UNGERBOECK PA-DSS IMPLEMENTATION GUIDE

A guide for customers using Ungerboeck Software Credit Card module v20.90 to ensure a PCI compliant implementation in their environment

Successfully implementing Ungerboeck Software in a PCI Compliant environment.

Ungerboeck PA-DSS Implementation Guide

Table of Contents

UNGERBOECK SOFTWARE

i. Executive Summary

Ungerboeck Software has been Payment Application – Data Security Standard (PA-DSS) validated in accordance with PA-DSS Version 3.2. For the PA-DSS Assessment, we worked with the following PCI SSC approved Payment Application Qualified Security Assessor (PA-QSA):

Tevora
One Spectrum Pointe Drive, Suite 200
Lake Forest, California 92630
www.tevora.com

This document also explains the Payment Card Industry (PCI) initiative and the Payment Application Data Security Standard (PA-DSS) guidelines. The document then provides specific installation, configuration, and ongoing management best practices for using Ungerboeck Software Credit Card module v20.90 as a PA-DSS validated application operating in a PCI DSS compliant environment.

The following are related, online resources that can be used as supporting documentation.

1. PA-DSS Version 3.2
   https://www.pcisecuritystandards.org/documents/PA-DSS_v3-2.pdf
2. PCI DSS Version 3.2
   https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf
3. List of Validated Payment Applications
   https://www.pcisecuritystandards.org/assessors_and_solutions/payment_applications
4. PA-DSS Program Guide – Version 3.2

https://www.pcisecuritystandards.org/documents/PA-DSS-v3_2-Program-Guide.pdf

ii. Application Summary

Payment Application Name	Ungerboeck Software
Payment Application Version	20.90
Payment Application Description	Ungerboeck Software is a web-based enterprise-level event management system designed to manage large scale events and conferences. Ungerboeck Software facilitates all aspects of event management and coordination including scheduling, training, service and payment management. Ungerboeck Software Credit Card module v20.90 can accept both card-present and card-not-present transactions. The application does not support PIN-based debit transactions. For the purpose of settling transactions, the application can retain the PAN, expiration date and cardholder name (if configured to do so) in a SQL Server database using AES256 encryption. Cardholder data can be either swiped or manually entered into the application. When manually entered, card validation codes (CVV2, etc.), can be required. In the case of an on-premise environment, Ungerboeck Software Credit Card module v20.90 is only sold as a software package with the responsibility of hardware purchase left to the purchaser. Ungerboeck Software provides functionality within the application to enter sensitive cardholder information (such as credit card numbers) in specific fields

<table>
<tr><td></td><td>on the user interface. The form fields that are intended to receive this information are clearly labeled and are designed with specific security controls such as data masking in the form and encryption when at rest. Entering this sensitive cardholder information in any other field (for example, Note fields or other freeform text fields) does not provide it with these increased security controls and is not consistent with the requirements for protecting cardholder data as detailed in the Payment Card Industry Data Security Standards (PCI DSS).</td></tr>
<tr><td>Typical Role of Application</td><td>Ungerboeck Software Credit Card module v20.90 is a payment application used to process credit card transactions and handling authorization and settlement. Ungerboeck Software Credit Card module v20.90 can handle card-present and card-not-present transactions but not debit or other PIN-based transactions. The application consists of a browser-based client application, a server-based application, and a database. The application accepts cardholder data, including PAN, magnetic track and CVV2 codes directly through the client and pass through to the server which is used to facilitate the authorization of transactions through communications with the merchant's processor. The database stores cardholder data including the PAN, cardholder name, and expiration date only for the purpose of settlement of transactions, using AES256 encryption.</td></tr>
<tr><td>Target Market for Payment Application</td><td>Others (please specify): Large event locations such as stadiums, event halls, hotels, and large event coordinators.</td></tr>
<tr><td>Stored Cardholder Data</td><td>
<table>
<tr><th colspan="4">Encrypted Database Tables & Fields</th></tr>
<tr><th>Table Name</th><th>Field Name</th><th>Comment</th><th>Cryptography</th></tr>
<tr><td>AR020_TRANSACTIONS</td><td>AR020_CC_NBR_ENC</td><td>Credit Card Number</td><td>AES 256 Bit</td></tr>
<tr><td>AR020_TRANSACTIONS</td><td>AR020_CC_EXP_DATE_ENC</td><td>Credit Card Expiration Date</td><td>AES 256 Bit</td></tr>
<tr><td>CC341_CASH_BATCH_DTL</td><td>CC341_CC_NBR_ENC</td><td>Credit Card Number</td><td>AES 256 Bit</td></tr>
<tr><td>CC341_CASH_BATCH_DTL</td><td>CC341_CC_EXP_DATE_ENC</td><td>Credit Card Expiration Date</td><td>AES 256 Bit</td></tr>
<tr><td>EV891_TRANS_INFO</td><td>EV891_CC_NBR_ENC</td><td>Credit Card Number</td><td>AES 256 Bit</td></tr>
<tr><td>EV891_TRANS_INFO</td><td>EV891_CC_EXP_DATE_ENC</td><td>Credit Card Expiration Date</td><td>AES 256 Bit</td></tr>
<tr><td>AR005_TRANS_TYPES</td><td>AR005_CC_MERCH_ID</td><td>Merchant ID</td><td>AES 128 Bit</td></tr>
<tr><td>AR005_TRANS_TYPES</td><td>AR005_CC_AUTH_USER</td><td>Authorized Merchant User ID</td><td>AES 128 Bit</td></tr>
<tr><td>AR005_TRANS_TYPES</td><td>AR005_CC_AUTH_PWD</td><td>Authorized Merchant User Password</td><td>AES 128 Bit</td></tr>
<tr><td>AR050_CC_AUTH_SPECS</td><td>AR050_CC_MERCH_ID</td><td>Merchant ID</td><td>AES 128 Bit</td></tr>
<tr><td>AR050_CC_AUTH_SPECS</td><td>AR050_CC_AUTH_USER</td><td>Authorized Merchant User ID</td><td>AES 128 Bit</td></tr>
<tr><td>AR050_CC_AUTH_SPECS</td><td>AR050_CC_AUTH_PWD</td><td>Authorized Merchant User Password</td><td>AES 128 Bit</td></tr>
</table>
</td></tr>
<tr><td>Output Location for Logs Related to the Application</td><td>Two levels of logging exist within the Ungerboeck Software application:

