MANAGED NETWORKS

IT'S WHO WE ARE.

Payment Card Industry Data Security Standards

What are they?

What's changed in the latest version?

What's next?

Published by Managed Networks on 25/03/2014

DESKTOPLIVE. from Managed Networks

Managed Networks Limited, 6-8 Bonhill Street, London, EC2A 4BX
t: +44 (0) 20 7496 8000 f: +44 (0) 20 7496 8001
sales@mn.co.uk **www.mn.co.uk**

Contents

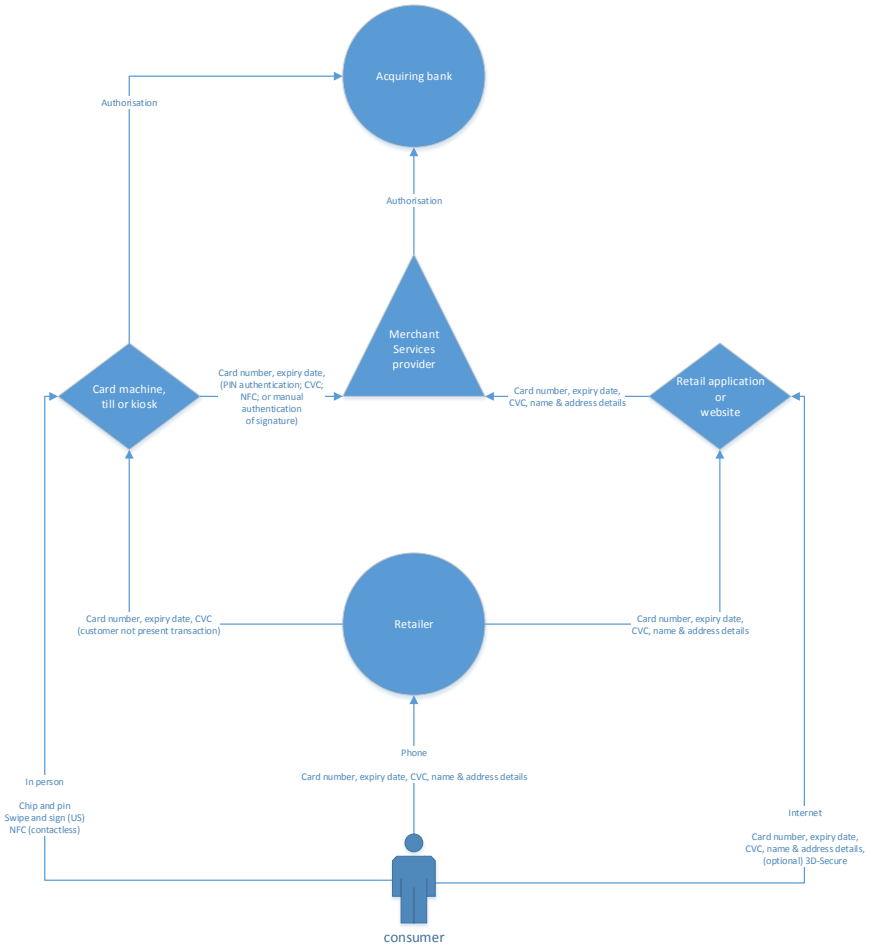
What is PCI-DSS?

The Payment Card Industry Data Security Standard is a set of rules for dealing securely with credit card details, and the associated customer information. It's mostly focused on doing this electronically, unsurprisingly, but is also concerned with how paper records are handled. PCI-DSS is administered by the PCI Security Standards Council, which was founded by five large payment card issuers and draws its membership from several hundred participating organisations including card issuers, banks, retailers and technology companies.

PCI-DSS does not have the force of law. However, accepting credit and debit cards is a commercial transaction between the retailer and (ultimately) the card issuer, and PCI-DSS is built into that commercial agreement. Retailers who aren't compliant with the standard can face fines for non-compliance – which may be as much as thousands of dollars per day and increased transaction charges. They can also – and this is common – be forced to take responsibility for all fraudulent transactions taking place in their account. The final sanction is termination of the retailers account.

