DeviceLock for Compliance with the PCI Data Security Standard

Contents

Introduction

Soon after they were introduced years ago, payment cards became one of the most popular means of making payments for goods and services among the public. But while payment cards provide their holders with maximum convenience, using them involves additional risks. If the information that is contained on a plastic card falls into the hands of a malicious user, the owner of that card risks losing money from his personal bank account.

It is equally important to note that cardholders aren't the only ones who have fallen victim to these risks – both banks and payment systems have also suffered. If payment information has been compromised, banks must issue new cards, and this process means additional expenses. In some cases, banks must restore material damages incurred by the cardholder. In addition to direct losses, financial institutions also face major indirect losses such as damaged reputation and diminished trust in payment cards.

The Payment Card Industry Data Security Standard (PCI DSS) was drawn up in order to reduce leakage and inappropriate use of plastic card information. Today, the requirements set out in PCI DSS apply to all companies who process, store or transfer data about cardholders: banks, processing centers, service providers, retail stores, e-commerce businesses, etc.

The first version of PCI DSS was adopted in early 2005 with the participation of leading payment systems (VISA, MasterCard, American Express, Discover, Diner's Club and JCB). One and a half years later, the standard underwent some minor amendments (PCI DSS v. 1.1) which remain in force today.

As of 2007, organizations which process information about credit and debit cards must comply with PCI DSS. Starting in 2008, payment systems plan to fine any companies that have not undergone certification procedures.

In general, PCI DSS is a comprehensive standard which contains over 100 clear requirements for an organization's information security. Despite the fact that many organizations already have an information security system in place, it is not always a simple task to make sure a company's system is aligned with PCI DSS. This process requires substantial financial investment, in addition to considerable time and labor.

This document will analyze the requirements set out in PCI DSS. Furthermore, it will explore the capabilities of DeviceLock, a product from DeviceLock, Inc., which can be used to help an organization achieve compliance with this standard much more effectively.

The Structure of PCI DSS and the Certification Process

PCI DSS applies to two types of organizations which are then divided into several sub-categories, depending on the quantity of transactions that are processed. PCI DSS requirements apply to:

- <u>Trade organizations</u> (merchants). These include organizations that deal in trade with the use of payment cards. It is implied that trade organizations play a direct role in transactions.

- <u>Service providers</u> (such as processing centers, for example). These include organizations which deal with the processing of transactions, but do not play a direct role in the transaction itself.

PCI DSS requirements may be modified depending on the type of business involved. The table below (see Table 1) illustrates an example of the requirements with which trade organizations must comply.

Table 1. PCI DSS Requirements for Trade Organizations			
Level	**Level Definition**	**PCI DSS Requirement**	**Executor**
One	Trade organizations which process over 6 million transactions annually and organizations that have already experienced data leakages.	A certified audit of PCI DSS compliance	a certified auditor
		A quarterly penetration test	an Approved Scanning Vendor (ASV)
Two	Trade organizations that process from one to six million transactions annually.	An annual survey	the organization itself
		A quarterly penetration test	ASV
Three	Trade organizations that process from 20,000 to one million transactions annually.	An annual survey	the organization itself
		A quarterly penetration test	ASV
Four	Trade organizations that process less than 20,000 transactions annually.	An annual survey	the organization itself
		A quarterly penetration test is recommended	ASV

In summary, two conditions must be met for PCI DSS compliance:

- Each quarter, the company must successfully pass a penetration test conducted by an Approved Scanning Vendor (ASV). The penetration test is essentially equivalent to a professional hacker attack that is conducted exclusively for audit purposes.

- Each organization must comply with the list of requirements set out in the Standard. At least one compliance audit must be conducted per year by a certified independent auditor.

PCI DSS presumes that successfully meeting all requirements will make it easy for a company to pass the penetration test and pass the compliance audits.

