PCI compliance

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements meant to ensure that companies involved in the process of card payment maintain a certain level of security to **protect the cardholder data**. It was designed by major card brands in response to the growing number of data security breaches and the resulting unlawful uses of this data.

PCI DSS in its current version (2.0) is defined as a set of twelve rules, which the involved entities must adhere to. The following table lists the requirements organized into logically related groups, called control objectives.

On this page

Control Objectives	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software on all systems commonly affected by malware 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

Who must comply?

PCI DSS is a mandatory standard which applies to all entities that take part in payment card processing. This includes **retailers**, **e-commerce sites**, **acquiring organizations**, **card issuers** and any other subject which accepts, transmits or stores cardholder information.

In other words, if you are a merchant and want to accept payment cards, you must comply with the standard.

PA DSS

Payment Application Data Security Standard enforces the security of software used to process, transmit and store **cardholder data**. Similarly to PCI DSS, it defines a list of requirements the applications have to comply with. The current version (2.0) of PA DSS poses the following requirements:

Requirements
1. Do not retain full magnetic stripe, card validation, code or value, or PIN block data.
2. Protect stored cardholder data.
3. Provide secure authentication features.
4. Log payment application activity.
5. Develop secure payment applications.
6. Protect wireless transmissions.
7. Test payment applications to address vulnerabilities.
8. Facilitate secure network implementation.
9. Cardholder data must never be stored on a server connected to the Internet.
10. Facilitate secure remote software updates.

11. Facilitate secure remote access to payment application.
12. Encrypt sensitive traffic over public networks.
13. Encrypt all non-console administrative access.
14. Maintain instructional documentation and training programs for customers, resellers, and integrators.

Who must comply?

PA DSS aims at **software developers** and **integrators** that deliver online payment applications, which are sold, distributed or licensed to third parties.

Relationship to PCI DSS

Both these standards ensure cardholder security, but at different levels. PA DSS is for software vendors, while PCI DSS is required for all merchants who handle cardholder information.

Although PA DSS is based on the PCI DSS requirements, **using PA DSS certified software does not make a merchant PCI DSS compliant**. The best way to mitigate payment card security threats is to implement PA DSS inside a PCI DSS compliant environment.

Kentico CMS compliance with PCI standards

Since PCI DSS is focused on merchants and the institutions that process card payments, **Kentico CMS doesn't need to comply with the standard**. However, you, as a merchant, may decide to employ Kentico CMS, particularly its built-in e-commerce module, as means to run your business. You may also wish to provide customers with the possibility to pay with their cards. This would require you to obtain a **PCI DSS certification**.

The PA DSS standard dictates that e-commerce solutions that offer online payment must be secured in order to protect cardholder data. Kentico CMS provides such an option. However, it is not a certified PA DSS compliant application. This means that **users of the E-commerce module would need to acquire the certification themselves**.

Despite the fact that Kentico CMS is not PA DSS certified, it is built in a way that doesn't prevent retailers from obtaining the required PCI DSS certification. The system doesn't store, transmit, or in any other way handle cardholder data, with the exception of a single feature – the Credit card payment method.

The built-in Credit card payment method uses the Authorize.NET payment gateway. However, when using this method of payment, customers do not enter their credit card numbers directly on the Authorize.NET website. Instead, they input the data on a page generated by Kentico CMS, which then passes the data to the Authorize.NET gateway. **This transfer is conducted over a secure protocol, hence it doesn't pose a security threat to sensitive data**.

To learn more about the standards discussed in this document and for information how to validate your compliance, visit the PCI Security Standards Council's website at https://www.pcisecuritystandards.org.