



Meeting the challenges of PCI and Visa CISP for credit card security

What are PCI and CISP security standards?

The Cardholder Information Security Program (CISP) is a set of rules established by Visa for securing your computer systems and data from unauthorized access and loss of credit card information. These rules have been in place for several years and were required of large credit card processors, but were only recommendations for most merchants accepting credit cards. The Payment Card Industry (PCI) data security standard is an industry-wide standard that incorporates many of the CISP standards and adds additional requirements. These are now generally referred to as the PCI data security standard or the PCI-CISP data security standard. Mastercard, American Express, Discover, and other card issuers use the new PCI standard as a part of their data security programs.

Who is subject to PCI-CISP rules?

There are slightly different rules for different credit card issuers. For Visa, any merchant processing over 500,000 transactions a year must comply with PCI-CISP rules. For Mastercard, any merchant accepting \$125,000 in transactions in a month must comply with PCI-CISP rules. Other card issuers have different rules. Almost all card issuers reserve the right to require any merchant to meet the rules, and any loss of data will certainly result in audit and rules requirements. You should consult with your bank or card processing vendor to determine if you must meet PCI-CISP rules.

Even if you don't meet the minimum requirements for PCI-CISP compliance, there are other good reasons to meet these rules. Complying with PCI-CISP will help in meeting other state and federal regulations for data security. These regulations include California Privacy Notification, Sarbanes-Oxley, HIPAA, Gramm Leach Bliley (GLBA), and others.

Where can I get information about PCI and CISP?

Each card issuer (Visa, Mastercard, etc.) can provide you with information about the PCI data security standard. In addition to the PCI standard you can get information on how to start planning for the implementation, who can help you with compliance audits, and initial self-audits. You can access the Visa web site at www.visa.com. Click on the link for Merchants, and then search on PCI or CISP. You will find a great deal of information on PCI and CISP in the public area for Merchants.

When do I need to be compliant with Visa PCI-CISP?

Merchants for whom Visa PCI-CISP rules are mandatory must be compliant by June 30, 2005. There may be slightly different due dates for Mastercard, American Express, and Discover. If you have not already started the process of becoming compliant, the deadline is very near. In order to meet the deadline it will be important to minimize the impact on your existing applications as much as possible. See the sections below for information about likely application impacts. Patrick Townsend & Associates can help you assess the best way to meet the data security requirements on your iSeries platform.

Do I need to pass a PCI-CISP audit?

Any merchant who processes more than 6 million transactions a year, or who is required by another card brand to submit to audit, or who has experienced a data loss, must pass a PCI-CISP audit by an independent assessor. Visa publishes a list of companies who can perform a PCI-CISP assessment of your compliance with the Visa rules. You can also access the list on our web site at:

http://www.patowndsend.com/Qualified_CISP_Assessor_List.pdf

I have credit card numbers in my iSeries database files. What do I need to do?

The first step is to become familiar with the PCI-CISP rules and guidelines. You can access these on the Visa web site, or your bank or processor can provide you with a copy of the rules. There is a self-assessment questionnaire that is very helpful in getting a first look at the requirements and where your company stands in the process.

After you understand the requirements for PCI-CISP security, you should develop a plan for encrypting credit card numbers and other sensitive data as soon as possible. This means identifying which database files or SQL tables contain credit card numbers, what logical views or SQL indexes use the credit card number, and what

applications create or access the credit card number. You may need to convert some numeric fields to character in order to avoid data access errors. You may need to remove logical views or indexes based on a credit card number, and develop an alternative method to access information. You will probably need to modify applications that insert credit card numbers into your database, and which access credit card numbers for interactive and batch processing. Be sure to have a good map of your applications with all impacted programs identified.

Once you have a development plan you will engage in a normal application development and testing process to support encrypting and decrypting credit card numbers as needed. This should incorporate your company's normal quality assurance process.

Our customer support applications do lookups by credit card number. How will these applications be impacted?

