

DATA TRANSMISSION SYSTEM AND METHODS

TECHNICAL FIELD

- 5 The present invention generally relates to data transmission system and methods, more particularly the present invention relates to a system and methods for data transmission in a communication network.

BACKGROUND OF INVENTION

10

There has been a rising problem where it has been difficult for data transmission process in a communication network involving establishments such as vendors or customers, institutions such as financial institutions, and various interrelated organizations.

- 15 The major concern in the data transmission process in a communication network is that nodes in the network belong to a myriad of operating environments that make communication between the nodes difficult. The process becomes more difficult when the data transmission concerns sensitive data, which requires paramount level of security.

- 20 Some prior art documents have disclosed the data transmission system and methods similar to the present invention. WO2011095988 discloses a system for extracting and consolidating unstructured data contained in a plurality of files in composite formats is disc, and that the system includes an input means which receives a plurality of files containing unstructured data in composite formats and forwards the received files to an extraction
25 means which extracts the unstructured data from the received files. The unstructured data extracted is forwarded to a conversion means which converts the unstructured data into a structured format, and the structured data is worked on by an interlinking means.

- 30 However, the processes disclosed in the prior art, WO2011095988 are directed to the processes of extracting unstructured, and converting the data into structured data for analysis. The prior art does not address the problem of data transmission process in a communication network is that nodes in the network belong to a myriad of operating environments that make communication between the nodes difficult.

WO2008047974 discloses a migration apparatus and method for converting a database of a mainframe system into an appropriate database for an open system, wherein the migration apparatus includes a data extraction module connected with a database of the mainframe system and extracting data composed of Extended Binary Coded Decimal Interchange Code (EBCDIC) in binary format, a code conversion module converting the extracted EBCDIC data into American Standard Code for Information Interchange (ASCII) code, full-width characters being converted into half-width characters corresponding to ASCII code using a previously set full-width/half-width conversion table, and a data transfer module, transferring the data converted into ASCII code to store it in a database previously built in the open system to correspond to the database of the mainframe system.

The prior art WO2008047974 discloses the data conversion process in Extended Binary Coded Decimal Interchange Code (EBCDIC) in binary format into American Standard Code for Information Interchange (ASCII) code, and that the prior art relates to migration apparatus and method for converting a database of a mainframe system into an appropriate database for an open system.

WO 2012090222 discloses a system for converting and presenting financial information from at least one accounting and reporting standard to another accounting and reporting standard comprising an access control means to verify credentials of a user logging in to get access of the system, an input source for feeding in transaction details and calculating account headwise trial balance, an extraction layer for fetching the head-wise trial balance from the input sources, a financial data management module (FDM) for validating and mapping account head-wise trial balance received from the input sources, an ETI block for fetching and populating account head-wise trial balance and populating the same into a database through an interface table, the interface table for converting head-wise trial balance and fetching other transaction details together known as financial information.

The prior art WO 2012090222 discloses a business logic block containing various business rules and logics and calculation methods for converting financial information from one accounting and reporting standard to another based on the user's requirement. The prior art however does not address the he problem of data transmission process in a communication

network is that nodes in the network belong to a myriad of operating environments, without comprising the data protection and data security levels.

5 The prior art documents however do not overcome the problem pertaining data transmission so as to provide a seamlessly secured network communication.

There is therefore a need for a system and methods to provide a seamless data transmission in a communication network between various establishments, and that the data transmission without compromising security levels of the data transmission and to maintain prudence.

10

SUMMARY OF INVENTION

The present invention pursuits system and methods for transmitting data in a communication network, whereby the data is transferred between a plurality of nodes through a module that interconnects the plurality of nodes, in that the nodes represent communicating nodes of establishments interconnected across the communication network.

15 It is one object of the present invention to provide a system for data transmission comprising at least a first node and at least a second node, each node for receiving and transmitting data, and a bridging module that establishes communication between said at least a first node and said at least a second node for data transmission.

25 It is an object of the present invention to provide a system for data transmission comprising a bridging module for receiving data in a variety of format from at least one node and mapping or converting the data into a format readable by at least one receiving node, and transmitting the mapped or converted data to that of said at least one receiving node.

30 It is another object of the present invention to provide a system for data transmission comprising at least a first node and at least a second node, each node for receiving and transmitting data, and a bridging module for data transmission, wherein said at least a first node comprises an extraction module for extracting data therefrom, an encryption module for encrypting data, a decryption module for decrypting data, a transmitter for transmitting data, a receiver for receiving data, or in any combination thereof.

