Payments Card Industry Data Security Standards (PCI DSS)

and

Spazio Managed File Transfer – Secure (MFT/S)

Primeur UK Ltd
32 Sackville Street
Royalty House
London W1S 3EA
United Kingdom
☎ +44 (0)20 3239 7456
🖷 +44 (0) 20 7432 6051

Primeur Group
Corso Paganini 3
16125 Genova
Italy
☎ +39 010 27811
🖷 +39 010 868 4913

www.primeur.com

April 2010

Table of Contents

1. Purpose

This White Paper reviews the Payment Card Industry (PCI) Data Security Standard from the perspective of Primeur's Spazio Managed File Transfer-Secure (MFT/S) suite.

Payment cards of various types (credit, debit, charge, stored-value etc) are increasingly used throughout the world and therefore are of interest to criminals. And the PCI DSS standards aim to combat that. Any business that handles payment card data must comply with the PCI standards.

Apart from having to comply with PCI, research suggests that adopting 'best practice' security makes good business sense....

> ***31% of customers affected by a data breach will terminate their relationship with the company*** *(and those are just the ones who are affected—not to mention potential customers that will avoid doing business with that company due to the perceived risk****). Statistically, 65% of the cost of any payment data breach is lost business—not fines or administration costs.***
>
> (Source ... Ponemon Institute)

Primeur are specialists in application data transfer (for the most part, file transfer and messaging) and our reputation rests on providing software and systems for the reliable, secure transfer of data complying with current industry standards and practices.

Enterprises handling payments made by cards are typically environments with a heterogeneous range of servers, networks and applications that need to intercommunicate and share data. Primeur's Spazio MFT/S can be a key component in a shared infrastructure service to provide this capability. In fact, industry analysts such as Gartner rate Spazio MFT/S as a leading product in delivering this.

This paper therefore is aimed at anyone with an interest in key IT infrastructure components that support business applications related to the processing of payment card data. And it outlines how Primeur can help with addressing the technology aspects of PCI compliance.

This paper does *not* deal with the formal compliance processes that may require one or more of a Qualified Security Assessor (QSA), an Approved Scanning Vendor (ASV) or a Self-Assessment Questionnaire (SAQ). More information on the formal processes and also up-to-date information about PCI can be found on the PCI Security Standards Council (PCI SCC) web pages:

https://www.pcisecuritystandards.org/index.shtml

2. Brief overview of PCI Standards

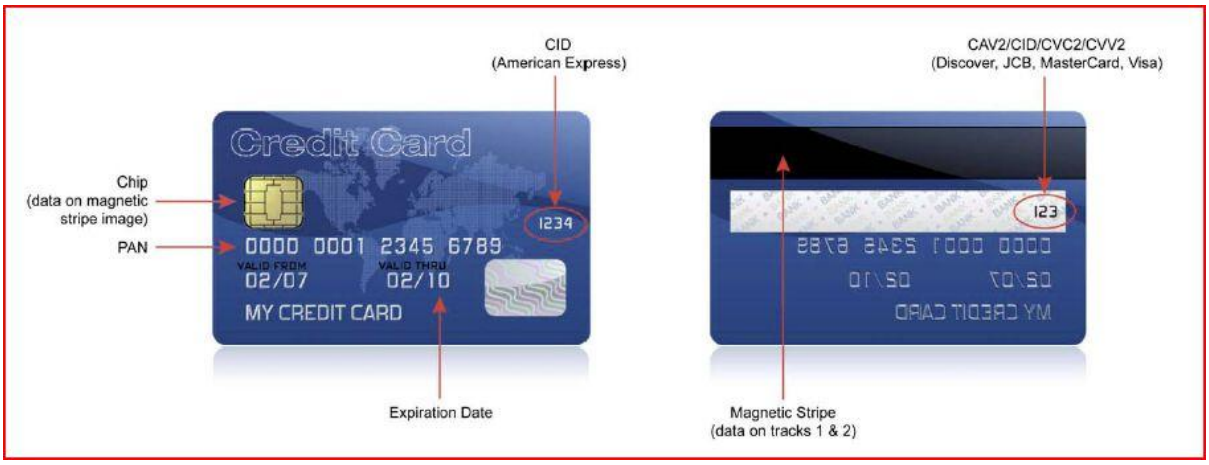
The Payment Card Industry (PCI) standards have been developed to create a secure framework for card payments systems. PCI aims to harness best practice processes and technologies to combat criminal attempts to access payment card information with the aim of defrauding merchants and/or their customers.