You will need to create an alternative method for locating records in your database. If you are currently looking up records by credit card number, consider accessing records by customer name and date range (from date, to date). Or, you may be able to access records by customer name and zip code. By eliminating the credit card number from the access logic you can create a much smaller set of records, and then decrypt and display the credit card number as needed.

The PCI-CISP rules allow you to store the last four digits of a card number in the clear. One method of locating a credit card number in your database is to store the last four digits in the clear, select a record set based on these last four digits, and then decrypt the credit card number for records of interest. This would be an alternative to using the name and date range.

Is there other information that I need to secure?

The PCI-CISP rules only require that you encrypt credit card numbers. However, they also specify rules related to CVV (card security) codes and other fields. These rules require that you not store card security codes in your database.

Looking beyond the requirements of PCI-CISP you should consider encrypting other fields in your database that relate to a cardholder's identity. This might include a zip code, home phone number, social security number, check number, birth place, birth date and other fields commonly used for identification and subject to identity theft. While PCI-CISP does not require that you secure these types of fields, you should consider securing them to insure the maximum privacy of customer information, and to reduce future legal liability.

What encryption methods are supported by PCI-CISP?

The PCI-CISP rules require that you use "strong encryption" and reference Triple DES and 256-bit AES encryption as examples. The term "strong encryption" is not defined and is therefore somewhat vague. There are several encryption algorithms that could be considered as "strong encryption." The inclusion of Triple DES and 256-bit AES is

probably not an accident – these encryption algorithms are the only ones accepted by the National Institute of Standards and Technology for federal use.

What is AES encryption and why is it important?

AES is the acronym for Advanced Encryption Standard. This is the encryption method adopted by the National Institute of Standards and Technology (www.nist.gov) after reviewing many encryption alternatives. It is now the federal standard for encryption (FIPS-197) and will replace Triple DES encryption in the near future. Although Triple DES is considered secure, you should avoid using it as it will soon be removed as a federal standard. Because AES is a federal standard it has been accepted by HIPAA and other agencies for use in securing sensitive information. Just as Visa is referencing AES for strong encryption, it is likely that further federal and state regulations will incorporate AES. By implementing on AES now you can meet future security requirements.

It is important to look beyond PCI-CISP. Federal and state regulations related to privacy notification and security practices also mandate the use of data encryption, and new regulations are being formulated now. By using AES as your encryption method you will probably avoid future re-work to meet these new regulations. By deploying AES encryption you will also help your corporate legal team mitigate future legal liability concerns. Basing your implementation on published federal standards is a smart decision.

Are there differences in AES key sizes?

Yes, AES encryption supports different key sizes including 128-bit and 256-bit keys. The Alliance products from Patrick Townsend & Associates implement the 256-bit key size for encryption to insure the strongest encryption level. In addition to providing stronger encryption, our performance tests showed very little difference in CPU utilization with the stronger algorithm. The Visa PCI-CISP recommendation is for 256-bit AES and Alliance will meet this recommendation perfectly.

Are there differences in how AES encryption is implemented?

Yes, AES supports two different modes of operation known as Stream mode and CTR, or counter, mode. Most AES encryption applications work in stream mode. That is, they accept one chunk of data and the key you specify, and return the encrypted data as a result. Many of these stream mode applications require that the data be padded to an 8 byte or 16 byte boundary. That is, if you have a 6 byte field you have to pad the field to 8 bytes in order to encrypt it. Stream mode encryption is commonly used in whole-file encryption or tape encryption where very large chunks of data are being processed. One aspect of stream mode operation is that if you encrypt the same data multiple times, you will get the same encrypted result. For this reason stream mode is not recommended for database field encryption where the same field in different records may have the same or similar values.

When you have small fields like credit card numbers in multiple records in a database file it is important to use a different approach to insure the strength of the encryption. By using AES CTR mode the data in each field you encrypt is secure even

if you have the same values in different records. AES CTR mode introduces additional key information on each encryption request. This means that the same credit card number in different fields will encrypt to a different value. Alliance database field encryption uses AES in CTR mode for the best possible data security.

Can I use encryption APIs in V5R3?