It is yet an object of the present invention to provide a system for data transmission comprising at least a first node and at least a second node, each node for receiving and transmitting data, and a bridging module for data transmission, wherein said at least a second node comprises an extraction module for extracting data therefrom, an encryption module for encrypting data, a decryption module for decrypting data, a transmitter for transmitting data, a receiver for receiving data, or in any combination thereof.

It is yet another object of the present invention to provide system for data transmission comprising at least a first node and at least a second node, each node for receiving and transmitting data, and a bridging module for data transmission, wherein the bridging module comprises an encryption module for encrypting data, a decryption module for decrypting data, a transmitter for transmitting data, or a receiver for receiving data.

The present embodiment aims to achieve a data transmission system and methods that provide seamless data transmission in a communication network between various establishments that belong to a myriad of operating environments.

BRIEF DESCRIPTION OF DRAWINGS

Figure 1 illustrates an overview of the system architecture for data transmission according to the present invention.

Figure 2 illustrates a schematic representation of the system architecture for data transmission according to the present invention.

Figure 3 illustrates a schematic representation of the system architecture for data transmission according to the present invention.

Figure 4 illustrates a graphical representation of the system architecture for data transmission according to the present invention.

Figure 5 illustrates a security process according to the present invention.

Figure 6 illustrates a schematic representation of the system architecture for data transmission according to the present invention.

Figure 7 illustrates a graphical representation of the system architecture for data transmission between various establishments according to the present invention.

DETAILED DESCRIPTION OF EMBODIMENTS

Described below are preferred embodiments of the present invention with reference to the accompanying drawings. Each of the following preferred embodiments describes an example not limiting in any aspect.

Referring to Figure 1, there is illustrated an overview of the system architecture for data transmission according to the present invention, wherein the system for data transmission comprising a communication network for transferring data between a plurality of nodes via a bridging module (8), wherein Figure 1 shows that the plurality of nodes are at least a first node (11) and at least a second node (12) connected via the bridging module (8).

The bridging module (8) receives data in a variety of format from at least one node and maps or converts the data into a format readable by at least one receiving node, and transmits the mapped or converted data to that of said at least one receiving node.

Ultimately, the system for data transmission comprising at least a first node (11) for receiving and transmitting data, and at least a second node (12) for receiving and transmitting data, wherein the bridging module (8) establishes communication between said at least a first node (11) and said at least a second node (12) by linking at least a path (9) between said at least a first node (11) and said at least a second node (12) for data transmission, in that said at least a path (9) regulates data transmitted to and received from said at least a first node (11) and said at least a second node (12).

30

The bridging module (8) is configured for receiving data from said at least a first node (11) in a format type incongruent with a required format in said at least a second node (12), mapping or converting the data into the required format such that the mapped or converted

data is readable by said at least a second node (12), and then transmitting the mapped or converted data to that of said at least a second node (12). In the similar context, the bridging module (8) provides a medium for data transmission between said at least a first node (11) and said at least a second node (12).

5

The data transmission according to the preferred system of the present invention, is executed in a transient data transmission. In the event a data is written to a queue by a user task, the queue can be used subsequently as input data by other tasks within a control region. All access is sequential, governed by read and write pointers. Once a record has
10 been read, it cannot be read subsequently by another task.

The transient data transmission in the preferred system of the present invention is operated in such a way that the transmitted data becomes unrecoverable once the data leaves the bridging module (8).

15

The system of the present invention aims to provide a solution to establish automated host to host connectivity with preferably but not limited to an ERP (Enterprise Resource Planning) system with financial institutions in the most cost efficient manner. In such a system, the implementation model envisages that the data transmission between a plurality
20 of nodes, wherein the information in one of the nodes, for example, said at least a first node (11), provided in an ERP format is transmitted to the bridging module (8) for onward conversion and transmission to another node, said at least a second node (12), for example to a receiver at a financial institution.

25 The objective of this system is to improve the end-to-end services for data transmission between various engaging establishments.

Particularly, the operating environment in said at least a first node (11) is different from that of the operating environment of said at least a second node (12), such that the data
30 generated or obtained at said at least a first node (11) is established in a format different from that of the format required by said at least a second node (12). The present invention therefore provides a system for regulating the data such that the consistency of the data transmission is maintained throughout the transmission process, whereby compliance of the

format of the data transmitted from said at least a first node (11) with the format required by said at least a second node (12) is consistently achieved for further processing.

