

PERSONAL SECURITY DEVICE AND METHOD

FIELD OF INVENTION

5 The present invention relates broadly to a system, device and method, for example in the field of information technology (IT) security and electronic security.

BACKGROUND

10 Computing products like personal computers, tablet computers, and smart phones may have different security features due to the installation of different IT security application software. These security software require some sort of security elements like cryptographic keys and/or passwords. For example, these cryptographic keys and/or passwords could be generated within the embedded processor of the computing product. Commonly, these security elements will be stored inside the computing product for different IT security applications according to requirement.

15 The IT security application could be for data encryption. This, for example the AES (Advanced Encryption Standard) algorithm, uses the symmetric cryptographic key. The encrypted data may be stored inside or outside the computing products. The IT security application could also be for an authentication process. This, for example the RSA (Rivest-Shamir-Adleman) algorithm, uses the asymmetric cryptographic keys for authentication by
20 using the computing product or another computing product.

Also, notably, security solutions do not share their security elements across different computers and/or IT security applications. This makes security management across many different applications, platforms and systems cumbersome.

Existing software based security solutions can face problems such as:

- 25 1. In one type of solution, the security elements are generated and managed not by the user, but by outside parties - the computing product manufacturers or security software developers. This requires the user's trust in the involvement of external parties in the user's security process. This may potentially compromise security.
- 30 2. In another type of solution, the security elements are self-managed, i.e. generated, stored inside the computing product and managed by the user themselves. However, these security elements may not be recoverable if the product storing them is lost or damaged, and this will lead to a permanent loss, for example, of the encrypted data.
- 35 3. Only passwords are generally used to control the access to the security elements. Many users choose to use easy-to-remember, weak passwords and this makes password-control security access systems vulnerable.

Therefore, for users who desire full control over their IT security (without the involvement of external parties), existing software solutions alone are inadequate.

Example embodiments of the present invention seek to address one or more of the above problems.

5 SUMMARY

In accordance with a first aspect of the present invention there is provided a method of providing a security functionality on computing products, the method comprising the steps of initializing a first security module on a dedicated security device, the initialized first security module comprising a first security element such as a first set of one or more cryptographic
10 keys and a first verification element such as a first password; generating and storing a second security module on the security device, the second security module comprising a second security element such as a second set of one or more cryptographic keys and a second verification element such as a second password; providing a first IT security application on a first computing product, wherein the first IT security application requires the first or second
15 security elements to operate; coupling the security device to the first computing product for enabling data communication between the first or second security modules and the first IT security application; and providing the first or second security elements to the first IT security application subject to verifying a user input using the first or second verification elements respectively.

20 In accordance with a second aspect of the present invention there is provided a dedicated security device for cooperating with IT security applications on computing products, the security device comprising an initialized first security module comprising a first security element such as a first set of one or more cryptographic keys and a first verification element such as a first password; a second security module, the second security module comprising a
25 second security element such as a second set of one or more cryptographic keys and a second verification element such as a second password; and an interface for coupling the security device to a first computing product for enabling data communication between the first or second security modules and a first IT security application on the first computing product for providing the first or second security elements to the first IT security application; wherein the
30 security device is configured for providing the first or second security elements to the first IT security application subject to verifying a user input using the first or second verification elements respectively.

In accordance with a third aspect of the present invention there is provided a computing product functioning as a security device proxy for the security device of the second aspect,
35 the computing product comprising the transferred second security module comprising the second security element and the second verification element; an interface for coupling the computing product to a further computing product for enabling data communication between the transferred second security module and an IT security application on the further computing product, wherein the IT security application requires the second security element
40 of the transferred second security module to operate; and wherein the computing product is

configured for providing the second security element of the transferred second security module to the IT security application subject to verifying a user input using the second verification element of the transferred second security module.

BRIEF DESCRIPTION OF THE DRAWINGS

- 5 Embodiments of the invention will be better understood and readily apparent to one of ordinary skill in the art from the following written description, by way of example only, and in conjunction with the drawings, in which:

Fig. 1 shows a high level schematic block diagram illustrating components internal to the dedicated security hardware, Security Device, according to an example embodiment.

- 10 Fig. 2 shows a high level schematic block diagram illustrating the security module, SM generated and stored inside the re-writable nonvolatile memory of the Security Device, according to an example embodiment.

- 15 Fig. 3a shows a high level schematic block diagram illustrating the equipment setup for the Security Device initial set-up, Master SM generating processing, according to an example embodiment.

Fig. 3b shows a flowchart illustrating the initial set-up process of the Security Device, including the generation of the Master SM, according to an example embodiment.

Fig. 4a shows a high level schematic block diagram illustrating the equipment setup for the process of generating the Secondary SM, according to an example embodiment.

- 20 Fig. 4b shows a flowchart illustrating the process of generating the Secondary SM, according to an example embodiment.

Fig. 5a shows a high level schematic block diagram illustrating the setup for the IT security applications running in the computing products, CP(s) that require security modules, SM(s) from the Security Device, according to an example embodiment.

- 25 Fig. 5b shows a flowchart illustrating the operation of IT security applications in the CP, while requiring the presence and interaction of the Master Security Module from the Security Device, according to an example embodiment.

- 30 Fig. 6a shows a high level schematic block diagram illustrating the equipment setup for the process to change the Name and Password of the SM which is stored inside the Security Device, according to an example embodiment.

Fig. 6b shows a flowchart illustrating the process to change the Name and Password of the SM which is stored inside the Security Device, according to an example embodiment.

Fig. 7a shows a high-level schematic block diagram illustrating the equipment setup for the process to reset the Password of the SM inside the Security Device, according to an example embodiment.

5 Fig. 7b shows a flowchart illustrating the process to reset the Password of the SM inside the Security Device, according to an example embodiment.

Fig. 8a shows a high level schematic block diagram illustrating the equipment setup for the process of deleting the SM inside the Security Device, according to an example embodiment.

Fig. 8b shows a flowchart illustrating the process to delete the SM inside the Security Device, according to an example embodiment.

10 Fig. 9a shows a high level schematic block diagram illustrating the equipment setup for the process of transferring SM from the Security Device to CP, according to an example embodiment.

Fig. 9b shows a flowchart illustrating the SM transfer process from the Security Device to CP, according to an example embodiment.

15 Fig. 10a shows a high level schematic block diagram illustrating the setup for the process of changing Name and Password of the SM inside the CP, according to an example embodiment.

Fig. 10b shows a flowchart illustrating the process that changes the Name and Password of the SM inside the CP, according to an example embodiment.

20 Fig. 11a shows a high level schematic block diagram illustrating the setup for the process of running a IT security application in a CP, which calls SM stored inside another CP-P, according to an example embodiment.

Fig. 11b shows a flowchart illustrating the process of running a IT security application in CP, which calls SM stored inside another CP-P, according to an example embodiment.

25 Fig. 12a shows a high level schematic block diagram illustrating the setup for the process of IT security application calls SM transferred and stored inside the same CP-P, according to an example embodiment.