PCI Security Standards Council (PCI SSC) was set-up in 2006 and owns and develops the standards and raises awareness of them. The PCI SSC is jointly-owned by the world's major card brands.

There are 3 PCI standards. All 3 of the standards have the same goal: ***protecting cardholder data***

Cardholder data is the sensitive data that in the wrong hands could be used for criminal purposes to defraud cardholders and merchants.

The picture below shows the types of sensitive data and where it may be stored on a payment card



(Source: PCI SSC)

The three standards are:

2.1 PCI Data Security Standard (PCI DSS)

This is the core standard and covers security technology and controls for protecting cardholder data.

This white paper concentrates on PCI DSS.

2.2 Payment Application Data Security Standard (PA DSS)

This standard is for software developers who sell applications for accepting and processing payment cards. The card payment schemes require merchants and processors to use approved software that complies with the standard.

2.3 PIN Entry Device Security Requirements (PED)

These are for the manufacturers of point-of-sale (POS) devices for payment cards.

3. PCI Data Security Standard (PCI –DSS) - summary

This is the standard that covers what is required for the technical and operational aspects of the components of any system that is in some way connected to cardholder data.

PCI DSS comprises 6 overall PCI goals. Each goal is broken down into 2 or 3 specific PCI DSS requirements, numbering 12 in total (sometimes referred to as the 'digital dozen').

The goal and requirements are summarised in the following table.

PCI Goal	PCI DSS Requirements	White Paper Paragraph
Build and maintain a secure IT network	1. Install and maintain a firewall configuration to protect cardholder data	4.1.1
	2. Do not use vendor-supplied defaults for system passwords and other security parameters	4.1.2
Protect cardholder data	3. Protect stored cardholder data	4.2.1
	4. Encrypt transmission of cardholder data across open, public networks	4.2.1
Maintain a vulnerability management program	5. Use and regularly update anti-virus software on all systems commonly affected by malware	4.3.1
	6. Develop and maintain secure systems and applications	4.3.2
Implement strong access control measures	7. Restrict access to cardholder data by business need-to-know	4.4.1
	8. Assign a unique ID to each person with computer access	4.4.2
	9. Restrict physical access to cardholder data	4.4.3
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data	4.5.1
	11. Regularly test security systems and processes	4.5.2
Maintain an information security policy	12. Maintain a policy that addresses information security	4.6.1

4. PCI Data Security Standard (PCI –DSS) in detail

The rest of this paper looks in more detail at each of the 12 requirements and highlights where Primeur's Spazio MFT/S suite can help to deliver the PCI requirements within an IT infrastructure environment where cardholder data is processed.

4.1 Build and maintain a secure IT network

4.1.1 Install and maintain a firewall configuration to protect cardholder data

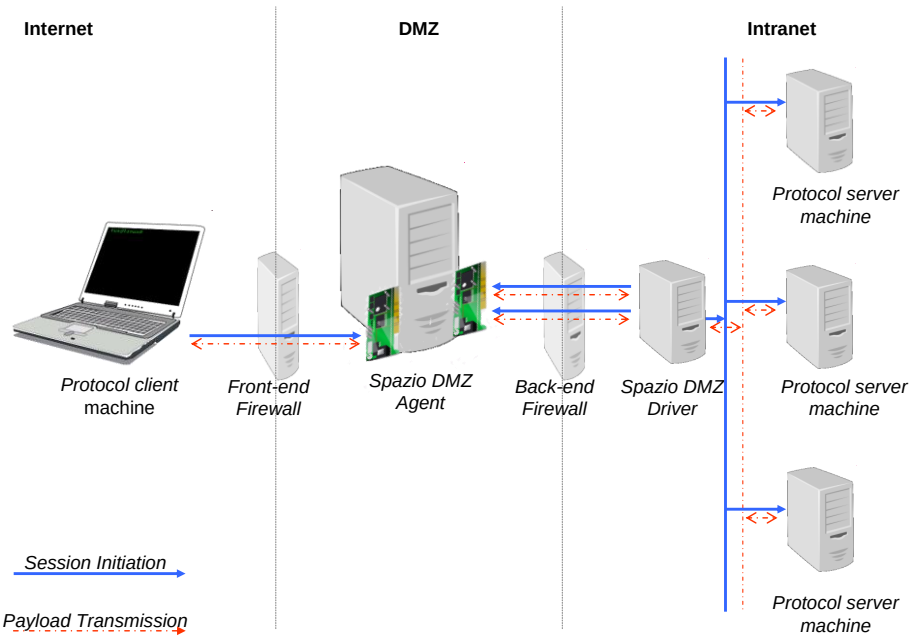
PCI *requires* use of firewalls, not only as a boundary for obvious 'un-trusted' networks such as the public Internet but in some cases, also to isolate payment card data from an organisation's other internal networks. An example might be an internal perimeter firewall between the internal network handling payment card data and any internal corporate wireless networks.

