

**METHOD AND SYSTEM OF SECURE COMPUTING ENVIRONMENT
HAVING AUDITABLE CONTROL OF DATA MOVEMENT**

5

FIELD OF THE INVENTION

The present invention relates to a secure computing system.
More particularly, a method and system for extending the
10 trusted computing environment of an organization or a central
host to untrusted remote computing devices outside the organ-
ization, with auditable control of data movement between the
organization and the untrusted computing devices.

15

BACKGROUND OF THE INVENTION

Work environments become increasingly dynamic. There is an
increasing trend that organizations approve their staffers to
20 temporarily move data out of the organizations. This may be
due to the needs for meeting organizational or customer re-
quirements in regard with productivity, service level commit-
ments and business continuity.

25 Data proprietary to an organization may be legitimately moved
out of the secure perimeter of the organization by a user
through transferring the organization data to an external
storage device such as a USB flash drive. The user may re-
motely access the organization data stored in the organiza-
30 tion server via an online means.

In prior-art solutions, such proprietary data may be protect-
ed against unauthorized access through cryptographic protec-

tion of data stored in the external storage device (US 20040103288 by Ziv et al.). Data in transit may be secured by cryptographic protection of the online access channel (US 6732269 by Baskey et al.) and even the data itself.

5

Effectively, such cryptographic protection extends the secure perimeter of the organization to include the storage device and the online access channel.

10 However, such conventional solutions fail to provide end-to-end protection. The organization data is susceptible to unauthorized access by malwares and file sharing software residing on the untrusted user computing device. The untrusted user computing device is a fixed or portable computer used to
15 exchange and process the organization data outside the organization. The untrusted user computing device may interface with the user external storage device for data exchange and it may be connected to the Internet and the organization extranet. The untrusted user computing device may be the user's
20 personal computer(s) at home, off-site computers, shared computers for public use and even computers owned or pre-approved by the organization.

Malicious codes may also be downloaded to said untrusted user
25 computing device via the Internet, Bluetooth and other means of wired and wireless communication without the user's knowledge. Said malwares, which include file sharing software and malicious scripts, may copy the organization data and send it to a remote requestor which may be an application executing from a server of dubious nature. The remote requestor
30 may be another individual user running the same file sharing software.

The organization data may not have sufficient protection when copied or downloaded to the untrusted user computing device. In addition, applications referencing the organization data on the untrusted user computing device are possible causes of data leakage when the malwares have successfully gained access to the organization data by prying into the registries, files and memories used by the applications.

10 SUMMARY OF THE INVENTION

The present application provides a method and system for implementing a secure computing environment having auditable control of data movement

15 A method of implementing a secure computing environment is provided. In the method, at least one secure organization computing platform executing a first auditable data exchange application capable of recording events in a first audit log can be interfaced to and in communication with at least one external storage device for exchanging organization data between the memory of the organization computing platform and a secure partition of the external storage device, and the external storage device comprising at least one read/write secure partition, which stores organization data in encrypted form, and one read-only partition, and the external storage device can further be interfaced and in communication with at least one untrusted user computing device to which the organization data can be transferred for processing with pre-authorized software modules comprising an operating system, a plurality of authorized applications and drivers pre-installed in the read-only partition of the external storage device, and the method comprises the steps of an organization

user interfacing the external storage device to the organization computing platform for checking out the organization data, the first auditable data exchange application recording parameters and events associated with data movement and any
5 other pre-determined events in the first audit log, the organization user decoupling the external storage device with the organization data stored in the secure partition and interfacing the external storage device with the untrusted user computing device, the untrusted user computing device booting
10 from the operating system pre-installed in the read-only partition of the external storage device, with the hard disk, any non-volatile storage devices, Internet and any other unauthorized network connections on the untrusted user computing device deactivated, the organization user invoking one
15 or a plurality of the authorized applications pre-installed in the read-only partition of the external storage device for processing the organization data stored in the secure partition of the external storage device, and the processed organization data can be transferred to the organization computing
20 platform in a data check-in process.

In the method, the checking out of the organization data may be performed by the first auditable data exchange application to encrypt the organization data from the organization computing platform with an unlocked cryptographic key for accessing the secure partition, followed by writing the encrypted organization data to the secure partition of the external storage device.

30 In the method, the data check-in process may be performed by the first auditable data exchange application to decrypt the data from the secure partition of the external storage device

with an unlocked cryptographic key and transfer the decrypted data to the memory of the organization computing platform.

In the method, the organization data protected in the secure
5 partition of the external storage device may be firstly unlocked or decrypted before being accessed by the authorized applications running in the untrusted user computing device, and processed organization data and other application related data generated in the untrusted user computing device may be
10 encrypted and transferred to the secure partition of the external storage device, and this data encryption and decryption may be executed by a cryptographic application executed in the user computing platform using an unlocked cryptographic key for accessing the secure partition, and the crypto-
15 graphic application may be one of the plurality of authorized applications pre-installed in the read-only partition of the external storage device.

In the method, the cryptographic key for accessing the secure
20 partition may be stored in protected form in a key memory of the external storage device.

In the method, the authorized applications may comprise a second auditable data exchange application which is loaded to
25 and executed by the untrusted user computing device upon the completion of the booting processes, and the second auditable data exchange application may be used to record in a second audit log the data movement between the external storage device and the untrusted user computing device, and all the parameters, events and the corresponding time stamps required
30 by the audit policies of the organization, and the second audit log may be stored in the secure partition of the external storage device.

In the method, the second auditable data exchange application may replace the cryptographic application for encrypting and decrypting data exchanged between the secure partition of external storage device and the untrusted user computing device.

