Version	Date	Comment
Current Version (v. 17)	**Nov 04, 2020 20:53**	**Tomas Nilsson**
v. 16	Feb 25, 2020 16:36	**Tomas Nilsson**
v. 15	Feb 25, 2020 11:37	**Tomas Nilsson**
v. 14	Feb 25, 2020 10:36	**Tomas Nilsson**
v. 13	Feb 25, 2020 10:27	**Tomas Nilsson**
v. 12	Feb 25, 2020 10:09	**Tomas Nilsson**
v. 11	Jan 17, 2019 07:58	**Mattias Lantz**
v. 10	Aug 30, 2018 16:55	**Patric Nilsson**
v. 9	Aug 30, 2018 16:55	**Patric Nilsson**
v. 8	Aug 30, 2018 16:49	**Mattias Lantz**
v. 7	Jun 20, 2018 14:19	**Mattias Lantz**
v. 6	Jun 20, 2018 14:17	**Mattias Lantz**
v. 5	Jun 07, 2018 17:29	**Mattias Lantz**
v. 4	Jun 07, 2018 17:19	**Mattias Lantz**
v. 3	May 16, 2018 16:57	**Mattias Lantz**
v. 2	May 15, 2018 11:49	**Mattias Lantz**
v. 1	May 15, 2018 11:45	**Mattias Lantz**

This implementation guide is valid for the following versions of the transaction engine:

West Transaction Engine 2.x

Terminals for which this implementation guide applies are:

Product	Manufacturers product name	PCI PTS Reference	PTS Version	PTS Expiry date
Westpay C100	xCL_AT-100	4-40234	5.x	30 Apr 2026
Westpay C10	xCL_AP-10	4-40231	5.x	30 Apr 2026
Westpay C305	xCL_T305 + P95	4-10242, 4-40246	5.x	30 Apr 2026

Contents

References

Reference no	Reference	Location
1	SPDH specification Swedbank	
3	Security Requirements	
4	XACT Integration Guide	

Introduction

The Payment Card Industry Data Security Standard (PCI DSS) defines a set of requirements for the configuration, operation, and security of payment card transactions. The requirements are designed for use by assessors conducting onsite reviews and for merchants who must validate compliance with the PCI DSS. The Payment Card Industry has also set the requirements for software applications that store, process or transmit cardholder data. These requirements are defined by the Payment Card Industry Payment Application Data Security Standard (PCI PA-DSS). In order to facilitate for anyone that use this West product to get a PCI DSS certification, this application has been approved by PCI to comply with the PCI PA-DSS requirements.

Failure to comply with these standards can result in significant fines if a security breach should occur. For more details about PCI DSS and PCI PA-DSS, please see the following link: http://www.pcisecuritystandards.org

Document usage

This Implementation guide is intended to be used for a user of this West product as a help for integration of the product in a manner that can be compliant with PCI DSS. The integration will commonly be with an ECR-system. Please note that West take no responsibility in the merchants overall PCI Compliance status. Each merchant is responsible for creating it's own PCI DSS compliant environment.

Intended readers

The project managers, and engineers at a merchant site responsible for developing and maintaining the payment systems. The document may also be used for the organization security department as well as in training of personnel/operators.

Overview of PCI DSS and PCI PA-DSS requirements

This overview covers briefly the PCI DSS/PA-DSS requirements that have a related PA-DSS
Implementation Guide topic. It also explains how the requirement is handled in the Westpay
application and also explains the requirement.
The full PCI DSS and PA-DSS documentation can be found at: http://www.pcisecuritystandards.org

Protecting sensitive- cardholder data

Requirement 1: Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2), or PIN block data
1. What the requirement says
"Do not store sensitive authentication data after authorization. Only those data elements needed for business should be stored."
2. How is this requirement met?
No specific setup for the terminal is required. When required by the application the PAN is always stored encrypted. Sensitive authentication data such as magnetic stripe data and CVV2 is deleted immediately after authorization and never stored.
3. How should the merchant handle this?
If the merchant need to enter PAN, expiration date and CVV2 manually or do a voice referral The operator should never write down or otherwise store PAN, expiration date or CVV2. Collect this type of data only when absolutely necessary to perform manual entry or voice referral.