Payment eco-system

There is a complex eco-system built up around PCI-DSS. First of all there are a number of ways for the ultimate consumer's payment card information to flow through to their card provider. From the retailer's point of view, it looks like this:



Note that "retailer" is used throughout this document synonymously with "merchant" which is the standard term in PCI documentation.

The retailer may have a direct commercial relationship with an "acquiring" bank – a bank that offers payment card services to its customers. Small shops that use PDQ terminals provided by their bank use this model. Alternatively (or in addition) the retailer may work with a merchant services provider. This provider may also offer PDQ machines – or "smart" alternatives such as the iPhone card reader from Square; more often the provider will offer a payment gateway which allows the retailer's tills or website to carry out card transactions.

Using an appropriate payment gateway can simplify PCI-DSS compliance

In some cases the retailer will use a dedicated application – for example a venue ticketing system or a hotel booking system – which integrates with the payment gateway. That application may be installed locally on the retailer's network or it may be provided by a software-as-a-service provider and hosted by them. In the latter case, there may be one relationship between the merchant services provider and the retail application provider, and another between the retail application provider and the retailer. Some tills also work in this way, where transactions pass through the till supplier's network on their way to the acquiring bank.

(Clearly there is further communication that happens "upstream" of the acquiring bank, as that bank authenticates the card with the original card issuer and gets approval for the amount transacted, but this is outside the scope of PCI-DSS for our purposes)

Summary of PCI-DSS

PCI-DSS is primarily concerned with protecting the security of the consumer's payment card information and associated personal details as it travels through this network of systems and providers. Each step in the process is separately covered by PCI-DSS.

PCI-DSS broadly deals with three areas. Not all of its provisions apply to all retailers, as we will show later. The key areas are:

- Core security processes and procedures. This is a documentation and evidence requirement, requiring the retailer to demonstrate that they have the recommended policies and procedures in place to ensure security. These policies are largely generic and concerned with overall security – critically this is as much concerned with staff, physical premises and paper records as it is with computer networks.
- Technical specification of a secure network. This area is explicitly concerned with computer security and is quite specific about the network design that is required to comply. If the retailer's network was not designed with PCI in mind, the costs of change to accommodate PCI-DSS requirements can be substantial.
- Cardholder-data specific prescriptions. These cover both policies and processes, and computer security, and are very specifically aimed at protecting cardholder data.

There are also three kinds of interaction with PCI-DSS, all of which must be renewed annually:

Self-assessment questionnaires ("SAQ")

These are completed by retailers. Which questionnaire applies depends on exactly what the retailer does with the payment card details, as follows:

- **SAQ 'A'** is for retailers who only use a "card not present" service – typing card details directly into a third-party authorisation terminal or web service and not retaining them in any way.

- **SAQ 'B'** is for those who only use old-style paper imprint machines or newer PDQ machines.
- **SAQ 'C'** is for retailers using a payment application – like a till system, for instance – but one which does not record the card details at any time.
- **SAQ 'D'** is for those whose payment system does record card details (including but not exclusively those who retain card numbers for future use in rebilling etc).

Each questionnaire has broader, deeper and more demanding requirements than the preceding one. Notably, it is often economically advantageous to make the systems and business practice changes necessary to "downgrade" from SAQ 'D' to SAQ 'C'.

SAQ 'C' compliance is much easier than SAQ 'D', but requires you to avoid ever storing PANs

SAQ's C and D also require successful completion of an automated vulnerability scan. This involves contracting with an authorised third party (an Authorised Scanning Vendor, or ASV) who scans the retailer's network from the outside looking for a defined set of weaknesses. It is the retailer's responsibility to ensure that their network is secured against these scans.

Retailers often use third-party consultants to help them complete SAQs. Some consultants are officially certified by PCI for such work; these are referred to as PCI-DSS Qualified Security Assessors (QSAs). Use of a certified QSA is not obligatory in completing SAQs.