MM999_AUDIT_LOG – Contains all configured tracking of base transactions in the application.

MM995_CC_AUDIT_LOG – Contains all tracking of credit card information access in the application.</td></tr>
</table>

Required Components of the Payment Application	Ungerboeck Software is a web-based application that is designed for Microsoft Internet Explorer and Google Chrome browsers. There are three main components: The browser client component which runs on Microsoft Internet Explorer or Google Chrome browsers, the application server component which typically runs on Windows Server 2012R2 or 2016 and the database server component which runs on Windows Server 2012R2 or 2016 and Microsoft SQL Server 2012, 2014, or 2016. The application requires the database server to run Microsoft SQL Server 2012, 2014, or 2016.
Required 3rd Party Payment Application Software	None
Database Software Supported	Microsoft SQL Server 2012 Microsoft SQL Server 2014 Microsoft SQL Server 2016
Required Other 3rd Party Software	Microsoft Silverlight 5 Microsoft .NET Framework 4.5
Supported Operating System(s)	Microsoft Windows Server 2012R2 Microsoft Windows Server 2016 Microsoft Windows 7 SP1 Microsoft Windows 8.1 Microsoft Windows 10
Application Authentication	Authentication to the application can be configured using a 3rd-party Active Directory (AD) service or authenticating within the application. During the authentication process, clear text credentials are not sent over the network. All communication including authentication traffic is done over HTTPS/TLS 1.2.
Application Functionality Supported	Card-Present, Card-Not-Present
Payment Processing Connections	Ungerboeck Software Credit Card module v20.90 does not have any specific connections but instead provides functionality to connection to the customer's desired payment gateway.
Description of Listing Version Methodology	The Ungerboeck Software application uses the following versioning methodology:  Major Release: Indicates a significant change in one or more core areas of the application. Also used to indicate a technology shift in the application. Minor Release: Indicates a minor change in one or more core areas of the application and/or a major change in a non-core area of the application. Service Release: Contains all minor enhancements and corrections that were implemented after the Minor Release was issued. Hot Fix Release: Contains all corrections that were implemented since the last Service Release was issued. Security-impacting enhancements will be issued in Minor Releases and will be revalidated according to PA-DSS requirements. Security-impacting corrections will be issued in Hot Fix Releases as soon as they are available.
Additional Post-Installation & Configuration Steps	1. Change the encryption key on an annual basis or whenever an individual who has direct access to the key leaves the organization (Section 3.14).

	2. Purge cardholder data on a regular basis when it is no longer needed for legal, regulatory, or business purposes. (Section 4.2)

1. Introduction

1.1 Purpose and Content

The information contained herein is intended to apply to the latest PA-DSS data security regulations and guidelines in effect as of May 2016 (PA-DSS version 3.2). This guide is intended to assist in implementing Ungerboeck Software in a manner that is compliant with these PA-DSS regulations and guidelines

1.2 Understanding the Relationship between PCI DSS and PA-DSS

It is important to understand that the PCI compliance programs governing data security, generally referred to as the Payment Card Industry (PCI) standards, are directed at entities that receive, store or transmit payment information. This means they apply, for example, to merchants and service providers (like gateways and processing companies), but do not apply to software providers like Ungerboeck Software International. A separate program called PA-DSS applies to software providers. Ungerboeck Software International does not have the ability or the authority to deem a merchant PCI compliant. Each merchant must make their own determination as to the creation of a PCI DSS compliant environment. Please refer to the www.pcisecuritystandards.org website for additional information on PCI DSS compliance.

Ungerboeck Software has been developed for use in a PCI DSS compliant environment. Independent, third-party validation of the Ungerboeck Software development process as well as the actual Ungerboeck Software application has been conducted by a QSA (Qualified Security Assessor) qualified to conduct PA-DSS assessments (Tevora Business Solutions – www.tevora.com).

Version 20.9 of the Ungerboeck Software Credit Card module has been validated as PA-DSS compliant.

1.3 Supporting Documentation

The following are related, online resources that can be used as supporting documentation.