5 The consistency of the data transmission is achieved by introducing the bridging module (8) in accordance with the present invention for providing a medium between said at least a first node (11) and said at least a second node (12) for regulating data exchange between said at least a first node (11) and said at least a second node (12). Objectively, the bridging module (8) receives data from said at least a first node (11), and maps or converts the data received from said at least a first node (11) to a format of the data readable by said at least a
10 second node (12). In the similar context, the data from said at least a first node (11) is processed by the bridging module (8) and made to conform to the data format requirements as specified by said at least a second node (12). The conformed data is then transmitted to said at least a second node (12), such that the conformed data facilitates subsequent processing.

15

With regards to security issues, the bridging module (8) in accordance to the present invention is configured to erase history of the data once the mapped or converted data is transmitted to said at least a second node (12), such that the processed data becomes untraceable.

20

Referring to Figure 2, there is illustrated a schematic representation of the system architecture for data transmission according to the present invention, wherein the Figure 2 illustrates the system architecture comprising at least a first node (11) for receiving and transmitting data, at least a second node (12) for receiving and transmitting data, and a
25 bridging module (8) that establishes communication between said at least a first node (11) and said at least a second node (12) by linking at least a path (9) between said at least a first node (11) and said at least a second node (12) for data transmission.

Said at least a path (9) regulates data transmitted to and received from said at least a first
30 node (11) and said at least a second node (12), whereby said at least a path (9) is subjected to providing a data transmission path between said at least a first node (11) and said at least a second node (12) by way of preferably but not limited to a secured File Transfer Protocol

(FTP). It should be also noted that said at least a path (9) can transmit data via other methods supported by said at least a first node (11) and said at least a second node (12).

5 The system of the present invention aims to provide a solution to establish automated host to host connectivity with preferably but not limited to an ERP (Enterprise Resource Planning) system with financial institutions in the most cost efficient manner. In such a system, the implementation model envisages that the data transmission between a plurality of nodes, wherein the information in one of the nodes, for example, said at least a first node (11), provided in an ERP format is transmitted to the bridging module (8) for onward
10 conversion and transmission to another node, said at least a second node (12), for example to a receiver at a financial institution.

The objective of this system is to improve the end-to-end services for data transmission between various engaging establishments.

15

Particularly, the operating environment in said at least a first node (11) is different from that of the operating environment of said at least a second node (12), such that the data generated or obtained at said at least a first node (11) is established in a format different from that of the format required by said at least a second node (12). The present invention
20 therefore provides a system for regulating the data such that the consistency of the data transmission is maintained throughout the transmission process, whereby compliance of the format of the data transmitted from said at least a first node (11) with the format required by said at least a second node (12) is consistently achieved for further processing.

25 The consistency of the data transmission is achieved by introducing the bridging module (8) in accordance with the present invention for providing a medium between said at least a first node (11) and said at least a second node (12) for regulating data exchange between said at least a first node (11) and said at least a second node (12). Objectively, the bridging module (8) receives data from said at least a first node (11), and maps or converts the data
30 received from said at least a first node (11) to a format of the data readable by said at least a second node (12). In the similar context, the data from said at least a first node (11) is processed by the bridging module (8) and made to conform to the data format requirements as specified by said at least a second node (12). The conformed data is then transmitted to

said at least a second node (12), such that the conformed data facilitates subsequent processing.

It is shown in Figure 2 that said at least a first node (11) comprises an extraction module
5 (101) for extracting data therefrom, an encryption module (102) for encrypting data, a
decryption module (103) for decrypting data, a transmitter (104) for transmitting data, a
receiver (105) for receiving data, or in any combination thereof.

The extraction module (101) at said at least a first node (11) extracts data for transmission
10 by the system and that these data are compiled and encrypted by an encryption module
(102) if the data is required to be encrypted, and that the encrypted data is transmitted from
said at least a first node (11) via the transmitter (104). Further, said at least a first node (11)
comprises a receiver (105) for receiving data transmitted to said at least a first node (11),
and that the received data is decrypted by the decryption module (103) for processing. It
15 should be noted that the process of encryption and decryption of data is according to the
data transmission system and method of the present invention, such that the data resides in
format that is subjected by the operating environment of said at least a first node (11).