Requirement 1.1.4: Historical data deletion
1. What the requirement says
"Securely delete any magnetic stripe data, card validation values or codes, and PINs or PIN block data stored by previous versions of the

payment application."
2. How is this requirement met?
No specific setup for the terminal is required. The application does not store any historical data so removal of historical data is not needed.
3. How should the merchant handle this?
You must make sure that historical data (magnetic stripe data, cardholder data and CVV2s) is removed from all surrounding storage devices used in the merchant system such as ECRs, PCs, servers etc. For further details please refer to the appropriate vendor.
Removal of historical data is necessary for PCI DSS compliance.

Requirement 1.1.5: Securely delete any sensitive data used for debugging or troubleshooting
1. What the requirement says
"Securely delete any sensitive authentication data (pre-authorization data) used for debugging or troubleshooting purposes from log files, debugging files."
2. How is this requirement met?
Generally troubleshooting is not done on production terminals. However, if logs are written,
no sensitive data is included in them.
3. How should the merchant handle this?
No action is needed.

Requirement 2: Protect stored cardholder data
1. What the requirement says
Protection methods such as encryption, truncation, masking, and hashing are critical
components of cardholder data protection. If an intruder circumvents other network security
controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person.
Other effective methods of protecting stored data
should be considered as potential risk mitigation opportunities. For example, methods for
minimizing risk include not storing cardholder data unless absolutely necessary, truncating
cardholder data if full PAN is not needed, and not sending PAN in unencrypted e-mails.
2. How is this requirement met?
Full magnetic stripe data from the card is never stored by the application. For transactions only the PAN and expiry date are stored encrypted following ref[1]. A 3DES key is used for encryption. The key is generated and stored in the POS TRM and is never revealed (not encrypted or in clear).
3. How should the merchant handle this?
For cards read by the terminal, magnetic stripe reader or chip card reader no action is needed.
For manually entered PAN and for voice referrals it is never allowed to write down or store the PAN, expiration date or CVV2. This must be implemented as a policy at the merchant (see ref[4]).

Requirement 2.1: Purging cardholder data
1. What the requirement says
Software vendor must provide guidance to customers regarding purging of cardholder data
after expiration of customer-defined retention period.
2. How is this requirement met?
All cardholder data is sent in the authorization message. In case of host unavailability, is the necessary data stored encrypted in the store and forward queue. When the next communication with host occurs is all data items in the store and forward queue sent.
Once accepted by the host the stored transaction is automatically deleted.

Locations of card holder data on the terminal:

- Encrypted card holder data is stored under Android/data/Westpay.WestPA/files/BIT_OW/PersistentData and as files beginning with TXN000. These can be manually deleted if one wants to manually delete sensitive data. However, its important to remember that if these files are deleted the transaction is as well.

Cardholder data, including SAD and PAN, is automatically deleted in a secure way by the PA. To securely delete data, the PA overwrites affected sectors on the disk three times starting with zeroes, then ones and finally with a random pattern.

3. How should the merchant handle this?
There is no need for action since no cardholder data is stored locally longer than necessary.

Requirement 2.2: Masked PAN when displayed

The PAN is displayed in the following places in the payment application:

(the PAN can not be configured to be unmasked)

- Customer reciepts -> Masked,
- Merchant reciepts -> Masked,
- ECR for reciepts -> Masked (both Merchant and Customer reciepts),
- On terminal screen if customer enters their card manually on the PED -> Masked during entry where each entered char is masked after a timeout period of 2 seconds.
  Ex. *******1 for two seconds then ********* or until next key is pressed.

Requirement 2.3a: Render PAN unreadable:

The PAN is **not** stored unmasked and can not be configured in any other way.

The S&F files are **not** available for reading. The S&F files can only be retrieved by the customer service.

Setting the log to debug mode will **not** write unmasked PAN to the log.

Requirement 2.5: Storage of cardholder data keys
1. What the requirement says

"Payment application must protect any keys used to secure cardholder data against disclosure and misuse"
2. How is this requirement met?
All keys in the terminal are stored in a secure part of the terminal. The application is never allowed access to keys. Key loading is handled in special secure environments. All key storage is performed according to industry standards including PCI PTS.
3. How should the merchant handle this?
No actions needed.

Requirement 2.6: Management of cardholder data protection keys
1. What the requirement says
"Payment application must implement key management processes and procedures for cryptographic keys used for encryption of cardholder data."
2. How is this requirement met?
The keys mechanism is based on a chain of trust were the most secure keys are loaded in a secure environment. The management of these keys follow specific procedures governed by the acquirer specifications and business standards such as PCI PTS.
3. How should the merchant handle this?
No actions needed.