1. PA-DSS Version 3.2
   https://www.pcisecuritystandards.org/documents/PA-DSS_v3-2.pdf
2. PCI DSS Version 3.2
   https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf
3. List of Validated Payment Applications
   https://www.pcisecuritystandards.org/assessors_and_solutions/payment_applications
4. PA-DSS Program Guide – Version 3.2
   https://www.pcisecuritystandards.org/documents/PA-DSS-v3_2-Program-Guide.pdf

UNGERBOECK SOFTWARE

2. Upgrading Ungerboeck Software

2.1 Hardware & Software Minimum Requirements

The minimum hardware and software requirements for running Ungerboeck Software can be found in the Technology Guidelines document on the Ungerboeck Support Center site (supportcenter.ungerboeck.com)

2.2 Required Downloads for Upgrading Ungerboeck Software

All of the required files can be obtained from the Support Downloads page of the Ungerboeck Support Center using the login credentials provided to you.

Reference: PA-DSS v3.2 Requirement #7.2.3 Software vendors must establish a process for timely development and deployment of security patches and upgrades.

Updates to Ungerboeck Software are provided on a regular basis via the Ungerboeck Support Center website (http://supportcenter.ungerboeck.com). Any update downloaded from the website should be verified to ensure the integrity of the update package.
For each update downloaded, an MD5 hash value is generated. These values for all update downloads can be found in their respective download directory.

Before applying any updates, validate the authenticity of the files by using the File Checksum Integrity Verifier (FCIV) application from Microsoft.

Download Details:
The Microsoft File Checksum Integrity Verifier (FCIV) can be found at the following location:

http://www.microsoft.com/downloads/details.aspx?FamilyID=b3c93558-31b7-47e2-a663-7365c1686c08&DisplayLang=en

Usage:
1. Download and install the FCIV application.
2. Download the desired update file from the Ungerboeck Support Center website. Do not apply it yet.
3. From a command line, type: "fciv <filename>" where <filename> is the full path and name of the Ungerboeck Software update file.
4. The output will be a long string of numbers and letters (MD5 hash value).
5. Compare this long string with the value published on the Verify Downloads page of the Ungerboeck Support Center website.
6. If the two strings do not match, do not apply the update file and contact Ungerboeck Support instead.

Example:

C:\>fciv C:\Download\U1710J_NewGen.zip
79ac8d043dc8739f661c45cc33fc07ac C:\Download\U1710J_NewGen.zip

3. Procedures for PA-DSS Compliance

3.1 Deleting sensitive authentication data stored by previous application versions

Reference: PA-DSS v3.2 Requirement #1.1.4
Securely delete any track data (from the magnetic stripe or equivalent data contained on a chip), card verification values or codes, and PINs or PIN block data stored by previous versions of the payment application, in accordance with industry-accepted standards for secure deletion, as defined, for example by the list of approved products maintained by the National Security Agency, or by other State or National standards or regulations.

Ungerboeck Software does NOT allow for the collection of sensitive authentication data.

To properly secure the Ungerboeck Software application in compliance with PA-DSS requirements, configure the application to only allow HTTPS communication. To do this, run the UngerboeckWebConfiguration.exe and check the 'Enable HTTPS' checkbox on the Application Settings tab.

3.2 Deleting sensitive authentication data gathered through troubleshooting

Reference: PA-DSS v3.2 Requirement #1.1.5
Do not store sensitive authentication data on vendor systems. If any sensitive authentication data (pre-authorization data) must be used for debugging or troubleshooting purposes, ensure the following:

- Sensitive authentication data is collected only when needed to solve a specific problem.
- Such data is stored in a specific, known location with limited access.
- The minimum amount of data is collected as needed to solve a specific problem.
- Sensitive authentication data is encrypted with strong cryptography while stored.
- Data is securely deleted immediately after use, including from:
    - Log files
    - Debugging files
    - Other data sources received from customers.

Ungerboeck Software does NOT allow for the collection of sensitive authentication data, even for troubleshooting purposes.

To properly secure the Ungerboeck Software application in compliance with PA-DSS requirements, configure the application to only allow HTTPS communication. To do this, run the UngerboeckWebConfiguration.exe and check the 'Enable HTTPS' checkbox on the Application Settings tab.

3.3 Securely implement wireless technology

Reference: PA-DSS v3.2 Requirement #6.1 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.

If wireless is used within the payment application environment that Ungerboeck Software is deployed on, ensure that a stateful inspection firewall is between the wireless network and all networks and systems that store, processes, or transmit cardholder data.

Change your vendor default configurations and passwords for SSID, Administrator Account(s), and encryption keys.

3.4 Secure transmission of cardholder data over wireless networks

Reference: PA-DSS v3.2 Requirement #6.2 For payment applications using wireless technology, payment application must facilitate use of industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. **Note:** The use of WEP as a security control is prohibited.

If wireless is used within the payment application environment that Ungerboeck Software is deployed on, ensure that secure, encrypted remissions are implemented. Configure appropriate wireless encryption using appropriate wireless encryption technologies such as WPA, WPA 2, IPSEC, SSL, or TLS.

Disable SSID Broadcasts as well as all console administration of wireless access points. Configure secure administration of wireless access points. Administration protocols should be limited to SSL and SSH.