In the method, at least one of the organization computing platform and untrusted user computing device may execute a device verification process for determining whether the interfaced external storage device has been pre-authorized by the organization.

In the method, at least one of the organization computing platform and untrusted user computing device may unlock the protected cryptographic key for accessing the secure partition of the external storage device by means of a user password provided by the organization user in an authentication process.

In the method, at least one of the organization computing platform and untrusted user computing device may execute a key verification process in which the unlocked cryptographic key for accessing the secure partition may be compared against a parameter derived from the original cryptographic key for validating whether the unlocked cryptographic key matches the original cryptographic key, and the parameter may comprise the cryptographic checksum of the original cryptographic key stored in the external storage device.

In the method, at least one of the organization computing platform and untrusted user computing device may enforce data control and security policies pre-determined by the organiza-

tion, and the policies may comprise verification, authentication and authorization results, file movement control in accordance with file types, file size, time of usage and any other pre-determined criteria.

5

In the method, any of the above device verification, authentication, key verification and policy enforcement processes executed on the user computing device may be executable processes provided by one or a plurality of the authorized applications pre-installed in the read-only partition of the external storage device.

In the method, any of the above device verification, authentication, key verification and policy enforcement processes may be executed by at least one of the first and second auditable data exchange applications.

In the method, the parameters logged by the first and second auditable data exchange applications may comprise the identifiers of either one or both of the organization computing platform and untrusted user computing device, and the identifiers can be constructed from one or a plurality of the identity codes associated with the central processing units (CPU) and subsystems of the organization computing platform and untrusted user computing device respectively.

In the method, the drivers may be software codes used for enabling control signals and data exchange between the respective authorized input-output devices and the untrusted user computing device, and the authorized input-output devices may include basic inputting devices such as mice and keyboards, essential outputting devices such as monitors and printers,

but exclude any conventional external storage devices such as portable flash drives and external hard disks.

In the method, the authorized input-output devices may include biometric scanners and portable crypto-token used for storing secret user cryptographic keys used in multi-factor authentication.

In the method, the untrusted user computing device may be a fixed or portable computer with which the organization user works outside the organization, and the untrusted user computing device may include the user's home computers, off-site computers and shared computers for public use, and the untrusted user computing device may have a standard Basic Input-Output system (BIOS) editor which can be used to register with the untrusted user computing device that the external storage device should be searched for the operating system when the untrusted user computing device is powered up.

In the method, the cryptographic key for accessing the secure partition may be cryptographically protected with a second cryptographic key derived from the user password and other parameters in accordance with a pre-determined algorithm, and the protected cryptographic key for accessing the secure partition can be unlocked in a decryption process with the second cryptographic key derived from the user password using the same pre-determined algorithm.

In the method, the cryptographic key for accessing the secure partition may be cryptographically protected by the user fingerprint to form a locked fingerprint module which is secure and can be stored in the external storage device without additional cryptographic protection.

In the method, the cryptographic operations handling the encrypting and decrypting of the data for the secure partition may be performed by a software application or a hardware module within the external storage device.

In the method, the operating system may allow the authorized applications pre-installed in the read-only partition of the external storage device to access the organization extranet, intranet and any other networks pre-authorized by the organization.

In the method, initialization of the external storage device may comprise the steps of deriving the cryptographic key for accessing the secure partition of the external storage device from at least a master key and the identifier of the external storage device, protecting or encrypting the cryptographic key for accessing the secure partition from an initial password assigned by the organization or selected by the user, and writing the protected cryptographic key for secure partition to the memory of the external storage device.

In the method, at least the volatile memory of the untrusted user computing device for holding any unlocked cryptographic key may be zeroized, followed by system shut-down of the untrusted user computing device when the external storage device is decoupled and disconnected from the untrusted user computing device.

In the method, the user computing device may be pre-configured to forbid the operating system to use any memory on the external storage device as the virtual memory.

A system of secure computing environment is provided. The system comprises at least one secure organization computing platform, at least one external storage device comprising at least one read/write secure partition and at least one read-only partition, and at least one untrusted user computing device, wherein the organization computing platform executing a first auditable data exchange application capable of recording data movement and other pre-determined events in a first audit log, the external storage device can be interfaced to and in communication with the organization computing platform which can transfer organization data to the external storage device in a data check-out process upon successful verification and authentication, the secure partition of the external storage device storing organization data in encrypted form, the external storage device can be interfaced to and in communication with the untrusted user computing device to which the organization data can be transferred for processing with authorized software modules comprising operating system, authorized applications and drivers pre-installed in the read-only partition of the external storage device, the organization user decoupling the external storage device from the organization computing platform with the organization data stored in its the secure partition, and interfacing the external storage device with the untrusted user computing device, the untrusted user computing device booting from the operating system pre-installed in the read-only partition of the external storage device, with the hard disk, any non-volatile storage devices, Internet and any other unauthorized network connections on the untrusted user computing device deactivated, the organization user invoking one or a plurality of the authorized applications pre-installed in the read-only partition of the external storage device for processing the organization data stored in the secure partition of the

external storage device, and the processed organization data can be transferred to the organization computing platform in a data check-in process upon successful verification and authentication.

5

In the system, the authorized applications may comprise a second auditable data exchange application which is loaded to the untrusted user computing device upon the completion of the booting processes, and the second auditable data exchange application may be used to record in a second audit log all the parameters, events and data movement between the external storage device and the untrusted user computing device as required by the audit policies of the organization, and the second audit log may be stored in the secure partition of the external storage device, and the second auditable data exchange application may be capable of encrypting and decrypting data for the secure partition of the external storage device.

