

SINGLE USER BINDED HARDWARE SECURITY MODULE (SUB HSM)

FIELD OF INVENTION

The invention relates to network security at the point of contact and access, typically the login/password process, by human to digital system which includes both hardware and software. More particularly, the invention relates to the replacement of current password part of the process that functioned as user authentication with the use of a ONE TOUCH hardware operation of SUB HSM, preferably a wirelessly charged battery powered card, as a root key to a series of cascading cryptographic authentication operations to establish a momentary trusted group of hardware and software during the login process and digital service operation procedure in the midst of untrusted zone, spanning from end-user device to the entry point of the trusted zone managed by secured access management, combined with utilization of non-interactive Zero Knowledge Proof cryptographic primitive to authenticate the user to secured access management, the gatekeeper, of digital system.

BACKGROUND OF THE INVENTION

According to various cybersecurity reports, the user login processing channel remains a common entry point for hackers, with estimates ranging from 60-80% of attacks involving compromised passwords or credentials. This suggests that login attacks are a significant entry point for attackers.

Other methods of attack may include network-based attacks such as phishing, malware, or other types of exploits, as well as email attacks that trick users into clicking on malicious links or downloading infected attachments. USB-based attacks can also be a potential threat if an attacker gains physical access to a system or device and is able to plug in a USB drive that contains malware. Their common aim is to obtain User's ID

and password including One Time Password delivered via SMS or hardware token device generated to be keyed-in or Application generated tokens to be keyed-in.

A wide arsenal of tools (predominantly software-based) and methods exists and are deployed to mitigate the above threats. Ironically, even these software-based tools have a similar user login process and more importantly their administrator's login process. Thus, they are exposed to similar threats and are as vulnerable as the systems they are designed and deployed to protect.

Therefore, when these systems that are protecting the protected systems are compromised but undetected, Zero-trust architecture has become an increasingly popular framework, implemented according to best practices and certified body or relevant standards, for securing systems and networks. The idea behind zero trust is simple: rather than assuming that all components within a system are trustworthy, the system should assume that no component can be trusted until proven otherwise. This means that every component, including applications, devices, and users, must be repeatedly verified and authenticated before being granted access to resources or executing functions of process. However, current tools that configure and enforce Zero Trust operations are software based too, hence have similar vulnerabilities as all the systems that they are deployed to protect. Furthermore, cybersecurity breaches such as infamous solar winds and recent CrowdStrike alongside with Microsoft defender confirmed their inadequacies.

Current computing and networking domain

The relationship between devices in the systems and networks are commonly based on client-server architecture used in current prevalent computer networking and distributed computing. Similar relationship has been adopted by digitally control devices such as doors, cars, consumer electronics and entertainment. In this model, a

central server provides resources or services to multiple clients that connect to it over a network. In a client-server reference model, there are typically two main components:

A) The client, which is a program or application overlaid by User Interface (UI) and User Experience (UX) that runs on the user's device (e.g. computer, smartphone, or tablet) and sends requests to the server. The User Interface (UI) refers to the visual and interactive aspects of an application or website that users interact with directly. It includes elements such as buttons, menus, text fields, and graphics, as well as the layout, typography, and colour scheme of the user interface. For example, the login screen presented to the User with fields to key in required information such as login ID and password. The User Experience (UX) refers to the overall experience that a user has when interacting with an application or website, including how easy it is to use, how efficient it is, and how enjoyable it is. UX design focuses on the user's needs, goals, and behaviour to create an interface that is intuitive, efficient, and satisfying to use. In other words, UI design is focused on creating an attractive and functional visual interface that users can interact with, while UX design is focused on creating an experience that meets the user's needs and goals. These software runs on the device operating systems and communication functions.

B) The server, which is a program or application that runs on a central computer or arrays of computers (cloud computing) or network device and responds to client requests by providing data, resources, or services. These components are connected by a network, such as the internet or a local area network (LAN). When the client needs to access a resource or service provided by the server, it sends a request over the network to the server. The server processes the request and sends a response back to the client. The client and server can be on different physical machines, and the server may handle requests from multiple clients simultaneously. This allows for efficient resource sharing and scalability in large-scale systems.