3.5 Store cardholder data only on servers not connected to the Internet

Reference: PA-DSS v3.2 Requirement #9.1 The payment application must be developed such that any web server and any cardholder data storage component (for example, a database server) are not required to be on the same server, nor is the data storage component required to be on the same network zone (such as a DMZ) with the web server.

Ungerboeck Software does not require any data storage in the DMZ or on Internet-accessible systems. If Ungerboeck Software is deployed on a system that is accessible from the internet, the Web Server, and the Database Server cannot be on the same server. The Web Server should be placed in the DMZ; segmented from the Database Server using a stateful inspection firewall. The Database Server should not be accessible from the internet. Ungerboeck Software has been developed so as not to require that the Database Server and Web Server be on the same server.

3.6 Securely implement remote access software

Reference: PA-DSS v3.2 Requirement #10.2
Any remote access into the payment application must be performed securely.

In the case of vendor remote access accounts, in addition to the standard access controls, vendor accounts should only be active while access is required to provide service. Access rights should include only the access rights required for the services being rendered, and it should be robustly audited.

If users and hosts within the payment application environment need to use third-party remote access software such as Remote Desktop/Terminal Server (RDP/TS), Virtual Network Computing (VNC), etc. to access other hosts within the payment processing environment, special care must be taken.

To be compliant, every such session must be encrypted with at least 128-bit encryption and must satisfy the requirement for multi-factor authentication for users connecting from outside the payment processing environment. For RDP/TS this means using the high encryption setting on the server and for VNC it means using symmetric or public key options for encryption. Additionally, the PCI user account and password requirements will apply to these access methods as well.

To securely implement remote-access software, perform the following steps:

- Change default settings in the remote-access software (i.e. change default passwords and use unique passwords for each customer).
- Allow connections only from specific (known) IP/MAC addresses.
- Use strong authentication and complex passwords for logins (See PA-DSS Requirements 3.1.1 through 3.1.11).
- Enable encrypted data transmission according to PA-DSS Requirement 12.1.
- Enable account lockout after a certain number of failed login attempts (See PA-DSS Requirements 3.1.9 through 3.1.10).
- Establish a VPN connection via a firewall before access is allowed.
- Enable the logging function.
- Restrict access to customer environments to authorized integrators/resellers personnel.

3.7 Secure transmissions of cardholder data over public networks

Reference: PA-DSS v3.2 Requirement #11.1
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 to safeguard sensitive cardholder data during transmission over open, public networks, including at least the following:

- Only trusted keys and certificates are accepted.
- The protocol in use only supports secure versions or configurations
- The encryption strength is appropriate for the encryption methodology in use

Note: SSL and early TLS are not considered strong cryptography. Payment applications must not use, or support the use of, SSL or early TLS. Applications that use or support TLS must not allow fallback to SSL.

Examples of open, public networks include but are not limited to:
- The Internet
- Wireless technologies, including but not limited to 802.11 and Bluetooth
- Cellular technologies, for example, Global System for Mobile Communications (GSM), Code division multiple access (CDMA)
- General Packet Radio Service (GPRS)
- Satellite communications

Configure the Ungerboeck Software web server to require TLS 1.2. Ungerboeck Software allows data transmission over public networks. When deployed to allow for data transmission over public networks, proper encryption technologies should be used to protect the transmission such as TLS 1.2 or IPSEC VPN. Ungerboeck Software natively supports the encryption of cardholder data prior to transmission via TLS 1.2 encryption.

To configure the Ungerboeck Software web server with TLS 1.2, make sure you have Microsoft Windows Server 2012 R2 or 2016 installed with all of the latest critical and security updates. Both of these versions have TLS 1.2 enabled automatically.

To ensure that TLS 1.2 is enabled, please check the following registry entries:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client\DisabledByDefault
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server\DisabledByDefault
```

Both of these should have a value of zero (0).

Also check the following registry entries:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client\Enabled
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server\Enabled
```

Both of these should have a value of one (1).

If you find this is not the case, make sure you have the latest critical and security updates installed.

3.8 Encrypt Cardholder Data sent over end-user messaging technologies

Reference: PA-DSS v3.2 Requirement #11.2
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.

Ungerboeck Software does not natively support messaging of PANS.

3.9 Encrypt non-console administrative access

Reference: PA-DSS v3.2 Requirement #12.1
If the payment application facilitates non-console administrative access, encrypt all such access

with strong cryptography.

Note:
- Clear-text protocols such as Telnet or rlogin must never be used for administrative access.
- SSL and early TLS are not considered strong cryptography. Payment applications must not use, or support the use of, SSL or early TLS. Applications that use or support TLS must not allow fallback to SSL.

Use appropriate encryption technologies for any non-console administration of Ungerboeck Software servers. Ungerboeck Software supports VPN encryption of any non-console administrative access by use of Site to site encryption, Remote access VPN network client, or PPTP with Microsoft Point-To-Point Encryption (MPPE).

3.10 Establish minimum acceptable password policies and practices

Reference: PA-DSS v3.2 Requirement #3.1
The payment application must support and enforce the use of unique user IDs and secure authentication for all administrative access and for all access to cardholder data. Secure authentication must be enforced to all accounts generated or managed by the application by the completion of installation and for subsequent changes after installation.