30 Fig. 12b shows a flowchart illustrating the running of IT security applications on the CP-P which calls the SM has been transferred and stored inside the same CP-P, according to an example embodiment.

Fig. 13a shows a high level schematic block diagram illustrating the equipment setup for the password reset processing of the SM inside the CP-P, according to an example embodiment.

Fig. 13b shows a flowchart illustrating the process to reset the Password of the SM inside the CP-P, according to an example embodiment.

Fig. 14a shows a high level schematic block diagram illustrating the setup for the process of deleting of SM inside a CP, according to an example embodiment.

Fig. 14b shows a flowchart illustrating the process that delete the SM inside the CP, according to an example embodiment.

- 5 Figure 15 shows a flow chart illustrating a method of providing a security functionality on computing products.

DETAILED DESCRIPTION

10 In the described embodiments of the present invention, a specially designed, dedicated Security Device may replace password access control. The Security Device can generate and store multiple sets of security elements or security modules for different IT security applications. The security modules stored inside the security device can be transferred to different computing products for example, the personal computer, laptop computer, tablet computer, smart phone etc. The same security module can be transferred to multiple computing products for shared security control or for security recovery when the original product storing the security module is lost or damaged. Multiple security modules may also be transferred to the same computing product for different IT security applications.

Definitions of terms used in the description of the preferred embodiments:

Security Device 100: a specially-designed, dedicated security hardware which generates and stores Security Modules.

- 20 Security Module (SM) 2000, 2001, ...: a module including a Name, a Password, a Counter and a set of one or more security elements, for example but not limited to Cryptographic Keys. Different SMs are required for different IT security applications.

Security Module Name (SMnm): a data field used to identify the SM.

- 25 Security Module Password (SMpw): a data field used to control user access to the SM 2000, 2001, The data field may contain data representing the password as in the example embodiments described below. In different embodiments, any other form of verification element such as pattern recognition, location recognition or biometric element including but not limited to finger print, face recognition, voice recognition or typing stroke recognition etc.

- 30 Security Module Counter (SMct): a small positive integer used to control the number of consecutive failed password retries. The counter value decreases by 1 for each consecutive incorrect password input and the SM 2000, 2001, ... will be disabled when the counter value reaches zero. However, the Counter will be reset to the original value when a correct password input is detected.

- 35 Security Module Cryptographic Key (SMck): a random secret key used for security functions like data encryption, decryption under a symmetric key algorithm or authentication under an

asymmetric key algorithm. In different embodiments, any other form of security element such as randomly generated password or Hash keys generated for example but not limited to password protection etc.

5 Master Security Module (MSM) 2000: the 1st SM set up by the user during the initialization of the Security Device.

Master Name (Mnm): the Device Name.

Master Password (Mpw): the Device access Password.

Master Counter (Mct): the allowed number of consecutive failed password attempts that can be chosen by a user or a default set by the manufacturer.

10 Master Cryptographic Key(s) (Mck): Set of one or more keys user-generated by the True Random Number Generator (TRNG) of Security Device 100.

Secondary Security Module (S2SM) 2001, 2002, ...: SM, other than the MSM 2000, generated by the Security Device 100 for different applications.

15 Secondary Name (S2nm): name linking an application with the required S2SM, e.g. S2nm 2101.

Secondary Password (S2pw): the password of a S2SM, e.g. S2pw 2201, which can be the same as the Mpw 2200.

Secondary Counter (S2ct): the counter of a S2SM, e.g. S2ct 2301, which can be the same as the Mct 2300.

20 Secondary Cryptographic Key(s) (S2ck): Set of one or more keys user-generated by the TRNG of Security Device 100.

IT security application e.g. 1002, 5002: Applications include but not limited to, for example storage data protection, data exchange protection, Cloud Computing access control and Cloud data protection, payment authentication, password management, login access control,
25 message protection, email protection and voice protection etc.

Computing Products (CP) 1000, 5000: machines which contain at least one build-in central processing unit (CPU) and a build-in memory; for example, a desktop computer, laptop computer, tablet computer, smart phone or a smart watch. Applications software can be installed and run inside the CP 1000, 5000.

30 Computing Product Proxy (CP-P) 1000: CP storing S2SM e.g. 2001 transferred from Security Device 100, acting as a proxy for the Security Device 100.

Security Module Interface Manager (SMIM) 1001, 5001: a specially designed software, installed inside the CP 1000, 5000 to manage the S2SM e.g. 2001, control the interface between the S2SM e.g. 2001 and applications.

Security Module Configuration Tool (SMCT) 3000: a machine used to configure the SM inside the Security Device 100. It can be any computing machine such as a desktop computer, a laptop computer, a tablet computer or a smart-phone. It may also be a specially designed machine that includes build-in processor or a virtual computer in a computing Cloud. It could also be an embedded processor of the Security Device 100, in which case the Security Device 100 can configure itself.

Security Module Configuration Manager (SMCM) 3001: a specially designed software, installed inside the SMCT 3000, to configure (generate, store, change or delete) the SM inside the Security Device 100.

Security Module Transportation Tool (SMTT) 9000: a machine used to transfer the S2SM e.g. 2001 from the Security Device 100 to a CP 1000. It can be any computing machine such as a desktop computer, a laptop computer, a tablet computer or a smart-phone. It may also be a specially designed machine that includes build-in processor or a virtual computer in a computing Cloud. It could also be an embedded processor of the Security Device 100, such that the Security Device 100 can be connected directly to the CP 1000.

Security Module Transportation Manager (SMTM) 9001: a specially designed software, installed inside the SMTT 9000, to control the transfer of the S2SM e.g. 2001 from the Security Device 100 to a CP 1000.

Software Installation: above software may be separately installed, e.g. from a CD-ROM or from the Security Device 100 or through the internet.

Communication Link (CL): an electrical communication means which includes, but is not limited to, any communication module or media such as radio frequency (RF) channels, WiFi, Bluetooth, NFC or any wired connection.

Password Verification Process: as part of the numerous user authentication processes described in the text below, users are asked for the passwords in order to verify their rights to use the various Security Modules. It is understood that these authentication processes mentioned below are broadly similar. When a user requests a SM transaction or operation, he is requested by the software security manager to enter his password. His password is then checked for correctness. When the entered password is correct, his request will be approved and the requested operation will proceed. If the password entered is incorrect, retries will be allowed. Up to N consecutive retries will be allowed. N is the initial integer set in the counter (SMct, Mct, or S2ct). Each consecutive incorrect entry will decrement the counter value by 1. This retry process is repeated until the value of the counter reaches 0 or a successful password entry is made. When the counter reaches 0, the password verification will be aborted and all further requests will be disabled. However, when a correct password entry is made, the counter value will be reset to N.

Some portions of the description which follows are explicitly or implicitly presented in terms of algorithms and functional or symbolic representations of operations on data within a

computer memory. These algorithmic descriptions and functional or symbolic representations are the means used by those skilled in the computer engineering arts to convey most effectively the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities, such as electrical, magnetic or optical signals capable of being stored, transferred, combined, compared, and otherwise manipulated.