Service provider certification

Merchant services providers – those who handle card transactions on behalf of others, or who offer applications on a software-as-a-service basis which include credit card payment – are required to complete service provider certification. Depending on the volume of business transacted by the service provider, this may only mean meeting the same requirements as PCI SAQ 'D', or it may require an on-site verification of their network security. The threshold of transaction volume above which on-site assessment is required is relatively low, so most service providers are subject to the full process.

Service providers are usually required to have their compliance validated on-site by an assessor.

The on-site verification is an extension of SAQ 'D' in terms of content, with additional provisions specific to service providers. It is carried out by a QSA and involves close inspection of policies, procedures and computer system design and documentation, and verification by observation that the policies and procedures are actually followed. Accordingly it can be both time-consuming and costly.

On completion of the on-site verification, the QSA writes and submits a report to the PCI council. The council must then approve this report before the service provider is deemed PCI-DSS compliant. This is in contrast to the SAQ where filing of a completed questionnaire without compliance exceptions automatically gives compliant status.

Application certification

Software houses who produce payment applications – till systems, venue ticketing applications, on-line shops etc – must obtain PA-DSS (Payment Application) certification for their application. This involves a similar process to service provider certification. This paper does not address PA-DSS in any detail, but it is important to note that:

A retailer (or service provider) cannot be PCI-DSS compliant unless all payment applications they use were PA-DSS certified in the version they are using even if that certification has subsequently lapsed.

No new installation of a payment application can be undertaken (in compliance with PCI-DSS) unless the PA-DSS certification for that application is current.

You can't install a payment application that doesn't have valid PA-DSS

The retailer or service provider is responsible for ensuring that all applications they are using have been certified and that any application they are proposing to install has current certification. It is important therefore to include evidence of current PCI PA-DSS certification as a prerequisite in tender responses and to check it as part of any upgrade process for existing applications.

What are the key provisions of PCI-DSS?

This is a brief overview, not an implementation guide; it is not complete, and it is in summary form. It is based on PCI-DSS 2.0 as this is the version that presently applies; the changes in the current version, 3.0, are dealt with later.

General processes and procedures

Information security policy

The starting point for IT security in general, and a key part of PCI-DSS. The infosec policy sets out the business's security goals and principles. It's supported by a number of other documents – both policies and more specific procedures.

Supplier management

PCI-DSS is specific about the need for policies covering selection and management of suppliers. This includes the suppliers' own compliance with PCI-DSS, where relevant, and clear procedures for regular verification that suppliers are actually delivering on their security promises.

Security awareness training

PCI-DSS also mandates regular security awareness training for staff, both in reinforcement of the general security policies and procedures and with specific attention to cardholder data.

Incident response

As a general principle, and as a specific PCI-DSS requirement, organisations should have clearly defined procedures for responding to security incidents, including measures to mitigate the impact of the incident, steps to diagnose the root cause, and lessons to learn for the future.

Technical requirements

Firewalls and perimeter defence

Unsurprisingly PCI-DSS sets out basic requirements for firewalls to secure access to retailer networks from outside. It also sets out requirements for the configuration of network devices, including changing default passwords and protecting configuration against unplanned changes.

Testing and vulnerability scanning

PCI-DSS requires both provision for internal testing of security measures – including specifically scanning for unauthorised WiFi networks on the premises, for instance – and external penetration tests. For most retailers, automated scanning of their network for known vulnerabilities by a recognised provider of this service is sufficient.

Logging

Record-keeping is an important part of compliance in PCI-DSS. For most retailers this is about logging network activity and retaining those logs to help in investigation if there is an incident. Service

providers are required to go further and have automated systems that review logs looking for evidence of intrusion or security weakness.

Authentication

As a general security point, making sure that all users of the network are properly authenticated – use an identifiable account coupled with a secure password – is good practice; it's also required by PCI-DSS. The standard goes further, however, in requiring that users who access the network remotely use two-factor authentication – in other words a physical code-generating token; a one-time passcode sent to their phone; or a similar additional layer of security, as well as a password.

