

Claims

~~1. A battery-less active and passive hybrid device for secure wireless data transaction comprising a secure element adapted for storing at least one secure applet and at least one data segment for secure contactless data transaction and operatively connected with an active operation unit and a passive operation unit; and preferably the active operation unit is adapted to be connected removably with the secure element; and~~

~~wherein the hybrid device is configured to be switchable between an active state in which the active operation unit is activated on demand to enable the hybrid device to function as an active device and adapted for provisioning one or more personalization information data, biometric data, health data, government related security data, hardware specific data, and/or a token of the device to the secure element; and a passive state in which the active operation unit is deactivated and the passive operation unit is activated / configured to enable the hybrid device to function as a passive device and adapted for conducting data verification and/or contactless data transaction operation via the secure element.~~

~~2. The hybrid device according to claim 1, wherein in the active state the active operation unit is activated by operatively coupled with and powered by a power transfer unit for conducting wireless data communication with a provisioning unit, preferably a smartphone, for provisioning of the personalization information data, biometric data, health data, government related security data, hardware specific data, and/or the token of the device to the secure element from the provisioning unit.~~

~~3. The hybrid device according to claim 1 or 2, wherein in the passive state the passive operation unit is activated by operatively coupled with and wirelessly powered by a data transaction unit, preferably a data transaction terminal, for conducting data verification and/or contactless data transaction operation with the data transaction unit via the secure element.~~

~~4. The hybrid device according to anyone of claims 2-3, wherein the active operation unit comprises a first wireless communication unit adapted for coupling and conducting wireless data communication with the provisioning unit, and operatively coupled with a power receiver unit and/or a transient power storage unit, preferably a supercap, adapted for receiving and/or storing power from the coupled power transfer unit.~~

~~5. The hybrid device according to claim 4, wherein the first wireless communication unit is a WIFI, BT, and/or NFC enabled communication unit, and preferably a BLE unit with contacts, preferably waterproof and/or exposed contacts.~~

~~6. The hybrid device according to claim 5, wherein the power transfer unit is a USB power transmitter, preferably equipped with connection members, preferably connection pins or hooks, and/or fixing or locking members for making contact and/or interlocking with the contacts of the BLE unit.~~

~~7. The hybrid device according to anyone of claims 3-6, wherein the passive operation unit comprises a second wireless communication unit, preferably a NFC enabled communication unit, adapted for coupling and conducting wireless data communication with the data transaction unit and operatively coupled with an antenna unit for receiving its operating power and data transaction data and~~

~~signals from the coupled data transaction unit.~~

~~8. The hybrid device according to claim 7, wherein the second wireless communication unit is a NFC enabled communication unit acting as a NFC passive target unit configured to draw its operating power from the data transaction unit acting as a NFC initiator unit.~~

~~9. The hybrid device according to claim 7 or 8, wherein the antenna unit comprises an antenna of a dimension of 10x24mm adapted to draw operating power directly from a data signal generated from the data transaction unit without incorporating any active booster for amplifying the data signal.~~

~~10. The hybrid device according to anyone of claims 1-9, wherein the secure element, the active operation unit, and the passive operation unit are configured to be operatively coupled with each other and mounted on a battery-less bendable board adapted for easy mounting on a non-planar or a curved surface or being readily insertable or embedded into a curved accommodating space; or the active operation unit is adapted to be removably connected with the secure element and/or integrated with the power transfer unit; and/or~~

~~the hybrid device further comprise a biometric unit for biometric authentication comprising one or more biometric readers / sensors for reading, writing and/or processing biometric data related to fingerprint, palm/finger vein pattern, voice pattern, face recognition, DNA, palm print, hand geometry, iris recognition, and/or retina.~~

~~11. The hybrid device according to claim 1, wherein the active operation unit is integrated with a power transfer or receiver unit and/or an interface for power transfer to form an universal passive provisioning unit for secure element being substantially in form of a clip / clamp or a forepart of clothes pin and comprising a lower part with a flattened portion located at its proximal end and a depressed portion at its distal end on which a plurality of connection members are arranged for enabling power and signal transmission; and an upper part hingeably mounted over the lower part to be switchable between an opened position/state in which its proximal end is configured to make contact with the proximal end of the lower part and its distal end is configured to disengage with the distal end of the lower part to make the connection members and depressed portion accessible and a closed position/state in which its distal end is configured to make contact with the distal end of the lower part and its proximal end is configured to disengage with the proximal end of the lower part to make the connection members and depressed portion covered and concealed by the upper part.~~