20 In the system, the verification and authentication may comprise a device verification process for determining whether the interfaced external storage device has been pre-authorized by the organization, and an authentication process may comprise prompting the organization user for a password
25 for unlocking a protected cryptographic key for encrypting and decrypting data for the secure partition of the external storage device.

The present invention provides an innovative method and system for implementing a secure computing environment comprising an organization secure computing system, external storage devices and untrusted user computing devices on which the users exchange and process data proprietary to the organization

30

in a secure manner. Authentication events and data movement are recorded in auditable logs as per the organization data movement policy.

5 As a result, the present secure computing system extends the trusted computing environment of an organization to untrusted user computing devices outside the organization. The present system allows secure home and off-site working by the organization staffers using low-cost and off-the-shelf external
10 storage devices.

BRIEF DESCRIPTION

15 Embodiments according to the present invention will now be described with reference to the following figures, in which like reference numerals denote like elements.

FIG. 1 illustrates the secure computing system of the present invention,
20

FIG. 2 illustrates the flow of a data check-in and check-out process executed by the first auditable data exchange application of FIG. 1,
25

FIG. 3 illustrates the flow of an audit logging process executed by a second auditable data exchange application in one embodiment of the secure computing system of FIG. 1, and
30

FIG. 4 illustrates a process executed for initializing the external storage device of the secure computing system of FIG. 1.

DETAILED DESCRIPTION

5 The present invention may be understood more readily by reference to the following detailed description of certain embodiments of the invention.

Secure Computing System

10 **FIG. 1** shows a secure computing environment 100 comprising an organization secure computing system 110, at least one external storage device 150 and at least one untrusted user computing device 190.

15 The organization secure computing system 110 comprises at least one organization server 112 for executing a plurality of organization applications. The organization server 112 is in communication with a plurality of organization computing platforms 120 which provide organization staffers or users
20 access to server and client applications and data. One such application is the first auditable data exchange application 130 for exchanging organization data 140 with external storage devices 150 authorized by the organization. The first auditable data exchange application 130 further monitors and
25 records device usage, data movement and it may enforce organizational governance requirements for auditable data control.

Organization data 140 is any data proprietary to the organization including text documents, image files and other multi-
30 media data.

Verification of external storage devices 150 may be carried out by the organization computing platforms 120 or the first

auditable data exchange application 130. Devices which have not been explicitly authorized are rejected. The device verification result is recorded in a first audit log (270).

5 The memory of each of the external storage devices 150 comprises at least one read-only partition 160 and one secure partition 170. The secure partition 170, which is read-and-write enabled, stores the organization data 140 and any other user and application-related data in encrypted form. The
10 cryptographic key for accessing secure partition 170 is stored in a key memory 180 of the external storage device 150 in a protected form. This protected cryptographic key can be unlocked by a user password provided by the organization user in an authentication process.

15

The read-only partition 160 stores an operating system 162 for booting the untrusted user computing device 190. The read-only partition 160 further stores authorized applications 164 for processing the organization data 140 stored in
20 the secure partition 170, as well as drivers of authorized input-output devices 166 allowed to be coupled to the untrusted user computing device 190.

The organization user may decouple an external storage device
25 150 from his assigned organization computing platform 120.

The user may interface the external storage device 150 to an untrusted user computing device 190 at home, a remote customer site or in public amenities. When the external storage device 150 is in communication with the untrusted user computing device 190, the boot firmware of the untrusted user computing device 190 searches and executes the operating system
30 162, which is capable of executing the authorized applica-

tions 164, pre-installed in the read-only partition 160 of the external storage device 150.

The untrusted user computing device 190 by itself is a fixed
5 or portable computer used to exchange and process the organization data 140 outside the organization. The untrusted user computing device 190 may interface with the external storage device 150 for data exchange. The untrusted user computing device 190 may be the user's personal computer(s) at home,
10 shared computers for public use and even computers owned or pre-approved by the organization.

In order to create a trusted environment in the untrusted user computing device 190, the operating system 162 has been
15 pre-configured to deactivate the local hard disk and any local non-volatile storage device of the untrusted user computing device 190. The operating system 162 further prohibits the untrusted user computing device 190 or its applications from access to any networks, such as the Internet, which have
20 not been pre-approved by the organization. Furthermore, the system 162 prohibits any input-output devices which have not been authorized by the organization from exchanging data and signals with the untrusted user computing device 190.

25 **First auditable data exchange application**

FIG. 2 illustrates the data check-in, check-out process and audit logging executed by the first auditable data exchange application 130 of FIG. 1.

30 The process begins with step 230 in which the cryptographic key for accessing the secure partition 170 of the external storage device 150 is retrieved and unlocked. To perform data check-out (240), the first auditable data exchange applica-

tion 130 encrypts organization data 140 from the organization computing platform 120 with the unlocked cryptographic key for accessing the secure partition 170 in step 260. The application 130 further writes the encrypted data to the secure partition 170 of the external storage device 150 in step 265.

To perform data check-in in step 240, the first auditable data exchange application 130 retrieves and decrypts data stored in the secure partition 170 of the external storage device 150 with the unlocked cryptographic key for accessing the secure partition 170 in step 250. The application 130 further writes the decrypted data to a pre-assigned or user-specified memory of the organization computing platform 120 in step 255.

The first auditable data exchange application 130 records all data movement in the first audit log in step 270 according to pre-determined organization policies. The audit logging process of step 270 may also be executed concurrently with any of the data check-in and check-out processes 200.

In another embodiment, during the data check-in and check-out processes 200, the first auditable data exchange application 130 retrieves and unlocks the protected cryptographic key for accessing secure partition 170 from a centralized database stored in the organization server 112.

In yet another embodiment, the first auditable data exchange application 130 retains a copy of any data being written to the external storage device 150.