Cardholder-data specific requirements

The main focus of PCI-DSS is on protecting card-holder data, and specifically payment card numbers, known in the standard as PANs ("Personal Account Numbers"). This focus extends the general security advice in a number of areas:

Segregation of card data environment

The computer systems which actually process or store PANs ("the card-holder data environment") have to be segregated from the rest of the network. This may mean additional internal firewalls, or the use of more complex network configurations, as well as additional hardware and software.

Segregation of WiFi

Any WiFi installations that are connected to the same network as the card-holder data environment have to be separated from that network by a firewall. This includes staff and internal WiFi as well as any publicly-accessible WiFi that may be present.

Encryption

If PANs are stored anywhere on the network, they must be encrypted. There are also requirements for controlling access to the encryption keys.

PAN transmission

PCI-DSS is very clear on the transmission of PANs around the organisation. In principle it should not happen; certainly forwarding PANs electronically in unencrypted form is prohibited. However since PANs may also be recorded on paper, there are clear provisions for the secure destruction of such records once they have been used, and for the chain of custody for them beforehand.

Data retention

It's good practice for all businesses to have a data retention policy – to decide what data to keep, and for how long, and to have a routine procedure for destroying data that is no longer required. PCI-DSS mandates this, with specific reference to PANs and cardholder data.

What does the future hold?

PCI-DSS 3.0

PCI-DSS has recently been updated from version 2.0 to version 3.0. There are some material changes in version 3.0 to account for the evolution of network systems and for changes in card-handling technology. This section assumes familiarity with PCI-DSS 2.0; if you're new to PCI-DSS, then this section is irrelevant since you will need to start your compliance process with PCI-DSS 3.0. **Version 3 is effective from 1 Jan 2015 for new (or currently non-compliant) users; others have until 1 January 2015 to upgrade.**

Inclusion of "Guidance"

The format of the standard has been changed to include significant explanatory guidance alongside the actual text of the standard itself. Although this will help organisations effect compliance, it will also shape how the standards are interpreted and may change some existing accepted interpretations.

Extension of scope to include PA-DSS applications

Even if your payment application has a current valid PA-DSS, it still has to be considered as part of your PCI-DSS assessment – in other words you can't just treat it as a black box and assume that it does everything in a compliant way. This will have the most significant impact on service providers who are not themselves application developers, as it brings a great deal more of their infrastructure into scope, and will make the Report on Compliance ("ROC") that their QSA has to produce significantly more onerous.

Requirement 1: install and maintain firewalls and routers to protect card-holder data

The requirement has been updated to include additional documentation, and to add further detailed configuration provisions. Apart from the production of that documentation, most existing v2.0 compliant networks should not require alteration.

Requirement 2: change default (vendor-supplied) passwords

This is also largely some clarification of the existing requirement and the addition of further documentation; again, an existing compliant network will not require material alteration.

Requirement 3: protect stored card-holder data

There are some material changes here for PCI SAQ 'D' retailers and service providers, in other words for those who retain PANs. The encryption standards have been strengthened, notably around key management to separate authenticating with the network - logging in – from gaining access to encryption/decryption keys. There are also enhanced provisions for deletion of data after use, and further documentation requirements.

Requirement 4: encrypt transmission of cardholder data on public networks

Clarification of existing requirements only.

Requirement 5: use and update anti-virus software

MAJOR CHANGE

May require a change of anti-virus system, or a lot of new licences, plus administration

Extended to include evaluation and mitigation of threats to systems not normally considered at risk – this would include smartphones, tablets and POS terminals for instance. Also adds a specific provision that users should not be able to disable anti-virus on their devices without case-by-case authorisation.

Both of these changes will require additional work even on currently-compliant networks. This may include purchasing additional anti-virus licensing or changing anti-virus vendor if the current application does not permit preventing the user from disabling it without permission.