It is shown in Figure 2 that said at least a second node (12) comprises an extraction module
20 (201) for extracting data therefrom, an encryption module (202) for encrypting data, a
decryption module (203) for decrypting data, a transmitter (204) for transmitting data, a
receiver (205) for receiving data, or in an combination thereof.

The extraction module (201) at said at least a second node (12) extracts data for
25 transmission by the system and that these data are compiled and encrypted by an encryption
module (202) if the data is required to be encrypted, and that the encrypted data is
transmitted from said at least a second node (12) via the transmitter (204). Further, said at
least a second node (12) comprises a receiver (205) for receiving data transmitted to said at
least a second node (12), and that the received data is decrypted by the decryption module
30 (203) for processing. It should be noted that the process of encryption and decryption of
data is according to the data transmission system and method of the present invention, such
that the data resides in format that is subjected by the operating environment of said at least
a second node (12).

It is shown in Figure 2 that the bridging module (8) comprises a processor (21), for regulating the data transmission on per session basis, and that the bridging module (8) comprises an encryption module (301) for encrypting data, a decryption module (302) for decrypting data, a transmitter (303) for transmitting data, a receiver (304) for receiving data, or that these modules can exist in the bridging module (8) in any combination.

The bridging module (8) establishes communication between said at least a first node (11) and said at least a second node (12) by linking at least a path (9) between said at least a first node (11) and said at least a second node (12) for data transmission. In the operation of the bridging module (8) establishing communication between said at least a first node (11) and said at least a second node (12), the bridging module (8), receives data from said at least a first node (11) via the receiver (304), processes the data via the processor (21) and transmits the data to said at least a second node (12) via the transmitter (303).

The bridging module (8) is implemented in a process that the bridging module (8) autonomously regulates the data transmission, whereby the data received from said at least a first node (11) is processed and established for conformity and compatibility with the operating environment of said at least second node (12), such that the format of data received from said at least a first node (11) is mapped or converted to that of the format of data for transmission to said at least a second node (12).

The bridging module (8) is configured for receiving data from said at least a first node (11) in a format type incongruent with a required format in said at least a second node (12), mapping or converting the data into the required format such that the mapped or converted data is readable by said at least a second node (12), and then transmitting the mapped or converted data to that of said at least a second node (12). In the similar context, the bridging module (8) provides a medium for data transmission between said at least a first node (11) and said at least a second node (12).

Once the data has been successfully transferred from said at least a first node (11) to said at least a second node (12), the bridging module (8) erases history of the data transmission for each session upon completion of the data transmission, such that the data transmission is performed in a secured manner, hence preventing malicious attacks and preventing

sensitive information from being leaked as the system is implemented for data transmission between at least an establishment and at least a financial institution.

Fundamentally, the operation of the system according to the present invention is targeted for data communication between various establishments and institutions, and that
5 information is seamlessly shared across the various establishments in a secured manner.

The data transmission in accordance with the present invention is initially generated from said at least a first node (11). Said at least a first node (11) transmits data to the bridging module (8) by the steps of first extracting data for transmission, encrypting the extracted
10 data, and transmitting the encrypted data. The data for transmission, which is information to be transmitted to said at least a second node (12), is extracted by an extraction module (101) and that the extracted data is encrypted by the encryption module (102). Said at least a first node (11) then transmits data to the bridging module (8) via the transmitter (104).

15 Subsequently, the encrypted data transmitted from said at least a first node (11) is received by the receiver (304) at the bridging module (8). The bridging module (8) then transmits data to said at least a second node (12) by the steps of decrypting the received data, mapping the decrypted data to a corresponding data, mapping or converting the decrypted data to the corresponding data, encrypting the mapped or converted data, and transmitting
20 the encrypted data to said at least a second node (12). The received data is decrypted to read and to analyze information that is transmitted from said at least a first node (11).

The decrypted data is then mapped via the processor (21) to a corresponding data, such that the corresponding data is the data fashioned in the format accustomed for data accessibility
25 and compatibility in the operating environment of said at least a second node (12). The mapped data is then mapped or converted by the processor (21) to the corresponding data for data conformity with the data format in the operating environment of said at least a second node (12). The mapped or converted data is encrypted by the encryption module (302) and the encrypted data is then transmitted to said at least a second node (12) via the
30 transmitter (303) for further processing by said at least a second node (12).

Then, the encrypted data transmitted from the bridging module is received by the receiver (205) at said at least a second node (12) for further processing. Said at least a second node

(12) receives and processes data by the steps of receiving encrypted data, decrypting the received data, validating the decrypted data, and processing the decrypted data. The received data is decrypted to analyze information transmitted from the bridging module (8).