The operation of the client-server model can be described as follows:

1. A client application running on a user's device (e.g. a computer, tablet, or smartphone) initiates a connection to a server application over a network by login process, commonly managed by LDAP servers with combination of authentication servers and access management servers collectively known as Identity Access Management (IAM) or as stated in NIST 800-207, the Policy Decision/Enforcement Point(PDP/PEP).
2. The server application listens for incoming connections from clients and accepts the connection request from the client that has been permitted by IAM.
3. Once the connection is established, the client sends a request to the server to perform a specific action, such as retrieving data or executing a function.
4. The server receives the request and processes it, using its available resources to generate a response.
5. The server sends the response back to the client over the network.
6. The client receives the response and takes the appropriate action based on the information received.
7. If necessary, the client may send additional requests to the server to complete a task or obtain more information.
8. Once the client is done with the server, it closes the connection.

The client-server model is used in a wide range of applications, such as web servers, email servers, database servers, and game servers that constitutes the foundation of Digital Domain. It allows for efficient resource sharing and provides a scalable architecture that can accommodate large numbers of clients that serves the users (Humans). There are two main categories, external users and internal users including admins, normal users, technicians, guest and relatives.

Log in page which is part of login process is normally the first User's touchpoint with the Digital Domain. The system login process typically involves the following steps:

1. The user navigates to the login page of the system they want to access.
2. The user enters their username or email address or service provider issued ID or government issued Digital ID and subsequent password into the appropriate fields on the login page.
3. The system checks the entered credentials against its database of authorized users to ensure that they are valid and match an existing user account.
4. If the credentials are valid, the system grants access to the user and directs them to the appropriate user interface. If the credentials are invalid, the system displays an error message and prompts the user to re-enter their credentials.
5. Depending on the system's security settings, the user may be prompted to provide additional authentication factors, such as a security question, biometric authentication (e.g. fingerprint, facial recognition that are centrally stored, retrieved and matched by systems that has similar login process), or a one-time code sent to their mobile device via SMS or an Application to be displayed and keyed-in or a hardware device generated code to be keyed-in.
6. Once the user is authenticated and authorized, they can access the features and functions of the system based on their permissions and privileges.

It's worth noting that the login process may vary slightly depending on the system and its security policies. Some systems may also include additional steps or require specific authentication methods to ensure a high level of security.

However, despite these robust approach to security, there is still two common points of weakness that hackers can exploit: the human factor plus the more sophisticated UI/UX that exposes vast surface for attack. Whether it's through human weakness exploited by social engineering or malware installed within UI/UX operating with more complex local, remote cloud-based servers and security tools before and after deployment, Therefore, the weakest link in any security system is often the user and end-user device (deemed in untrusted zone), particularly during login. The problem is that every

security system has the same common point of vulnerability: the login process. As a result, even the most secure systems are only as strong as their weakest link, in particular, this weak link. The current method, mainly user focused, identity and authentication methods of managing passwords and access controls relies on software-based systems that can themselves be hacked, thus, making it difficult to trust them to perform their role of protecting systems against software-based threats.

To strengthened User identity authentication, most financial related operation added the use of one-time passwords (OTPs) as 2 Factor Authentication (2FA). Some deployed additional authentication methods called Multi-Factored Authentication (MFA). OTPs are unique codes generated for a single use are utilized as additional authentication of users when accessing a system or network. OTPs can be sent via SMS, email, or generated using mobile applications. While OTP is considered as a stronger authentication method than static password, they are not completely immune to vulnerabilities. Various techniques exist frequently used by cybercriminals to remotely intercept, retrieve or acquire OTPs sent through SMS or email if these channels are not secure. For example: like any other security mechanism, OTPs are not fool proof and has been vulnerable to different types of attacks. Here are some examples of OTP hacks:

1. Social engineering: Attackers can trick the user into revealing the OTP by phishing or other social engineering techniques. For example, an attacker may send an email or SMS claiming to be from the user's bank or other trusted organization, and ask the user to provide the OTP for verification.
2. Man-in-the-middle attack: In a man-in-the-middle attack, the attacker intercepts the communication between the user and the server and can steal the OTP. This can be done by intercepting the SMS containing the OTP or by using a fake login page to capture the OTP entered by the user.
3. Configuration attack: A Configuration attack is done by gaining access to permission settings and permit access to messages that allow hackers to access OTP codes.

4. OTP interception: An attacker can use malware or other techniques to intercept the OTP as it is generated on the user's device. This can be done by infecting the user's device with malware or by exploiting vulnerabilities in the device or the OTP generation process.
5. Pretexting: Pretexting involves the attacker impersonating the user or a trusted entity and requesting the OTP from the service provider. This can be done by using stolen credentials or other information to convince the service provider to provide the OTP.