External Storage Device

The memory of the external storage device 150 comprises at least one read-only partition 160 and at least one secure partition 170. The secure partition 170, which is read-and-write enabled, stores the organization data 140 and any other user and application-related data in encrypted form. The read-only partition 160 stores software modules comprising an operating system 162, authorized applications 164 and drivers of authorized input-output devices 166 allowed to be coupled to the untrusted user computing device 190.

The read-only and secure partitions 160 & 170 are implemented in the non-volatile memory of the external storage device 150 such that the stored information is retained even when the external storage device is not electrically powered. The non-volatile memory may be flash memory, hard disk or optical based provided that the read-only partition 160 and the secure partition 170 can be created.

The secure partition 170 may be implemented in the form of disk encryption or file system encryption.

The external storage device 150 may comprise a controller and other means for enabling the required data access processes.

The external storage device 150 may be a customized or off-the-shelf product, typically with the aforesaid non-volatile memory, controller and other sub-systems housed in a portable chassis.

The external storage device 150 comprises an interface capable of exchanging signals and data with the untrusted user computing device 190 and the organization computing platform 120. The interface may conform to international and proprie-

tary interface standards adopted by manufacturers of fixed and portable computing devices. The interface may support any of the wired or wireless data communications including the Universal Serial Bus (USB with specifications available at
5 www.usb.org), IEEE 1394 (Firewire with specifications available at www.ieee.org) and Bluetooth (a short range communication standard - www.bluetooth.com). The interface standards include but are not limited to the protocols used by USB tokens, external hard disks, memory sticks, multimedia cards,
10 secure digital (SD) cards, xD-picture cards, smart media cards and compact flash cards.

The external storage device 150 may be integrated with another device used primarily for telecommunications, entertainment
15 or other applications.

An operating system 162 together with a plurality of authorized applications 164 and drivers for pre-approved input-output devices 166 are pre-installed in the read-only partition 160. The operating system 162 may be Microsoft Windows,
20 Linux and their variants. The operating system 162 may be any suitable system capable of executing the plurality of authorized computing applications 164 and drivers 166 can be executed in the untrusted user computing device 190.

25

The input-output device drivers are software codes used for enabling control signals and data exchange between the corresponding input-output devices and the untrusted user computing device 190. Only the drivers for pre-approved input-output devices are pre-installed in the read-only partition
30 160 of the external storage device 150. The pre-approved input-output devices may include basic inputting devices such as mice and keyboards, as well as essential outputting devices.

es including monitors and printers. The pre-approved input-output devices may further include biometric scanners and portable crypto-tokens for storing secret user cryptographic keys used in multi-factor authentication applications. Drivers conforming to open standards, such as BioAPI (under BioAPI Consortium with specifications available at www.bioapi.org) for biometric devices and PKCS#11 (under RSA Security with specifications available at www.rsa.com) for portable cryptographic tokens may be used.

It is important that the pre-approved input-output devices should exclude any conventional type of external storage devices. Conventional external storage devices, such as a USB flash drive or external hard disk, may inject malwares into the untrusted user computing device 190, hence diminishing the security level of the present secure computing environment 100.

Untrusted user computing device

The untrusted user computing device 190 is a fixed or portable computer used to exchange and process the organization data 140 outside the organization. It may be the user's personal computer(s) at home, off-site computers and shared computers for public use.

The boot firmware of the untrusted user computing device 190 is capable of searching and executing the operating system 162 pre-installed in the external storage device 150 when the external storage device 150 is interfaced to and in communication with the untrusted user computing device 190. The authorized applications 164 pre-installed in the same read-only partition 160 are executable by the operating system 162 within the untrusted user computing device 190. The local

hard disk and any local non-volatile storage device of the untrusted user computing device 190 are deactivated such that the external storage device 150 has no access to the local hard disk. Possible harmful executables, such as malwares,
5 residing in the untrusted user computing device 190 are unable to execute because the executables have no access to the processing resources of the untrusted user computing device 190.

10 The user computing device 190 may be pre-configured to forbid the operating system 162 to use any memory on the external storage device 150 as the virtual memory for processing.

The standard Basic Input-Output System Editor (BIOS editor)
15 on the untrusted user computing device 190 may be used to register with the untrusted user computing device 190 that the connected external storage device 150 should be searched for the operating system 162 when the untrusted user computing device 190 is powered up. The external storage device
20 150 may be listed as the first boot device in the booting sequence of the untrusted user computing device 190.

The operating system 162 may further prohibit the untrusted user computing device 190 or its applications from access to
25 any networks, such as the Internet, which have not been pre-approved by the organization.

Organization data 140 protected in the secure partition 170 of the external storage device 150 is first decrypted before
30 the authorized applications 164 running in the untrusted user computing device 190 can access it. Processed organization data and other application related data generated in the untrusted user computing device 190 are encrypted and trans-

ferred to the secure partition 170 of the external storage device 150. Analogous to the aforesaid data check-in and check-out processes 200, these cryptographic operations are transparent to the user and they are performed by a cryptographic software application executable in the user computing platform 190. Said cryptographic software application is one of the plurality of authorized applications 164 pre-installed in the read-only partition 160 of the external storage device 150. The cryptographic software application is loaded to the untrusted user computing device 190 when the external storage device 150 is connected and in communication with the untrusted user computing device 190. The protected cryptographic key for accessing secure partition 170 is unlocked by at least the password provided by the user in the aforesaid authentication process.

Data communication between the untrusted user computing device 190 and the external storage device 150 includes reading of authorized applications 164 and drivers 166 and transferring data associated with the secure partition 170. Within the secure computing environment 100, such data communication does not require the establishment of a special secure channel or tunnel.