- 5 The decrypted data is validated for accuracy and security, and then the decrypted data is processed by said at least a second node (12). Upon verification and whilst processing, said at least a second node (12) transmits an acknowledgement message to said at least a first node (11) via the same path in reverse, that is through the bridging module (8) to said at least a first node (11). The acknowledgement message is transmitted via the transmitter
- 10 (204) of said at least a second node (12) to the receiver (304) of the bridging module (8), and from the transmitter (303) of the bridging module (8) to the receiver (105) of said at least a first node (11). Said at least a second node (12) transmits a status update message to said at least a first node (11) in the same manner after processing of the validated data.
- 15 Referring to Figure 3, there is illustrated a schematic representation of the system architecture for data transmission according to the present invention, wherein the Figure 3 illustrates the system architecture comprising at least a first node (11) for receiving and transmitting data, at least a second node (12) for receiving and transmitting data, and a bridging module (8) that establishes communication between said at least a first node (11)
- 20 and said at least a second node (12).

Further, it is shown in Figure 3 that bridging module (8) comprises layers for data protection and security. The system according to a preferred embodiment in the present invention runs from physical servers in a virtual machine environment. Data protection and

25 security is governed on both an application layer and during data transfer layer, whereby the data is protected during transmission and during data mapping, and that data security is applied during data transmission and during data mapping, which shall be discussed in more detail as follows.

- 30 The first node (11) according to the preferred embodiment of the present invention, advises, implements and replaces ungoverned document transfer and storage methods with secure, reliable, and compliant information exchange processes that ensure data integrity for end-to-end process. These processes assist establishments, more particularly financial

institutions to move confidential data between locations in a secure, accurate, controlled, and documented manner that addresses the full range of current and evolving legislative and regulatory mandates.

- 5 A secure file transfer solution enables financial institutions to send data more securely with return receipts and extensive tracking and auditing capabilities to ensure compliance with the rules and regulations imposed by regulatory bodies. Security protocols that secure and increase the reliability of data transfer are preferably but not limited to Secure Sockets Layer (SSL) and Secure Shell (SSH). Both are specifically designed to encrypt file transfers
- 10 as well as the associated administrative network traffic. SSL and SSH enhance the security and reliability of file transfer by using encryption to protect against unauthorised viewing and modification of high-risk data during transmission across open networks.

Ultimately, the bridging module (8) comprises a risk management module to protect data

15 from attacks. Data protection and security is an important component of the risk management module, as it entails enterprise-wide planning, co-ordination of key resources and establishment of procedures to enable users to resume their critical services in the event of unplanned security breaches.

- 20 Data protection is vital while the data is being processed, in transit, and in storage. The preferred embodiment of the present invention implements the cryptography method for storing and transporting data in high bit encryption, such as 256-bit Advanced Encryption Standard (AES) SSL. Combining SSL and SSH security with preferably but not limited to Open pretty good privacy (OpenPGP) provides an additional level of protection for data at
- 25 rest. OpenPGP encrypts files in storage through the use of cryptographic key pairs that authenticate users and data.

Essentially, the data transmitted from said at least a first node (11) is encrypted through cryptographic key pairs. Recipients at the second node (12) are required to use a

30 corresponding private key in order to decrypt the file. The cryptographic key pairs authenticate users and data, and thereafter the system uses the corresponding key to decrypt the data.

In additional to that, advanced security measures is used including the use of preferably but not limited to Federal Information Processing Standards (FIPS) 140-2 validated encryption libraries to secure files in transit, using 256-bit AES encryption and (Security Hash Algorithm) SHA-1 libraries to secure files in storage, and using buffers to secure files when
5 processing them between transfer and storage encryption in order to prevent the exposure of large chunks of sensitive information in memory. To prevent even encrypted files from lingering on disk longer than absolutely necessary, files are overwritten with cryptographic-quality random data upon deletion. The ideal level of data erasure is preferably but not limited to National Institute of Standards and Technology (NIST) 800-88 compliant and
10 fulfils a critical (Payment Card Industry) PCI requirement.