Notes:
- The term "subsequent changes" as used throughout Requirement 3 refers to any application changes that result in user accounts reverting to default settings, changes to existing account configurations, and changes that generate new accounts or recreate existing accounts.
- These password controls are not intended to apply to personnel who only have access to one card number at a time to facilitate a single transaction. These controls are applicable for access by personnel with administrative capabilities, for access to systems with cardholder data, and for access controlled by the payment application.
- This requirement applies to the payment application and all associated tools used to view or access cardholder data.

The Ungerboeck database is shipped with the USIADMIN user account already configured. It is recommended that this account not be used by your application administrators and instead create unique Administrator accounts for each application administrator.

The password policy for accessing the Ungerboeck application can be configured within the application if no other authentication (i.e. Active Directory, SSO, etc.) is being used. The minimum configuration should require the following:

- Passwords should be at least seven characters in length
- Passwords should have both a numeric and alphabetic character included in them
- Password changes should be required at least once every 90 days.
- Passwords cannot be set to one of the last four previously used values
- User Accounts should be locked after 6 invalid login attempts

- Locked User Accounts should remain locked for at least 30 minutes unless manually unlocked by an Administrator
- Sessions idle for more than 15 minutes should require re-authentication by the user

Likewise, user accounts accessing the systems on which the Ungerboeck Software application or its database are kept should use unique user IDs for each user account. Also, the following minimum user account security configuration should be followed:

- Passwords should be at least seven characters in length
- Passwords should have both a numeric and alphabetic character included in them
- Password changes should be required at least once every 90 days.
- Passwords cannot be set to one of the last four previously used values
- User Accounts should be locked after 6 invalid login attempts
- Locked User Accounts should remain locked for at least 30 minutes unless manually unlocked by an Administrator
- Sessions idle for more than 15 minutes should require re-authentication by the user

3.11 Securely display sensitive cardholder information

Reference: PA-DSS v3.2 Requirement #2.2
Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.

Note: This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.

Ungerboeck Software is shipped with the display of PAN information limited to the first two and last four digits. Those users with legitimate business reasons for seeing the full PAN can be configured to do so through the Organization Access Privilege – Access to Credit Card Numbers. This dialog can be accessed through the **Organization Administration** module and the **'Access Privileges'** option.

The displays that are affected by this privilege are as follows:

Add/Edit Deposit	Edit Credit Card Information
Add/Edit Cash Application	Edit Service Order
Cash Batch Transactions	Edit Registration Order
A/R Transaction Inquiry	Edit Fulfillment Order
Cash Application	Invoice Register
Receipt Reconciliation	Edit Standing Membership Order
Customer Payment Plans	Add/Edit Account
Add/Edit Payment	

No reports in the system display the full PAN information and, therefore, are not affected by this privilege.

3.12 Securely store sensitive cardholder data within the application

Reference: PA-DSS v3.2 Requirement #2.3
Render PAN unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs) by using any of the following approaches:

- One-way hashes based on strong cryptography (hash must be of the entire PAN)
- Truncation (hashing cannot be used to replace the truncated segment of PAN)
- Index tokens and pads (pads must be securely stored)
- Strong cryptography with associated key-management processes and procedures.

PAN information stored in the database is rendered unreadable through the use of strong cryptography. Upon initial install of the software, the Administrator should change the encryption keys from their default, shipped values using the **'Create Credit Card Encryption Key'** option in the **System Administration** module. Details on using this option are available in section 3.14 of this document.

3.13 Secure keys used to protect sensitive cardholder data within the application

Reference: PA-DSS v3.2 Requirement #2.4
Payment application must protect keys used to secure cardholder data against disclosure and misuse.

Note: This requirement applies to keys used to encrypt stored cardholder data, as well as to key-encrypting keys used to protect data-encrypting keys. Such key-encrypting keys must be at least as strong as the data-encrypting key.

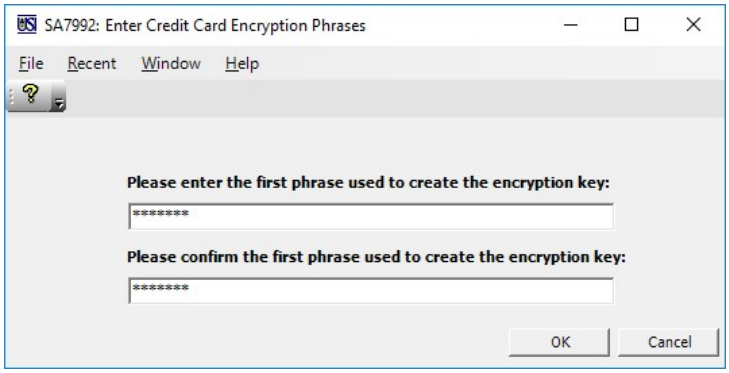
The keys used to encrypt the sensitive cardholder data within the Ungerboeck Software application are not accessible and therefore are adequately protected against disclosure or misuse.