Requirement 2.7: Cryptographic material removal
1. What the requirement says
"Securely delete any cryptographic key material or cryptogram stored by previous versions of
the payment application, in accordance with industry-accepted standards for secure deletion.
These are cryptographic keys used to encrypt or verify cardholder data."
2. How is this requirement met?
All cryptographic material must be removed to comply with PCI DSS. The removal of this material is automatically handled by the Westpay application so there is no need to re-encrypt historical data or take any action.
See chapter 5 for detailed information about key management and removal of cryptographic material.
3. How should the merchant handle this?
No actions needed.

User IDs, secure authentication and user access logging

Requirement 3: Provide secure authentication features
1. What the requirement says
Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.
2. How is this requirement met?
There is no user access to cardholder data allowed.
3. How should the merchant handle this?
No action needed.

Requirement 3.1: Unique user IDs and secure authentication for administrative access
1. What the requirement says
The "out of the box" installation of the payment application in place at the completion of the
installation process, must facilitate use of unique user IDs and secure authentication for all
administrative access and for all access to cardholder data.
2. How is this requirement met?
No administrative access to the application is available beside basic management/configuration.
3. How should the merchant handle this?
No action needed.

Requirement 3.2: Unique user IDs and secure authentication for access to servers etc
1. What the requirement says
Access to PCs, servers, and databases with payment applications must require a unique user ID and secure authentication.
2. How is this requirement met?
No administrative access to the application is available beside basic management/configuration.
3. How should the merchant handle this?
No action needed.

Requirement 4: Log payment application activity
1. What the requirement says
Logging mechanisms and the ability to track user activities are critical in preventing, detecting,or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.
2. How is this requirement met?
Logging is provided to the ECR. Logging levels are configurable via a management function from the ECR device. The amount of information captured may be varied but the logging can never be turned completely off. A Management functions exist to extract/deliver the log files to the ECR device. Integrators are responsible for the onward transportation and storage of the log files. Logging can not be disabled in the terminal.
3. How should the merchant handle this?
When integrating the Westpay application with the ECR, handling of logfiles according to this requirement should be properly implemented. For more information see chapter on logging in this document and Westpay application documentation (ref [4]).

Requirement 4.2: Implement automated audit trails
1. What the requirement says

Payment application must implement an automated audit trail to track and monitor access.
2. How is this requirement met?
Logging of audit trail is built in to the application.
3. How should the merchant handle this?
Logging need to be set up properly. See requirement 4 above.

Requirement 4.4: Centralized logging
1. What the requirement says
Payment application must facilitate centralized logging
2. How is this requirement met?
All logs are provided from the Westpay application to the ECR. The logfiles are provided in a basic text format that can be easily converted to the logformat of choice applicable in the merchant environment. All events needed to comply with this requirement are logged.
For terminals running in standalone mode using the POSInterface, logs are automatically compressed and sent up once per day to an ftp server the customer selects. This information needs to be provided to West prior to creating the release package.

In order to clean the logs from HTML formatting, the following can be removed:

Header:**<head><meta http-equiv="Content-Type" content="text/html; charset=utf-8"></head><body>**

Tags: **<font color='#FF2020'>, <b>, <font color='#D06060'>, <font color='#0000FF'>, </b>, </font>**, and **<br/>**

3. How should the merchant handle this?
When integrating the Westpay application with the ECR, handling of logfiles according to this requirement should be properly implemented. For more information see chapter on logging in this document and Westpay application documentation implementation handbook (see ref[4]) for more details.

Requirement 5.4: Protocols used
1. What the requirement says
"The payment application must only use or require use of necessary and secure services, protocols, daemons, components, and dependent software and hardware, including those provided by third parties, for any functionality of the payment application."
2. How is this requirement met?

The following service is the only ones provided by the Westpay application:Protocol	Description
EPAS retailer protocol	The ECR integration protocol provided as a TCP/IP socket service on port 3000
NEXO retailer protocol	The ECR integration protocol provided as a TCP/IP socket service on port 3000
Oracle OPI protocol	The ECR integration protocol provided as a TCP/IP socket service on port 8992
PAaS Interface	An ECR integration protocol provided as a library using Android intents.

3. How should the merchant handle this?
The merchant should interface these protocols according to the detailed descriptions in respective protocol specification or for PAaS on https://sdk.westpay.se

No other services are available from the terminal.

Requirement 6: Protect wireless transmissions

1. *What the requirement says*
   *"*For payment applications using wireless technology, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. The wireless technology must be implemented securely.*".*
2. *How is this requirement met?*
   By taking measures to set up a potential wireless network securely.
3. *How should the merchant handle this?*
   If the merchant is using wireless network within its business, make sure that firewalls are installed that deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the application environment. Please refer to the firewall man.