An effective data transfer solution is to ensure end-to-end security, reliability, and auditability throughout the file transfer process, and provide management visibility over the process via integrated, application level security, compliance reporting, auditing, workflow
15 monitoring, and automation. The preferred embodiment of the present invention is able to provide these important features in a data transfer solution include the ability to:

1. Reduce the risk of providing access to financial data;
2. Simplify and automate file transfer processes to better understand, monitor, and
20 respond to changing requirements without compromising data confidentiality;
3. Protect file transfer communications through embedded security;
4. Provide robust data management, monitoring, and scheduling that includes tracking, auditing, and guaranteed delivery with non-repudiation.

25 The data transfer capability of the preferred embodiment of the present invention is to ensure the critical considerations, such confidentiality, integrity, availability and auditing are contributed to compliance.

Confidentiality ensures that information can only be consumed by authorized individuals
30 and only for approved uses. Confidentiality begins with authentication of login credentials and setting secure password policy in place, with features like expiring accounts and password management. Access control includes support for requiring 256-bit AES SSL encryption and Transport Layer Security (TLS) 1.1 or higher on all connections. This level

of access is mandatory for all nodes connecting into the network infrastructure. If the nodes connecting to the transfer platform are unable to connect at 256-bit SSL or SSH or higher, access should be denied in order to protect a potential data breach.

- 5 The integrity means ensures uncompromised delivery of all correct data with full SHA-512 support. Secure, encrypted data delivery is critical for ensuring business continuity. Secure hashing algorithms ensure that files have not been compromised during transport, and that the source and destination files are exact matches. A single change in a file or writing a file to a bad sector on a disk can corrupt a file and produce faulty workflow notifications and
10 business process events. Non-repudiation takes data security to the highest level currently available by adding digital certificate management to secure delivery and data encryption.

- Availability is achieved through load balancing and clustering architectures that support automatic failover and centralized configuration data storage for preventing data breach.
15 This also helps protect against anti-hammering and distributed denial of service attacks. Availability is also achieved by building checkpoint restart and robustness into the solution that can overcome hardware failures or interruptions in Internet connectivity.

- Auditing provides comprehensive logging and log viewing with tamper evident security to
20 guarantee the integrity of the log files. For technology, security, and other auditing purposes, all client/server interactions and administrative actions is logged. A full managed file transfer solution includes analyzing capabilities, and features native and custom reporting and event driven notifications and workflow to ensure financial institutions are aware of the networks, and that the financial instructions are prepared to respond in the
25 event of a compliance audit.

- Referring to Figure 4, there is illustrated a schematic representation of the system architecture for data transmission according to the present invention, wherein the Figure 4 illustrates the system architecture comprising at least a first node (11) for receiving and
30 transmitting data, and at least a second node (12) for receiving and transmitting data.

The preferred embodiment of the present inventions provides a solution to deliver secure and managed end-to-end file transfer, right from the first node (11) to the second node (12),

enabling the second node (12) to meet compliance objectives of regulatory bodies, yet having ready access to necessary data information.

File transfer solutions of the present invention provides preferably but not limited to 256-bit
5 AES encryption for transfers over SSL (FTPS, HTTP/S), SSH (SFTP, SCP2), and
(Electronic Data Interchange-Internet Intergration) EDIINT (AS1, AS2 and AS3) protocols,
providing secure solutions for financial institutions that require confidentiality when
transferring financial data over the Internet. The preferred embodiment of the present
invention also leverage preferably but not limited to OpenPGP file encryption, up to SHA-
10 512 integrity, to ensure uncompromised transfers and non-repudiation.

The preferred embodiment of the present invention provides secure, automated, and reliable
solutions track data access and security enforcement policies to enable a level of
compliance unrivaled by other file transfer methods. With the ability to create multiple
15 hosts, control user access down to the file level, and block attacking Internet Protocol
addresses in real time, administrators can help to ensure that confidential data is only
accessible by those with explicit permissions.

Software assurance encompasses development and implementation of methods and
20 processes for ensuring that software functions as intended while mitigating the risks of
vulnerabilities and malicious code that potentially pose threat. Recognizing that software
assurance is a vital defense in today's increasingly dynamic and complex threat
environment, the preferred embodiment of the present invention overcome vulnerabilities,
improve resistance to attack and protect the integrity of information.

25

The preferred embodiment of the present invention implements preferably but limited to the
Change-Driven Security Engineering Process introduced by Safe Assurance Forum for
Excellence in Code (SAFECode). A review of the security-related disciplines used by the
highly diverse SAFECode members reveals in Figure 5 that there are corresponding
30 security practices for each stage of the software development lifecycle that can improve
software security and integrity, and are applicable across diverse environments. The
examination of these practices reinforces the assertion that software assurance has be

addressed throughout the software development lifecycle to be effective and not treated as a one-time event or single box on a check list.