Unless specifically stated otherwise, and as apparent from the following, it will be appreciated that throughout the present specification, discussions utilizing terms such as "scanning", "calculating", "determining", "replacing", "generating", "initializing", "outputting", or the like, refer to the action and processes of a computer system, or similar electronic device, that manipulates and transforms data represented as physical quantities within the computer system into other data similarly represented as physical quantities within the computer system or other information storage, transmission or display devices.

The present specification also discloses apparatus for performing the operations of the methods. Such apparatus may be specially constructed for the required purposes, or may comprise a general purpose computer or other device selectively activated or reconfigured by a computer program stored in the computer. The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. Various general purpose machines may be used with programs in accordance with the teachings herein. Alternatively, the construction of more specialized apparatus to perform the required method steps may be appropriate. The structure of a conventional general purpose computer will appear from the description below. These general computers may include computers in a distributed computing network and computers in a computing Cloud.

In addition, the present specification also implicitly discloses the algorithm of a computer program, in that it would be apparent to the person skilled in the art that the individual steps of the method described herein may be put into effect by computer code. The computer program is not intended to be limited to any particular programming language and implementation thereof. It will be appreciated that a variety of programming languages and coding thereof may be used to implement the teachings of the disclosure contained herein. Moreover, the computer program is not intended to be limited to any particular control flow. There are many other variants of the computer program, which can use different control flows without departing from the spirit or scope of the invention.

Furthermore, one or more of the steps of the computer program may be performed in parallel rather than sequentially. Such a computer program may be stored on any computer readable medium. The computer readable medium may include storage devices such, as magnetic or optical disks, memory chips, or other storage devices suitable for interfacing with a general purpose computer. The computer readable medium may also include a hard-wired medium such as exemplified in the internet system, or wireless medium (for example wi-fi, bluetooth device and the mobile telephone system). The computer program when loaded and executed

on such a general-purpose computer effectively results in an apparatus that implements the steps of the preferred method.

The invention may also be implemented as hardware modules. More particular, in the hardware sense, a module is a functional hardware unit designed for use with other components or modules. For example, a module may be implemented using discrete electronic components, or it can form a portion of an entire electronic circuit such as an application specific integrated circuit (ASIC). Numerous other possibilities exist. Those skilled in the art will appreciate that the system can also be implemented as a combination of hardware and software modules.

10 General Description of Example Security Device

Fig. 1 shows a high-level schematic block diagram illustrating a Security Device 100 according to an example embodiment. The Security Device 100 is a specially-designed, dedicated security hardware which generates and stores Security Modules. The Security Device 100 contains a random number generator, for example a True Random Number Generator (TRNG) 110, Re-writable Nonvolatile Memory 120, an Embedded Controller (EC) 130 and an Interface 140, according to this example embodiment.

Fig. 2 shows a high level schematic block diagram illustrating a Master Security Module, MSM 2000, a Secondary Security Module, S2SM 2001, and optionally additional Secondary Security Modules S2SM 200n (n=2, 3, ...) stored inside the re-writable nonvolatile memory 120 (Figure 1), according to an example embodiment. Each Security Module includes a Name (Mnm 2100, S2nm 2101, 210n), a Password (Mpw 2200, S2pw 2201, 220n), a Counter (Mct 2300, S2ct 2301, 230n) and Cryptographic Key(s) (Mck 2400, S2ck 2401, 240n). The Names are used to identify the respective Security Module. The Passwords are used to control user access to the respective Security Modules. The Counters are used to control the number of consecutive failed password retries. The Cryptographic Keys are random secret keys as described in the Definitions section above, according to this example embodiment.

Security Device Initialization, Key and Master Security Module Generation

Fig. 3a shows a high-level schematic block diagram illustrating the equipment setup for the Security Device initialization. A Security Module Configuration Tool (SMCT) 3000 is connected with the Security Device 100 using communication link 3100, according to an example embodiment. The communication link (CL) 3100 represents the media through which data is communicated between the Security Device 100 and the SMCT 3000. The communication link 3100, described in the Definition section above, includes, but is not limited to, any communication module or media such as radio frequency (RF) channels, WiFi, Bluetooth, NFC or any wired connection. The Security Device 100 and the SMCT 3000 are described in the Definitions section above. The SMCT 3000 contains a Security Module Configuration Manager (SMCM) 3001, which may be separately installed, e.g. from

a CD-ROM or from the Security Device 100 or through the internet, according to an example embodiment.

Fig. 3b shows a flowchart illustrating the initial set-up process including the generation of the Master Security Module (MSM) 2000, according to an example embodiment. To generate this MSM 2000, a user connects his Security Device 100 to the SMCT 3000 and starts the SMCM 3001. The user then requests to generate the MSM 2000 in step 3101. The SMCM 3001 will then ask the user to input the Master Name (Mnm) 2100 (Figure 2) and Master Password (Mpw) 2200 (Figure 2) in step 3102. The SMCM 3001 then processes step 3103 where the set of one or more cryptographic keys (Mck) 2400 is generated by the TRNG 110 (Figure 1) and stored inside the memory 120 (Figure 1) together with the Mnm 2100, Mpw 2200 and Mct 2300, as the MSM 2000 (Figure 2), according to an example embodiment. In one embodiment, the password and the set of one or more cryptographic keys are stored in encrypted form.

New Key and Secondary Security Module (S2SM) Generation

Fig. 4a shows a high-level schematic block diagram illustrating the equipment setup for the generation of the Secondary Security Module (S2SM) 2001. The SMCT 3000 is connected with the Security Device 100 using communication link (CL) 3100 (as described in the Definitions section above), according to an example embodiment. The SMCT 3000, is installed with a SMCM 3001 (as described in the Definitions: software installation section above).

Fig. 4b shows a flowchart illustrating the process of generating the S2SM 2001, according to an example embodiment. To generate S2SM 2001, a user connects his Security Device 100 to the SMCT 3000 and starts SMCM 3001. User requests to generate the S2SM 2001 in step 4101. The SMCM 3001 asks the user to input the Master Name (Mnm) 2100 and/or Master Password (Mpw) 2200 in step 4102. The SMCM 3001 then checks the correctness of the Mnm 2100 and/or Mpw 2200 in step 4103 against the data stored in the Security Device 100 according to the Password Verification Process described above. If the password is incorrect, the operation is halted in step 4104. If the password is correct the process continues to step 4105 where user is asked to input a Name (S2nm) 2101 and a Password (S2pw) 2201 for the S2SM 2001. A set of one or more new cryptographic keys 2401 is generated by the TRNG 110 (Figure 1) and this is stored inside the memory 120 (Figure 1) together with the S2nm 2101, S2pw 2201 and S2ct 2301, as the S2SM 2001.

The Secondary counter S2ct 2301 could be the same as Master counter Mct 2300 or a new number input by the user, according to an example embodiment.

Running IT security application on the CP together with the Security Device

Fig. 5a shows a high level schematic block diagram illustrating the equipment setup for the operation of IT security applications running in the CP 5000, which calls the MSM 2000 or S2SM 2001/200n from the Security Device 100. The CP 5000 is installed with a SMIM 5001

and a IT security application 5002. The software installation is described in the Definitions section. The CP5000 and the Security Device 100 are connected via communication link (CL) 5100 (as described in the Definitions section above), according to an example embodiment.