PCI DSS requirements have a hierarchical structure (see Figure 1). Most of the Standard's provisions are related to protecting information about cardholders. All of the security requirements are divided into six control components, each of which is then divided into several sub-requirements (the Standard features 12 key requirements in total). The list of PCI DSS provisions

also includes requirements to store payment data, in addition to special compensative measures. These measures are ways to reduce the risk of data leakage by following different methods from the methods specified in PCI DSS. These measures may only be used by organizations who are unable to comply with the main provisions of PCI DSS due to insurmountable reasons.
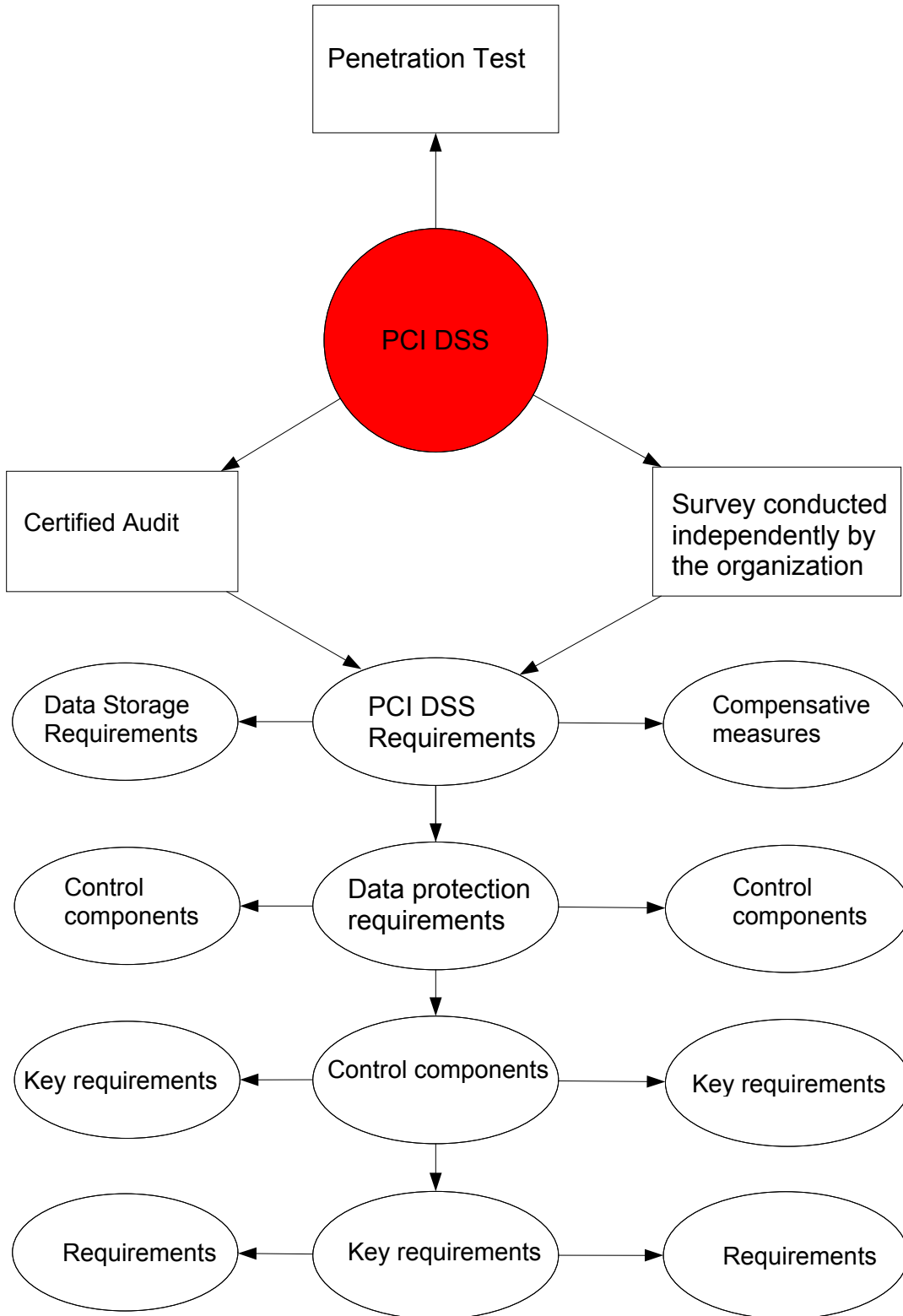
Figure 1. The Structure of PCI DSS

Key PCI DSS Provisions

A review of all of the requirements of PCI DSS is beyond the scope of this document. This section will concentrate on only the key provisions of the standard. For more in-depth information, you can view the original text of PCI DSS at https://www.pcisecuritystandards.org/.

The second key provision, which is comprised of two main requirements (requirements 3 and 4), plays an important role in PCI DSS. In order to meet compliance with this section, an organization must protect payment information on-site where data is stored and in data exchange channels. This component is one of the most difficult to complete, as a modern IT infrastructure can have a multitude of places of storage and exchange channels[1].