5 The practices used by the preferred embodiment of the present invention are as diverse as the SAFECode, spanning shrink-wrapped applications, database applications as well as operating systems and embedded systems.

10 In most organizations, the efforts to protect backend systems focus on Roles, Authorizations, Segregation of Duties, Encryption, Password Policies, Firewalls, Network Infrastructure and Patch Management.

Most establishments are neither aware that business security depends on secure code, nor there are efforts to write secure custom applications.

15 The risk introduced by insecure code is very high, and establishments that outsource development, may have an even higher risk. The preferred embodiment of the present invention is aware of this potential threat.

20 The preferred embodiment of the present invention is preferably developed but not limited to using Advance Business Application Programming (ABAP) programming language. ABAP is a proprietary business programming language that provides several integrated security mechanisms to protect the design and integrity of Enterprise Resource Planning (SAP) standard mechanisms.

25 Maximum security on data protection is achieved through the encrypted data imported said at least a second node (12) and must not be stored anywhere in the database when the data is being left idle. The encrypted data file will be decrypted during the process of application execution, which in turn means that the data will be protected from any unwanted access login to the system.

30

The ABAP runtime is a component in the Enterprise Resource Planning (SAP) Kernel that processes the ABAP byte code. If an ABAP module is called for which no byte code exists, the corresponding source code is first compiled into byte code and then the byte code is

executed. There is also an explicit command in ABAP that generates the corresponding byte code: GENERATE REPORT. In theory, all source code and all byte code executed by the ABAP runtime are preserved in the database.

- 5 Dynamic ABAP programming introduces commands that are not entirely compiled into byte code. Although most of the ABAP statement is turned into static byte code, some sections of the byte code are dynamically computed based on the contents of variables the statement processes. This concept is somewhat similar to Prepared Statements in SQL.
- 10 However, in ABAP the variable that is dynamically used can contain commands. The preferred system of the present invention utilizes ABAP commands that contain dynamic portions that are evaluated by the ABAP runtime each time a statement is executed. In this case, neither the entire source code nor the effectively executed byte code is preserved. As the result, ABAP commands can be executed in a more secured environment as and when
- 15 there is an input file preserved.

Referring to Figure 6, there is illustrated a schematic representation of the system architecture for data transmission according to the present invention, wherein the Figure 6 illustrates the system architecture comprising at least a first node (11) for receiving and transmitting data, at least a second node (12) for receiving and transmitting data, and a bridging module (8) that establishes communication between said at least a first node (11) and said at least a second node (12).

20

The preferred embodiment of the present invention is operated in a safe environment with strict security access. Only authorized personnel from an establishment or institution are allowed to hold the identification with the appropriate authorization to access. However, these authorized personnel are not able to retrieve any information on the data as long as the data file is encrypted. No data from the imported data file will be stored in bridging module (8). Data file will be decrypted at the application layer and purged after the output file is successfully encrypted and sent.

25

30

Referring to Figure 7, there is illustrated a graphical representation of the system architecture for data transmission between various establishments according to the present

invention, wherein the system for data transmission comprising a communication network for transferring data between a plurality of nodes via a bridging module (8), wherein Figure 3 shows that the plurality of nodes are at least a first node (11) and at least a second node (12) connected via the bridging module (8).

5

The system aims to provide a solution to efficiently establish automated host-to host connectivity with preferably but not limited to an ERP (Enterprise Resource Planning) system in the most cost efficient manner. In such a system, the implementation model envisages that the data transmission between a plurality of nodes, wherein the information in one of the nodes, for example, said at least a first node (11), provided in an ERP format is transmitted to the bridging module (8) for onward conversion and transmission to another node, for example, said at least a second node (12) for further processing.

10

The system and method of the present invention aims to provide a solution to financial institutions and companies with corporate banking connectivity and transaction-related applications. The focus is on reliable and highly secure connectivity. This is complemented by powerful applications that can monitor incoming and outgoing data in batch mode.

15

Further, corporate companies are able to connect to bank institutions, monitor all incoming and outgoing information for compliance, and reconcile information. Additionally, messages can be converted into various formats. All messages are archived and based on request, can be retrieved online for a specific period of time.

