CLAIMS

1. A single user binded hardware security module (1), SUB HSM, in the form of a wirelessly charged battery powered card comprising:

a card body (2) integrated with a plurality of hardware modules;

wherein the hardware modules include:

one or more peripheral modules to which a user can interact therewith for providing input and/or output data,

one or more transmission modules (20) for establishing a data transfer link to connect with a device which a user interface is operated thereon via a communication protocol,

a battery module (30) for supply electricity to the operational modules, and

a centralised microcontroller unit (40) for controlling the operations of the hardware modules;

wherein the transmission module (20), the battery module (30), and the microcontroller unit (40) are entirely housed within the card body (2);

wherein the battery module (30) includes an ultra-thin battery (31), one or more induction coils (33) and associated circuitry (32) configured to receive and convert electromagnetic fields into electrical energy for charging the ultra-thin battery (31);

wherein the centralised microcontroller unit (40) comprises one or more direct drive applications that directly control the hardware modules and directly process input data acquired by the peripheral modules so that the hardware modules are operated by the centralised microcontroller unit (40) without their respective dedicated microcontroller units;

wherein the centralised microcontroller unit (40) is further configured to perform hardware accelerated execution of cryptographic primitives, including encryption, hashing, and cryptographic signatures, thereby creating a trusted zone within the SUB HSM (1) to prevent unauthorized access or tampering through physical and/or software exploitation; and

wherein at least two types of the peripheral modules are coupled to allow the user to interact with the different types of the peripheral modules in just one action;
wherein the one action is performed by a biometric reader (13) embedded with a soft switch input sensors (14) to enable the user to activate the SUB HSM (1) by switching it from a low energy deep sleep mode to a full powered active mode and then perform a biometric fingerprint scanning operation, all in response to a single touch on the biometric reader (13);
wherein the centralised microcontroller unit (40) is configured to operate the cryptographic key generation and credential signing entirely in an offline mode with the exception of a single instance where the SUB HSM (1) is switched to an online mode to transmit the generated cryptographic keys and/or the signed credentials, and after which it switches back to the offline mode;
the centralised microcontroller unit (40) is configured to operate in an unbalance communication mode where the SUB HSM (1) exclusively initiates and/or disconnects the data transfer link; and
wherein the centralised microcontroller unit (40) is configured to store one or more digital identities which is bound to the sole designated user via biometrics of the user, it serves as a presentation to present the user to appropriate predetermined and pre-associated digital system.

2. The SUB HSM (1) according to claim 1, wherein the peripheral modules include one or more light indicators (11) or a display unit for providing visual feedback to the user.

3. The SUB HSM (1) according to claim 1 or claim 2, wherein the peripheral modules include one or more sound generators for providing audible feedback to the user.

4. The SUB HSM (1) according to any one of claims 1 to 3, wherein the peripheral modules include one or more piezoelectric vibrators (12) for providing tactile feedback to the user.

5. The SUB HSM (1) according to claim 1, wherein the centralised microcontroller unit (40) is configured to process the captured biometric traits of the user and verify an identity of the user using a template-free Artificial Intelligent driven biometric authentication method and/or conventional template based matching method.

6. The SUB HSM (1) according to claim 5, wherein the peripheral modules include one or more mechanical or electrical actuators (14) embedded with the biometric reader (13) for receiving input data from the user.

7. The SUB HSM (1) according to claim 5 or claim 6, wherein the peripheral modules include one or more inertial sensors embedded with the biometric sensors (13) for capturing motions and/or orientations of the SUB HSM (1) as input data.

8. The SUB HSM (1) according to claims 5 to 7, wherein the biometric sensor (13) is a biometric fingerprint sensor and the centralised microcontroller unit (40) is configured to perform a first level of authentication that requires a submission of a predetermined sequence of input data from the peripheral modules to authenticate the user prior to the processing of input data by a single action of placing user's finger on the biometric fingerprint sensor.

9. The SUB HSM (1) according to claim 8, wherein the centralised microcontroller unit (40) is configured to perform a second level of authentication that determines liveness of the user by detecting electrical charges that naturally exists on a surface of the user (live) and further perform third level of authentication by analysing behavioural patterns of the user based on the predetermined sequence of input data, habitual handling, movement of device, or any combination thereof.

10. The SUB HSM (1) according to any one of claims 1 to 9, wherein the centralised

microcontroller unit (40) is configured to generate cryptographic keys and sign credentials upon successful authentication and verification of the user.