In particular, provision 3.4 of PCI DSS states that a Personal Account Number (PAN - the number on the plastic card) must be rendered "unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks)…" In practice, this requirement means that access to some places of storage (such as a removable device) must be blocked, since it is unrealistic (or simply too costly) to install total protection at each location.

On the other hand, it would be near impossible to achieve compliance without any special tools designed for data protection, since plastic card numbers must be stored and processed somewhere. PCI DSS recommends encryption tools.

Requirement 4 of PCI DSS is similar to requirement 3, except that it governs the protection of information when that information is being exchanged, rather than when it is being stored. The standard states that organizations must "Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission..." As a result, just as with requirement 3, some of the channels will have to be blocked, while the remaining channels will require protection.

In addition to the second key component, another important role is played by the fifth component, which also contains two key requirements (requirements 10 and 11). Despite the fact that both of these requirements are essentially auxiliary, as they do not have an impact on the information security of an IT infrastructure, the fifth component is one of the most complex and difficult to execute.

In particular, requirement 10 of PCI DSS requires that all actions with payment information be logged. The Standard clearly requires that a company "implement automated assessment trails for all system components to reconstruct … all individual user accesses to cardholder data" and record the parameters related to such. Furthermore, organizations must "review logs for all system components at least daily," and "retain assessment trail history for at least one year, with a minimum of three months online availability." In other words, PCI DSS compliance means more than just keeping a variety of logs; these logs must also be analyzed on a regular basis. That means that all protocol logs need to be structured and collected into a common database that supports different analytical requests.

Requirement 11 stipulates that an organization conduct regular testing of the infrastructure network to look for security problems. This requirement essentially echoes the standard's certification scheme, which states that an organization must conduct a penetration test at least once every three months.

Aside from its "tactical" requirements, PCI DSS contains several "strategic" provisions which govern the general principles of information security. In particular, the sixth requirement stipulates

---

[1] For example, data may be kept on file servers, stored on different information systems, on local workstations or removable devices. Data may be exchanged through channels such as email, local ports, wireless interfaces, etc.

that an organization must bring an information system in line with programming security guidelines, and the twelfth requirement stipulates that a company must maintain a policy that sets out the rules and regulations for information security.

DeviceLock from DeviceLock, Inc.

DeviceLock is endpoint device control software developed by DeviceLock, Inc. (formerly SmartLine Inc) for corporate users. With DeviceLock, a company of any size can ensure comprehensive control over data which leave a corporate network via the ports, wireless networks, external drives, and printers attached or integrated into a Microsoft Windows workstation endpoint.

DeviceLock's key features include more than just control over local computer communications based on assigned policies – it also provides complete shadow copying of all outgoing data. In contrast to the great number of solutions that sift through email correspondence to detect leakage of sensitive data, DeviceLock gives security administrators the power to judiciously shut user access to workstation ports and drives so that data leakage doesn't happen in the first place. Should security administrators choose to leave endpoint resources unlocked, DeviceLock provides for the collection and analysis of data leaving the corporate network via workstation ports and drives including documents sent to local and network printers. In other words, DeviceLock not only controls access to endpoint input/output resources based on assigned policies, it can also "shadow" all outgoing data so that audit and forensic experts have the evidence they need to prove compliance or catch malfeasance.

There is an ever-increasing number of mobile devices maintained and, in some cases, purchased by employees connecting to corporate networks. Experts at Yankee Group and SCS Research studied this trend toward the 'consumerization of corporate IT networks' and advised IT department managers and directors neither to ignore nor to attempt to completely prohibit the plethora of portable devices used by employees. They simply must provide support for employees' mobile computers. Otherwise, the company risks losing its innovative and competitive edges by reducing the productivity of its employees. Meanwhile, mass consumerism is rife with new, serious risks in information security, as mobile devices may be used for fraudulent purposes, information leaks and other internal breaches. DeviceLock can help address these challenges.