20

The present invention provides the services for the entire connectivity process and seamlessly integrates applications as well as ERP systems (i.e. SAP ERP). This will enable institutions and establishments the true experience of high level of automation (Straight through Processing STP). The objective of this system is to improve the end-to-end services for data transmission between various engaging establishments.

25

SFTP, or secure FTP, is a program that uses SSH to transfer files. Unlike standard FTP, it encrypts both commands and data, preventing passwords and sensitive information from being transmitted in the clear over the network. Secure Shell or SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices.

30

SFTP connection will be established between the institutions to facilitate to/from transmission of payment instruction files and the corresponding reports.

5 In as much as the present invention is subject to many variations, modifications and changes in detail, it is intended that all matter contained in the foregoing description or shown in the accompanying drawings shall be interpreted as illustrative and not in a limiting sense.

10

15

20

25

30

CLAIMS

1. A system for transferring data between a plurality of nodes through a bridging module
5 (8), wherein the system comprising:
 at least a first node (11) for receiving and transmitting data;
 at least a second node (12) for receiving and transmitting data; and
 the bridging module (8) establishes communication between said at least a first node
 (11) and said at least a second node (12) and regulates data transmitted to and received
10 from said at least a first node (11) and said at least a second node (12);
 wherein the bridging module (8) receives data from said at least a first node (11) in
 a format type incongruent with a required format in said at least a second node (12),
 maps the data into the required format such that the mapped data is readable by said at
 least a second node (12), and transmits the mapped data to that of said at least a second
15 node (12);
 wherein the data transmission is executed in a transient data transmission process.
2. A system according to claim 1, wherein said at least a first node (11) comprises any
one or in a combination of an extraction module (101) for extracting data therefrom, an
20 encryption module (102) for encrypting data, a decryption module (103) for decrypting
data, a transmitter (104) for transmitting data, a receiver (105) for receiving data.
3. A system according to claim 1, wherein said at least a second node (12) comprises any
one or in a combination of an extraction module (201) for extracting data therefrom, an
25 encryption module (202) for encrypting data, a decryption module (203) for decrypting
data, a transmitter (204) for transmitting data, a receiver (205) for receiving data.
4. A system according to claim 1 or 2, wherein the bridging module (8) comprises a
processor (21) for regulating the data transmission on per session basis.
- 30 5. A system according to claim 1, wherein the bridging module (8) regulates the data
transmitted for maintaining consistency of the data transmission from said at least a
first node (11) and said at least a second node (12).

6. A system according to claim 1, wherein the bridging module (8) comprises an encryption module (301) for encrypting data, a decryption module (302) for decrypting data, a transmitter (303) for transmitting data, a receiver (304) for receiving data, or in any combination thereof.
- 5 7. A system according to claim 1, wherein the data is protected during transmission.
8. A system according to claim 1, wherein the data is protected during data mapping.
- 10 9. A system according to claim 1, wherein data security is applied during transmission.
10. A system according to claim 1, wherein data security is applied during data mapping.
11. A system according to claim 1, wherein said at least a first node (11) transmits data by
15 the steps of:
 - extracting data for transmission;
 - encrypting the extracted data; and
 - transmitting the encrypted data.
- 20 12. A system according to claim 1, wherein the bridging module (8) transmits data by the steps of:
 - receiving encrypted data;
 - decrypting the data;
 - mapping the decrypted data to a corresponding data;
 - 25 encrypting the mapped data; and
 - transmitting the encrypted data.
13. A system according to claim 1, wherein said at least a second node (12) receives and processes data by the steps of:
30
 - receiving encrypted data;
 - decrypting the received data;
 - validating the decrypted data; and
 - processing the decrypted data.

14. A system according to claim 13, wherein said at least a second node (12) transmits an acknowledgement message to said at least a first node (11).
15. A system according to claim 13, wherein said at least a second node (12) transmits a status update message to said at least a first node (11).
16. A system according to claim 1, wherein the bridging module (8) comprises a risk management module to protect the data from attacks.
17. A system according to claim 1, wherein the data transmitted from said at least a first node (11) is encrypted through cryptographic key pairs.
18. A system according to claim 17, wherein the cryptographic key pairs authenticates users.
19. A system according to claim 1, wherein the system uses a corresponding key to decrypt the data.
20. A system according to claim 1, wherein the system comprises integrity means for delivering data.
21. A system according to claim 1, wherein the system is configured to prevent data breach.
22. A system according to claim 1, wherein the system operates in a virtual machine environment.