All firewall configurations must:

- have up-to-date documentation
- be subject to strict configuration control
- be regularly tested

And all of this should be reviewed a minimum of every 6 months.

Spazio MFT/S supports all firewall configurations. In addition, Spazio MFT/S can be configured with a DMZ gateway, which will act as a firewall DMZ proxy, as illustrated in the diagram below.



The firewall proxy means that parties beyond the external firewall can only ever initiate sessions with the proxy, which is situated in the DMZ (between the Enterprise's internal firewall layer and external firewall layer). Furthermore, data is never stored in the DMZ; it is always transient.

Spazio MFT/S supports a wide range of data transfer protocols. Primeur product documentation details the wide range of configuration possibilities and recommends secure practices and highlights those configuration options which may be a security concern.

4.1.2 Do not use vendor-supplied defaults for system passwords and other security parameters

It is common for both software and hardware to have initial default passwords such as 'admin' or 'password' or even nothing at all. For popular products, these default values are well-known or easily found via an Internet search.

Primeur's Spazio MFT/S does **not** install with a default user or password. The 'owning userid' for the Managed File Transfer (MFT) service is entirely a matter of choice for the system administrator. So, the userid and password can be set to any values that conform to local installation requirements. In addition, the userid can be assigned within whatever group is appropriate for the local security policies.

Industry best practice is to restrict access to the administrative user for any software that manages a shared service such as MFT. So, although you can choose any userid/password values that you want, we recommend that the administration of the product is strictly controlled.

The latest version of Spazio MFT/S has introduced A3SP, which addresses:

- **Authorization** - establishing a user identity and group ownership (who you are)
- **Authentication** - access permissions (what you can do)
- **Auditing** - real-time monitoring of all events for compliance (what you have been doing)

This provides a further level of control and is discussed in more detail below in section 4.4.2.

4.2 Protect cardholder data

4.2.1 Protect stored cardholder data

The storage of any cardholder data must be kept to a minimum. So there must be a *clear policy* that specifies retention periods and safe disposal of any cardholder data.

Sensitive authentication data should NEVER be stored (see appendix 2 for a description of authentication data).

Other data can be stored, such as the cardholder's name, the primary account number (PAN), and the expiration date, **where required for business processing**. However, at a minimum the PAN must always be rendered unreadable wherever it is stored. The means to achieve this can be include:

- Strong one-way hash functions. These result in 'index data' that point to a database record that contains the PAN.
- Truncation. This deletes the majority of the PAN leaving only the last 4 digits.
- Strong cryptography. This provides the technology to make data extremely resilient to unauthorised access (provided that keys are not vulnerable to exposure).

All of this can be implemented using features within Spazio MFT/S.

Included in the product is Data Secure for Spazio (DSSP) which is designed for securing data in transit and is built on the Data Secure Toolkit (DSTK). DSSP has a powerful set of tools and offers support for strong cryptography requirements well beyond those asked for by PCI DSS, including:

- Symmetric encryption: **AES up to 256**, DES, 3DES, RC4
- Asymmetric encryption: **RSA up to 4096 bit**
- Hashing algorithms: SHA-1, **SHA-2**, MD5

Primeur are committed to developing our products to keep them up-to-date with current standards.

Where encrypting data at rest in a file system is required, a further extension of DSTK called Data Secure File Sec (DSFS) can be used. With both DSSP and DSFS, cryptographic keys can be **securely stored** in a Hardware Security Module (HSM).

DSSP and DSFS complement each other and provide a complete end-to-end solution.

The support for storage of keys in hardware is built around PKCS #11 (Cryptographic Token Interface Standard). So any device conforming to this standard should operate with Spazio MFT/S, although we do publish a list of devices that have been successfully tested.

4.2.2 Encrypt transmission of cardholder data across open, public networks

As stated above, DSSP can be used to the secure data in transit between 2 application end-points i.e. application to application.