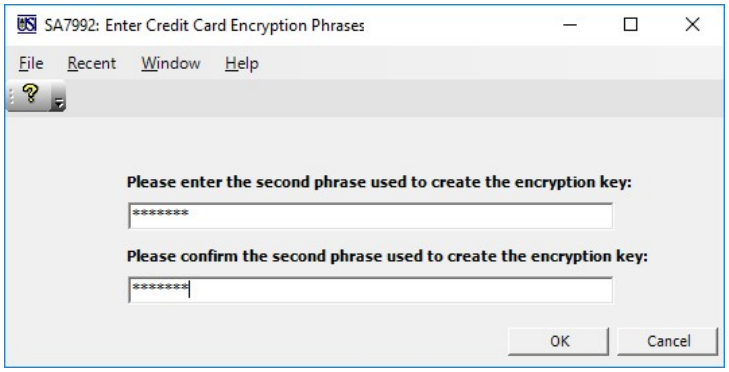
3.14 Implement key-management processes to application secure encryption keys

Reference: PA-DSS v3.2 Requirement #2.5
Payment application must implement key-management processes and procedures for cryptographic keys used for encryption of cardholder data.

Upon initial install of the software, the Administrator should change the encryption keys from their default, shipped values using the **'Create Credit Card Encryption Key'** option in the **System Administration** module.

This option provides a process that supports a Separation of Duties practice whereby two individuals independently supply a word or phrase that, when combined with additional information, are used to generate a unique encryption key for the sensitive cardholder data stored in Ungerboeck Software for your site.





It is recommended that the encryption key be changed on an annual basis or whenever an individual that has direct access to the key is no longer with the organization.

3.15 Secure keys used to protect sensitive cardholder data within the application

Reference: PA-DSS v3.2 Requirement #2.6
Provide a mechanism to render irretrievable any cryptographic key material or cryptogram stored by the payment application, in accordance with industry-accepted standards.

These are cryptographic keys used to encrypt or verify cardholder data.

Note: This requirement applies only if the payment application uses, or previous versions of the payment application used, cryptographic key materials or cryptograms to encrypt cardholder data.

The Administrator can change the encryption keys using the **'Create Credit Card Encryption Key'** option in the **System Administration** module. When the encryption key used to secure cardholder data within Ungerboeck Software is changed, the previous key is overwritten by the new key and therefore is no longer present.

Please note that changing the key affects the current data only. Previous backups are not affected and will continue to use the key value configured at the time the backup was made.

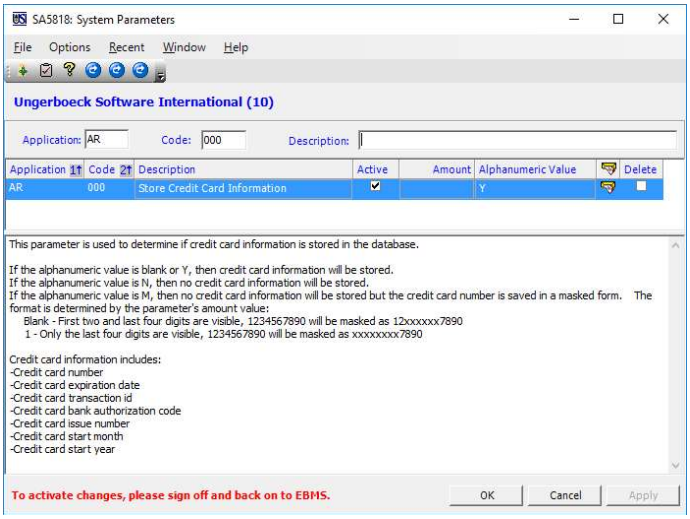
4. PA-DSS Maintenance

After you have successfully upgraded your Ungerboeck Software installation, ongoing maintenance of your environment will be necessary to ensure compliance.

4.1 Implement Audit Trails

Reference: PA-DSS v3.2 Requirement #4.1
At the completion of the installation process, the "out of the box" default installation of the payment application must log all user access and be able to link all activities to individual users.

If your organization has elected to store credit card information in Ungerboeck Software, the application will need to track whenever this information is accessed. This tracking is done through the Credit Card Audit logs. These logs are automatically activated if Ungerboeck Software is configured to store allowed credit card information. To activate the storage of allowed credit card information in the application, place a Y in the alphanumeric value field of the AR 000 system parameter. The System Parameters dialog can be accessed from the **System Administration** module under the option '**System Parameters**.'



Once credit card information storage is activated, the Credit Card Audit Log cannot be disabled.

In addition to the Credit Card Audit logs in Ungerboeck Software, the Windows Audit Logs should be activated on all application servers:

From the start menu navigate to **Settings → Control panel → Local security policy**

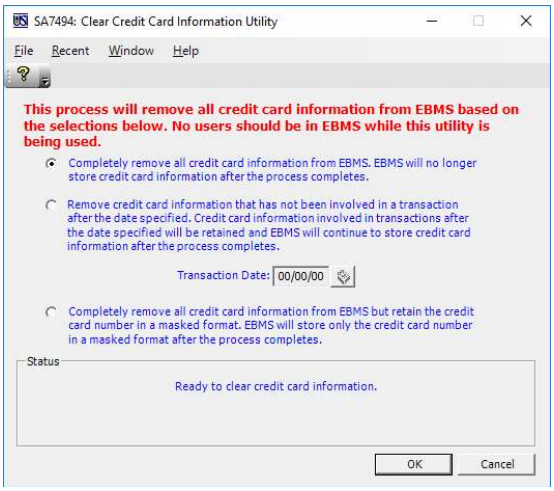
Under security settings, navigate to **Account policies → Audit Policy**

Ensure that the following parameters are set: Account Logon Events: Success, Failure

4.2 Purge Cardholder Data after customer-defined retention period

Reference: PA-DSS v3.2 Requirement #2.1
Software vendor must provide guidance to customers regarding secure deletion of cardholder data after expiration of customer-defined retention period.