The interception of OTPs can lead to severe consequences for the victim, as cybercriminals can assume easy access passage because all those institutions that implemented OTP as THE final and decisive step of User authentication, they can gain unauthorized access to sensitive information or systems or services that require authentication. This access can result in a wide range of issues, including financial losses, data breaches, identity theft, operational disruption, loss of data integrity and other forms of cybercrime. For instance, if a cybercriminal intercepts an OTP used to authenticate online banking transactions, they can potentially make fraudulent transactions using the victim's account, leading to financial losses for the victim. Similarly, if the OTP is used to access confidential business information, the interception can lead to corporate espionage, loss of intellectual property, and damage to the organization's reputation. Moreover, cybercriminals can use the intercepted OTP to steal personal information, such as social security numbers, credit card numbers, and other sensitive information. This information can be used for identity theft, which can lead to long-lasting financial and legal consequences for the victim. In some cases, cybercriminals may even use the intercepted OTP to gain control of the victim's device or system, enabling them to conduct further attacks or to install malware that can cause even more damage.

Therefore, by adding another layer of authentication that is already hacked by many

methods over the weak static password authentication method including industry standard based password managers (eg FIDO2 complied password manager) and proprietary password managers to be regarded and depended as the final pass have to be seriously reconsidered.

There are several alternative security methods to OTPs that can be used to protect sensitive information and prevent unauthorized access. One of them is biometric authentication, where a user's biometric data collected from their smartphone is compared to a template stored either on the mobile device or a cloud server. While biometric authentication on smartphones or servers offers several advantages, including convenience and enhanced security, it also has some drawbacks that need to be carefully considered. The potential risks of using biometric authentication on smartphones or servers include the multipurpose nature of smartphones that can prompt hacking and the transmission of biometric data over insecure networks that can be intercepted.

A similar method of the biometric authentication can be found in US20030139984A1. This Patent discloses a system and method that enables cashless and clerkless transactions to purchase a wide variety of products. The system is made up of four key functional components, including a point-of-sale terminal, identification devices, databases, and a network to link them. To carry out a cashless and clerkless transaction, the system collects information about the product, personal details, and biometric information of the individual who wants to buy the product. This captured biometric information is matched against stored, typically in a centralized multiuser database not the point of usage, biometric data to verify the buyer's identity. If the buyer's identity is confirmed, the system permits the sale transaction and updates inventory and financial databases accordingly. Additionally, the system can be used to confirm that the customer has legitimately purchased merchandise as they exit the store.

Nevertheless, the biometric templates are stored on the server which leads to a potential loop hole where the transmission of biometric information can be intercepted by cybercriminals if the network is not secure and compromising the user's biometric data. If the biometric data is stolen, it cannot be easily changed like a password, making it a significant risk for users. Furthermore, Biometric data is considered sensitive personal information that is impossible to alter or replace when stolen or compromised, like the way we change and replace stolen or compromised password, and is subject to data privacy regulations, such as the Personal Data Protection Act (PDPA) in some countries. The PDPA outlines strict guidelines for the collection, use, and disclosure of personal data, including biometric data. Therefore, any company or organization that collects, uses, or stores biometric data on a server must ensure that they comply with the PDPA or similar data privacy regulations to protect the privacy and security of their customers' personal information. Failure to do so can result in severe legal and financial consequences, as well as damage to the company's reputation.

In the digital realm, hackers can unlawfully obtain an individual's credentials to create an account on a social media platform, subsequently posting defamatory content, including unauthorized or fake pictures or videos. When the victim lodges a complaint with the social media platform, it is difficult for the victim to authenticate their identity. This underscores the challenge in digitally verifying one's identity, as even photographs or videos can be manipulated using face-swapping technology to falsify credentials.

To address these challenges, a new approach is needed that complements Trusted Zone of Zero Trust Architecture with establishment of momentary trust in the Untrusted Zone of derives the security protocol based on Zero Trust of all related operating entities, that use dedicated hardware without operating system and normally offline and only online to transmit its generated cryptographic key as the root key for series of cascading authentication operations between neighbouring entities(hardware, software) resulting in Zero Knowledge Proof operation of User authentication without any subsequent need

of key storage or recovery, hence reduce to the space for hacks via social engineering that exploit human weakness to the minimum. This hardware-rooted authentication protocol provides a stronger layer of protection against unauthorized access and breaches without any further reading or keying in of any secret codes by the User. By moving away from layers of software only-based security operations, organizations can better protect their systems and networks from attacks that exploit the human factor. To even begin, this user hardware needs to be completely isolated in order to establish a Trusted Zone within the environment of the hardware itself. This invention provides such a hardware device and system thereof.