~~12. A method for providing contactless data transaction capabilities to a traditional wearable device by a battery-less active and passive hybrid device for secure wireless data transaction comprising a secure element adapted for storing at least one secure applet and at least one data segment for secure contactless data transaction and operatively connected with an active operation unit, preferably adapted to be connected removably with the secure element, and a passive operation unit, comprising steps of;~~

~~mounting or embedding the battery-less active and passive hybrid device at or into the traditional wearable device;~~

~~switching or setting the hybrid device to an active state by having the active operation unit activated on demand to enable the hybrid device to function as an active device and the secure element provisioned with one or more~~

personalization information data, biometric data, health data, government related security data, hardware specific identification data, and/or a token of the device; and

switching or setting the hybrid device to a passive state by having the active operation unit deactivated and the passive operation unit activated / configured to enable the hybrid device to function as a passive device and the secure element configured for conducting data verification and/or contactless data transaction operation via the secure element.

13. The method for providing contactless data transaction capabilities to a traditional wearable device according to claim 12, wherein in the active state the active operation unit is activated by operatively coupled with and powered by a power transfer unit for conducting wireless data communication with a provisioning unit, preferably a smartphone, for provisioning of the personalization information data, biometric data, health data, government related security data, hardware specific identification data, and/or the token of the device to the secure element from the provisioning unit; and/or

in the passive state the passive operation unit is activated by operatively coupled with and wirelessly powered by a data transaction unit, preferably a data transaction terminal, for conducting data verification and/or contactless data transaction operation with the data transaction unit via the secure element.

14. The method for providing contactless data transaction capabilities to a traditional wearable device according to anyone of claims 12-13, wherein the active operation unit comprises a first wireless communication unit adapted for coupling and conducting wireless data communication with the provisioning unit, and operatively coupled with a power receiver unit and/or a transient power storage unit, preferably a supercap, adapted for receiving and/or storing power from the coupled power transfer unit.

15. The method for providing contactless data transaction capabilities to a traditional wearable device according to claim 14, wherein the first wireless communication unit is a WIFI, BT, and/or NFC enabled communication unit, and preferably a BLE unit with contacts, preferably waterproof and/or exposed contacts.

16. The method for providing contactless data transaction capabilities to a traditional wearable device according to claim 15, wherein the power transfer unit is a USB power transmitter, preferably equipped with connection members, preferably connection pins or hooks, and/or fixing or locking members for making contact and/or interlocking with the contacts of the BLE unit.

17. The method for providing contactless data transaction capabilities to a traditional wearable device according to anyone of claims 13-16, wherein the passive operation unit comprises a second wireless communication unit, preferably a NFC enabled communication unit, adapted for coupling and conducting wireless data communication with the data transaction unit and operatively coupled with an antenna unit for receiving its operating power and data transaction data and signals from the coupled data transaction unit.

18. The method for providing contactless data transaction capabilities to a traditional wearable device according to claim 17, wherein the second wireless communication unit is a NFC enabled communication unit acting as a NFC passive target unit configured to draw its operating power from the payment transaction unit acting as a NFC initiator unit; and/or

the antenna unit comprises an antenna of a dimension of 10x24mm adapted to draw operating power directly from a data signal generated from the data transaction unit without incorporating any active booster for amplifying the data signal.

