PCI… DSS and SSC – what are these?

What does PCI DSS mean?

PCI DSS is the English acronym for Payment Card Industry Data Security Standard.

What is the PCI DSS programme?

The bank card data, which are the account number of the card, the expiry date and the three digits on the signature pannel on the back of the card, are sensitive because they allow a payment to be made over the Internet without the physical presence of the card. Fraudsters seek to capture these numbers by attacking the information systems of entities who store these data. The PCI DSS programme aims to improve the physical and logical security of information systems by asking players to comply to security requirements.

What is the PCI DSS standard?

The PCI DSS standard lists a set of points to be checked relative to information systems that capture, transport, store and process bank card data. The points to be checked are relative to IT techniques and also to procedures and organisational checks on these systems.

The PCI DSS standard and many other associated standards are available on the PCI Security Standards Council site (PCI SSC, see below) at https://www.pcisecuritystandards.org/security_standards/documents.php

What is compliance with PCI DSS?

Compliance with PCI DSS verifies that the points to be checked are properly implemented and that they are effective for protecting bank card data. This compliance is assessed according to the volume of transactions of the merchant (see "level" of merchant) by an audit carried out by an approved auditor or by a self-assessment questionnaire to be completed by the merchant concerned and provided to the acquiring bank. This compliance must be checked annually as well as through technical tests validating the proper protection of the e commerce web site.

Who is the PCI DSS addressed to?

PCI DSS is addressed to all entities that capture, transport, store and/or process bank card data. Card present/face to face merchants, e- commerces, transport networks, call centres, banks and card issuers are among the entities concerned by PCI DSS.

Does PCI DSS apply to me?

The PCI DSS programme applies to any player who stores, processes or transmits bank card data. The number of items of card data processed is of little importance, even though the risk is proportional to the volume of payment transactions processed.
Players who manually process and store paper media containing bank card data are also concerned (paper receipts, order stubs, and data received by fax or e-mail).

A -The roles of Payment Schemes and of PCI SSC

What is the PCI Security Standards Council (PCI SSC)?

The PCI SSC is an global organisation whose role is to define PCI standards and manage their life cycle on behalf of the community of players concerned, networks, banks and merchants. The PCI SSC also maintains a list of companies approved for performing compliance checks and analyses of the vulnerability of information systems. Lastly, the PCI SSC provides training courses (ISA, Internal Security Assessor), qualifies security auditors (QSA, Qualified Security Assessor) who are authorised to carry out upon-site audits, and approves suppliers of security solutions for carrying out vulnerability scans (ASV, Approved Scanning Vendor).

The presentation of the PCI SSC and the associated standards are available on the PCI SSC web site at **https://www.pcisecuritystandards.org**

What is the connection between PCI DSS and MasterCard's SDP programme and Visa's AIS programme?

MasterCard's Security Data Protection programme and Visa's Account Information Security programme are contractual rules established between these Schemes and their members (banks and payment institutions), which define the level of compliance with regard to standards defined by the PCI SSC. For example, it is not the PCI SSC that sets up mandates, schedules or applies any penalties, but each Scheme according to its own rules.

B – How can compliance with PCI DSS be validated?

Must all merchants be compliant with PCI DSS?

Yes, all merchants eventually will have to be compliant with PCI DSS

What does the classification by levels 1 to 4 mean?

Whether a merchant accepts a few payments by card per year or several million, they may be classified in one of the following four levels defined by the global Schemes:

Level	Volume of activity	Actions required for compliance
1	Any merchant processing more than 6 million Visa or MasterCard transactions per year, Any merchant that has suffered a compromise	On-site security audit (or SAQ for Visa Europe) Quarterly vulnerability scan (if online commerce)
2	Any merchant processing between 1 and 6 million Visa or MasterCard transactions per year	Annual self-assessment questionnaire Quarterly vulnerability scan (if online commerce)
3	Any merchant processing between 20,000 and 1 million Visa or MasterCard transactions per year	Annual self-assessment questionnaire Quarterly vulnerability scan (if online commerce)
4	Any merchant processing less than 20,000 Visa or MasterCard on-line commerce transactions per year. All other merchants processing up to 1 million Visa or MasterCard transactions per year	Annual self-assessment questionnaire Quarterly vulnerability scan recommended (if online commerce) (this depends if the data is captured, stored or transmitted by the merchant's infrastructure or by a service provider)

If a compromise occurs at a merchant or one of its service providers, the merchant is automatically reclassified to level 1 for 12 months after having validated their compliance.

