Enabling compliance with the PCI Data Security Standards
December 2007

Information Management software

Employing IBM Database Encryption Expert to meet encryption and access control requirements for the Payment Card Industry Data Security Standards (PCI DSS)

Introduction

In 2004, Visa USA, MasterCard International, American Express and Discover aligned their individual data protection programs to create the Payment Card Industry Data Security Standard (PCI DSS or PCI). This alignment in standards provided an industry-wide framework that complemented each brands' individual security policies—MasterCard's Site Data Protection program (SDP), Visa USA's Cardholder Information Security Program (CISP), American Express' Data Security Operating Policy (DSOP), and Discover's Information Security and Compliance (DISC).

In September 2006, the card brands aligned again to create the Payment Card Industry Security Standards Council (PCI-SSC). The purpose of the Council, as stated on their website, is "to enhance payment account data security by fostering broad adoption of the PCI Security Standards." The Council will have responsibility for the development and maintenance of the standard. The move will also provide the industry with one definitive voice on the compliance issues that are facing the companies obligated to comply. In conjunction with the debut of the PCI-SSC, a new version of the PCI Standard was released. This new iteration, called Version 1.1, provides a greater level of granularity on a number of requirements, specifically Requirement 3, which calls for the protection of stored cardholder data.

Compliance with the PCI has become an increasingly prominent concern for companies that process, store or transmit credit card data. While many companies have undertaken arduous and expensive compliance projects, adoption of pertinent technologies that enable compliance has been slow.

Many companies, during the course of their compliance projects, look to point solutions to address many of the requirements. This frequently results in using resources beyond the initial project scope to make the various solutions compatible. Encryption provides just such an example. While encryption is an industry best practice, it is only one small portion of the PCI requirements. Many encryption solutions enable compliance only with those requirements that directly pertain to encryption. In selecting a point solution to solve the encryption problem, the company leaves access controls, auditing and logging, and system configurations unaddressed and adds untold complexity to the compliance project.

IBM Database Encryption Expert is an essential tool for any company that must comply with the PCI DSS. Database Encryption Expert is a cost-effective and easy-to-manage solution for high-speed data encryption of data both online and offline (backups), audit and log files, application and host integrity, and policy-based user access control. It is easy to install, non-disruptive and transparent to existing applications, business operations and the IT infrastructure.

Database Encryption Expert and the PCI DSS v 1.1

The Payment Card Industry Data Security Standard is a multi-faceted approach to the protection of cardholder data. The Requirements provide a list of mandates designed to increase the overall level of security in the Payment Services Industry. The objective of these requirements is to prompt companies to enact measures that protect cardholder information. While all of the requirements are strict, there are four major categories of requirements. They are: auditing and logging, standard configurations (application and host integrity), access controls, and encryption.

1. Auditing and logging

There are a number of auditing and logging requirements within the PCI standard. These stringent requirements include:

10.2 Implement automated audit trails to reconstruct the following events, for all system components:

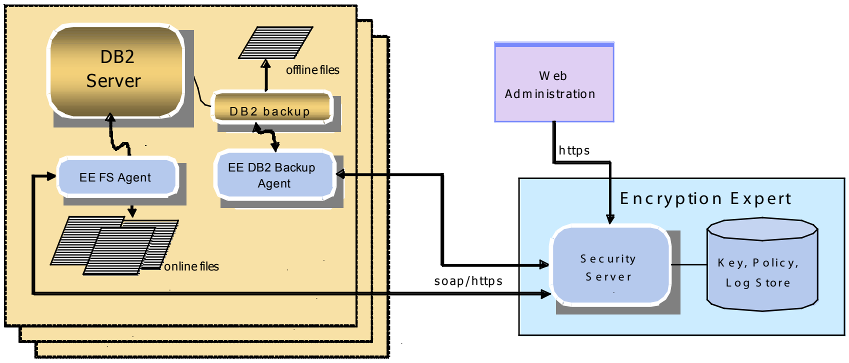
- *10.2.1 All individual user accesses to cardholder data*
- *10.2.2 All actions taken by any individual with root or administrative privileges*
- *10.2.3 Access to all audit trails*
- *10.2.4 Invalid logical access attempts*
- *10.2 5 Use of identification and authentication mechanisms*
- *10.2.6 Initialization of the audit logs*
- *0.2.7 Creation and deletion of system-level objects*