A wide range of protocols are supported and these will enable PCI compliance. Data transfers can be secured using:

- **SSLv3/TLSv1** supporting **HTTP/S** and **FTP/S**
- **SSHv2** supporting **SFTP** and with the *added capability* of X509 certificates and storage of keys in hardware (Smartcards or HSM)

Web browser file uploads and downloads implemented using HTTP/S can have *server AND client authentication*, if required, again with the possibility of storing sensitive keys in hardware.

In addition to FTP/S or SFTP, file transfers can also be implemented between multiple Spazio MFT/S servers using Spazio's own protocol that implements a SSL security model.

A selection of adapters is available, allowing seamless interoperation with a number of popular proprietary file transfer products from other vendors, using the appropriate security support (SSL for example) available in those products.

4.3 Maintain a vulnerability management program

4.3.1 Use and regularly update anti-virus software on all systems commonly affected by malware

Spazio MFT/S has the capability of invoking virus-checking, malicious software checking or indeed any other programs or scripts, automatically, at various points in file transfer operations.

For example, on an inbound transfer of a file from an external party, it is possible to invoke virus-checking on a file as it is received by Spazio MFT/S but before it is stored on a local file system.

Of course, additional procedures must always to be implemented to ensure that the anti-virus software and any associated 'virus database' is kept up-to-date.

4.3.2 Develop and maintain secure systems and applications

This requirement is concerned with such things as:

- Timely maintenance of software, in particular with security patches
- Testing and 'best practice' change control for software maintenance (this would include appropriate backup/back-out plans around system changes)
- Complete separation of development/test and production environments
- Secure storage of any cryptographic components (software and keys)

These requirements can be met by adopting good 'industry best practice' IT infrastructure processes. For example, in a robust change management system that meets PCI compliance requirements, we would expect to see:

- Changes categorized by type and priority (normal, standard, emergency)
- A method for impact of change analysis
- A change authorization process (strongly link to 'type' and 'priority' mentioned above)
- A means to fully document the implementation process (and the back-out/remediation process if required)
- A post-implementation review process

Primeur has a policy of continuous product improvement. Plans and timetables for new products or new functionality are shared in a timely way allowing customers to plan for software upgrades.

Alongside this, Primeur also issue software patches in response to specific defects that have been identified. And these are prioritised and distributed in-line with best practice in the software industry.

4.4 Implement strong access control measures

4.4.1 Restrict access to cardholder data by business need-to-know

This requirement establishes the need for rigorous 'access control'. There is complete flexibility with the Spazio MFT/S suite to create as many userids are required to both administer the system and access files within MFT/S.

Userids with administrative access must be strictly controlled and the use and ownership should be reviewed regularly (at least annually).

Also it is possible to create userids that are only able to access *specific* files within the MFT environment, whilst being unable to access other files. This will allow restricting access to sensitive files.

If further security of files is required simply within the file system, then Data Secure File Sec (DSFS) can be used to encrypt files. Further granularity of security of encrypting data at the field level within records is possible using the Data Secure Tool Kit (DSTK), although this would require application development.

4.4.2 Assign a unique ID to each person with computer access

The ability of Spazio MFT/S to support as many userids as are required, mentioned above, fulfils this requirement. Each individual in your enterprise can use a unique userid (with appropriate levels of authority) for access to the MFT/S server. And the activities of each userid are tracked in the logs associated with the product.

We normally recommend use of an external service such LDAP or Windows Active Directory for the management of user credentials. Spazio MFT/S implements A3SP to provide **Authentication, Authorization** and **Auditing (AAA)**. A3SP can be configured to fulfil the other PCI requirements related to user passwords i.e.

- Enforcing a mix of characters, numbers and special characters
- Minimum length
- Previous values of the password cannot be re-used
- Passwords must be changed at regular intervals e.g. every 90 days
- Strong 2-factor authentication (using certificates, one-time passwords and hardware devices, as required)

Primeur's A3SP has been designed to be integrated into other AAA frameworks and services, e.g. RADIUS, RACF.

4.4.3 Restrict physical access to cardholder data

This requirement is concerned with the physical access to cardholder data or systems that have cardholder data in them.