SUMMARY OF INVENTION

In a first aspect of the invention, there is provided a SUB HSM in the form of a wirelessly charged battery powered card, comprises a card body 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 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 for supply electricity to the operational modules, and a centralised microcontroller unit for controlling the operations of the hardware modules; wherein the transmission module, the battery module, and the microcontroller unit are entirely housed within the card body; wherein the battery module includes an ultra-thin battery, one or more induction coils and associated circuitry configured to receive and convert electromagnetic fields into electrical energy for charging the ultra-thin battery; wherein the centralised microcontroller unit 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 without their respective dedicated microcontroller units; and wherein the centralised microcontroller unit is further configured to execute

hardware accelerated cryptographic primitives, including encryption, hashing, and cryptographic signatures, thereby creating a trusted zone within the SUB HSM to prevent unauthorized access or tampering through physical and/or software exploitation.

Preferably, the peripheral modules may include one or more light indicators or a display unit for providing visual feedback to the user.

Preferably, the peripheral modules may include one or more sound generators for providing audible feedback to the user.

Preferably, the peripheral modules may include one or more piezoelectric vibrators for providing tactile feedback to the user.

Preferably, the peripheral modules may include one or more biometric readers for capturing biometric traits of the sole designated user. The centralised microcontroller unit may be configured to process the captured biometric traits of the sole designated user and verify an identity of the user using a template-free Artificial Intelligent driven biometric authentication method and/or conventional matching method. The biometric module be embedded with Artificial Intelligent driven soft switch input sensors to trigger the SUB HSM switching from lowest energy deep sleep mode (to conserve battery stored energy) to attain full powered active mode in shortest time duration to then perform the biometric fingerprint scanning operation thus acheiving ONE TOUCH SUB HSM operation.

Preferably, the peripheral modules may include one or more mechanical or electrical buttons embedded in the fingerprint scanning module for receiving input data from the user.

Preferably, the peripheral modules may include one or more inertial sensors embedded in the fingerprint module for capturing motions and/or orientations of the SUB HSM as input data.

Preferably, the centralised microcontroller unit may be 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.

Preferably, the centralised microcontroller unit may be 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 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. In one example, the second level of authentication detects whether the biometrics provided by the user are fake such as 3-D printed fingers or chopped fingers.

Preferably, the centralised microcontroller unit may be configured to generate cryptographic keys and signed credentials upon successful authentication and verification of the user by single action of placing user's finger on the fingerprint scanner module embedded with input sensors.

Preferably, the centralised microcontroller unit may be 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 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 that will not response to any wake-up calls or any form of wireless connection attempt initiated by any devices.

Preferably, the centralised microcontroller unit may be configured to operate in an unbalance communication mode where the SUB HSM exclusively initiates and/or disconnects the data transfer link.

Preferably, the centralised microcontroller unit may be configured to store a digital identity which is bound to the sole designated user via biometrics, it serves as a presentation to present the user to a digital system.

One skilled in the art will readily appreciate that the invention is well adapted to carry out the objects and obtain the ends and advantages mentioned, as well as those inherent therein. The embodiments described herein are not intended as limitations on the scope of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

For the purpose of facilitating an understanding of the invention, there is illustrated in the accompanying drawing the preferred embodiments from an inspection of which when considered in connection with the following description, the invention, its construction and operation and many of its advantages would be readily understood and appreciated.

Fig. 1 is a schematic diagram illustrating a SINGLE USER BINDED HARDWARE SECURITY MODULE (SUB HSM) in the form of a card.

Fig. 2 is a schematic diagram illustrating a general architecture of the SUB HSM.

Fig. 3 is a schematic diagram illustrating a general architecture of the SUB

HSM integrated with a ONE TOUCH arrangement.

DETAILED DESCRIPTION OF THE INVENTION

It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer program instructions. These computer program instructions may be provided to a processor of a general-purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, that execute via the processor of the computer or other programmable data processing apparatus, create means for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

These computer program instructions may also be stored in a computer-readable memory that can direct a computer or other programmable data processing apparatus to function in a particular manner, such that the instructions stored in the computer-readable memory produce an article of manufacture including instruction means that implement the function/act specified in the flowchart and/or block diagram block or blocks.

The computer program instructions may also be loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer implemented process such that the instructions that execute on the computer or other programmable apparatus provide steps for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

The invention will now be described in greater detail, by way of example, with reference to the drawings.