10.3 Record at least the following audit trail entries for each:

- *10.3.1 User identification*
- *10.3.2 Type of event*
- *10.3.3 Date and time*
- *10.3.4 Success or failure indication*
- *10.3.5 Origination of event*
- *10.3.6 Identity or name of affected data, system component, or resource*

Database Encryption Expert provides complete auditing capabilities by logging any attempted access to any file data by any user and associated application. The system not only can audit authorized access requests, but also all attempts to circumvent authorized access channels, notifying you of policy violations in real time. Database Encryption Expert records all context attributes of the request—who, what, where, when and how—enabling complete tracking of host intrusion and data access on the application and user level, and providing an extensive access log for detailed analysis. For example, the Database Encryption Expert log would include when the access occurred, who made the request, the application used to make the request, the host where the request occurred, and the file system operation requested. Database Encryption Expert combined with IBM Audit Management Expert provides a comprehensive PCI compliance solution.

The IBM Database Encryption Expert System



EE Agents

- Communicates with security server to enforce policy
- Encrypts data, controls access
- Sends audit events to server

Security Server

- Key and Policy Management
- Centralized Audit Logs
- High Availability (failover support)
- Authenticates agent communication

An additional requirement, Requirement 10.5, mandates the protection of the audit trail.

10.5 Secure audit trails so they cannot be altered, including the following:

- *10.5.1 Limit viewing of audit trails to those with a job-related need*
- *10.5.2 Protect audit trail files from unauthorized modifications*
- *10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter*

Database Encryption Expert limits access to audit logs or records to authorized individuals on a need-to-know basis. It controls root or administrator access to cardholder data in the same way the system restricts access to the data itself. Database Encryption Expert audit logs are protected from any type of unauthorized modifications, and they can also be integrated with a syslog server and SNMP applications.

Database Encryption Expert's rich auditing capability allows you to review the file IO activity of tests performed on your security systems. Because Database Encryption Expert logs *failed attempts*, you can track and analyze simulated security breach attempts to verify that your data is safe.

2. Data access controls

The use of data access controls allows companies to restrict access to sensitive information to only those that need the information in order to perform their job duties. This is essential protection against internal threats, as well as against threats originating from outside of the network. The PCI regulation has set forth a number of strict access control requirements. Specifically, Requirement 7 states that companies "restrict access to cardholder data by business need-to-know." Further requirements surrounding access controls include:

- *7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access*
- *7.2 Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed*

Database Encryption Expert adds a layer of access control on top of the file system's access control. Database Encryption Expert access control follows a least-privilege model, which means that any activity not expressly authorized will be denied, in accordance with Requirement 7.2. Database Encryption Expert's context-aware access control protects data by granting access only to authorized users performing authorized operations using the intended application during specified time windows. Using a five-factor system—based on who, what, where, when and how—Database Encryption Expert requires the context of each access attempt to be validated by the established data security policies. Any attempt at data access that is not authorized according to these well-defined pre-set policies will be blocked by Database Encryption Expert.

Database Encryption Expert's "separation of duties" feature further restricts access to data by allowing system administrators and root users to maintain the system and backup data, without being able to view the cardholder data. This provides the means to manage systems and process without granting administrators the ability to view protected sensitive data – like cardholder information. Even though your IT personnel may be highly trained and trusted professionals, relying on the honor system does not meet the PCI requirements. Database Encryption Expert enables you to comply with the PCI's data access restriction requirement, and truly restrict access on a need-to-know basis.

In cases when a root or system password is compromised, Database Encryption Expert prevents system administrators or other unauthorized users from decrypting protected files and viewing cardholder information. This feature is provided by Database Encryption Expert to enable system administrators to handle and back up sensitive files without being able to view that data. With regard to this particular rule, the feature protects cardholder data in case a default password is not changed by mistake, leaving the system open to an unauthorized user who has access to the vendor's default system password. With Database Encryption Expert, even in this worst case scenario, the unauthorized user would still not be able to read the cardholder data.