~~19. The method for providing contactless data transaction capabilities to a traditional wearable device according to anyone of claims 12-18, wherein the secure element, the active operation unit, and the passive operation unit are configured to be operatively coupled with each other and mounted on a bendable board adapted for easy mounting on a non-planar or a curved surface or being readily insertable or embedded into a curved accommodating space; or the active operation unit is adapted to be removably connected with the secure element and/or integrated with the power transfer unit; and/or~~

~~the hybrid device further comprise a biometric unit for biometric authentication comprising one or more biometric readers / sensors for reading, writing and/or processing biometric data related to fingerprint, palm/finger vein pattern, voice pattern, face recognition, DNA, palm print, hand geometry, iris recognition, and/or retina.~~

The invention claimed is:

1. A battery-less active and passive hybrid device for secure wireless data transaction comprising: a secure element adapted for storing at least one secure applet and at least one data segment for secure contactless data transaction and operatively connected with an active operation unit and a passive operation unit; and preferably the active operation unit is adapted to be connected removably with the secure element; and

wherein the hybrid device is configured to be switchable between an active state in which the active operation unit is activated on demand to enable the hybrid device to function as an active device and adapted for provisioning one or more personalization information data, biometric data, health data, government related security data, hardware specific data, and/or a token of the device to the secure element; and a passive state in which the active operation unit is deactivated and the passive operation unit is activated/configured to enable the hybrid device to function as a passive device and adapted for conducting data verification and/or contactless data transaction operation via the secure element.

2. The hybrid device according to claim 1, wherein in the active state the active operation unit is activated by operatively coupled with and powered by a power transfer unit for conducting wireless data communication with a provisioning unit, preferably a smartphone, for provisioning of the personalization information data, biometric data, health data, government related security data, hardware specific data, and/or the token of the device to the secure element from the provisioning unit.

3. The hybrid device according to claim 1, wherein in the passive state the passive operation unit is activated by operatively coupled with and wirelessly powered by a data transaction unit, preferably a data transaction terminal, for conducting data verification and/or contactless data transaction operation with the data transaction unit via the secure element.

4. The hybrid device according to claim 2, wherein the active operation unit comprises a first wireless communication unit adapted for coupling and conducting wireless data communication with the provisioning unit, and operatively coupled with a power receiver unit and/or a transient power storage unit, preferably a supercap, adapted for receiving and/or storing power from the coupled power transfer unit.

5. The hybrid device according to claim 4, wherein the first wireless communication unit is a WIFI, BT, and/or NFC enabled communication unit, and preferably a BLE unit with contacts, preferably waterproof and/or exposed contacts.

6. The hybrid device according to claim 5, wherein the power transfer unit is a USB power transmitter, preferably equipped with connection members, preferably connection pins or hooks, and/or fixing or locking members for making contact and/or interlocking with the contacts of the BLE unit.

7. The hybrid device according to claim 3, wherein the passive operation unit comprises a second wireless communication unit, preferably a NFC enabled communication unit, adapted for coupling and conducting wireless data communication with the data transaction unit and operatively coupled with an antenna unit for receiving its operating power and data transaction data and signals from the coupled data transaction unit.

8. The hybrid device according to claim 7, wherein the second wireless communication unit is a NFC enabled communication unit acting as a NFC passive target unit configured to draw its operating power from the data transaction unit acting as a NFC initiator unit.

9. The hybrid device according to claim 7, wherein the antenna unit comprises an antenna of a dimension of 10×24 mm adapted to draw operating power directly from a data signal generated from the data transaction unit without incorporating any active booster for amplifying the data signal.

10. The hybrid device according to claim 1, wherein the secure element, the active operation unit, and the passive operation unit are configured to be operatively coupled with each other and mounted on a battery-less bendable board adapted for easy mounting on a non-planar or a curved surface or being readily insertable or embedded into a curved accommodating space; or the active operation unit is adapted to be removably connected with the secure element and/or integrated with the power transfer unit; and/or

the hybrid device further comprise a biometric unit for biometric authentication comprising one or more biometric readers/sensors for reading, writing and/or processing processing biometric data related to fingerprint, palm/finger vein pattern, voice pattern, face recognition, DNA, palm print, hand geometry, iris recognition, and/or retina.

11. The hybrid device according to claim 1, wherein the active operation unit is integrated with a power transfer or receiver unit and/or an interface for power transfer to form an universal passive provisioning unit for secure element being substantially in form of a clip/clamp or a forepart of clothes-pin and comprising a lower part with a flattened portion located at its proximal end and a depressed portion at its distal end on which a plurality of connection members are arranged for enabling power and signal transmission; and an upper part hingeably mounted over the lower part to be switchable between an opened position/state in which its proximal end is configured to make contact with the proximal end of the lower part and its distal end is configured to disengage with the distal end of the lower part to make the connection members and depressed portion accessible and a closed position/state in which its distal end is configured to make contact with the distal end of the lower part and its proximal end is configured to disengage with the proximal end of the lower part to make the connection members and depressed portion covered and concealed by the upper part.