In case a wireless network is used, you must also make sure that:

- Encryption keys were changed from vendor defaults at installation.
- Encryption keys are changed anytime someone with knowledge of the keys leaves the company or changes position.
- Default SNMP community strings on wireless devices were changed.
- Default passwords/passphrases on access points were changed.
- Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks, for example IEEE 802.11i. Please note that the use if WEP as a security control was prohibited as of 30 June 2010.
- Other security related wireless vendor defaults were changed.
- When someone with knowledge of the values above leaves the company or changes position to a different position within the company these values must be changed.

What steps to take when changing these values:

- First of all its the merchants responsibility to consult their manual for their firewall and/or wireless access points to ensure they know what settings to change.
  - Enter the setup menu of the wireless gateway and consult the manual on how to edit the wireless settings for the affected network.
  - Make sure to change the encryption keys used to new keys (Please note that use of WEP keys are not allowed!!).
  - Change any SNMP communication strings to new values.
  - If needed, update the password for access to the wireless gateway if these values are know to the person that left.
  - Reboot the gateway if necessary.
- Enter the payment application setup menu. (information on how to access the menu on the different devices is found in the manual or quick start guide for the terminal)
  - Enter the new WiFi settings and connect the terminal to the new network.
  - SNMP strings are not used by the Westpay payment application.
  - Restart the terminal.

Ports used by the wireless networking component

When the terminal is connected wirelessly all traffic is routed via the wireless network. This includes authorization traffic, parameters and logging. (SPDH, PPL/FTP and HTTP (only in cases where its manually activated via the factory menu))
The wireless network in the terminal does not use or open any other ports than the ports used by the payment application. The only ports used currently for this is port 3000 for EPAS TCP/IP communication and port 80 for log extraction.

Requirement 6.2.c
1. What the requirement says
The implementation guide should instruct the customer how they use industry best practices for strong encryption and authentication
2. How is this requirement met?
By instructing the merchant to use highest possible security levels when configuring their wireless network
3. How should the merchant handle this?
It is suggested that the merchant follow these recommendations

- Change the default SSID to a 'Secure' SSID.
  Access points come with standard network names such as tsunami, default, link sys etc that broadcasts to clients to advertise the availability of the access point. <u>This should be changed as the first thing upon installation!</u>
- Use strong encryption and authentication.
  Default settings for most access points does not include any form of security being enabled. It is recommended that highest available over-the-air enterprise encryption and authentication is used. <u>This should be done immediately at installation!</u>
- Use WPA2 if possible or at least WPA encryption if WPA2 is not supported.
- Segment user populations using VLANs.
- Manage access to the firewalls, wireless gateways, access points etc in a secure manner.
- Physically secure the wireless access points. Preferably the access points could be placed above a suspended ceiling so that they are 'out of sight, out of mind'.

Requirement 7.2.3: Security of patches and updates

1. *What the requirement says?*
   How the vendor will communicate notifications of new patches and updates. How patches and updates will be delivered in a secure manner with a known chain of trust.
2. How is this requirement met?
   The customers will be informed when there is a new patch available via e-mail. The patch can be downloaded via an internal FTP or via the gateway PPL. The packages are signed to ensure that they have not been tampered with.
3. How should the merchant handle this?
   The merchant don't have to take any actions to ensure the integrity and security of the package.

Requirement 8.2: Facilitate secure network implementation

1. *What the requirement says*
   The payment application must be able to be implemented into a secure network environment. Application must not interfere with use of devices, applications, or configurations required for PCI DSS compliance.
2. *How is this requirement met?*
   By making sure the payment application does not use any conflicting components that would make the merchants PCI DSS compliance difficult.
3. *How should the merchant handle this?*
   The payment application does not rely on any none-secure protocols or functionality to allow for any functionality.
   The following services are used:

Protocol	Port	Protocol	Direction	Type of data sent
SPDH	6092, 55002 depending on processor	TCP	both	Authorization data encrypted by terminal encryption keys.
PPL	21, 55001 depending on processor	TCP	both	Swedish solution where files are sent over a plain ftp link but the files are all signed with secure keys
EPAS / NEXO	3000	TCP	both	EPAS / NEXO XML over TCP/IP
Logs	80	TCP	out only	Terminal log (only available after entering a randomized daily factory password)

FTP	21	TCP	out only	Upload of log files to local log files server
OPI	8992	TCP	both	Transaction data from the registry and fetching of table data to the terminal

Requirement 8.2.c: Hardware dependencies

1. *What the requirement says*
   What hardware platforms are supported?
2. *How is this requirement met?*
   By making sure the payment application does not run on any other components than the ones that are PCI DSS approved.
3. *How should the merchant handle this?*
   The payment application can only run on the hardware defined at the top of this page.