Similar tables giving the specifics of each scheme may be consulted on the sites of **Visa** and **MasterCard**.

What are the self-assessment questionnaires?

A merchant of levels 2 to 4 must complete a self-assessment questionnaire appropriate to their activity. The Self Assessment Questionnaires (SAQ) are documents containing a series of questions that the merchant must answer. The model formats of these questionnaires are maintained by the PCI SSC and are available on its web site.
The merchant must complete two documents, the self-assessment questionnaire and the statement of compliance by which they certify that the replies to the questionnaire are true and that they have implemented all of the measures of PCI DSS to protect payment card data that they process.

What process must the self-assessment questionnaire follow?

Once the questionnaire and the statement of compliance has been completed and signed by the merchant concerned, it must be returned to the payment acquiring institution with which the merchant has a contract for the acceptance of payment cards.

How can I choose the self-assessment questionnaire for my field of activity?

There are five different types of questionnaire according to the merchant's activity:

Questionnaire A: applies to an activity where the card is not present (electronic commerce or orders by telephone or e-mail) or when all of the functions related to bank card data are outsourced.

Questionnaire B: applies to an activity where only a print of the card is taken without electronic data storage or for an independent terminal which does not store data.

Questionnaire C-VT: applies to an activity that uses virtual terminals based on a website without electronic storage of data.

Questionnaire C: applies to an activity that uses a payment application connected to the Internet without electronic storage of data.

Questionnaire D: applies to all the other activities not described in types A to C above and all service providers defined by an international network eligible to complete a self-assessment questionnaire.

Are all the requirements of the PCI DSS standard mandatory?

All of the requirements of the 12 security categories must be completed. On the other hand, certain requirements may not be applicable due to the very nature of the merchant's activity (remote sales, face-to-face, electronic commerce, etc.). For example, if a merchant does not use Wi-Fi solutions, the corresponding requirements are not applicable.

What is a compensatory measure?

A compensatory measure is a solution aiming to achieve a security objective for a requirement, which may be different to that proposed by the standard. In certain cases, due to restrictions related to the business activity or particular technical implementations, the requirement cannot be fulfilled according to the instructions explicitly given in the standard.
The compensatory measure must present the same risk coverage as the initially-specified measure and must satisfy specific criteria:

- They must have the same intention and rigour as the initial measure;
- They must supply similar protection to that of the initial measure, so that the compensatory measure covers the risk as much as the initial measure would do;
- It must not be reduced to taking other measures already in place in order to cover the security objective concerned, but it must go beyond the other measures of PCI DSS;
- It must take into account the additional risk that is implied by strict non-compliance with the initial measure.

What should I do if my CB traffic is handled by several banks?

Currently, each bank is required to communicate its own declaration of compliance with PCI DSS to international schemes, for the merchants and service providers that it manages.

Is there a deadline for being compliant?

YES – it depends on the Schemes' regulations on this subject:

VISA:

Implementation through the AIS (Account Information Security) and DCRS (Data Compromise Recovery Solution of July 2007) programmes.

The implementation of this programme is mandatory since 27 February 2009 (see ML VE 28/06) and see ML VE 27/09:

Since 1 October 2009: All Internet merchants must either be compliant with PCI DSS or use a service provider compliant with PCI DSS.

Since 1 October 2010: acquirers must make sure that all their service subcontractors relative to payment are certified PCI DSS.

As of 31 December 2012: acquirers must make sure that all their merchants are fully compliant with PCI DSS or that they use an application that is compliant with PA DSS.

MCW:

Implementation through the SDP (Site Data Protection) and ADC (Account Data Compromise of April 2010) programmes. *See Global Security Bulletin N°12 (December 2009), modified by Q2 2010 newsletter:*

Immediately:

For level 1 merchants : they must be compliant with PCI DSS. The audit by a QSA is not formally obligatory (may be performed internally).

From 1 July 2011: In the case of "self audit", the internal auditor must have followed a PCISSC (ISA training) course and successfully passed the examinations.

Immediately:

For level 2 merchants : they must be compliant with PCI DSS, through the completion of a SAQ.

From 1 July 2011: internal audit staff must have followed the PCISSC ISA training course and successfully passed the examinations.

CB:

June 2007manufacturers are requested to develop the masking of the discretionary zone on the magnetic stripe (CB Bulletin N°10).