The invention provides a single user binded hardware security module **1**, ONE TOUCH operated SUB HSM, in a card form that can be easily carried around and safely kept by a user. The aim of the SUB HSM **1** is to establish a trusted zone within its own environment with the most convenient yet safe operation. To achieve this, it needs to fulfil any combination or all of the following requirements: Firstly, the SUB HSM **1** requires a physical isolation arrangement to safeguard it against unauthorised access and it itself is a hardware based Trusted Execution Environment. Secondly, it should have no wired connections (both data and power supply) to ensure further security. Thirdly, the processing unit of the SUB HSM **1** must directly drive its connected peripheral modules, particularly, the input peripherals, eliminating the need for individual microcontroller units within these modules, which could be vulnerable to hacking (known as side-channel attack). Fourth, all modules within the SUB HSM **1** must execute at the hardware level, thereby eliminating reliance on operating systems and addressing potential weaknesses associated with the operating systems, such as login procedures, deposition of malwares and etc. Last but not least, the SUB HSM **1** operates in an unbalance communication mode where it exclusively initiates and/or disconnects any data transfer link. Furthermore, the data transfer is a one directional transfer, which means that the SUB HSM **1** is only allow to transmit data to external device and will only pick specific authenticated data of particular format/type from designated momentarily connected authorised device, and it is prevented from receiving data of any type from any external device or unauthorised external device.

Referring to **Fig. 1** and **Fig. 2**, an example of the SUB HSM **1** is illustrated. The SUB HSM **1**, which takes the form of a wirelessly charged battery powered card as an initial form. It should be understood that the SUB HSM **1** can be further manifested in other form of portable shapes such as capsule, key chains, watch, ring, arm band and etc. The

SUB HSM **1** comprises a card body **2** integrated with a plurality of hardware modules. Preferably, all functions of the SUB HSM **1** are carried out by the dedicated hardware modules so that malwares cannot be deposited into the SUB HSM **1**. As a result, the risk of malware or other software-based attacks can be prevented. Preferably, the card body **2** is a durable and compact substrate that encapsulates the components of the SUB HSM **1**. The card body **2** serves as the physical framework for the components of the SUB HSM **1**, ensuring secure integration and protection for the components. The card body **2** can be made of a resin material which includes but not limited to polyvinyl chloride, polycarbonate, polyethylene terephthalate glycol, acrylonitrile butadiene styrene, polyethylene, polyester or any combination thereof. The hardware modules include one or more peripheral modules, a transmission module **20**, a battery module **30**, and a centralised microcontroller unit **40**. Preferably, the transmission module **20**, the battery module **30**, and the centralised microcontroller unit **40** are entirely housed within a protective layer of the card body **2**, whereas the one or more peripheral modules **11-15** can be partially exposed. The resin card body **2** makes it challenging for unauthorised individuals to access by peeling or modify the hardware modules without causing irreparable damage. Traces, that connect the hardware modules to one another, will break if the resin card body is breached. Alternatively, the card body **2** can comprise a QR code that contains the unique identity of the SUB HSM **1**, and the unique identity is retrievable through scanning the QR code.

Preferably, the one or more peripheral modules allow the user to interact with it for providing input and/or output data, thereby activating the SUB HSM **1**. In one embodiment, dedicated microprocessor units within these peripheral modules have been removed or omitted during their respective manufacturing processes.

The peripheral modules may include a plurality of different modules for providing visual, audible and tactile feedbacks to the user, indicating the status of the SUB HSM **1**. Preferably, the peripheral modules may include one or more light indicators **11** or a

display unit for providing visual feedback to the user. By way of example, the light indicators **11** can be in the form of Light-Emitting Diode, LED indicators which emit different colours or patterns to convey different status information to the user. For example, a green colour light may indicate that the device is operating normally, while a red colour light could be a signal of an error or security alert. The display unit can be in the form of a Liquid Crystal Display, LCD screen or any other state of the art screen which has the features of low power consumption and thin profile. The display unit could display alphanumeric characters, symbols, and graphical elements to convey detailed information and prompts to the user.

The peripheral modules may include one or more sound generators for providing audible feedback to the user. Preferably, the sound generators can be in the form of one or more piezoelectric buzzer for producing audible sounds. By way of example, the buzzer could emit a short beep to confirm successful authentication, or it could also sound a continuous tone to indicate an error or security breach.