5 Fig. 5b shows a flowchart illustrating the operation of IT security applications in the CP 5000, while requiring the presence and interaction of the MSM 2000 or S2SM 2001/200n from the Security Device 100.

Initially a SMIM 5001 is installed in the CP 5000 (as described in the Definitions: software installation section above) at step 5101. The user then installs a IT security application 5002
10 to the same CP 5000 (as described in the Definitions: software installation section above) at step 5102, according to an example embodiment.

After initial installation of the SMIM 5001 and IT security application 5002, the user may run the IT security application 5002 that requires security elements from the MSM 2000 or S2SM 2001/200n inside Security Device 100 in step 5103. The SMIM 5001 checks for the presence
15 of the Security Device 100 in step 5104. The presence of the Security Device 100 may be checked/determined based on, by way of example and not limitation, the SMIM 5001 sending a signal which, by pre-arrangement, is recognized by the Security Device 100 through for example the USB ports and/or the Bluetooth channels. When the pre-arranged signal is received/recognized by the Security Device 100, it sends a pre-arranged reply to the SMIM
20 5001 and then to the IT security application 5002, and thus communication between the IT security application 5002 in the CP 5000 and the MSM 2000 or S2SM 2001/200n in the Security Device 100 is established.

If the Security Device 100 is not present, the operation is aborted in step 5105. If the Security Device 100 is present, the process continues to step 5106 where the SMIM 5001
25 requires the user to input the Mnm 2100 and/or Mpw 2200 or S2SMnm 210n and/or S2SMpw 220n. The SMIM 5001 then checks for the correctness of the password in step 5107 against the data stored in the Security Device 100 according to the Password Verification Process described above. If the password is incorrect, the operation will be halted in step 5108. If the password is correct the process continues to step 5109 where
30 Security Device 100 provides the required element(s) of MSM 2000 or S2SM 2001/200n (e.g. cryptographic keys) for the IT security application 5002 on CP 5000 to operate, according to an example embodiment. .

Change of Name and/or Password of SM in the Security Device

Fig. 6a shows a high-level schematic block diagram illustrating the equipment setup for the
35 process of changing Name and/or Password of the security module inside the Security Device 100. The SMCT 3000 is connected to the Security Device 100 using communication link (CL) 3100 (as described in the Definitions section above), according to an example embodiment. The SMCT 3000 is installed with a SMCM 3001 (as described in the Definitions: software installation section above).

Fig. 6b shows a flowchart illustrating the process to change the Mnm and/or Mpw of the MSM 2000 or the S2nm and/or S2pw of S2SM 2001/200n inside the Security Device 100. The user chooses to change the Mnm and/or Mpw or S2nm and/or S2pw at step 6101. SMCM 3001 asks the user to input the current Mnm and/or Mpw or S2nm and/or S2pw in step 6102, and the SMCM 3001 then checks the correctness of the password in step 6103 against the data stored in the Security Device 100 according to the Password Verification Process described above. If the password is incorrect, the operation is halted in step 6104. If the password is correct, the process continues to step 6105 where a new Mnm and/or Mpw or S2nm and/or S2pw is entered by the user and then stored in the Security Device 100, replacing the old Mnm and/or Mpw or S2nm and/or S2pw, according to an example embodiment. .

Reset the Password of Secondary Security Module inside the Security Device if the user has forgotten the original password for the Secondary Security Module

The following will describe the process of resetting the password of S2SM 2001 (Figure 2) if the user has forgotten the original password, according to an example embodiment.

Fig. 7a shows a high-level schematic block diagram illustrating the equipment setup for the process of resetting the password of the S2SM 2001 inside the Security Device 100. The SMCT 3000 is connected to the Security Device 100 using communication link (CL) 3100 (as described in the Definitions section above), according to an example embodiment. The SMCT 3000 is installed with a SMCM 3001 (as described in the Definitions: software installation section above).

Fig. 7b shows a flowchart illustrating the process to reset the Password of the S2SM 2001 inside the Security Device 100. The user chooses to reset password at step 7101. SMCM 3001 then asks the user to input the Master Name, Mnm 2100 and/ or Master Password, Mpw 2200 in step 7102. SMCM 3001 then checks the correctness of the Mpw in step 7103 against the data stored in the Security Device 100 according to the Password Verification Process described above. If password is incorrect, the operation is halted in step 7104. If the password is correct the process continues to step 7105 where a new S2pw 2201 is entered by the user and then stored; or a default Password is installed, according to an example embodiment.

Delete the Secondary Security Module inside the Security Device

Fig. 8a shows a high-level schematic block diagram illustrating the equipment setup for the process of deleting the security module inside the Security Device 100. A SMCT 3000 is connected to the Security Device 100 using communication link (CL) 3100 (as described in the Definitions section above), according to an example embodiment. The SMCT 3000 is installed with a SMCM 3001 (as described in the Definitions: software installation section above).

Fig. 8b shows a flowchart illustrating the process to delete the S2SM 2001 inside the Security Device 100. The user chooses to delete S2SM 2001 at step 8101. SMCM 3001 then asks the user to input the Mnm 2100 and/or Mpw 2200 in step 8102. SMCM 3001 then checks the correctness of the Mpw in step 8103 against the data stored in the Security Device 100 according to the Password Verification Process described above. If password is incorrect, the operation is halted in step 8104. If the password is correct, the process continues to step 8105 where S2SM 2001 is deleted from the Device, according to an example embodiment.

It is noted that alternatively, any Secondary Security Module may be deleted subject to verifying the Secondary Password of the relevant Secondary Security Module.

10 Transfer the Secondary Security Module from Security Device to CP

Fig. 9a shows a high level schematic block diagram illustrating the equipment setup for the transfer process of S2SM 2001 from the Security Device 100 to CP 1000. In one example, the user presents the Security Device 100 together with the CP 1000 to a Security Module Transportation Tool (SMTT) 9000. It is noted that the SMTT may be running on the same computing machine as the SMCT 3000 or a different computing machine. The CP 1000 and the Security Device 100 may be connected to the SMTT 9000 via respective communication links (CL) 1900 and 9100 (as described in the Definitions section above). The Security Device 100 and the CP 1000 may be simultaneously connected to the SMTT 9000, or may be connected in sequence, for example where only one communication interface for connecting to the SMTT 9000 may be available. The SMTT 9000 is installed with a SMTM 9001 (as described in the Definitions: software installation section above), according to an example embodiment.