Ungerboeck Software includes a utility for purging of Credit Card data to support customer-defined retention policies. The Clear Credit Card Information Utility can be found in Ungerboeck Software under: **System Administration → Clear Credit Card Information Utility**



It is recommended that all cardholder data should be deleted when it is no longer needed for legal, regulatory, or business purposes.

Please note that any database backups or test environments will contain cardholder data unless removed using the purge process identified above. If you elect to leave the cardholder data in these copies, the environments in which they reside must be properly secured in order to remain in compliance.

Cardholder data is encrypted using a strong encryption process and stored in the following database locations:

Encrypted Database Tables & Fields			
Table Name	**Field Name**	**Comment**	**Cryptography**
AR020_TRANSACTIONS	AR020_CC_NBR_ENC	Credit Card Number	AES 256 Bit
AR020_TRANSACTIONS	AR020_CC_EXP_DATE_ENC	Credit Card Expiration Date	AES 256 Bit
CC341_CASH_BATCH_DTL	CC341_CC_NBR_ENC	Credit Card Number	AES 256 Bit
CC341_CASH_BATCH_DTL	CC341_CC_EXP_DATE_ENC	Credit Card Expiration Date	AES 256 Bit
EV891_TRANS_INFO	EV891_CC_NBR_ENC	Credit Card Number	AES 256 Bit
EV891_TRANS_INFO	EV891_CC_EXP_DATE_ENC	Credit Card Expiration Date	AES 256 Bit
AR005_TRANS_TYPES	AR005_CC_MERCH_ID	Merchant ID	AES 128 Bit
AR005_TRANS_TYPES	AR005_CC_AUTH_USER	Authorized Merchant User ID	AES 128 Bit
AR005_TRANS_TYPES	AR005_CC_AUTH_PWD	Authorized Merchant User Password	AES 128 Bit
AR050_CC_AUTH_SPECS	AR050_CC_MERCH_ID	Merchant ID	AES 128 Bit
AR050_CC_AUTH_SPECS	AR050_CC_AUTH_USER	Authorized Merchant User ID	AES 128 Bit
AR050_CC_AUTH_SPECS	AR050_CC_AUTH_PWD	Authorized Merchant User Password	AES 128 Bit

4.3 Cycle encryption keys for securing sensitive cardholder information

Reference: PA-DSS v3.2 Requirement #2.3
Render PAN unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs) by using any of the following approaches:

- One-way hashes based on strong cryptography (hash must be of the entire PAN)
- Truncation (hashing cannot be used to replace the truncated segment of PAN)
- Index tokens and pads (pads must be securely stored)
- Strong cryptography with associated key-management processes and procedures.

PAN information stored in the database is rendered unreadable through the use of strong cryptography. Upon initial install of the software, the Administrator should change the encryption keys from their default, shipped values using the **'Create Credit Card Encryption Key'** option in the **System Administration** module.

This option provides a process that supports a Separation of Concerns practice whereby two individuals independently supply a word or phrase that when combined are used to generate the encryption key for the sensitive cardholder data in Ungerboeck Software.

It is highly recommended that access to the encryption key process be restricted to the fewest number of custodians necessary.

4.4 Export log information for use in a centralized logging system

Reference: PA-DSS v3.2 Requirement #4.4
Payment application must facilitate centralized logging.

Note: Examples of this functionality may include, but are not limited to:

- Logging via industry standard log file mechanisms such as Common Log File System (CLFS), Syslog, delimited text, etc.
- Providing functionality and documentation to convert the application's proprietary log format into industry standard log formats suitable for prompt, centralized logging.

The Ungerboeck Software application uses an audit log process that tracks all required information regarding access and modification of sensitive cardholder data. If you wish to use this log information in a centralized logging system, it is recommended that you export the log information from table MM995_CC_AUDIT_LOG and import it into your system.

To automate this process, Microsoft provides SQL Server Integration Services (SSIS). A step-by-step walkthrough is provided by Microsoft at the following link:

https://docs.microsoft.com/en-us/sql/integration-services/ssis-how-to-create-an-etl-package

4.5 Application Versioning

Reference: PA-DSS v3.2 Requirement #5.5.4
The payment application vendor must document and follow a software-versioning methodology as part of their system development lifecycle.

The Ungerboeck Software application uses the following versioning methodology:

Major Release: Indicates a significant change in one or more core areas of the application. Also used to indicate a technology shift in the application.

Minor Release: Indicates a minor change in one or more core areas of the application and/or a major change in a non-core area of the application.

Service Release: Contains all minor enhancements and corrections that were implemented after the Minor Release was issued.

Hot Fix Release: Contains all corrections that were implemented since the last Service Release was issued.