The peripheral modules may include one or more vibration modules **12** for providing tactile feedback to the user. The one or more vibration modules **12** can be configured to vibrate at least one section of the card body **2** with at least one vibration pattern selected from a plurality of pre-stored vibration patterns based on predetermined conditions when the user interacts with the one or more peripheral modules. Preferably, the vibration module **12** is a piezoelectric vibrator that can be arranged to stack with the one or more peripheral modules, to partially or entirely surround the one or more peripheral modules, or to dispose at any location within the card body **2**. By way of example, the predetermined conditions may include a vibration pattern that provide one-time tactile feedback indicating a successful verification of the user during a biometric authentication process. In another example, the predetermined conditions may include a vibration pattern that provide two-time tactile feedback indicating a failed verification of the user during the biometric authentication process. Yet in

another example, the predetermined conditions may include a vibration pattern that provide a few seconds long tactile feedback indicating a successful activation of the SUB HSM **1**. For individuals with visual challenges, the vibration patterns generated by the vibration module as a feedback mechanism, allowing them to discern the outcome of their interaction with the one or more peripheral modules. This provides a practical solution for blind users who may rely on distinct vibration patterns to interpret pressing results and operation status, thereby enhancing the overall user experience and usability of the SUB HSM **1** for individuals with diverse accessibility requirements. The piezoelectric actuator is preferably a tactile feedback-piezo haptic configured to provide at least one vibration pattern selected from a plurality of pre-stored vibration patterns based on predetermined conditions when the user interacts with the one or more peripheral modules. The kinetic energy generated to produce tactile feedback can be harvested for recharging the battery module **30**. Alternatively, the piezoelectric actuator can be used as an energy generator to recharge the battery module **30**. For example, the user can shake the card for a predetermined time which is enough for a one-time operation.

The one or more peripheral modules may include one or more mechanical or electrical actuators **14** for receiving input data from the user. Mechanical actuators can be in the form of mechanical buttons which can be pressed or moved by the user. The mechanical buttons typically consist of tactile switch mechanism that makes or breaks electrical contract when activated. Electrical actuators can be in the form of touch-sensitive, capacitive buttons, or even virtual buttons provided by a touch screen, which do not have moving parts like the mechanical buttons. Instead, they rely on changes in capacitance when touched by a finger or conductive object to detect input.

The one or more peripheral modules may include one or more biometric sensors **13** for capturing distinctive biometric traits of a user. Preferably, the biometric sensors **13** can be fingerprint sensors for capturing unique fingerprint characteristics of the user upon

contact. The inclusion of the biometric sensors **13** effectively contributes to the elimination of the need for traditional password-based authentication which is susceptible to hack due to its inherent vulnerabilities as explained in the background art. The biometric sensors **13** may also detect electrical charge that naturally exists on a surface of the user. Such information is useful for determining the liveness of the user. In one example, the biometric sensors **13** may detect whether the biometrics provided by the user are fake such as 3-D printed fingers or chopped fingers.

The one or more peripheral modules may include one or more inertial sensors for capturing motions and/or orientations of the SUB HSM **1** as input data. The inertial sensor can be but is not limited to accelerometer and/or gyroscope. The one or more inertial sensors are capable of detecting gestures or movements initiated by the users as input data. The one or more inertial sensors can be activated by the centralised microcontroller unit to capture gestures or movements as a security input feature for activating the SUB HSM **1**. It should be understood that not only the inertial sensors can perform the function of converting mechanical energy into electricity for recharging the battery module **30**, the other peripheral modules may also perform the same function. For example, the user may also repeatedly press the buttons so that the mechanical energy obtained from the pressing can be converted into electricity for recharging the battery module **30**.

Fig. 3 illustrates a further embodiment of the SUB HSM **1** where different peripheral modules such as the one or more mechanical or electrical actuators **14** and the one or more biometric sensors **13** can be combined to achieve the functionality of the ONE TOUCH arrangement. The main purpose of integrating the ONE TOUCH arrangement into the SUB HSM **1** is to significantly improve the user experience when activating the SUB HSM **1**. By way of example, the ONE TOUCH arrangement may incorporate a biometric module **13** embedded with Artificial Intelligent driven soft switch input sensors **14** to enable the user to activate the operation of the SUB HSM **1** in just one

action instead of multiple subsequent actions. For example, when the user places their finger on the biometric module **13**, the soft switch input sensors **14** can trigger the SUB HSM **1** to switch from its lowest energy deep sleep mode to attain full powered active mode in shortest time duration to then perform the biometric fingerprint scanning operation in just one action. Moreover, such soft switch input sensors **14** can be coupled with a liveness detection module **15** for preventing accidental activation of the SUB HSM **1**. The biometric sensors **13** may further combine with the inertial sensor.