Fig. 9b shows a flowchart illustrating the S2SM 2001 transfer process from the Security Device 100 to CP 1000. The user starts the SMTM 9001 and chooses to transfer the S2SM 2001 from the Security Device 100 to a CP 1000 at step 9101. The SMTM 9001 then asks the user to input the Mnm 2100 and/or Mpw 2200 in step 9102. SMTM 9001 then checks the correctness of the Mpw in step 9103 against the data stored in the Security Device 100 according to the Password Verification Process described above. If password is incorrect, the operation is halted in step 9104. If the password is correct, the process continues to step 9105 where SMTM 9001 installs the SMIM 1001 to the CP 1000. Security Device 100 encrypts the SM 2001 at step 9106. The encrypted SM 2001 is sent to the CP 1000, for example via the SMTM 9001, at step 9107. The SMIM 1001 of CP 1000 decrypts the SM 2001 received from the Security Device 100. The SM 2001 is then stored in the CP 1000 at step 9108. Accordingly, the CP 1000 is now converted into a CP Proxy (CP-P) that is matched to, i.e. associated with, the Security Device 100, according to an example embodiment.

It is noted that alternatively, any Secondary Security Module may be transferred from the security device to CP subject to verifying the Secondary Password of the relevant Secondary Security Module.

It is noted here that in example embodiments, more than one secondary SM is permitted. Hence the Security Device 100 can generate multiple S2SMs, for example, S2SM 2001, 200n (n=2, 3, ...) and so on. Each of these may be needed for different IT security applications.

It is also noted here that one S2SM can be duplicated and transferred to more than one CP as described above. It is also noted that more than one different S2SMs can be transferred to one CP. A combination of both of these possibilities is also possible.

It is further noted that the same S2SM may be needed for different IT security applications, which can advantageously result in a single password being “automatically” applicable to different IT security applications, thus reducing cumbersome setting of the password(s) for each of the different IT security applications.

Change Name and/or Password of Secondary Security Module inside CP-P

Fig. 10a shows a high level schematic block diagram illustrating a CP-P 1000 containing security module S2SM 2001 and installed with SMIM 1001 (as described in the Definitions: software installation section above), according to an example embodiment. Optionally, additional Secondary Security Modules S2SM 200n (n=2, 3, ...) are contained in the CP-P 1000. This diagram will be used to explain the process that is used to change the Name and/or Password of the S2SM 2001 inside a CP-P.

Fig. 10b shows a flowchart illustrating the process that changes the Name S2nm and/or Password S2pw of the S2SM 2001 inside the CP 1000. The user starts the SMIM 1001 and chooses to change the S2nm and/or S2pw at step 10101. The SMIM 1001 then asks the user to input the current S2nm and/or S2pw of S2SM 2001 in step 10102. The SMIM 1001 then checks the correctness of the password in step 10103 according to the Password Verification Process described above. If password is incorrect, the operation is halted in step 10104. If the password is correct, the process continues to step 10105 where new S2nm 2101 and/or S2pw 2201 is input and stored, according to an example embodiment.

It is noted that alternatively, the name and/or password of any transferred Secondary Security Module may be changed subject to verifying the Master Password with the security device 100 connected, similar to what will be described below in relation to resetting the password of a transferred Secondary Security Module.

Running IT security application on CP together with CP-P

Fig. 11a shows a high level schematic block diagram illustrating a CP 5000 connected with the CP-P 1000 via communication link (CL) 1500 (as described in the Definitions section above). The CP-P 1000 is installed with a SMIM 1001 and the CP 5000 is installed with a SMIM 5001 and application 5002. The S2SM 2001 has been transferred from the Security Device 100 (Figure 1) and stored inside the CP-P 1000, according to an example embodiment. Optionally, additional Secondary Security Modules S2SM 200n (n=2, 3, ...) have been transferred and stored in the CP-P 1000.

Fig. 11b shows a flowchart illustrating the process of a IT security application 5002 in CP 5000, which calls S2SM 2001 stored inside CP-P 1000 as part of its operation.

Initially a user installs the SMIM 5001 in the CP 5000 (as described in the Definitions: software installation section above) at step 11101. The user then installs the IT security application 5002 in the CP 5000 (as described in the Definitions: software installation section above) at step 11102, according to an example embodiment.

The user then runs the IT security application 5002, which requires items from S2SM 2001 stored inside CP-P 1000 in step 11103. The SMIM 5001 checks for the presence of the CP-P 1000 in step 11104. The presence of the CP-P 1000 may be checked/determined based on, by way of example and not limitation, the SMIM 5001 of CP 5000 sending a signal which, by pre-arrangement, is recognized by the SMIM 1001 of CP-P 1000 through for example the USB ports and/or the Bluetooth channels. When the pre-arranged signal is received/recognized by the CP-P 1000, it sends a pre-arranged reply to the SMIM 5001 and then to the IT security application 5002, and thus communication between the IT security application 5002 in the CP 5000 and the S2SM 2001 in the CP-P 1000 is established. If CP-P 1000 is not present, the operation is aborted in step 11105. If the CP-P 1000 is present, the process continues to step 11106 where the SMIM 5001 requires the user to input the S2nm 2101 and/or S2pw 2201. The SMIM 5001/1001 then checks for the correctness of the password in step 11107 against the data stored in the CP-P 1000 according to the Password Verification Process described above. If password is incorrect, the operation will be halted in step 11108. If the password is correct the process continues to step 11109 where required security element(s) from S2SM 2001 is sent to CP 5000 securely, according to an example embodiment.

Running IT security application on CP-P in a Standalone Mode

Fig. 12a shows a high level schematic block diagram illustrating the setup of a CP-P 1000 that has been installed with SMIM 1001 and IT security applications 1002 (as described in the Definitions: software installation section above), according to an example embodiment. The security module S2SM 2001 has been transferred from the Security Device 100 (Figure 1) and stored inside CP-P 10000. Optionally, additional Secondary Security Modules S2SM 200n (n=2, 3, ...) have been transferred and stored in the CP-P 1000.

Fig. 12b shows a flowchart illustrating the process where the IT security application 1002 on the CP-P 1000 calls the S2SM 2001 during its operation.

The user installs the IT security application 1002 (as described in the Definition: software installation section above) at step 12101, according to an example embodiment. The user then runs the IT security application 1002, which requires items from the S2SM 2001 in step 12102. The SMIM 1001 requires the user to input the S2nm 2101 and/or S2pw 2201 of the S2SM 2001 in step 12103. The SMIM 1001 then checks the correctness of the password in step 12104 according to the Password Verification Process described above. If password is incorrect, the operation is halted in step 12105. If the password is correct the process

continues to step 12106 where the required security element(s) of S2SM 2001 is sent as an input to the IT security application 1002, according to an example embodiment.

Reset the Password of Secondary Security Module inside CP-P

In the following, it will be described how the Security Device 100 can advantageously be used for authentication processing prior to resetting the password of S2SM 2001 on the CP-P 1000 if the user has forgotten the original password of the S2SM 2001, in an example embodiment.

Fig. 13a shows a high level schematic block diagram illustrating the equipment setup for the password reset processing of the S2SM 2001 of CP-P 1000 which is installed with SMIM 1001. In one example, the user presents the Security Device 100 together with the CP-P 1000 to a SMTT 9000. The CP 1000 and the Security Device 100 are connected to the SMTT 9000 via respective communication links 1900 and 9100 (as described in the Definitions section above). The Security Device 100 and the CP-P 1000 may be simultaneously connected to the SMTT 9000, or may be connected in sequence, for example where only one communication interface for connecting to the SMTT 9000 may be available. A SMTM 9001 is installed on the SMTT 9000 (as described in the Definitions: software installation section above), according to an example embodiment.