12. A method for providing contactless data transaction capabilities to a traditional wearable device by a battery-less active and passive hybrid device for secure wireless data transaction comprising a secure element adapted for storing at least one secure applet and at least one data segment for secure contactless data transaction and operatively connected with an active operation unit, preferably adapted to be connected removably with the secure element, and a passive operation unit, comprising steps of:

mounting or embedding the battery-less active and passive hybrid device at or into the traditional wearable device; switching or setting the hybrid device to an active state by having the active operation unit activated on demand to enable the hybrid device to function as an active device and the secure element provisioned with one or more personalization information data, biometric data, health data, government related security data, hardware specific identification data, and/or a token of the device; and switching or setting the hybrid device to a passive state by having the active operation unit deactivated and the passive operation unit activated/configured to enable the hybrid device to function as a passive device and the secure element configured for conducting data verification and/or contactless data transaction operation via the secure element.

13. The method for providing contactless data transaction capabilities to a traditional wearable device according to claim 12, wherein in the active state the active operation unit is activated by operatively coupled with and powered by a power transfer unit for conducting wireless data communication with a provisioning unit, preferably a smartphone, for provisioning of the personalization information data, biometric data, health data, government related security data, hardware specific identification data, and/or the token of the device to the secure element from the provisioning unit; and/or

in the passive state the passive operation unit is activated by operatively coupled with and wirelessly powered by a data transaction unit, preferably a data transaction terminal, for conducting data verification and/or contactless data transaction operation with the data transaction unit via the secure element.

14. The method for providing contactless data transaction capabilities to a traditional wearable device according to claim 12, wherein the active operation unit comprises a first wireless communication unit adapted for coupling and conducting wireless data communication with the provisioning unit, and operatively coupled with a power receiver unit and/or a transient power storage unit, preferably a supercap, adapted for receiving and/or storing power from the coupled power transfer unit.

15. The method for providing contactless data transaction capabilities to a traditional wearable device according to claim 14, wherein the first wireless communication unit is a WIFI, BT, and/or NFC enabled communication unit, and preferably a BLE unit with contacts, preferably waterproof and/or exposed contacts.

16. The method for providing contactless data transaction capabilities to a traditional wearable device according to claim 15, wherein the power transfer unit is a USB power transmitter, preferably equipped with connection members, preferably connection pins or hooks, and/or fixing or locking members for making contact and/or interlocking with the contacts of the BLE unit.

17. The method for providing contactless data transaction capabilities to a traditional wearable device according to claim 13, wherein the passive operation unit comprises a second wireless communication unit, preferably a NFC enabled communication unit, adapted for coupling and conducting wireless data communication with the data transaction unit and operatively coupled with an antenna unit for receiving its operating power and data transaction data and signals from the coupled data transaction unit.

18. The method for providing contactless data transaction capabilities to a traditional wearable device according to claim 17, wherein the second wireless communication unit is a NFC enabled communication unit acting as a NFC passive target unit configured to draw its operating power from the payment transaction unit acting as a NFC initiator unit; and/or the antenna unit comprises an antenna of a dimension of 10×24 mm adapted to draw operating power directly from a data signal generated from the data transaction unit without incorporating any active booster for amplifying the data signal.

19. The method for providing contactless data transaction capabilities to a traditional wearable device according to claim 12, wherein the secure element, the active operation unit, and the passive operation unit are configured to be operatively coupled with each other and mounted on a bendable board adapted for easy mounting on a non-planar or a curved surface or being readily insertable or embedded into a curved accommodating space; or the active operation unit is adapted to be removably connected with the secure element and/or integrated with the power transfer unit; and/or the hybrid device further comprise a biometric unit for biometric authentication comprising one or more biometric readers/sensors for reading, writing and/or processing processing biometric data related to fingerprint, palm/finger vein pattern, voice pattern, face recognition, DNA, palm print, hand geometry, iris recognition, and/or retina.