The transmission module **20** establishes a data transfer link with an external device which the user interface is operated thereon. Specifically, the transmission module **20** is configured to establish the data transfer link to connect with the external device via a communication protocol. Such communication protocols may include but is not limited to short-range wireless communication protocols such as Bluetooth, WiFi, Near Field Communication, ZigBee, Z-Wave, IrDA, ANT, RFID, WiGi and any other new short range wireless protocols or any combination thereof. Preferably, the transmission module **20** is a Bluetooth module to enable secure communicate with the user using a Bluetooth protocol. The transmission module **20** can be instructed by the centralised microprocessor unit **40** to operate only in a one directional data transmission mode where the SUB HSM **1** can only transmit data and not receive any data but pick data of specific format/type as part of specific operations from designated authorised device.

The battery module **30**, which is chargeable wirelessly, is designed to mitigate against well-known hacks via physical connections of both Data and power channels. 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**. It should be understood that the induction coils **33** and associated circuitry **32** may change as technology advances. As shown in **Fig. 3**, the induction coils **33** can be magnetised for precise alignment to an external charger. This setup is designed for energy harvesting only without any passage

for incoming data transfer to reduce surface of attack. Different power modes can be implemented by the centralised microcontroller unit **40** to optimize power consumption and extend the battery life. The ultra-thin battery **31** can be thin-film battery which offers thin and flexible form factor, high energy density, and rapid charging capabilities. Preferably, the power modes may include an active mode where all components of the SUB HSM **1** are fully powered or operated at full capacity, and a deep sleep mode where some or all components are disabled or power supply to those components are being reduced and/or minimized.

The centralised microcontroller unit **40** is preferably connected to the different hardware modules via the conductive traces for controlling their respective operations and processing the input data. The centralised microcontroller unit **40** comprises can be provided with secured memory modules for pre-storing a plurality of computer implementable instructions. Such instructions may include but are not limited to:

- (a) execute 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;
- (b) execute cryptographic primitives, including encryption, hashing, and cryptographic signatures, the tamperproof nature of the SUB HSM **1** allows the centralised microcontroller unit **40** to initiate its boot process in a secure manner, to ensure all subsequent operations and code execution occur within a secure environment, and to ensure data is securely stored in its hardware based secured memory zone. The centralised microcontroller unit **40** can be integrated with further hardware components to accelerate cryptographic primitives so that the performance and efficiency of the cryptographic operation can be enhanced while maintaining a high level of security operating in secured execution zone;
- (c) verify an identity of the user using an in-device hardware secure memory stored template and/or template-free Artificial Intelligent driven biometric authentication

method, for example, the in-device hardware secure memory stored template and/or template-free biometric authentication analyses raw biometric data captured from the user during the authentication process and use machine learning algorithms or deep learning techniques to analyse the biometric traits and determine whether they match previous instances of the same trait that were previously captured from the same user. Alternatively, if a person is identified as not the holder of the SUB HSM 1, that person's biometrics will be recorded and stored in the data storage of the centralised microcontroller unit 40 as evidence of attempted break in;

(d) 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, for example, the user may be prompted to shake or orientate the SUB HSM 1 in a predetermined pattern of personal choice, scan different fingerprint in a sequential manner, or perform both of the mentioned actions;

(e) perform a second level of authentication that determines liveness of the user by analysing behavioural patterns of the user based on the predetermined sequence of the acquired input data, the biometric data, habitual handling, movement of device, or any combination thereof;

(f) generating cryptographic keys and signing credentials upon successful verification of the user;

(g) operate the SUB HSM 1 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, by keeping the SUB HSM 1 in the offline mode, it reduces the attack surface and potential vulnerabilities that could be exploited by attackers to steal or manipulate the cryptographic keys and signed credentials;

(h) operate in an unbalanced communication mode where the SUB HSM 1 exclusively initiates and/or disconnects the data transfer link, effectively allowing the SUB HSM 1 to determine when and how data is transmitted; and

(i) execute a counterparty cryptography processor to ensure the operations of the SUB

HSM 1 are performed securely and cannot be intercepted or compromised, the counterparty cryptography processor is mainly used in the setup phase of every communication link between the SUB HSM 1 and the cryptographic processor to verify identities and provide protection for the SUB HSM 1 from unauthorized access or interception.

The cryptographic keys are cryptographic keys that are generated for a short period of time and then discarded or destroyed. Since these keys are only used for a short period of time, even if they are intercepted, they cannot be used to decrypt data from other sessions or messages. Preferably, the cryptographic keys may include a signature key and a verification key. The signature key can be used to digitally sign credentials or messages for ensuring that the credentials or messages have not been tampered with during transmission. The verification key can then be used to check the authenticity and integrity of the signed credentials or messages so as to ensure that the signed credentials or messages were not modified or forged. The generated cryptographic keys and signed credentials are configured to be transmitted in a consistent and secure manner, with a predetermined structure and size. This is important for ensuring that the keys and credentials can be transmitted and processed efficiently, and that they cannot be intercepted or modified by an attacker during transmission.