When it comes to PDAs, smartphones and other communicators, DeviceLock does more than just support the shadow copying of all of the data exchanged to a Windows Mobile® or Palm® OS personal mobile device – it also allows a company to apply flexible security policies and then track the enforcement of these policies. For example, DeviceLock may permit a user to synchronize his contacts and calendar, but prohibit copying files or synchronizing email with attachments.
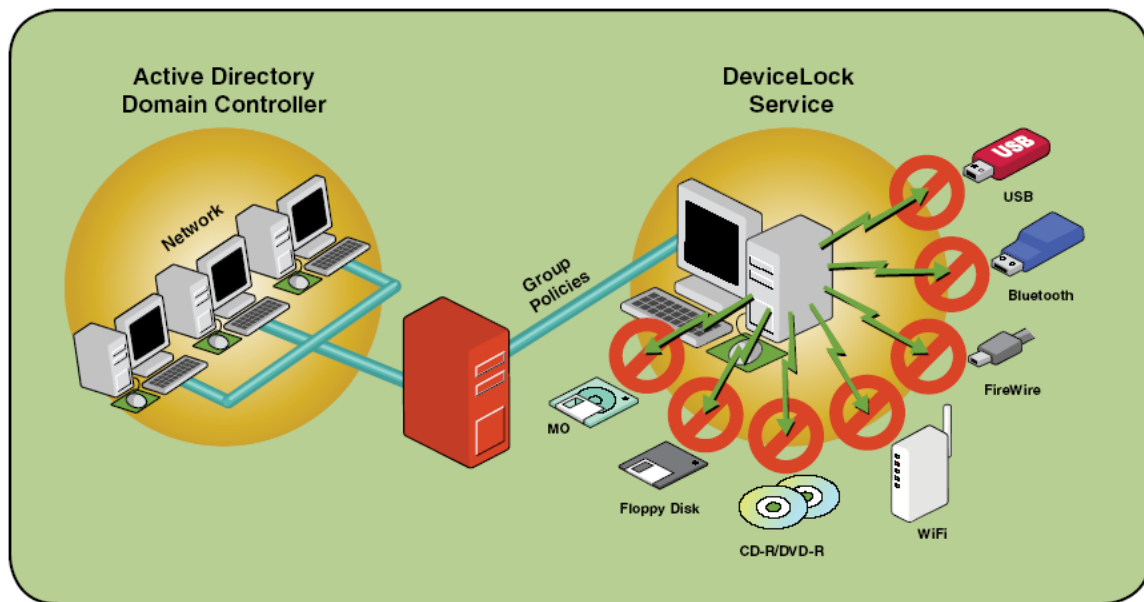
Another important feature of DeviceLock is granular control over user access rights to printers, including virtual printers. DeviceLock not only ensures the enforcement of corporate information security policies by defining user access rights to printers and thus minimizing the risk of unauthorized data leakages, it also keeps a log of events and conducts shadow copying of all printed documents. To ease review and analysis of these comprehensive logs and shadow copies, DeviceLock also has built-in presentation tools for graphing or charting data sets.

DeviceLock also provides protection against hardware keyloggers. This variety of malware is surreptitiously connected between a computer's keyboard and the system unit in order to steal valuable data from employee workstations. If DeviceLock detects the exchange of data from an endpoint computer to a keylogger, it will block the keylogger, warn the user and create a record in the events log.

Through all these features, DeviceLock protects companies against the leakage of consumer information and unwanted content, and serves as a tool for retrospective analysis of all data which company employees copy to external drives or personal mobile devices and take with them, as well as send to local, network and even virtual printers. It also affords a company the flexibility it needs to set up information security policies for mobile devices.

DeviceLock consists of three parts: the agent, the server and the management console:

1. DeviceLock Service (the agent) is the core of DeviceLock. DeviceLock Service is installed on each client system, runs automatically, and provides device protection on the client machine while remaining invisible to that computer's local users.

2. DeviceLock Enterprise Server (the server) is the optional component for centralized collection and storage of the shadow data and audit logs. DeviceLock Enterprise Server uses MS SQL Server to store its data.

3. The management console is the control interface that systems administrators use to remotely manage each system that has DeviceLock Service. DeviceLock ships with three different management consoles: DeviceLock Management Console (the MMC snap-in), DeviceLock Enterprise Manager and DeviceLock Group Policy Manager (integrates into the Windows Group Policy Editor).

DeviceLock can be controlled using group policies in Windows Active Directory, making it easy to integrate it into the IT infrastructure of an organization of any size. A company can easily secure dozens of thousands of remote computers with DeviceLock by using management via Active Directory group policies.

How DeviceLock Helps Achieve Compliance with PCI DSS

DeviceLock controls the exchange of data via local workstation ports, wireless networks and removable drives based on flexible policies. Each time, the decision to either permit or prohibit access to an external device is made automatically. That means DeviceLock's settings and policies are easily audited, and DeviceLock itself does not create any additional information security risks.