25 Second auditable data exchange application

FIG. 3 illustrates an embodiment in which an audit logging process flow is executed by a second auditable data exchange application.

30 The second auditable data exchange application 320 is a pre-installed authorized application 164 stored in the read-only partition 160 of the external storage device 150.

As soon as the external storage device 150 is interfaced and in communication with the untrusted user computing device 190, the boot firmware of the untrusted user computing device 190 executes the operating system 162 pre-installed in the read-only partition 160 of the external storage device 150 in step 310, followed by executing the second auditable data exchange application (320) within the untrusted user computing device 190. In the next step 330, the second auditable data exchange application records in a second audit log 330 all the parameters, events and the corresponding time stamps, and any information, such as the sizes, types and attributes associated with the transferred data, in accordance with the audit policies of the organization. The second audit log 330 may be stored in the secure partition 170 of the external storage device 150 with its content directly updated by the second auditable data exchange application 320. The second audit log 330 may be read and transferred (340) to the organization computing platform 120 by the first auditable data exchange application 130 when the external storage device 150 is interfaced and in communication with the first auditable data exchange application 130.

The second auditable data exchange application 320 may replace and perform the functions of the aforesaid cryptographic software application for encrypting data written from the untrusted user computing device 190 to the secure partition 170 of the external storage device 150, as well as decrypting data copied from the secure partition 170 of the external storage device 150 to the memory of the untrusted user computing device 190. The cryptographic key for accessing secure partition 170 may be stored in protected form in the key memory 180 of the external storage device 150, and this pro-

tected key is unlocked upon the user entering his or her password.

User Authentication

5 The cryptographic key for accessing secure partition 170 is stored in a key memory 180 of the external storage device 150 in a protected form. This protected cryptographic key can be unlocked by a user password provided by the organization user through the aforesaid authentication process in which the user
10 er is prompted to enter at least his or her password among other credentials.

The authentication process may be executed by the organization computing platform 120 or the first auditable data exchange application 130 upon the connection of the external
15 storage device 150 with the organization computing platform 120.

The authentication process may be executed by the second auditable data exchange application (320) or one of the authorized applications 164 pre-installed in the read-only partition 160 of the external storage device 150 upon the connection of the external storage device 150 with the untrusted
20 user computing device 190.

25

Device Verification

Either one or both of the organization computing platform 120 and the untrusted user computing device 190 may perform device verification of the external storage device 150 prior to
30 transfer of any organization data 140 or the execution of any authorized applications 164. Devices which have not been explicitly authorized by the organization are rejected. A "white list" of pre-authorized external storage devices,

which comply with the security requirements and device configuration described herein, is maintained in the organization server 112. During the device verification, the identifier of the external storage device 150 is compared against the white list of authorized devices each time an external storage device 150 is interfaced to the organization computing platform 120 and/or untrusted user computing device 190. Devices which have not been explicitly authorized are rejected. The device verification result may be recorded in the audit logs 270 & 330. The identifier of the external storage device 150 may be read from the device. The identifier may be hardcoded in the device by the device manufacturer. Some devices may allow the organization administrators with sufficient administrative right to amend the identifier through a suitable software development kit. The identifier of the external storage device 150 together with the organization user to whom the device 150 has been allocated may be stored by the organization for accountability enforcement as per the data control policy requirements of the organization.

20

The first auditable data exchange application 130 may perform the device verification prior to executing the data check-in and the data check-out processes 200. The authorized external storage device 150 may store the device verification status in its read-only partition 160 for use by the second auditable data exchange application 320 to determine whether the interfaced external storage device 150 has been authorized.

The second auditable data exchange application 320 may perform the device verification prior to transfer of any organization data 140 or the execution of any authorized applications 164. Identifier of the external storage device 150 may be used for device verification. Alternatively, second au-

auditable data exchange application 320 may check said device verification status stored in the read-only partition 160 of the authorized external storage device 150.

5 **Key Verification**

The unlocked cryptographic key for accessing secure partition 170 may be verified, in a key verification process, against a parameter derived from the original cryptographic key for validating whether the unlocked cryptographic key matches the original cryptographic key. The key verification process is executed by either one or both of the organization computing platform 120 and the untrusted user computing device 190 after the cryptographic key for accessing secure partition 170 of the external storage device 150 is unlocked in the afore-said authentication process. The parameter may comprise the cryptographic checksum of the original cryptographic key. The parameter may be stored side by side with the protected cryptographic key for accessing secure partition 170 in the external storage device 150. Key verification results may be recorded in the audit logs 170 & 330. Any negative key verification results may cause the termination of any data transfer requests.

The key verification process may be executed by either one or both of the first (130) and second (320) auditable data exchange applications.

Policy Enforcement

Either one or both of the organization computing platform 120 and the untrusted user computing device 190 may enforce policies by file types, file size, time of usage, keywords and any other pre-determined criteria. For instance, all executables are blocked from being transferred as they may be embed-

ded with malwares which may undermine the security level of the secure computing environment 100. Any requests for data transfer which have been rejected as a result of policy enforcement may be recorded in the audit logs 270 & 330.

5

The policy enforcement process may be executed by either one or both of the first (130) and second (320) auditable data exchange applications.

10 **Audit Log**

The audit logs 270 & 330 have entries and formats conforming to the organizational governance requirements. The audit logs 270 & 330 may record the identifier of the external storage device 150, the identifier of the organization computing platform 120, the identifier of the untrusted user computing device 190, any user identifier, device and key verification status, as well as any information, such as event time stamps, sizes, types and attributes, associated with data read from and written to the secure partition 170 of the external storage device 150. The identifiers of the organization computing platform 120 and untrusted user computing device 190 may be constructed from one or a plurality of the identity codes associated with the central processing unit (CPU) and subsystems of the respective organization computing platform 120 and untrusted user computing device 190. The component and subsystem identity codes are typically set by the respective manufacturers.