In V5R3 and i5OS IBM introduced new APIs that support Triple DES and AES encryption. These APIs are a starting point for developing a field level encryption strategy. You can think of these APIs as a set of tools and a starting point for creating a security strategy. If you use these APIs you should be aware of the following limitations:

- The IBM encryption APIs do not support any type of key management. You will need to construct key management routines and be prepared to defend your approach. Please see the PCI data security standards for information about key management.
- The 256-bit AES encryption routine only supports stream mode of operation, and not CTR mode. See the section above on differences in AES encryption. AES CTR mode is important for the best field-level security.
- The IBM encryption APIs do not use the iSeries cryptographic hardware support even if it is installed. There will be no performance advantage with hardware support.
- In addition to field level encryption programming, you may need to develop additional applications to encrypt for tape, spooled files, and cross-platform transfer.

For all of the reasons above you may want to deploy a solution that meets your immediate needs for PCI-CISP compliance, and other regulatory mandates.

Can I use SQL encryption on my iSeries platform?

The iSeries DB2 SQL interface does support the ENCRYPT key word and RC2 encryption when inserting or updating fields in SQL tables. However, there are several reasons why you might not want to use the SQL encryption support:

- Traditional RPG or Cobol applications will have to be converted to using SQL for all of your database access, or you will need to implement stored procedures or triggers – not a good security practice.
- The use of SQL will require expanding the size of encrypted fields based on options you select. This may require changes to all of your iSeries applications that use the database file or table.
- IBM iSeries SQL encryption does not use the 256-bit AES encryption, which is the federal standard and a recommendation from Visa.
- IBM iSeries SQL implementation does not have a solution for key management which is required for PCI-CISP compliance. You will need to create key management routines and be prepared to defend your implementation approach.

For all of these reasons you may wish to consider another approach to encrypting fields in your SQL applications. The Alliance field encryption routines will work fine

with iSeries SQL and provide a solution that will help you meet your security and key management needs.

Can I use other encryption algorithms such as RC2, RC4, or Twofish?

AES encryption is not the only encryption algorithm that provides strong encryption. There are other encryption algorithms that can be used to secure your data. However, AES encryption is the current federal standard, and likely to be the basis for future state and federal regulations. AES encryption is the only algorithm that has a federally supported certification process. When you consider all of the reasons you want to encrypt data (PCI-CISP compliance, Sarbanes-Oxley, California Privacy Notification, legal liability limitation, etc.) choosing an AES encryption solution that is standards-based is the right decision.

What is key management and why is it important?

Encryption requires the use of keys, or pass phrases, as a part of the encryption process. It is very important to secure the key from loss just as you would secure your iSeries password. You would want to avoid storing your pass phrase in source code, storing it in the clear in a database file, or giving access to the pass phrase to unauthorized users. For users new to system security and encryption the importance of key management is often overlooked.

You should be sure that your keys and pass phrases are stored in a secure manner, and that access to these keys is restricted to appropriate users. The storage mechanism should provide a means of avoiding the display of the key in application code, or in the clear in database files. The PCI-CISP rules make several recommendations on how keys should be stored. The Alliance AES/400 application from Patrick Townsend & Associates implements a secure key store mechanism.

Do I have to store my keys in hardware?

No, this is not a requirement of the PCI-CISP rules. You can store keys on disk. However, you should provide a mechanism for secure key storage (see above) and be prepared to describe and defend the mechanism you use.

What impact will encryption have on my existing applications and system resources?

It is almost certain that you will need to modify some applications that access the credit card number. Any application that adds a record to a database file or table will need to secure the data before the record is inserted. Any application that uses the credit card number for display on a report, transmission to the processor during settlement, or other use, will need to be modified to decrypt the data as needed.

All encryption routines require additional CPU resources to secure data. You should avoid a large number of decryption tasks in interactive applications. You should also avoid decrypting all records in a file in batch processes when the credit card number

is not required. These steps will minimize the impact on applications and system resources.

Can I use Triggers or Stored Procedures to secure credit card numbers?