Fig. 13b shows a flowchart illustrating the process to reset the Password, S2pw of the S2SM 2001 inside the CP-P 1000, in the case where the user has forgotten his S2pw. It is assumed that both Security Device 100 and CP-P 1000 are connected to SMTT 9000. The user chooses to reset password at step 13101. SMTM 9001 requires the user to enter the Master Name Mnm and/or Master Password Mpw for the Security Device 100 in step 13102. SMTM 9001 checks the correctness of the password entered in step 13103 against the data stored in the Security Device 100 according to the Password Verification Process described above. If the password is incorrect, the operation is halted in step 13104. If the password is correct the process continues to step 13105 where Security Device 100 encrypts its S2SM 2001, and sends the encrypted S2SM 2001 to the CP-P 1000 in step 13106. The SMIM 1001 then decrypts the encrypted S2SM 2001 received from the Security Device 100, to check the SM 2001 at step 13107. If the received S2SM 2001 “matches” the S2SM 2001 stored in the CP-P 1000, then the match between the Security Device 100 and the transferred secondary security module S2SM 2001 is successfully established in this example embodiment. A new password, S2pw is entered by the user and then stored on both CP-P 1000 and Security Device 100, or a default Password is installed in step 13108. If there is no match, the Password reset is aborted in step 13109, according to an example embodiment.

In one alternative embodiment, the CP-P 1000 can perform encryption of its S2SM 2001 and send the encrypted S2SM 2001 to the Security Device 100 for decryption and checking of the match. As will be appreciated by a person skilled in the art, the final result, i.e. that the match is checked, can advantageously be the same in such an alternative embodiment.

Accordingly, only if a person presents the "matching" Security Device 100 and transferred security module, will a reset of the password be allowed. This can advantageously overcome the problems associated with existing solutions described in the background section above, for example when a user forgets his current password for the S2SM 2001.

5 Delete the Security Module (SM) in CP-P

Fig. 14a shows a high level schematic block diagram illustrating the setup for the SM deleting process of a CP-P 1000 containing S2SM 2001 and installed with SMIM 1001 (as described in the software installation section above), according to an example embodiment. Optionally, additional Secondary Security Modules S2SM 200n (n=2, 3, ...) are contained in
10 the CP-P 1000.

Fig. 14b shows a flowchart illustrating the process to delete the S2SM 2001 inside the CP-P 1000. The user chooses to delete the S2SM 2001 at step 14101. The SMIM 1001 asks the user to input the current S2nm and S2pw of S2SM 2001 in step 14102. The SMIM 1001 then checks the correctness of the password in step 14103 according to the Password Verification
15 Process described above. If password is incorrect, the operation is halted in step 14104. If the password is correct, the process continues to step 14105 where the S2SM 2001 is deleted, according to an example embodiment.

It is noted that alternatively, any transferred Secondary Security Module may be deleted subject to verifying the Master password with the security device connected, similar to what
20 has been described above in relation to resetting the password of a transferred Secondary Security Module.

Reset the Master Password of the Master Security Module inside the Security Device

The Mpw of the MSM 2000 in the Security Device 100 may be reset by making use of an authentication device as described in WO/2014/185865, without involvement of a third party,
25 with and without verification of a specific authentication password. All of the additional advantages of the method and system described in WO/2014/185865 can also be exploited in conjunction with the Security Device 100 of example embodiments of the present invention.

Duplicating the Security Device on another, uninitialized Security Device

The Master Security Module and any Secondary Module can be transferred from the Security
30 Device 100 to another, uninitialized Security Device, subject to verifying the Master Password. This may involve connecting to the Security Device 100 and the other, uninitialized Security Device to the SMTT 9000. This can be useful, for example, for creating a "spare" Security Device.

Figure 15 shows a flow chart 15000 illustrating a method of providing a security functionality
35 on computing products, the method comprising the steps of (15002) initializing a first security module on a dedicated security device, the initialized first security module comprising a first security element such as a first set of one or more cryptographic keys and a

first verification element such as a first password; (15004) generating and storing a second security module on the security device, the second security module comprising a second security element such as a second set of one or more cryptographic keys and a second verification element such as a second password; (15006) providing a first IT security application on a first computing product, wherein the first IT security application requires the first or second security elements to operate; (15008) coupling the security device to the first computing product for enabling data communication between the first or second security modules and the first IT security application; and (15010) providing the first or second security elements to the first IT security application subject to verifying a user input using the first or second verification elements respectively.

The first IT security application may require the first security element to operate, and the method may further comprise providing a second IT security application on the first computing product or on a second computing product, wherein the second IT security application requires the second security element to operate; coupling the security device to the first or second computing products for enabling data communication between the second security module and the second IT security application; and providing the second security element to the second IT security application subject to verifying a user input using the second verification element.

The method may further comprise changing the first verification element subject to verifying a user input using the first verification element; and/or changing the second verification element subject to verifying a user input using the second or the first verification elements.

The method of may further comprise resetting the second verification element subject to verifying a user input using the first verification element; and/or deleting of the second security module from the security device subject to verifying a user input using the first verification element.

The method may further comprise transferring the second security module from the security device to the first or second computing products subject to verifying a user input using the first verification element. The method may further comprise changing the second verification element of the transferred second security module subject to verifying a user input using the second verification element of the transferred second security module or the first verification element of the first security module; and/or deleting the transferred second security module subject to verifying a user input using the second verification element of the transferred second security module or the first verification element of the first security module. The method may further comprise coupling the first or second computing product to a third computing product for enabling data communication between the transferred second security module and a third IT security application on the third computing product, the third IT security application requiring the second security element to operate; and providing the second security element of the transferred second security module to the third IT security application subject to verifying a user input using the second verification element of the transferred second security module. The method may further comprise providing the second

security element of the transferred second security module on the first or second computing products to the second IT security application on the same of the first or second computing products subject to verifying a user input using the second verification element of the transferred second security module. The method may further comprise resetting the second verification element of the transferred second security module subject to verifying a user input using the first verification element of the first security module on the security device, and subject to verifying a match between the transferred second security module and the security device. Transferring the second security module may comprise coupling the security device and the first or second computing product to a transportation tool; and/or wherein resetting the second verification element of the transferred second security module may comprise coupling the security device and the first or second computing product to the transportation tool.

Initializing the first security module on the security device may comprise coupling the security device to a configuration tool; and/or generating and storing the second security module on the security device may comprise coupling the security device to the configuration tool; and/or changing of the first verification element of the first security module on the security device may comprise coupling the security device to the configuration tool; and/or changing of the second verification element of the second security module on the security device may comprise coupling the security device to the configuration tool; and/or resetting of the second verification element of the second security module on the security device may comprise coupling the security device to the configuration tool; and/or deleting of the second security module from the security device may comprise coupling the security device to the configuration tool.

The method may comprise generating and storing two or more different second security modules. The method may comprise transferring two or more of the different second security modules from the security device to the same or different computing products.