Data and Key Protection in External Storage Device

30 The cryptographic key for accessing secure partition 170 used for encrypting and decrypting data in the secure partition 170 of the external storage device 150 may be a single symmetric key or an asymmetric key pair.

The cryptographic key for accessing secure partition 170 may be cryptographically protected with a second cryptographic key derived with the user password and other parameters in accordance with a pre-determined algorithm. In this case, the protected cryptographic key for accessing secure partition 170 may be unlocked in a decryption process with the second cryptographic key derived from the user password using the same pre-determined algorithm. The encrypted data stored in the secure partition 170 can be recovered if and only if the password entered by the user for unlocking the protected cryptographic key for accessing secure partition 170 is identical to the password used for locking the original cryptographic key for accessing secure partition 170.

Data encryption and decryption algorithms for the secure partition 170 may conform to an open cryptography standard such as AES (NIST FIPS 197 with specifications available at <http://csrc.nist.gov/publications/PubsFIPS.html>) and triple DES (NIST FIPS 463 with specifications available at <http://csrc.nist.gov/publications/PubsFIPSArch.html>).

The cryptographic operations handling the encryption and decryption of the data for the secure partition 170 may be performed by a software application or a hardware module within the external storage device 150.

The cryptographic key for accessing secure partition 170 may be encrypted by the user fingerprint to form a locked fingerprint which is by itself secure. Therefore, the locked fingerprint may be stored in the read-only partition 160 of the external storage device 150 without further cryptographic protection. An authorized fingerprint scanner attached to or

integrated with the external storage device 150 may be used to capture the user fingerprint for regenerating the original cryptographic key for accessing secure partition 170.

5 The operating system 162 may allow applications pre-installed in the read-only partition 160 of the external storage device 150 to access a remote organization server 112 through the organization extranet which may be a virtual private network. The organization data 140 may be centrally stored in the or-
10 ganization server 112 and accessed by the user on a need-to-use basis. This further reduces the risk of data leakage when external storage device 150 is misplaced or lost. The organization data 140 may be further secured with application-level cryptographic protection.

15

External Storage Device Initialization

Deployment of external storage devices 150 for the implementation of the secure computing environment 100 may be managed centrally.

20

FIG. 4 illustrates a process flow executed for initializing an external storage device 150 of the secure computing environment 100 of FIG. 1.

25 The cryptographic key for accessing secure partition 170 used for encrypting and decrypting data stored in the secure partition 170 in each external storage device 150 may be derived from a master key (410) and a plurality of parameters in step 420. The master key 410 is securely held by one or a plurality of personnel with sufficient privileges assigned by the
30 organization. In the next step 430, the derived cryptographic key for accessing secure partition 170 is protected by an initial password assigned by the organization or selected by

the user. The password-protected cryptographic key for accessing secure partition 170 is then written to the key memory 180 in the external storage device 150 in step 440.

5 The organization master key 410 may be an asymmetric key or a symmetric key. The master key may be stored in a secure smart chip on a smart card. The master key may be split and stored in the secure smart chips of a plurality of smart cards each of which may be retained by a staffer assigned by the organization.
10 zation.

The cryptographic key for accessing secure partition 170 used for encrypting and decrypting data stored in the secure partition 170 in each external storage device 150 may be derived
15 from the master key 410 and an identifier unique to each external storage device 150 in step 420. The identifier may be the serial number hardcoded in the external storage device 150 by the device manufacturer. The algorithm(s) involved in the key derivation may be a standard or proprietary symmetric
20 or asymmetric cryptographic algorithm. The inputs to the cryptographic algorithm comprise the master key 410, the unique identifier of the external storage device 150 and any other parameters required to ensure that the master key 410 cannot be deduced from the derived cryptographic key for accessing secure partition 170 and / or the unique identifier
25 of the external storage device 150. The parameters may comprise a random value or salt.

In the event that the user fails to recall the password used
30 to protect the cryptographic key for accessing secure partition 170, the cryptographic key for accessing secure partition 170 can be derived when the user is able to provide the user identifier assigned by the organization or selected by

the user, as well as the identifier of the external storage device 150. The unique identifier of the external storage device 150 may be obtained by either reading the code from the external storage device 150 or through looking up a table or
5 database which stores the device identifier corresponding to the user identifier provided by the user.

User passwords may be changed on the organization computing platform 120 or in a credential management application pre-
10 installed in the read-only partition 160 of the external storage device 150. Upon request, the credential management application is executed on the untrusted user computing device 190. A new password is accepted only if the user is able to provide the details of the current credentials including
15 user identifier and current user password.

System Shut-Down

During device verification and user authentication, when the number of failed attempts has exceeded a pre-determined
20 threshold value(s), the authentication status is firstly recorded in the audit logs 270 & 330 and the untrusted user computing device 190 shuts down automatically.

Furthermore, decoupling the external storage device 150 from
25 the untrusted user computing device 190 causes the untrusted user computing device 190 to shut down automatically, resulting in loss of data which has not been saved to the external storage device 150.

30 Before shutting down the untrusted user computing device 190 upon user request, or other reasons including decoupling of the external storage device 150 from the untrusted user computing device 190 and failed authentication attempts, the

volatile memory in the untrusted user computing device 190 which is used to temporarily hold the unlocked cryptographic key for accessing secure partition 170 may be zeroized as per the Federal Information Processing Standard (FIPS) Publication 140-2 Level 3 and above
5 (csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf).