Database Encryption Expert's access control features further support compliance by integrating with your company's existing ID management system and leveraging those capabilities to determine whether access is authorized based on the unique ID and the data security policies.

3. System configurations

The requirements mandating standardized system configurations are often the most arduous with which to comply. Traditionally, these requirements have been met either by following the NIST guide on server hardening or by purchasing an expensive point solution. Requirement 2.2 directly addresses the system configuration issue:

2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards as defined, for example by SysAdmin Audit Network Security (SANS) National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).

- *2.2.1 Implement only one primary function per server (for example, web servers, database servers, and DNS should be implemented on separate servers)*
- *2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function).*
- *2.2.3 Configure system security parameters to prevent misuse.*
- *2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems (e.g., unnecessary web servers).*

Database Encryption Expert enables implementation and maintenance of secure systems and applications ensuring that only authorized applications can operate and access protected database files. Database Encryption Expert does this via the digital signing of application files to verify it is authentic and has not been altered in any way. Any application that is not recognized or has been modified would not be allowed to read sensitive data. This verifies that applications and resource files are trusted and authorized.

4. Encryption

The objective of the PCI regulation is to protect cardholder data. PCI DSS specifies that companies use encryption to protect cardholder data. Database Encryption Expert adheres to the PCI requirements and encrypts data using standard AES in 128-bit or 256-bit key lengths. Database Encryption Expert is the easiest way to encrypt cardholder data within databases, audit and debug logs, and back up archives. Database Encryption Expert inserts above the file system layer so it is transparent to users, applications and the database itself. No modification to the application or database is required. It adds very little performance overhead and is much faster than the column-level encryption approach. The PCI states, *"Encryption is a critical component of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person."* The requirement that directly relates to encryption is:

Requirement 3: Protects stored data

3.4 Render PAN (Primary Account Number) at a minimum unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches:

- *Strong one-way hash functions (hashed indexes)*
- *Truncation*
- *Index tokens and PADs, (PADs must be securely stored)*
- *Strong cryptography, with associated key management processes and procedures*

Database Encryption Expert protects online and offline data by encrypting the entire database and related files. Security policies govern which processes (applications) and/or system users can decrypt those files. Encrypting data is important, but it is even more important to control the decryption of data. The advantage of Database Encryption Expert is the combination of access control with encryption, ensuring that only an authorized user running an intended unmodified application can decrypt cardholder data and other sensitive information.

Effective encryption must be accompanied by secure key management procedures. Requirements 3.5 and 3.6 discuss the manner in which the cryptographic keys are to be managed. Database Encryption Expert enterprise key management was designed to follow the guidelines prescribed by the Federal Information Protection Standard (FIPS) 140-3.

3.5 Protect encryption keys against both disclosure and misuse.

- *3.5.1 Restrict access to keys to the fewest number of custodians necessary*
- *3.5.2 Store keys securely in the fewest possible locations and forms*

3.6 Fully document and implement all key management processes and procedures, including:

- *3.6.1 Generation of strong keys*
- *3.6.2 Secure key distribution*
- *3.6.3 Secure key storage*
- *3.6.4 Periodic changing of keys*
  - *As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically*
  - *At least annually*
- *3.6.5 Destruction of old keys*
- *3.6.6 Split knowledge and dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key)*
- *3.6.7 Prevention of unauthorized substitution of keys*
- *3.6.8 Replacement of known or suspected compromised keys*
- *3.6.9 Revocation of old or invalid keys (mainly for RSA keys)*

Database Encryption Expert provides further protection of stored data by managing secure distribution and storage of decryption keys. The Database Encryption Expert product includes a Security Server for key storage and management, and access to this server is limited to only authorized security administrators.detailed publish and subscribe architecture for the Data Integration Layer.