In one embodiment, a dedicated security device for cooperating with IT security applications on computing products is provided, the security device comprising an initialized first security module comprising a first security element such as a first set of one or more cryptographic keys and a first verification element such as a first password; a second security module, the second security module comprising a second security element such as a second set of one or more cryptographic keys and a second verification element such as a second password; and an interface for coupling the security device to a first computing product for enabling data communication between the first or second security modules and a first IT security application on the first computing product for providing the first or second security elements to the first IT security application; wherein the security device is configured for providing the first or second security elements to the first IT security application subject to verifying a user input using the first or second verification elements respectively.

The first IT security application may require the first security element to operate, and security device may be further configured for coupling the security device to the first or a second

computing products for enabling data communication between the second security module and a second IT security application on the first or second computing products, wherein the second IT security application requires the second security element to operate; and providing the second security element to the second IT security application subject to verifying a user input using the second verification element.

The interface may be for coupling to a configuration tool and the security device may be configured for initializing the first security module; and/or changing of the first verification element subject to verifying a user input using the first verification element. The interface may be for coupling to a configuration tool and the security device is configured for generating and storing the second security module on the security device; and/or changing the second verification element subject to verifying a user input using the second or the first verification elements; and/or resetting the second verification element subject to verifying a user input using the first verification element, and/or deleting the second security module from the security device subject to verifying a user input using the first verification element.

The interface may be for coupling to a transportation tool and the security device may be configured for transferring the second security module from the security device to the first or second computing products subject to verifying a user input using the first verification element; and/or resetting the second verification element of the transferred second security module subject to verifying a user input using the first verification element of the first security module of the security device, and subject to verifying a match between the transferred second security module and the security device.

The security device may comprise two or more different second security modules. The security device may be configured for transferring two or more of the different second security modules from the security device to the same or different computing products.

In one embodiment, a computing product functioning as a security device proxy for the security device is provided, the computing product comprising the transferred second security module comprising the second security element and the second verification element; an interface for coupling the computing product to a further computing product for enabling data communication between the transferred second security module and an IT security application on the further computing product, wherein the IT security application requires the second security element of the transferred second security module to operate; and wherein the computing product is configured for providing the second security element of the transferred second security module to the IT security application subject to verifying a user input using the second verification element of the transferred second security module.

The computing product may further comprise a further IT security application; and wherein the computing product is configured for providing the second security element of the transferred second security module to the further IT security application on the same computing product subject to verifying a user input using the second verification element of the transferred second security module.

The computing product may be configured for changing the second verification element of the transferred second security module subject to verifying a user input using the second verification element of the transferred second security module or the first verification element of the first security module; and/or deleting the transferred second security module from the computing product subject to verifying a user input using the second verification element of the transferred second security module or the first verification element of the first security module.

The interface may be for coupling to the transportation tool and the computing product may be configured for resetting the second verification element of the transferred second security module subject to verifying a user input using the first verification element of the first security module of the security device, and subject to verifying a match between the transferred second security module and the security device; and/or transferring the second security module from the security device to the computing product.

In example embodiments, there is provided a method and apparatus for generating and storing Security Modules inside a specially designed security hardware device (Security Device). The Security Module can replace the software-generated security elements that are required by different IT security applications on different Computing Products. The Security Module can be transferred from the dedicated Security Device to be stored in different Computing Devices. Then:

1. Different IT security applications running on a Computing Product call the Security Module stored inside the Security Device through an appropriate interface, and/or,
2. Different IT security applications running on a different Computing Product call the Security Module (that was transferred from the Security Device through the appropriate interface) stored inside a Computing Product that is acting as a Security Device proxy, and/or
3. Different IT security applications running on a Computing Product call the Security Module stored inside the same Computing Product that was transferred from the Device through an appropriate interface.

The example embodiments may comprise one or more of the following features:

- a. Initialization, generation and storage of a Master Security Module on the Security Device;
- b. Generation and storage of one or more Secondary Security Modules on the Security Device;
- c. Running IT security applications on a Computing Product that calls the Security Module (Master or Secondary) from the Security Device;
- d. Change of the Name and Password of the Security Module (Master or Secondary) on the Security Device;
- e. Resetting of the Password of the Secondary Security Module on the Security Device;
- f. Deletion of the Secondary Security Module on the Security Device;

- g. Transfer of the Secondary Security Module from the Security Device to the Computing Product, which becomes a Security Device Proxy;
- h. Change of the Name and Password of the Secondary Security Module stored inside a Security Device Proxy;
- 5 i. Running the IT security application on another Computing Product with the Secondary Security Module from a Security Device Proxy;
- j. Running a IT security application on the Security Device Proxy in a Standalone Mode;
- k. Resetting the Password of the Secondary Security Module in the Security Device
- 10 Proxy;
- l. Deleting the Secondary Security Module in the Security Device Proxy.

Example embodiments of the present invention can have the following advantageous characteristics:

- 15 1. The security element (e.g. cryptographic key) and the verification element (e.g. password) are stored inside the dedicated Security Device and “follow” the user who holds the Security Device.
- 2. The security element (e.g. cryptographic key) and the verification element (e.g. password) are stored inside the dedicated Security Device and “physically separated” from the IT security application device or protected element, like encrypted data.
- 20 This can provide higher security when the IT security application device or protected element is lost or hacked.
- 3. The security element (e.g. cryptographic key) and the verification element (e.g. password) are not stored outside the Security Device, except in the Security Device Proxy embodiments, which represents a compromise between security and
- 25 convenience.
- 4. A user control solution is provided, i.e. security element (e.g. cryptographic key) and verification element (e.g. password) are generated, managed and controlled by the user, without involvement of others/third party.

30 Unlike existing software solutions in which a password is the only security control, in example embodiments of the present invention the dedicated Security Device, i.e. hardware is the security control, while e.g. a password is merely used for proving a user is the hardware owner, to prevent illegal usage of the hardware.

In embodiments using the Security Device Proxy, the Computing Product on which the Security Device Proxy is implemented is the major part of the security control, while e.g. a

35 password is merely used for proving a user is the owner of the Computing Product on which the Security Device Proxy is implemented, to prevent illegal usage of the Security Device Proxy.

In embodiments using the Security Device Proxy in standalone mode, software with e.g. a password is the security control. However, in such embodiments, security control can be

recovered from the Security Device if the Security Device Proxy is lost or damaged, which existing software solution cannot provide.

In embodiments of the present invention, the Security Device or the Security Device Proxy by itself, is not a security product because it has no IT security application within itself.

5 However it works with and supports different IT security applications by providing them the different security element(s) or security module which they require.

It will be appreciated by a person skilled in the art that numerous variations and/or modifications may be made to the present invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present
10 embodiments are, therefore, to be considered in all respects to be illustrative and not restrictive. Also, the invention includes any combination of features, in particular any combination of features in the patent claims, even if the feature or combination of features is not explicitly specified in the patent claims or the present embodiments.

