-coupled device or complementary metal-oxide semiconductor imagers, (e) motion detection sensors, (f) accelerometer sensors, (g) gyroscopic sensors such as rotary, vibrating, or optical / MEMS sensors, (h) optical sensors such as photodetector, fiber optic detector, pyrometer, or proximity detectors.