Requirement 6: develop and maintain secure systems and applications

This section is relevant only to organisations that develop payment applications; this paper is not aimed at that audience. Largely v3.0 clarifies existing requirements; in summary, the main changes extend security awareness training for developers, add a requirement for countermeasures against authentication and session exploits and provide for a broader approach to preventing web-based attacks than the original narrow definition of a "web-application firewall".

Requirement 7: restrict access to cardholder data

Largely clarification, with greater focus on applying the principles of least privilege and role-based access control. This may mean refining user's job descriptions and reviewing their security privileges in order to remain compliant.

Requirement 8: assign unique IDs to users

This has some significant changes. It reiterates the need for users to have unique login IDs, which may have a material operational and cost impact on organisations that routinely use generic accounts shared by more than one user. Note that there is an apparent conflict here between 8.1.1 which requires unique IDs for all users and 8.5 which prohibits shared IDs for system administration (implying that shared IDs are acceptable for non-administrative users). We will be seeking clarification on this point.

It extends and clarifies the notorious requirement 8.3 for two-factor authentication for remote access, making it clearer that it applies to remote access by staff and by third-parties including support providers. It still does not entirely clarify what is meant by "the network" leaving open the question of whether networks connected by hardware VPNs require two-factor authentication for cross-network access. However it is clear that remote access by e.g. hardware vendors will require provision of two-factor authentication in some fashion, probably requiring a move away from physical tokens in order to make this possible.

MAJOR CHANGE

Extends the scope of two-factor authentication; you'll need more of it, and may need to change system or provider.

Requirement 9: restrict physical access to cardholder data

MAJOR CHANGES

You need to be able to revoke physical access on employee termination – this may mean new physical security systems

You also need to protect card terminals (tills) against tampering, and document how.

Two major changes here: firstly a requirement that physical access to "sensitive areas" can be revoked immediately on termination; this means at a minimum changing exit policies to ensure compliance, and may also mean upgrading existing security systems to mitigate the risk of former or unauthorised personnel gaining access – e.g. replacing key or code locks with biometric systems or badge readers.

Secondly a requirement to protect card readers from tampering. This is a substantial new section; it requires documentation and procedural change – mostly to ensure routine inspection and keep appropriate records of POS equipment. There is no requirement for increased physical security or automatic tamper detection.

Requirement 10: track and monitor all access to network

Largely clarification, but a significant extension of the logging requirement to include in the security log changes to identification and authentication (e.g. the creation of new users or the assignment of new privileges) and all changes to administrative accounts. This may have material impact if systems are in use which do not provide for automated logging at this level of detail; it will also increase the volume of security logs.

There is also a new requirement to log interruptions to logging (stopping or pausing logs); again not all systems have this capability, so this makes it likely that organisations will either have to adopt a central log aggregation system or change systems that do not have this capability.

Requirement 11: regularly test security

Further weight is given to scanning for unauthorised WiFi points, including a new requirement for a business justification for scanning and an incident response plan if unauthorised points are discovered. There is also a more general emphasis on repeating vulnerability scans of all kinds until all significant issues have been resolved.

There is a major new requirement in this section for the implementation of a penetration testing methodology. This goes well beyond the existing requirement for automated scans and will require both significant planning and the engagement of third parties, including, potentially, ethical (so-called "white hat") hackers. There is a material paragraph in the guidance notes whose interpretation will be critical in mitigating the cost of compliance with this section:

MAJOR CHANGE

Introduction of penetration testing from July 2015

Penetration testing techniques will be different for different organizations, and the type, depth, and complexity of the testing will depend on the specific environment and the organization's risk assessment.

By implication the level of penetration testing required will to some extent depend on the approach of the organisation's QSA if one is involved, and in the business case that the organisation constructs for carrying out the testing. This will be most relevant to those organisations that require on--premises assessments rather than self-assessment questionnaires.

Note that the requirement for penetration testing takes effect from 1 July 2015.