The PCI-SSC has rendered their opinion on Database Encryption Expert's key management processes and their impact on PCI compliance. According to the PCI-SSC, *"the controls outlined…appear consistent with the intent and objectives of the PCI and sufficiently robust to support compliance in cases where companies are unable to meet exact compliance with PCI 3.6.4 and/or 3.6.6." (For more information or to get the whole opinion for PCI-SSC please speak to an IBM sales representative.)*

The following table summarizes the PCI DSS rules and which of those Database Encryption Expert addresses (highlighted in blue).

1	Install and maintain a firewall
2	Do not use vendor-supplied defaults for passwords Develop configuration standards
3	**Protect stored data**
4	Encrypt transmission of cardholder data across public networks
5	Use and regularly update anti-virus software
6	**Develop** and maintain **secure systems** and **applications**
7	**Restrict access to data by business need-to-know**
8	Assign a unique ID to each person with computer access
9	Restrict physical access to cardholder data
10	**Track and monitor all access** to network resources and cardholder data
11	Systems should be tested to **ensure security is maintained over time and through changes**
12	Maintain an information security policy

Additional areas where Database Encryption Expert meets the PCI requirements

- *6.5.10 – Insecure configuration management*

Typically, the first target of an intruder is not sensitive data files, but the configuration files of the applications that manage the data. The configuration files may contain valuable information to locate the sensitive data, and if the configuration files can be modified, there are many more potential attacks possible. Database Encryption Expert provides an additional layer of access control on configuration files that could prevent even privileged users (root, system administrators) from reading or writing these files. Database Encryption Expert can also encrypt the DB2 configuration files and ensure that only the authorized application can open and process them.

- *8.4 Encrypt all passwords during transmission and storage on all system components*

Applications often need to read a password from a file in order to initiate. For example, when an application server first starts, it may need to log into a database. It is common for the application server to retrieve the database logon from a configuration file or have it hard coded in a startup-script. Database Encryption Expert can easily protect these files by encrypting the script of the configuration file that contains the password, and ensure that only the authenticated application running under the designated OS user can open and decrypt the file containing the password.

- *11.5…alert personnel to unauthorized modification of critical system or content files…*

Gaining additional advantages with Database Encryption Expert

Database Encryption Expert is able to address more of the PCI requirements than any other single product. Below is an outline of Database Encryption Expert's benefits:

Affordability: Database Encryption Expert is an economical option, costing much less than the other available solutions. The low cost of Database Encryption Expert is due in part to the fact that four essential capabilities – encryption, access control, host protection and auditing – are delivered within one tool.

Fast implementation: One of the many benefits to the Database Encryption Expert approach and architecture is that it does not require any changes to applications, the database or the network and storage infrastructures. This result is quick and easy implementations with minimal downtime – database has to be brought down when the tablespaces are encrypted.

Performance: Database Encryption Expert's data encryption process operates with limited performance impact to database operations. Traditional column-level encryption consumes significant overhead and requires changes to field properties and negatively affects index performance. Database Encryption Expert's minimal drag on performance makes the product ideal for protection of cardholder data.

Transparency: Database Encryption Expert's policy-based management and high degree of transparency to existing applications, business operations and IT infrastructure allow easy and economical deployment, management and scalability. In contrast to alternative data encryption solutions, Database Encryption Expert operates seamlessly with IBM databases and requires no changes to application software.

Conclusion: Database Encryption Expert enables PCI compliance

The PCI standards place substantial new data protection burdens on companies, but you can embrace this opportunity to examine the security of your data and install Database Encryption Expert to fill the gaps in your data protection efforts. Database Encryption Expert provides a single, affordable tool to meet many of the PCI requirements that are not already covered by the basic security applications you may have in place. By implementing this comprehensive solution, you can add encryption, access control, host protection and auditing to your data protection initiative, and achieve compliance with this critical industry standard.

For additional information please visit the Database Encryption Expert Product Page at **ibm.com**/software/data/db2imstools/database-encryption-expert/ or the DB2 and IMS™ tools website at **ibm.com**/software/data/db2imstools/.

IBM Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
12-07

Each IBM customer is responsible for ensuring its own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.

TAKE BACK CONTROL WITH Information Management