It covers such things as:

- Monitoring and logging access to buildings e.g. data centres
- Distribution, movement and destruction of media

4.5 Regularly monitor and test networks

4.5.1 Track and monitor all access to network resources and cardholder data

The Spazio MFT/S suite provides comprehensive logging of all aspects of both access to the MFT/S environment and also the transmission of files between endpoints under the control of MFT/S. This includes

- Entries identified by type of activity (e.g. HTTP/S, FTP/S, etc.)
- The userid and the files involved in the case of a file transfer
- The date and time that the event took place (in common with other application software, the accuracy of the date and time is dependent on the underlying operating maintaining the correct date and time)

4.5.2 Regularly test security systems and processes

Primeur development laboratories follow best software industry practice for software design, development and testing to ensure that products are robust and reliable when they are supplied to customers. The whole process is ISO 9001 compliant. However, each

enterprise will still need to able to demonstrate that they have thoroughly tested their own end-to-end business processes.

In the secure environment required for processing payment card data particular attention should be paid to tracking and monitoring all access to network resources and cardholder data. And there should be regular testing of important operational processes for functions such as:

- Key and certificate renewals
- Response to suspected or confirmed security breaches

4.6 Maintain an information security policy

4.6.1 Maintain a policy that addresses information security

Organisations handling payment card data are required to have a formal comprehensive information security policy that is applicable to all employees or other agents (contractors, suppliers etc). The policy should be reviewed regularly (at least annually) and should cover such things as:

- Usage of technologies (mobile devices, removable media, email, remote access)
- General Information Security responsibilities e.g. Data Protection Act
- Specific responsibilities for individuals or teams e.g. key management
- Security incident response/escalation procedures
- Ongoing Information Security awareness/Education

As a software and services specialist in Information Security, Primeur can help with detailed advice on many aspects of 'best practices' for a local Information security policy, in particular, of course, with respect to administering Spazio MFT/S in a PCI-DSS compliant environment.

Appendix 1 - Payment Card Processes Simplified

There are four steps to processing a payment card transaction:

(Illustration courtesy of Royal Bank of Scotland)

1. **Collect payment data**. Payment details are entered into the payment device or system. This could be:
    - entered by a call centre operator
    - read by a card-reader which may be a 'point of sale' (POS) terminal
    - entered directly into an secure (HTTP/S) internet page

2. **Authentication Details** of the purchase. The details from the card and the PIN are sent through to the 'Acquirer' (this is the bank that the merchant is using to accept card transactions). The Acquirer identifies the relevant card scheme (Visa, MasterCard etc.) and sends the details via the card scheme's network to the bank or other institution that issued the card (the 'Issuer'). If the details cannot be verified, the payment is declined.

3. **Authorisation**. The issuing bank (the 'issuer') checks the cardholder's identity, that the account has sufficient funds and that the card hasn't been reported lost or stolen. If everything is OK, the issuing bank authorises the amount requested and reserves those funds.

4. **Clearing and Settlement**. The transaction 'acquirer' and card 'issuer' exchange information about the purchases via card scheme's network (Visa, MasterCard etc). Typically, this is a batch process handling bulked-up transactions and involving file transfer. The merchant's

bank account will be credited for the cardholder's purchase and the cardholder is billed for the purchase.

In addition to the card payment transaction process, there are several other processes associated with payment cards. These include:

- Card issuing. A customer will join a payment card scheme and be issued with a card. Essentially the card data is critical (and subject to PCI controls) as soon as the card is created i.e. possibly before it is associated with a customer

- Lost/Stolen/Cancelled cards. Card issuers distribute details of cards that should no longer be accepted for payment, that have not reached their published expiry date.

Appendix 2 - Authentication data

The **Card Security Code** (**CSC**), sometimes also called:

- Card Verification Value (CVV or CV2)
- Card Verification Value Code (CVVC)
- Card Verification Code (CVC)
- Verification Code (V-Code or V Code)
- Card Code Verification (CCV)

It is a security feature for credit or debit card transactions, giving increased protection against credit card fraud

They can be broken down as follows:

- The first code, called CVC1 or CVV1, is encoded on the magnetic stripe of the card and used for transactions in person
- The second code, and the most cited, is CVV2 or CVC2. This **CSC** (also known as a **CCID** or Credit Card ID) is often asked for by merchants for them to secure "card not present" transactions occurring typically over the Internet, or via the phone. In many countries in Western Europe, due to increased attempts at card fraud, it is now mandatory to provide this code when the cardholder is not present in person.
- Contactless card and chip cards may supply their own codes generated electronically, such as CVV or Dynamic CVV.