November 2007: All "secure remote-sales" acceptance contracts must be modified with a clause prohibiting the storage of sensitive data, worded as follows: "the Acceptor undertakes not to store, in any form whatsoever, any of the following card data: card verification value code, the entire magnetic track or the confidential code".

➡ **Aspects mandatorily included in "secure remote-sales CB acceptance" contracts from July 2008.**

June 2010: A clause clearly mentioning the obligation for compliance with PCI DSS has to be incorporated into all CB acceptance contracts from the 2nd half of 2010.

CB bulletin N°13 CB (mandated from 1st January 2011) allows compliance with PCI DSS for truncation of the PAN present on the merchant ticket.

C - Quarterly external scans

Who should be contacted to perform external scans?

To be compliant with PCI DSS, all entities must perform quarterly vulnerability tests of access points on the Internet.
For this, the e commerce may choose from among PCISSC approved suppliers of security solutions for performing vulnerability scans (ASV, Approved Scanning Vendors) available on the PCI SSC site.

What is an IP address?

An IP (Internet Protocol) address is an identification number that is assigned each time an application is connected to a computer network using the Internet Protocol. In particular, the network points of access to the Internet are referenced by an IP address.
During a vulnerability scan, the system analyses each of the player's IP addresses to check the vulnerability of the services available on this address.

Why perform scans?

The services available behind an IP address may sometimes present known vulnerabilities that are usable by persons with malicious intent (hackers) to penetrate the information system without the knowledge of its owner. If the hacker manages to take control of the information system, they may find files or databases containing bank card numbers. They are then able to steal them.
The vulnerability scans analyse the known vulnerabilities and establish a report which, where necessary, allows the player concerned to correct these vulnerabilities.

Why renew the scans every quarter?

An information system is constantly developing, with new hardware being added or removed, applications and operating systems being updated, and with changes being made to the configuration of security hardware and networks.
Even though, at a given moment, the scan report shows no vulnerabilities, changes made to the system or programming errors that could have taken place after the scan could open new vulnerabilities. Also, vulnerability monitoring regularly shows new vulnerabilities that are quickly identified by the analysis tools.
It is therefore important to perform scans periodically. It is even advisable to perform scans immediately after a major change to the information system, without waiting for the next quarterly scan.

Don't scans only apply to Internet sites?

The scans apply to any information systems visible from the Internet (IP address accessible from the Internet). They may concern a merchant's website, but also any other entry point to an information system belonging to the involved partt (e.g.: IP telephony).

Could performing scans have consequences for my system?

Yes, the scans must be performed by authorised professionals (ASVs)

For example, the scanning software often uses attacks of the "port scan" type, which will scan all of the ports. This activity is considered suspect by an **intrusion detection system** (IDS). An intrusion detection system may be set to various levels of sensitivity. A high level of sensitivity will generate more false alarms, while a low level of sensitivity risks not detecting scans carried out by sophisticated systems such as "**Nmap**", which has various options for camouflaging scans.

To deceive detection systems and **firewalls**, the scans can be performed in a random order, with an excessively slow speed (for example, over several days), or from several **IP addresses**.

Port scanning is done usually using the **TCP** protocol; nevertheless, certain software can also perform **UDP** scans. This last functionality is much less reliable, as UDP is not connection oriented, and the service only replies if the request corresponds to a particular model that varies depending on the server software that is used.

What is contained in the scan report?

A scan report lists, for each IP address declared within the scope of the analysis, the list of observations made by the tool concerning the services visible behind this IP address. The tool is based on the vulnerabilities known according to the state of the art of security monitoring.
The report generally presents a classification by the importance of the security vulnerabilities observed on the analysed system. The report must be analysed by an IT specialist so that appropriate measures can be taken to correct the observed vulnerabilities.

D - Service providers

How do I know if my provider of payment services is compliant with PCI DSS?

Just consult the regularly-updated lists on the sites:

MasterCard: http://www.mastercard.com/us/sdp/serviceproviders/index.html
Click on "Service Providers" then "Compliant Service Providers" then "Compliant Service Provider List"

Visa: http://www.visaeurope.com/aboutvisa/security/ais/resourcesanddownloads.jsp
Click on "List of Service Providers" in the "Procedures and guidelines" section
You can also ask the service provider for a Certificate of Compliance.

What other service providers are we talking about?

These are any service providers that, for any reason, store, process or transmit card data. Such service-providers may be: third party provider, payment service providers (PSP), web site hosts, data manager (airlines, hotel booking, T&E sector), call centres, etc.