Claims

1. A method of providing a security functionality on computing products, the method comprising the steps of:

initializing a first security module on a dedicated security device, the initialized first security module comprising a first security element such as a first set of one or more cryptographic keys and a first verification element such as a first password;

generating and storing a second security module on the security device, the second security module comprising a second security element such as a second set of one or more cryptographic keys and a second verification element such as a second password;

providing a first IT security application on a first computing product, wherein the first IT security application requires the first or second security elements to operate;

coupling the security device to the first computing product for enabling data communication between the first or second security modules and the first IT security application; and

providing the first or second security elements to the first IT security application subject to verifying a user input using the first or second verification elements respectively.

2. The method of claim 1, wherein the first IT security application requires the first security element to operate, and the method further comprises:

providing a second IT security application on the first computing product or on a second computing product, wherein the second IT security application requires the second security element to operate;

coupling the security device to the first or second computing products for enabling data communication between the second security module and the second IT security application; and

providing the second security element to the second IT security application subject to verifying a user input using the second verification element.

3. The method of claims 1 or 2, further comprising:

changing the first verification element subject to verifying a user input using the first verification element; and/or

changing the second verification element subject to verifying a user input using the second or the first verification elements.

4. The method of any one of claims 1 to 3, further comprising:

resetting the second verification element subject to verifying a user input using the first verification element; and/or

deleting of the second security module from the security device subject to verifying a user input using the first verification element.

5 5. The method of any one of claims 1 to 4, further comprising:

transferring the second security module from the security device to the first or second computing products subject to verifying a user input using the first verification element.

6. The method of claim 5, further comprising:

10 changing the second verification element of the transferred second security module subject to verifying a user input using the second verification element of the transferred second security module or the first verification element of the first security module; and/or

deleting the transferred second security module subject to verifying a user input using the second verification element of the transferred second security module or the first verification element of the first security module.

15 7. The method of claims 5 or 6, further comprising:

coupling the first or second computing product to a third computing product for enabling data communication between the transferred second security module and a third IT security application on the third computing product, the third IT security application requiring the second security element to operate; and

20 providing the second security element of the transferred second security module to the third IT security application subject to verifying a user input using the second verification element of the transferred second security module.

8. The method of any one of claims 5 to 7, further comprising:

25 providing the second security element of the transferred second security module on the first or second computing products to the second IT security application on the same of the first or second computing products subject to verifying a user input using the second verification element of the transferred second security module.

9. The method of any one of claims 5 to 8, further comprising:

30 resetting the second verification element of the transferred second security module subject to verifying a user input using the first verification element of the first security module on the security device, and subject to verifying a match between the transferred second security module and the security device.

10. The method of any one of claims 5 to 9,

wherein transferring the second security module comprises coupling the security device and the first or second computing product to a transportation tool; and/or

5 wherein resetting the second verification element of the transferred second security module comprises coupling the security device and the first or second computing product to the transportation tool.

11. The method of any one of the preceding claims,

wherein initializing the first security module on the security device comprises coupling the security device to a configuration tool; and/or

10 wherein generating and storing the second security module on the security device comprises coupling the security device to the configuration tool; and/or

wherein changing of the first verification element of the first security module on the security device comprises coupling the security device to the configuration tool; and/or

wherein changing of the second verification element of the second security module on the security device comprises coupling the security device to the configuration tool; and/or

15 wherein resetting of the second verification element of the second security module on the security device comprises coupling the security device to the configuration tool; and/or

wherein deleting of the second security module from the security device comprises coupling the security device to the configuration tool.

20 12. (Security Device)A dedicated security device for cooperating with IT security applications on computing products, the security device comprising:

an initialized first security module comprising a first security element such as a first set of one or more cryptographic keys and a first verification element such as a first password;

25 a second security module, the second security module comprising a second security element such as a second set of one or more cryptographic keys and a second verification element such as a second password; and

30 an interface for coupling the security device to a first computing product for enabling data communication between the first or second security modules and a first IT security application on the first computing product for providing the first or second security elements to the first IT security application;

wherein the security device is configured for providing the first or second security elements to the first IT security application subject to verifying a user input using the first or second verification elements respectively.

13. The security device of claim 12, wherein the first IT security application requires the first security element to operate, and security device is further configured for:

coupling the security device to the first or a second computing products for enabling data communication between the second security module and a second IT security application on the first or second computing products, wherein the second IT security application requires the second security element to operate; and

providing the second security element to the second IT security application subject to verifying a user input using the second verification element.

14. The security device of claims 12 or 13, wherein the interface is for coupling to a configuration tool and the security device is configured for:

initializing the first security module; and/or

changing of the first verification element subject to verifying a user input using the first verification element.

15. The security device of claim 14, wherein the interface is for coupling to a configuration tool and the security device is configured for:

generating and storing the second security module on the security device; and/or

changing the second verification element subject to verifying a user input using the second or the first verification elements; and/or

resetting the second verification element subject to verifying a user input using the first verification element, and/or

deleting the second security module from the security device subject to verifying a user input using the first verification element.

16. The security device of claims 14 or 15, wherein the interface is for coupling to a transportation tool and the security device is configured for:

transferring the second security module from the security device to the first or second computing products subject to verifying a user input using the first verification element; and/or

resetting the second verification element of the transferred second security module subject to verifying a user input using the first verification element of the first security module of the security device, and subject to verifying a match between the transferred second security module and the security device.

17. (Security Device Proxy)A computing product functioning as a security device proxy for the security device of any one or claims 12 to 16, the computing product comprising:

the transferred second security module comprising the second security element and the second verification element;

an interface for coupling the computing product to a further computing product for enabling data communication between the transferred second security module and an IT security application on the further computing product, wherein the IT security application requires the second security element of the transferred second security module to operate; and

wherein the computing product is configured for providing the second security element of the transferred second security module to the IT security application subject to verifying a user input using the second verification element of the transferred second security module.

18. The computing product of claim 17, further comprising:

a further IT security application; and

wherein the computing product is configured for providing the second security element of the transferred second security module to the further IT security application on the same computing product subject to verifying a user input using the second verification element of the transferred second security module.

19. The computing product of claims 17 or 18, wherein the computing product is configured for:

changing the second verification element of the transferred second security module subject to verifying a user input using the second verification element of the transferred second security module or the first verification element of the first security module; and/or

deleting the transferred second security module from the computing product subject to verifying a user input using the second verification element of the transferred second security module or the first verification element of the first security module.

20. The computing product of any one of claims 17 to 19, wherein the interface is for coupling to the transportation tool and the computing product is configured for:

resetting the second verification element of the transferred second security module subject to verifying a user input using the first verification element of the first security module of the security device, and subject to verifying a match between the transferred second security module and the security device; and/or

transferring the second security module from the security device to the computing product.

21. The method of any one of claims 1 to 11, comprising generating and storing two or more different second security modules.

22. The method of claim 21, comprising transferring two or more of the different second security modules from the security device to the same or different computing products.

23. The security device of any one of claims 12 to 16, comprising two or more different second security modules.

5 24. The security device of claim 23, wherein the security device is configured for transferring two or more of the different second security modules from the security device to the same or different computing products.