In summary, the secure computing environment 100 allows a user to transfer organization data 140 to an external storage
10 device 150 authorized by the organization. The external storage device 150 comprises two partitions one of which is read-only 160 whereas the second read/write-enabled secure partition 170 stores data in encrypted form. When the user interfaces the external storage device 150 with an untrusted user
15 computing device 190, the untrusted user computing device 190 is booted from the external storage device 150 followed by device verification, user authentication and deactivation of the Internet connection, local hard disk and all unauthorized input-output devices. A cryptographic software application
20 performs encryption and decryption of data to and from the secure partition 170 of the external storage device 150. Authentication events and data movement are recorded in audit logs 270 & 330 as per the organization security and data movement policy. The secure computing environment 100 extends
25 the trusted organization secure computing environment 100 to untrusted user computing devices 190 outside the organization.

Although the above description contains much specificity,
30 these should not be construed as limiting the scope of the embodiments but merely providing illustration of the foreseeable embodiments. Especially the above stated advantages of the embodiments should not be construed as limiting the scope

of the embodiments but merely to explain possible achievements if the described embodiments are put into practise. Thus, the scope of the embodiments should be determined by the claims and their equivalents, rather than by the examples
5 given.

CLAIMS

1. A method of implementing a secure computing environment,
wherein

5 at least one secure organization computing platform
executing a first auditable data exchange application
capable of recording events in a first audit log can be
interfaced to and in communication with at least one ex-
ternal storage device for exchanging organization data
10 between the memory of said organization computing plat-
form and a secure partition of said external storage de-
vice, and said external storage device comprising at
least one read/write secure partition, which stores or-
ganization data in encrypted form, and one read-only
15 partition, and said external storage device can further
be interfaced and in communication with at least one un-
trusted user computing device to which said organization
data can be transferred for processing with pre-
authorized software modules comprising an operating sys-
tem, a plurality of authorized applications and drivers
20 pre-installed in said read-only partition of said exter-
nal storage device, and

 the method comprising the steps of
 an organization user interfacing said external
25 storage device to said organization computing platform
for checking out said organization data,

 said first auditable data exchange application re-
cording parameters and events associated with data move-
ment and any other pre-determined events in said first
30 audit log,

 said organization user decoupling said external
storage device with said organization data stored in its
said secure partition and interfacing said external

storage device with said untrusted user computing device,

said untrusted user computing device booting from said operating system pre-installed in said read-only partition of said external storage device, with the hard disk, any non-volatile storage devices, Internet and any other unauthorized network connections on said untrusted user computing device deactivated,

said organization user invoking one or a plurality of said authorized applications pre-installed in said read-only partition of said external storage device for processing said organization data stored in said secure partition of said external storage device, and

said processed organization data can be transferred to said organization computing platform in a data check-in process.

2. The method of claim 1, wherein

said checking out of said organization data being performed by said first auditable data exchange application to encrypt said organization data from said organization computing platform with an unlocked cryptographic key for accessing said secure partition, followed by writing said encrypted organization data to said secure partition of said external storage device.

3. The method of claim 1, wherein

said data check-in process being performed by said first auditable data exchange application to decrypt the data from said secure partition of said external storage device with an unlocked cryptographic key and transferring said decrypted data to the memory of said organization computing platform.

4. The method of claim 1, wherein
said organization data protected in said secure
partition of said external storage device being firstly
5 unlocked or decrypted before being accessed by said au-
thorized applications running in said untrusted user
computing device, and processed organization data and
other application related data generated in said un-
trusted user computing device being encrypted and trans-
10 ferred to said secure partition of said external storage
device, and this data encryption and decryption being
executed by a cryptographic application executed in said
user computing platform using an unlocked cryptographic
key for accessing said secure partition, and said cryp-
15 tographic application being one of the plurality of au-
thorized applications pre-installed in said read-only
partition of said external storage device.
5. The method of any of claims 1 to 4, wherein
20 said cryptographic key for accessing said secure
partition being stored in protected form in a key memory
of said external storage device.
6. The method of claim 1, wherein
25 said authorized applications comprising a second
auditable data exchange application which is loaded to
and executed by said untrusted user computing device up-
on the completion of said booting processes, and said
second auditable data exchange application being used to
30 record in a second audit log the data movement between
said external storage device and said untrusted user
computing device, and all the parameters, events and the
corresponding time stamps required by the audit policies

of the organization, and said second audit log being stored in said secure partition of said external storage device.

- 5 7. The method of claims 4 and 6, wherein
 said second auditable data exchange application replacing said cryptographic application for encrypting and decrypting data exchanged between said secure partition of external storage device and said untrusted user
10 computing device.
8. The method of any of the above claims, wherein
 at least one of said organization computing platform and untrusted user computing device executing a device verification process for determining whether said
15 interfaced external storage device has been pre-authorized by said organization.
9. The method of any of the above claims, wherein
20 at least one of said organization computing platform and untrusted user computing device unlocking said protected cryptographic key for accessing said secure partition of said external storage device by means of a user password provided by said organization user in an
25 authentication process.
10. The method of any of the above claims, wherein
 at least one of said organization computing platform and untrusted user computing device executing a key
30 verification process in which said unlocked cryptographic key for accessing said secure partition being compared against a parameter derived from the original cryptographic key for validating whether said unlocked

cryptographic key matches said original cryptographic key, and said parameter comprising the cryptographic checksum of said original cryptographic key stored in said external storage device.

5

11. The method of any of the above claims, wherein
at least one of said organization computing platform and untrusted user computing device enforcing data control and security policies pre-determined by the organization, and said policies comprising verification, authentication and authorization results, file movement control in accordance with file types, file size, time of usage and any other pre-determined criteria.