Security impacting enhancements will be issued in Minor Releases and will be revalidated according to PA-DSS requirements. Security impacting corrections will be issued in Hot Fix Releases as soon as they are available.

4.6 Required software and hardware services and components

Reference: PA-DSS v3.2 Requirement #8.2
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.

Note: SSL and early TLS are not considered strong cryptography. Payment applications must not use, or support the use of, SSL or early TLS. Applications that use or support TLS must not allow fallback to SSL.

The Ungerboeck Software application does not use any third-party components or any dependent software and hardware for its payment application. It does not hard-code any port numbers for making web requests. The default port for making HTTPS requests is 443. The Ungerboeck Software application does require and fully support TLS 1.2 for secure communication.

The secure services and components for both software and hardware that the Ungerboeck Software application requires can be found in the Ungerboeck Software Technology Guidelines document. Please contact Client Care for the appropriate version of this document.

Appendix A: Key Terms

AES	Abbreviation for "Advanced Encryption Standard." Block cipher used in symmetric key cryptography adopted by NIST in November 2001 as U.S. FIPS PUB 197 (or "FIPS 197").
Card Verification Code or Value	Also known as Card Validation Code or Value, or Card Security Code. Refers to either: (1) magnetic-stripe data, or (2) printed security features. 1. Data element on a card's magnetic stripe that uses secure cryptographic processes to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as CAV, CVC, CVV, or CSC depending on payment card brand. The following list provides the terms for each card brand: • **CAV –** Card Authentication Value (JCB payment cards) • **PAN CVC –** Card Validation Code (MasterCard payment cards) • **CVV –** Card Verification Value (Visa and Discover payment cards) • **CSC –** Card Security Code (American Express) 2. For Discover, JCB, MasterCard, and Visa payment cards, the second type of card verification value or code is the rightmost three-digit value printed in the signature panel area on the back of the card. For American Express payment cards, the code is a four-digit unembossed number printed above the PAN on the face of the payment cards. The code is uniquely associated with each individual piece of plastic and ties the PAN to the plastic. The following list provides the terms for each card brand: • **CID –** Card Identification Number (American Express and Discover payment cards) • **CAV2 –** Card Authentication Value 2 (JCB payment cards) • **PAN CVC2 –** Card Validation Code 2 (MasterCard payment cards) • **CVV2 –** Card Verification Value 2 (Visa payment cards)
Complex Password	A complex password is made up of at least 8 characters, consisting of one alphabet character, one numeric character, one special character, and no dictionary words.
Encryption	Process of encoding data so that it is unreadable to those without the proper permissions or "key" to decode it.
Merchant	For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.
Multi-Factor Authentication	Method of authenticating a user whereby at least two factors are verified. These factors include something the user has (such as a smart card or dongle), something the user knows (such as a password, passphrase, or

	PIN) or something the user is or does (such as fingerprints, other forms of biometrics, etc.).
PA-DSS	Acronym for Payment Application Data Security Standard PA-DSS is a PCI Security Standards Council standard for validation of payment processing applications such as Point-of-Sale. PA-DSS compliant applications have built-in card protection features, and provide tools and information to help retailers comply with PCI DSS. Ungerboeck Software is considered a payment application because it provides features that allow payment processing and the collection of credit card information.
PAN	Acronym for "Primary Account Number." It is also referred to as "Account Number." It is a unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.
PCI DSS	Acronym for Payment Card Industry Data Security Standard. Retailers that use applications, like Point-of-Sale, to process, store, or transmit payment card data to authorize or settle transactions are subject to this standard. This standard applies more to the environment in which credit card information is collected. Ungerboeck Software is one part of this environment. Other aspects may include but are not limited to web servers, network protocols, staff, and internal policies and procedures.
PIN	Acronym for "Personal Identification Number." Secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provided matches the PIN in the system. Typical PINs are used for automated teller machines for cash advance transactions. Another type of PIN is one used in EMV chip cards where the PIN replaces the cardholder's signature.
SSL	Acronym for Secure Sockets Layer. Industry standard that encrypts the channel between a web browser and web server. Now superseded by TLS. See TLS.
TLS	Acronym for "Transport Layer Security." Designed with goal of providing data secrecy and data integrity between two communicating applications. TLS is successor of SSL.
Track Data	Also referred to as "full track data" or "magnetic-stripe data." Data encoded in the magnetic stripe or chip used for authentication and/or authorization during payment transactions. Can be the magnetic-stripe image on a chip or the data on the track 1 and/or track 2 portion of the magnetic stripe.
Triple DES (3DES or TDES)	3DES is an encryption algorithm using 3 separate 56-bit DES keys. In this implementation, 3DES is used to securely transmit create credit transaction data between Kiosks.
VPN	Acronym for "virtual private network." A computer network in which some of connections are virtual circuits within some larger network, such as the Internet, instead of direct connections by physical wires. The end points of the virtual network are

	said to be tunneled through the larger network when this is the case. While a common application consists of secure communications through the public Internet, a VPN may or may not have strong security features such as authentication or content encryption. A VPN may be used with a token, smart card, etc., to provide two-factor authentication.

Additional PCI and PA-DSS terms can be found on the PCI Council website at:

https://www.pcisecuritystandards.org/documents/PCI_DSS_Glossary_v3-2.pdf