CLAIMS

1. A computer implementable protocol for establishing a momentary trust zone as part of a procedure, comprising the steps of:

receiving, by a user interface (20), an input of a user to initiate the procedure;

instructing, by the user interface (20), the user to activate a personal cryptographic key generator (10);

performing, by the personal cryptographic key generator (10), an ephemeral key generation and/or credentials signing upon activation by the user;

transmitting, by the personal cryptographic key generator (10), newly generated ephemeral keys and/or signed credentials to a cryptographic processor (30) which is embedded within the user interface (20);

processing, by the cryptographic processor (30), data received from the user interface (20) and the personal cryptographic key generator (10); and

transmitting, by the cryptographic processor (30), the processed data to a verification processor (40) which is embedded within service provider servers;

whereby the momentary trust zone is established when the processed data is authenticated and verified by the verification processor (40) with non-interactive Zero Knowledge Proof cryptographic primitive;

wherein the procedure includes a user on boarding process, a user login process, an operation process, or any combination thereof;

wherein the personal cryptographic key generator (10) is configured to: (a) operate entirely in an offline mode with the exception of a single instance where the personal cryptographic key generator (10) is switched to an online mode in which a data transfer link is established to transmit the generated ephemeral keys and/or the signed credentials, and after which it switches back to the offline mode; and (b) operate in an unbalance communication mode where the personal cryptographic key generator (10) exclusively initiates and/or disconnects the data transfer link to a device which the user interface (20) is operated thereon;

wherein the cryptographic processor (30) is configured to (a) perform an encryption and/or decryption on the received data to ensure data confidentiality, (b) perform a data integrity checking algorithm on the received data, and (c) perform signatures signing on the user interface credential to authenticate and verify the user interface (20); and

wherein the personal cryptographic key generator (10) is a wirelessly charged battery powered card having one or more input modules (12) to which the user can interact therewith for the activation of the personal cryptographic key generator (10), and a vibration module (13) configured to vibrate the one or more input modules (12) or at least one section of the wirelessly charged battery powered card using a vibration pattern selected from a plurality of pre-stored vibration patterns based on predetermined conditions when the user interacts with the one or more input modules (12).

2. The computer implementable protocol according to claim 1, wherein the protocol, during the user onboarding process, comprises the steps of:

retrieving, by the cryptographic processor (30), a signed certificate from a certificate authority server (60);

receiving, by the user interface (20), a unique identity of the personal cryptographic key generator (10) to verify with a device registry server (50);

registering, by the cryptographic processor (30), the user interface' (20) signed credential verification key;

instructing, by the user interface (20), the user to activate the personal cryptographic key generator (10);

performing, by the personal cryptographic key generator (10), an ephemeral key generation and/or credentials signing upon activation by the user;

transmitting, by the personal cryptographic key generator (10), the generated ephemeral keys and/or signed credentials to the cryptographic processor (30);

forwarding, by the cryptographic processor (30), a verification key of the personal

cryptographic key generator (10) to the verification processor (40); and

binding, by the verification processor (40), the verification key with the user's profiles including pseudo/Official Digital Identities.

3. The computer implementable protocol according to claim 1 or claim 2, wherein the protocol, during the operation process for user to login into a targeted service provider's system, comprises the steps of:

providing, by the user interface (20), functional options for the user to select and execute upon successful establishment of the momentary trusted zone established and user authentication completed with non-interactive Zero Knowledge Proof cryptographic primitive;

instructing, by the cryptographic processor (30), the user interface (20) to request for activating the personal cryptographic key generator (10) upon receiving one or more instruction messages of the function options which required signatures from the user interface (20);

instructing, by the user interface (20), the user to activate the personal cryptographic key generator (10);

performing, by the personal cryptographic key generator (10), an ephemeral key generation and/or credentials signing upon activation by the user;

transmitting, by the personal cryptographic key generator (10), the newly generated ephemeral keys and/or signed credentials to the cryptographic processor (30);

performing, by the cryptographic processor (30), signature signing on the instruction messages; and

transmitting, by the cryptographic processor (30), the signed instruction messages, the signed credential, and a newly generated verification key to the verification processor (40) that will complete the user authentication using the non-interactive Zero Knowledge Proof cryptographic primitive to complete the login operation into the targeted service provider's system.

4. The computer implementable protocol according to any one of claims 1 to 3, wherein the personal cryptographic key generator (10) comprises a physical isolation arrangement for protecting it physically against unauthorised access and a counterparty cryptography processor to establish the data transfer link in a secure fashion via one or more cryptographic protocols.