In the process of credential signing, the credentials are first hashed to create a unique and irreversible string of characters. These hashed credentials are then encrypted to protect it from unauthorized access, and the resulting encrypted string is signed by digital signature algorithm to provide additional authentication and verification. By using this combination of hashing, encryption, and signed credentials, the system can ensure that only authorized users are granted access to the signed credential. The hashed and encrypted signed credential acts as the foundation or root of the authentication process, providing a secure and reliable method for verifying the identity of the user.

The arrangement of the SUB HSM **1** is such that a trusted zone can be established within the SUB HSM **1** to prevent unauthorized access or tampering through physical and/or software exploitation.

From a broader perspective of the invention, the SUB HSM **1** can be tailored to establish a trusted zone between itself and an external device so that various security applications can be facilitated. In this perspective, verifying the integrity of both the SUB HSM **1** and the external device is essential to establish the trust zone between the two. Subsequently, the cryptographic operations and applications can be carried out between the two devices.

In one exemplary application, the SUB HSM **1** can be bounded with a digital ID associated to a specific user. As such, the user now holds the cryptographic key, allowing any operations, which require approval from the user, to be signed using the SUB HSM **1** as an absolute proof of the user authorising the signed operations.

In a further application, the centralised microcontroller unit **40** of the SUB HSM **1** can have and/or coupled with a high capacity data storage for storing personal data. This allows the user to manage their personal data, as defined by data sovereignty, using the cryptographic functionalities of the SUB HSM **1**. By way of example, the users may choose to back up their personal data such as personal health data into the SUB HSM **1** instead of uploading it to the cloud storage, ensuring that only they themselves can access their personal data. In this application, the SUB HSM **1** can have gigabytes of memory packed into a slim profile under 1.5mm in height. The memory may come equipped with power mode management for efficient energy use and the capability to partition memory so that only used partition is turned on to conserve energy. Additionally, it incorporates personal data access management to enable control over who can access the stored contents within the SUB HSM **1**.

Yet in a further application, the centralised microcontroller unit **40** of the SUB HSM **1** can have and/or coupled with an AI engine designed to conduct personalised data training using one or more machine learning algorithms. Now, the users possess control over their own knowledge, trained through this AI engine, and with such trained personalised data securely stored in the SUB HSM **1**. This effectively enables the users to manage their own knowledge and potentially authorize others, depending on the subscription, to access their trained AI engine using their own credential keys generated by the SUB HSM **1**. In this embodiment, the hardware architecture is configured to provide an environment that is suitable for AI applications. The transmission of large volume trained data to be inferred can be achieved through high speed SUB HSM **1** to SUB HSM **1** wireless communication. A large data throughput (in gigabits/second) transfers can be achieved using high speed wireless point to point channel.

Still in a further application, the user of the SUB HSM **1** can trigger a distress signal by a predetermined input. The distress signal will then transmit to the server or local authority, and the server or local authority can further initiate a distress mode. The distress mode can include various features aimed to improve the safety and security of the user, which includes fake visual presentation to mislead potential threats and embedding data tracing mechanism within digital assets to aid in locating the digital asset event after multiple transfers.

The present disclosure includes as contained in the appended claims, as well as that of the foregoing description. Although this invention has been described in its preferred form with a degree of particularity, it is understood that the present disclosure of the preferred form has been made only by way of example and that numerous changes in the details of construction and the combination and arrangements of parts may be resorted to without departing from the scope of the invention.

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.

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 any one of claims 1 to 4, wherein the peripheral modules include a biometric reader (13) for capturing biometric traits of a user.

6. The SUB HSM (1) according to claim 5, 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.

7. The SUB HSM (1) according to claim 5 or claim 6, 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.

8. The SUB HSM (1) according to any one of claims 5 to 7, 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.

9. The SUB HSM (1) according to claims 5 to 8, 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.

10. The SUB HSM (1) according to claim 9, 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.

11. The SUB HSM (1) according to any one of claims 1 to 10, wherein the centralised microcontroller unit (40) is configured to generate cryptographic keys and sign credentials upon successful authentication and verification of the user.

12. The SUB HSM (1) according to claim 11, 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.

13. The SUB HSM (1) according to claim 11 or claim 12, wherein 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.

14. The SUB HSM (1) according to any one of claims 1 to 13, 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.