Data storage and application update

Requirement 9: Cardholder data must never be stored on a server connected to the Internet
1. What the requirement says
Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary
for the cardholder data environment. Limit inbound Internet traffic to IP addresses within the
DMZ. Do not allow internal addresses to pass from the Internet into the DMZ.
2. How is this requirement met?
The application is designed to operate behind a firewall
3. How should the merchant handle this?
The merchant must make sure that cardholder data is never stored on a server accessible from the Internet.

Requirement 10: Facilitate secure remote access to payment application
1. What the requirement says
These requirements handle updates via remote access to the payment application.
2. How is this requirement met?
No remote access to the payment application is allowed. Updates are provided via the secure PPL-protocol.The implementation of the PPL terminal management system should be included in a PCI DSS assessment.
3. How should the merchant handle this?
If the merchant host the PPL terminal management system (PPL TMS) it must be included in the PCI DSS assessment if not must the merchant make sure that the third party PPL TMS is implemented in a PCI DSS certified environment.

Sensitive traffic/access encryption

Requirement 11.1: Encrypt sensitive traffic over public networks
1. What the requirement says
If the payment application sends, or facilitates sending, cardholder data over public networks, the payment application must support use of strong cryptography and security protocols (for example, TLS, Internet protocol security (IPSEC), SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.
Examples of open, public networks that are in scope of the PCI DSS are:

- The Internet
- Wireless technologies
- Global System for Mobile Communications (GSM)
- General Packet Radio Service (GPRS).

2. How is this requirement met?
The application provides strong encryption of sensitive data according to specification from Swedish acquirers (see ref[1]). The application is not intended to send clear text cardholder data over public networks.
3. How should the merchant handle this?
The merchant should consult with the acquirer and a PCI QSA before considering sending transactions over public networks.

Requirement 11.2: Encrypt sensitive traffic in end user messages
1. What the requirement says
If the payment application facilitates sending of PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat), the payment application must provide a solution that renders the PAN unreadable or implements strong cryptography, or specify use of strong cryptography to encrypt the PANs.
2. How is this requirement met?
The Westpay application does not provide any end-user messaging technologies.
3. How should the merchant handle this?
No action is needed.

Requirement 12.1: Encrypt all non-console administrative access
1. What the requirement says
Instruct customers to encrypt all non-console administrative access with strong cryptography, using technologies such as SSH, VPN, or TLS for web-based management and other non-console administrative access.
2. How is this requirement met?
The PPL-protocol for distribution of parameters and software is implemented according to the specifications from acquirer. The terminal part of this protocol is implemented in this application and is part of the PA-DSS review.

3. How should the merchant handle this?
The remote (server) implementation of the PPL protocol should be included in a PCI DSS assessment.

Westpay application logging

There are four levels of logging provided within the application. The logging level is controlled from the ECR. The protocols that can be used for logging are defined in **Requirement 5.4.** Regardless of the logging level set, the following items are always logged:

Logged Information

- Type of the event
- Date and Time
- Source of the event (name of the program or module)
- User Identification (N/A for terminal payment application as there is no concept of authenticated users).
- Details of the event including the pass/fail status (e.g. for logon attempts this needs to record both successful and unsuccessful attempts).

Events to be logged:

- Logon attempts (in our case from the ECR and to the SPDH host).
- All actions (this shall include all requests from the ECR, financial transactions, management functions, logon etc).
- Changes to settings including the logging levels.
- Access to management functions (record when any of the management functions are executed, or attempted to be executed and failed password checks).
- Upgrades to PPL Files, Key files and software. Please ensure that the name (with version) of the PPL file is recorded. Unsuccessful loads must be recorded also.

Excluded Information

The information logged must exclude the card sensitive data. PANs may only be logged if shown in the obscured form (as would appear on a receipt). CVV2 and expiry date information must never be logged.

Log file transfer

If Westpay Payment Gateway is used all terminal logs are automatically uploaded to our centralized logging servers. This happens every time the log file is truncated driven by the log file size.