10

12. The method of any of claims 1, 8 to 11, wherein
any of said device verification, said authentication, said key verification and said policy enforcement processes executed on said user computing device being executable processes provided by one or a plurality of said authorized applications pre-installed in said read-only partition of said external storage device.

20

13. The method of any of claims 1, 8 to 12, wherein
any of said device verification, said authentication, said key verification and said policy enforcement processes being executed by at least one of said first and second auditable data exchange applications.

25

14. The method of any of claims 1, 6, 7 and 13, wherein
said parameters logged by said first and second auditable data exchange applications comprising the identifiers of either one or both of said organization computing platform and untrusted user computing device, and

30

said identifiers can be constructed from one or a plurality of the identity codes associated with the central processing units (CPU) and subsystems of said organization computing platform and untrusted user computing device respectively.

15. The method of claim 1, wherein

said drivers being software codes used for enabling control signals and data exchange between the respective authorized input-output devices and said untrusted user computing device, and said authorized input-output devices including basic inputting devices such as mice and keyboards, essential outputting devices such as monitors and printers, but excluding any conventional external storage devices such as portable flash drives and external hard disks.

16. The method of claim 15, wherein

said authorized input-output devices including biometric scanners and portable crypto-token used for storing secret user cryptographic keys used in multi-factor authentication.

17. The method of any of claims 1, 4, 6 to 11, 14 and 15, wherein

said untrusted user computing device being a fixed or portable computer with which the organization user works outside the organization, and said untrusted user computing device including said user's home computers, off-site computers and shared computers for public use, and said untrusted user computing device having a standard Basic Input-Output system (BIOS) editor which can be used to register with said untrusted user computing de-

vice that said external storage device should be searched for said operating system when said untrusted user computing device is powered up.

5 18. The method of any of the above claims, wherein
said cryptographic key for accessing said secure
partition being cryptographically protected with a se-
cond cryptographic key derived from the user password
and other parameters in accordance with a pre-determined
10 algorithm, and said protected cryptographic key for ac-
cessing said secure partition can be unlocked in a de-
cryption process with said second cryptographic key de-
rived from said user password using said same pre-
determined algorithm.

15 19. The method of any of the above claims, wherein
said cryptographic key for accessing said secure
partition being cryptographically protected by the user
fingerprint to form a locked fingerprint module which is
20 secure and can be stored in said external storage device
without additional cryptographic protection.

20. The method of any of the above claims, wherein
said cryptographic operations handling said en-
25 crypting and decrypting of the data for said secure par-
tition being performed by a software application or a
hardware module within said external storage device.

21. The method of claim 1, wherein
30 said operating system allowing said authorized ap-
plications pre-installed in said read-only partition of
said external storage device to access the organization

extranet, intranet and any other networks pre-authorized by the organization.

22. The method of claim 1, wherein

5 initialization of said external storage device comprising the steps of

 deriving said cryptographic key for accessing said secure partition of said external storage device from at least a master key and the identifier of said external storage device,

10 protecting or encrypting said cryptographic key for accessing said secure partition from an initial password assigned by the organization or selected by said user, and

15 writing said protected cryptographic key for secure partition to the memory of said external storage device.

23. The method of any of the above claims, wherein

20 at least the volatile memory of said untrusted user computing device for holding any unlocked cryptographic key being zeroized, followed by system shut-down of said untrusted user computing device when said external storage device is decoupled and disconnected from said untrusted user computing device.

25

24. The method of any of the above claims, wherein

 said user computing device being pre-configured to forbid said operating system to use any memory on said external storage device as the virtual memory.

30

25. A system of secure computing environment comprising

 at least one secure organization computing platform, at least one external storage device comprising at

least one read/write secure partition and at least one read-only partition, and at least one untrusted user computing device, wherein

5 said organization computing platform executing a first auditable data exchange application capable of recording data movement and other pre-determined events in a first audit log,

10 said external storage device can be interfaced to and in communication with said organization computing platform which can transfer organization data to said external storage device in a data check-out process upon successful verification and authentication,

15 said secure partition of said external storage device storing organization data in encrypted form,

20 said external storage device can be interfaced to and in communication with said untrusted user computing device to which said organization data can be transferred for processing with authorized software modules comprising operating system, authorized applications and drivers pre-installed in said read-only partition of said external storage device,

25 said organization user decoupling said external storage device from said organization computing platform with said organization data stored in its said secure partition, and interfacing said external storage device with said untrusted user computing device,

30 said untrusted user computing device booting from said operating system pre-installed in said read-only partition of said external storage device, with the hard disk, any non-volatile storage devices, Internet and any other unauthorized network connections on said untrusted user computing device deactivated,

said organization user invoking one or a plurality of said authorized applications pre-installed in said read-only partition of said external storage device for processing said organization data stored in said secure partition of said external storage device, and

said processed organization data can be transferred to said organization computing platform in a data check-in process upon successful verification and authentication.

26. The system of claim 25, wherein

said authorized applications comprising a second auditable data exchange application which is loaded to said untrusted user computing device upon the completion of said booting processes, and said second auditable data exchange application being used to record in a second audit log all the parameters, events and data movement between said external storage device and said untrusted user computing device as required by the audit policies of the organization, and said second audit log being stored in said secure partition of said external storage device, and said second auditable data exchange application being capable of encrypting and decrypting data for said secure partition of said external storage device.

27. The system of claim 25, wherein

said verification and authentication comprising a device verification process for determining whether said interfaced external storage device has been pre-authorized by said organization, and

an authentication process comprising prompting said organization user for a password for unlocking a protected cryptographic key for encrypting and decrypting

data for said secure partition of said external storage device.