It is not recommended that you use database triggers or stored procedures. A trigger will be activated when any application or utility is used to access the file. For example, if you use FTP to transfer a file to another platform, the trigger application will be activated to decrypt a field. This defeats the intent of the security and may result in very little additional security of your data.

In addition to the security concerns, triggers and stored procedures may be activated when encryption services are not needed resulting in overuse of system resources. Running a query on a secure database with triggers can be a very expensive process in terms of system resources!

If you do decide to use triggers or stored procedures for encryption and decryption tasks be sure to implement proper access controls. You should be sure that system utilities such as DFU, Query, Copy File (CPYF), FTP, and other utilities, do not expose sensitive data to unauthorized users.

What do I need to do about my Point of Sale systems?

Your POS systems should be reviewed in the same way as your iSeries applications for data security. While most POS systems do not store credit card numbers for more than a day, you should discuss this with your POS vendor.

If you transfer data from your POS system to your iSeries system on a daily basis you should review the transfer process to be sure it is secure. If you use a public network for the transfer, consider implementing secure VPN, SSL FTP, or other secure transfer mechanism to secure the data.

The Alliance AES/400 product contains Windows file encryption software that can be used for data security during transfer. If your POS system is using Windows for its operating system the Alliance software may be able to help you with this data security.

How can I secure my tape backups?

If you have properly secured sensitive data in your iSeries database files, you will probably feel secure about your existing backup routines. However, if you have sensitive data in your iSeries files that is not encrypted, you should deploy a backup encryption solution. This will be either a hardware device or software solution designed to secure backups to tape. Alliance AES/400 provides several encryption routines to help you secure your tapes as needed.

What part does California Privacy Notification play in PCI-CISP?

There is no direct relationship between PCI-CISP rules and the California Privacy Notification law (SB1386). The PCI-CISP rules are payment industry and Visa rules required of merchants using their system. You are obligated to follow these rules as a part of your merchant agreement. The California Privacy Notification law affects any merchant selling products in California. If sensitive information, such as credit card numbers, is lost or may have been lost, it requires that you notify anyone who may be affected. There is quite a broad definition of what it means to lose sensitive information, and most companies will begin the notification process on any suspicion that private information may have been compromised.

The California law has a "safe harbor" exception that lets companies avoid notification requirements. If you encrypt the sensitive information you are excused from these requirements. The California law does not specify which encryption algorithm to use. However, if you use an encryption algorithm that is not a standard, you might reasonably expect less protection from legal liability.

The California law is a template for the regulations being created in several other states. It is also probably the basis for eventual federal law.

What part does Sarbanes-Oxley and Gramm Leach Bliley play in PCI-CISP?

There is no direct relationship between Sarbanes-Oxley and GLBA, and PCI-CISP. However, there are many IT security requirements in the Sarbanes-Oxley Act. You can be sure that securing all sensitive information in your iSeries database files will fall under the purview of a SOX audit.

What experience does Patrick Townsend & Associates have with PCI-CISP?

The company has over 10 years of experience with credit card authorization systems and sells a software solution for credit card authorization (Alliance AuthExpress). The solution has been certified by Visa, Vital, and First Data. Data security is an integral part of this solution and the company has been helping its customers meet CISP requirements from the beginning. Alliance AuthExpress customers also use encryption APIs to secure sensitive data in their own files.

No other company provides more experience with credit card solutions or a more secure solution for iSeries customers.

I am an IBM iSeries software vendor. How can I secure information in our applications?

Patrick Townsend & Associates has a special Alliance Partners program for ISVs. This program provides you with implementation support, development assistance, special pricing, and product distribution. You can request information on our ISV programs on our web site at <http://www.patowndsend.com/Partners.htm>

How can I get started?

You can contact Patrick Townsend & Associates for an initial consultation at the following locations:

Web: www.patowndsend.com
Phone: (800) 357-1019
(360) 357-8971
International: +1 360 357 8971
Email Info@patowndsend.com

A fully functional free trial is available for all Alliance products. You can evaluate Alliance capabilities on your own systems.