If the customer is using the terminals without Westpay Payment Gateway, they can use the logging facility in the terminal bu the following means:
Log files are delivered to an FTP sever within the ECR device (assumed to be on the same IP address and port 21).
The log file names are made up of the terminal number, date and time to provide a unique name. This ensures that log files from different terminals will all have a unique name, allowing the files to be placed on a central server.

Westpay application versioning

Each software release is identified with a version number.

Example release candidate: 2.0.0.101
Example patched version: 2.0.0.1
PCI version number for these releases: 2.0.*.*
The last two positions are considered wild-cards from a PCI perspective and will never be used to indicate changes with a security impact.

Product version [0-99]: 2
Major version [0-99]: 0
Minor version [0-99]: 0
Release candidate version/patch version [101-199] / [1-99]: 101/1

Product version (PCI High Impact Change)

The product version is only changed (if ever changed) on very big structural changes to the payment application and is probably driven by a strategical decision by management at West.

> ***If changes to the Payment Application meet any of the following criteria the released version must undergo a full PA-DSS Assessment:***
>
> - Four or more high-level PA-DSS Requirements are affected, not including Requirements 13 and 14.
> - Half or more of all PA-DSS Requirements/sub-Requirements are affected, not including Requirements 13 and 14.
> - Half or more of the Payment Application’s functionality is affected, or half or more of the Payment Application’s code-base is

changed.
- Addition of tested platform/operating system to include on the List of Validated Payment Applications or the change is otherwise ineligible for treatment as a Low Impact change.

For reference on the impacts you can find in the the requirement under 5.2.3.4 in the PA-DSS Program Guide.

Major version (PCI Low Impact Change)

The major version relates to changes in functionality relating to security or PCI. When this number is changed a minor or major PCI PA-DSS review is required.
PA-QSA Change Impact document required; may be eligible for delta assessment.

Low Impact changes are limited to changes to the Payment Application where all of the following conditions are met:

- Three or fewer high-level PA-DSS Requirements are affected, not including Requirements 13 and 14;
- Less than half of all PA-DSS Requirements/sub-Requirements are affected, not including Requirements 13 and 14; and
- Less than half the Payment Application’s functionality is affected and less than half the Payment Application’s code-base is changed.

For reference on the impacts you can find in the the requirement under 5.2.3.3 in the PA-DSS Program Guide.

Minor version (PCI No Impact Change)

The minor version changes when bugs and none-PCI related changes are done to the code. These changes does not trigger a new PCI PA-DSS audit and relates to one of the stars in the PA-DSS versioning.

> *Definition of No Impact Changes*
>
> No Impact changes are limited to changes that have no impact to PA-DSS Requirements or Payment Application security, PA-DSS related functions, tested platforms, operating systems or dependencies. Examples of No Impact changes include, but are not limited to user-interface changes, database-schema modifications, updates to reporting modules, and changing/deleting payment gateways.

For reference on the impacts you can find in the the requirement under 5.2.3.2 in the PA-DSS Program Guide.

Patch version / Release candidate version (PCI No Impact Change)

The last position is used for one of two purposes.

1. Defines if the release is a release candidate and if so, what release candidate version it is.
   Versions from 101 and up to 199 are all possible release candidate versions where the PA will recognize the last two digits as release candidate and will present it in the PA version as RC 99.
   The example above would be presented in the PA as 2.0.0 RC 1
2. Defines a patched version number used so that we when needed can patch software even if a later version has been released.
   The example above represents patch number 1 in version 2.0.0.1

For definition of No Impact change, see Minor version.

First release versions (PA-DSS version)

The first released PA-DSS version should always start at version 2 and patch version 0. The first version of for example 2.0 would then be made as 2.0.0.0.

Definitions and acronyms

West	Westpay AB	Acronyme for company name
Cardholder Data	PAN, Expiration Date, Cardholder Name and Service Code	As defined in the PCI DSS standard.
PCI DSS	Payment Card Industry Data Security Standard	Retailers that use applications to store, process or transmit payment card data are subject to the PCI DSS certification.

PA-DSS	Payment Application Data Security Standard	a standard for validation of payment applications that store, process or transmit payment card data. Applications that comply with PA-DSS have built in protection of card data and hereby facilitates for retailers to comply with PCI DSS
PAN	Primary Account Number	PAN, also called card number, is part of the magnetic stripe data and is also printed or embossed on the card. PAN can also be stored in the chip of the card.
ECR	Electronic Cash Register	
Sensitive Authentication Data	Magnetic Stripe Data, CVV2 and PIN as defined in PCI DSS	
CVV2	CVV2, CID, CAD, CVC2	Security codes