5. The computer implementable protocol according to any one of claims 1 to 4, wherein the personal cryptographic key generator (10) comprises a notifier to provide a notification of a current operation status.

6. The computer implementable protocol according to any one of claims 1 to 5, wherein the one or more input modules (12) are in the form of one or more biometric sensors for capturing biometric traits of a user and a processor for verifying an identity of the user using an in-device hardware secure memory stored template and/or template-free Artificial Intelligent driven biometric authentication method, whereby the ephemeral keys and credentials are respectively generated and signed upon successful verification of the user’s biometric.

7. The computer implementable protocol according to any one of claims 1 to 6, wherein the one or more input modules (12) are in the form of one or more mechanical or electric actuators for receiving inputs from the user.

8. The computer implementable protocol according to any one of claims 1 to 7, wherein the vibration module (13) is a piezoelectric vibrator or electro-magnetic actuator.

9. The computer implementable protocol according to claim 8, wherein the piezoelectric vibrator or electro-magnetic actuator is stacked with the one or more input modules.

10. The computer implementable protocol according to claim 8, wherein the piezoelectric vibrator or electro-magnetic actuator is arranged to partially or entirely surround the one or more input modules.

11. The computer implementable protocol according to any one of claims 1 to 10, wherein the generated ephemeral keys and/or signed credentials are of a predetermined structure and size for them to be transmitted in a consistent and secure manner.

12. The computer implementable protocol according to any one of claims 1 to 11, wherein the credential is signed using one or more hashing algorithms with Digital Signature Algorithms executed by secured hardware accelerated execution of user's identity binded personal cryptographic key generator (10).

13. The computer implementable protocol according to any one of claims 2 to 12, wherein the personal cryptographic key generator (10) comprises a QR code that contains the unique identity of the personal cryptographic key generator (10), and the unique identity is retrievable through scanning the QR code.

14. The computer implementable protocol according to any one of claims 3 to 13, wherein the cryptographic processor (30) is configured to perform a cascading signature operation that signs a batch of instruction messages.

15. A personal cryptographic key generator (10) in the form of a wirelessly charged battery powered card comprising:

a card body (11);

one or more input modules (12) to which a user can interact therewith for activating the personal cryptographic key generator (10);

a vibration module (13) configured to vibrate the one or more input modules or at least one section of the card body;

a transmission module (14) for establishing a data transfer link to connect with a device which the user interface (20) is operated thereon via a communication protocol;

a battery (15) for supply electricity to components of the personal cryptographic key generator (10); and

a processing unit (16) connected to the one or more input modules (12), the vibration module (13), the transmission module (14), and the battery (15);

wherein the processing unit (16) is configured to:

(a) generate ephemeral keys and sign credentials upon the user activates the personal cryptographic key generator (10) via the one or more input modules (12);

(b) instruct the vibration module (13) to perform a vibration pattern selected from a plurality of pre-stored vibration patterns based on predetermined conditions when the user interacts with the one or more input modules (12);

(c) operate the cryptographic key generator (10) entirely in an offline mode with the exception of a single instance where the personal cryptographic key generator (10) is switched to an online mode in which the data transfer link is established to transmit the generated ephemeral keys and/or the signed credentials, and after which it switches back to the offline mode; and

(d) operate in an unbalance communication mode where the personal cryptographic key generator (10) exclusively initiates and/or disconnects the data transfer link.

16. The personal cryptographic key generator (10) according to claim 15, the one or more input modules (12) are in the form of one or more biometric sensors for capturing biometric traits of a user and the processor unit (16) for verifying an identity of the user using an in-device hardware secure memory stored template and/or

template-free Artificial Intelligent driven biometric authentication method, whereby the ephemeral keys and credentials are respectively generated and signed upon successful verification of the user.

17. The personal cryptographic key generator (10) according to claim 15 or claim 16, wherein the one or more input modules (12) are in the form of one or more mechanical or electric actuators for receiving inputs from the user.

18. The personal cryptographic key generator (10) according to any one of claims 15 to 17, wherein the vibration module (13) is a piezoelectric vibrator or an electro-magnetic actuator stacked with the one or more input modules.

19. The personal cryptographic key generator (10) according to claim 18, wherein the piezoelectric vibrator or electro-magnetic actuator is arranged to partially or entirely surround the one or more input modules.

20. The personal cryptographic key generator (10) according to claim 15, wherein the battery is wirelessly rechargeable by wireless charging modules (27, 28) having a coil or antenna (28) for capturing the electromagnetic field generated by an external transmitter and a rectifier and control circuitry (27) for converting an initial current induced in the coil or antenna (28) into a current voltage suitable for charging the battery (15).