6

In a corporate environment, DeviceLock will help ensure compliance with the two key requirements of PCI DSS:

- **Control over information in transit.** PCI DSS requirements reflect the ultimate goal of the standard, which is to prevent the leakage of payment information outside of the organizations that process this information. DeviceLock provides control over the use of local ports of corporate computers, printers, wireless networks and mobile devices, which helps minimize the risk of unauthorized payment data leaks.

- **Audits.** Requirement 10 of PCI DSS is dedicated to keeping records and logs of events for subsequent analysis. DeviceLock offers a one-of-a-kind feature: shadow copying of all data leaving the corporate network via local workstation ports, removable drives, wireless networks and personal mobile devices. All of this information is automatically transferred to a special centralized database, which is then made available for subsequent audits and retrospective analyses.

The table below (Table 2) provides a summary of DeviceLock features and how they can help organizations achieve compliance with PCI DSS.

Table 2. DeviceLock Features and PCI DSS Compliance	
PCI DSS Requirements	**DeviceLock**
3.1. Organizations must develop a policy for the storage and handling of cardholder data.	One of the main objectives of an internal security policy is to protect confidential information (including cardholders' data) against potential leakage. Clearly, company employees have the most opportunities to steal information, since they unlike outside malicious users have legitimate access to the information. DeviceLock helps minimize risks related to the leakage of confidential data via the local ports of computers, printers, wireless networks and personal mobile devices. DeviceLock can help protect an organization from premeditated theft and from accidental or negligent employee actions.
12.1. Organizations must draw up, publish, distribute and maintain a security policy.	
9.1. Organizations must use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data [and] … restrict physical access to publicly accessible network jacks.	A system administrator can use DeviceLock to restrict access to local computer ports in a corporate network. Software-based restrictions in this case are equivalent to physical restrictions, since access to the agent is granted only to specially authorized administrators (members of the local group of Administrators for operating systems on computers protected by DeviceLock are not authorized by default).
10.2. Automated assessment trails for all system components must be implemented for the subsequent reconstruction of events.	DeviceLock features advanced shadow copying, which not only keeps logs of all attempts to exchange data between a computer and an external device, but also copies all exported data and delivers them to a special database. This data are stored together with detailed data about every event (the time of the event, the type of event and the exchange channel, the user ID and other details). That means that DeviceLock can help a security administrator to keep completely up-to-date on all of the company's data exchanged via local ports and workstation interfaces. The information is centrally stored in a way that makes subsequent audits and analysis convenient for investigating information security incidents.
10.3. Records must be kept of all events and their related details (the type of event, date and time, etc.).	

About DeviceLock, Inc.

DeviceLock, Inc. (formerly SmartLine Inc) was established in 1996 to provide effective and economical network management solutions to small, medium and large-scale business. Early on, we made it our mission to design software that is robust and reliable when it comes to enforcing network policy, while being easy and intuitive for system administrators to use. Furthermore, we made it our job to deliver solutions that are well-integrated and cost-effective. Based on this formula, we've introduced and developed category-leading products like DeviceLock for enforcing security policy related to personal devices.

DeviceLock, Inc. is a worldwide leader in endpoint device control security. Our DeviceLock product is currently installed on more than 3 million computers in more than 55 000 organizations around the world.

The company's customers include BAE SYSTEMS, AEROTEC Engineering GmbH, HSBC Bank, Barclays Bank, Chase Manhattan Bank, and various state and federal government agencies and departments.

DeviceLock, Inc. is an international organization with offices in San Ramon (California), London (UK), Ratingen (Germany), Moscow (Russia) and Milan (Italy).

Contact Information

DeviceLock Germany:

Halskestr. 21, 40880 Ratingen, Germany

TEL: +49 (2102) 89211-0
FAX: +49 (2102) 89211-29

DeviceLock Italy:

Via Falcone 7, 20123 Milan, Italy

TEL: +39-02-86391432
FAX: +39-02-86391407

DeviceLock UK:

The 401 Centre, 302 Regent Street, London, W1B 3HH, UK

TEL (toll-free): +44-(0)-800-047-0969
FAX: +44-(0)-207-691-7978

DeviceLock USA:

2010 Crow Canyon Place, Suite 100, San Ramon, CA 94583, USA

TEL (toll-free): +1-866-668-5625
FAX: +1-646-349-2996

sales@devicelock.com

support@devicelock.com

www.devicelock.com