The requirement for intrusion-detection and change-detection systems is expanded and clarified. There is also now a requirement to have a process to respond to alerts from these systems.

Requirement 12: maintain an information security policy

Clarification that risk assessments should be performed after any significant change to the environment. This is good practice in any case, but for organisations not currently following this practice it will increase the cost and time required for network changes.

There is a new requirement to maintain documentation of the responsibility for PCI-DSS compliance, and specifically which service providers manage what elements of compliance. This may require material effort in complex environments.

MAJOR CHANGE

From July 2015 you have to get supplier agreement that they will comply with PCI; you have to monitor their compliance

Finally there is a substantial new requirement to seek service provider agreement to maintain PCI-DSS requirements in their own processing of card-holder data on behalf of the organisation, and to monitor that compliance. This takes effect from 1 July 2015. We expect most reputable service providers to supply such agreements routinely, but effort may be needed to secure suitable agreement and documentation from suppliers less familiar with PCI or of smaller scale.

Looking ahead

Payment is changing faster now that at any time since the introduction of plastic cards in the '50s. Not only are we seeing a number of different ways of using existing card accounts – Google Wallet, Apple's Passbook, PayPal and so on – there are also new technologies being embedded in the cards themselves, including NFC (Near Field Communications – 'touch/wave to pay') – and, for the US, the eventual inevitable adoption of the chip and PIN technology we've had in Europe since 2002.

More importantly, there are several new ways to pay that don't involve traditional card issuers – and so aren't part of PCI-DSS – but will share many of the same security concerns. There's PayPal again, which is increasingly seen as an additional payment mechanism on ecommerce websites – and which can directly debit a user's bank account (or act as an account in its own right) – and iDeal, a European web-payment system that again uses direct bank debits; Monitise offers a similar service alongside mobile banking platforms and ecommerce transaction services. Faster Payment in the UK provides another way for consumers quickly to settle transactions electronically – and has no cost to the retailer, unlike the other alternatives. The Payments Council has just announced Paym, a payments system allowing consumers to make payments directly from their bank account using their mobile phone. Finally there are the "crypto-currencies" like Bitcoin, Litecoin and Doge, all of which again allow instant electronic settlement without involving card issues, or indeed banks in this case.

As ever the IT industry, retailers and regulators will be playing catch-up as they work to enable these payment mechanisms for their customers while maintaining security. PayPal direct bank debit, Paym, Monitise and iDeal offer the first real threats to the dominance of traditional card issuers in ecommerce, and Paym in particular is a real threat to their revenue stream even in traditional commerce. Bearing in mind that many phones incorporate NFC, it's not much of a stretch to see this integrating with Paym to allow customer-present purchasing just by touching their phone to a retailer's till point.

If successful, Paym offers a real threat to the dominance of credit card issuers in mobile **and** in-person transactions

In theory, some of these new mechanisms move the security problem away from the retailer – since possession of the customer's mobile phone number, for instance, doesn't give a hacker the same opportunity to steal money as possession of their payment card details. On the other hand, experience tells us that all of these systems will have unanticipated risks, and that the obvious opportunity to exploit those risks is by compromising the retailer. We only have to look at Target's recent experience in the US, where 40 million card numbers were stolen by an attack which suborned their till systems, to see that IT security should still be right in the forefront of retailers' minds.

References

Payment Card Industry Security Standards Council: https://www.pcisecuritystandards.org/

PCI Report on Compliance Template for service providers: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_ROC_Reporting_Template.pdf

History of payment cards: http://www.theukcardsassociation.org.uk/Advice_and_links/

Target POS attack: http://techcrunch.com/2013/12/19/target-confirms-point-of-sale-data-breach-announces-it-exposed-40-million-credit-card-numbers/

Payments Council, details of Paym: http://www.paymentscouncil.org.uk/mobile_payments/overview_of_paym/

PCI-DSS version 3.0, full text: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

PCI-DSS version 3.0, changes: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_Summary_of_Changes.pdf