Applies to:
SAP POS Data Management (SAP POS DM) BI CONT 7.0.3 and SAP ECC 6.0. For more information, visit the Business Process Expert homepage.

Summary
PCI Security Standards require strict compliance from merchants, vendors and software vendors. The purpose of this article is to provide a background on PCI requirements and the functionality within SAP POS DM and SAP ECC 6.0 to assist customers in adhering to these standards.

Author: David Mick
Company: SAP Retail Group
Created on: July 15, 2009

Author Bio
David Mick is a Managing Principal Consultant for POS Data Management with the SAP Retail Group. David joined SAP in 1998 and has been focused in POS DM and SAP Retail POS Inbound and Outbound Interfaces. David’s responsibilities include managing & building the POS DM practice as well as carrying out projects and supporting in POS SDM presales phases.
# Table of Contents

Introduction .......................................................................................................................................................... 3

PCI Background ................................................................................................................................................... 3
  PCI Data Security Standard for Merchants & Processors .................................................................................... 3
  PIN Entry Device (PED) Security Requirements for Manufacturers ................................................................. 5
  Payment Application Data Security Standard for Developers ........................................................................... 5
  Additional Links to PCI Security Standards Council Documents ................................................................. 6

SAP POS DM Requirements Based on PCI Requirements ................................................................................. 6
  Encryption Library SAPCRYPTOLIB ............................................................................................................... 7
  Payment Card Security Settings ....................................................................................................................... 8
  Security Level Samples in the POS Workbench ............................................................................................... 9
  Payment Card Type Customizing .................................................................................................................. 11
  POS DM Encryption Reports/Programs ........................................................................................................... 13

SAP ERP PCI Security ....................................................................................................................................... 17
  Security Level Samples in the POS Interface Workbench .............................................................................. 20

Summary .......................................................................................................................................................... 23

Copyright ........................................................................................................................................................... 24
Introduction

In today’s economy, retailers are experiencing an increase in threats to their data security, especially credit card data. Credit cards have become the most popular method of paying for goods and services within retail establishments which make them prime targets for security breaches. In an effort to assist in this area and to protect the consumer, the Payment Card Industry Security Standards Council was formed. As of 2007, compliance of the standards developed by this council is mandatory for all retailers who accept, transmit and store credit card information. Those retailers who are found to be non-compliant are subject to hefty fines imposed by the individual credit card institutions with which they do business. The fines are charged on a monthly basis and remain in effect until compliance is reached. Fines may start at $10,000 per month and rise to $100,000 per month.

POS Data Management (POS DM) is an integral part to the SAP POS Integration solution. POS sales are processed and cleansed in POS DM before being transmitted to the SAP Retail system for financial postings and inventory management and to SAP Business Warehouse (SAP BW) for analytical reporting. In an effort to assist retailers in obtaining and maintaining their PCI compliance, POS DM affords its customers security settings for processing, storing and transmitting credit card information.

PCI Background

The Payment Card Industry (PCI) has taken action to develop security standards to protect retail consumers and their cardholder data. These standards are set by the Payment Card Industry Security Standards Council and are applicable to merchants and organizations who store, process or transmit cardholder data. In addition, there are requirements for software manufacturers and developers of applications involved in the movement and storage of the payment card data. Major payment card brands (American Express, MasterCard Worldwide, Visa Inc., Discover Financial Services and JCB International) enforce the standards and compliance by merchants and organization is mandatory.

PCI Standards include the following:

- **PCI Data Security Standards (PCI DSS)**
  - These data security standards are applicable to any and all entities which transmits stores and/or processes cardholder data.

- **PIN Entry Device Security Requirements (PCI PED)**
  - PIN refers to Personal Identification Number of the cardholder. Any and all manufacturers of PIN capturing devices/terminals must adhere to the established requirements.

- **Payment Application Data Security Standard (PA-DSS)**
  - This covers the security standards that must be followed by manufacturers, software developers and integrators of applications that are used in the storage, processing and transmission of cardholder data during the authorization and settlement process.

**PCI Data Security Standard for Merchants & Processors**

Per the PCI website, “The PCI DSS is the global data security standard that any business of any size must adhere to in order to accept payment cards. It presents common sense steps that mirror best security practices.”
Below is a chart of the goals and requirements as provided in the website:

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

Even though the PCI Security Standards Council has established the above requirements, the compliance program of each payment card brand can differ. One should contact each payment card provider to determine the actual compliance program requirements.

The PCI Security Standards Council also provides the following:

**Qualified Assessors.** The Council provides programs for two kinds of certifications: Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV). QSAs are companies that assist organizations in reviewing the security of its payments transaction systems and have trained personnel and processes to assess and validate compliance with PCI DSS and PA-DSS. ASVs provide commercial software tools to perform certified vulnerability scans for your systems. Additional details can be found on our Web site at: [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**Self-Assessment Questionnaire.** The “SAQ” is a validation tool for merchants and service providers who are not required to do on-site assessments for PCI DSS compliance. Different SAQs are specified for various business situations; more details can be found on our Web site at: [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org) or contact the acquiring financial institution to determine if you should complete an SAQ.”
PIN Entry Device (PED) Security Requirements for Manufacturers

Since personal identification numbers (PIN) are captured as part of the payment card processing operation, the PCI Security Standards Council established requirements for manufacturers of the PIN Entry Devices. Below are the requirements from the PCI website.

The council recommends that “Merchants and service providers should use certified PED devices and should check with their acquiring financial institution to understand requirements and associated timeframes for compliance.”

<table>
<thead>
<tr>
<th>PIN Entry Device Security Requirements – Validated by PED Laboratory</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Characteristics</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Physical Security Characteristics (to prevent the device from being stolen from its location)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Logical Security Characteristics (to provide functional capabilities that ensure the device is working appropriately)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Device Management</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Device Management during manufacturing</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Device Management between manufacturer and initial cryptographic key loading</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Considers how the PED is produced, controlled, transported, stored and used throughout its lifecycle</td>
</tr>
<tr>
<td>(to prevent unauthorized modifications to its physical or logical security characteristics)</td>
</tr>
</tbody>
</table>

Payment Application Data Security Standard for Developers

As part of the payment application process, the PCI Security Standards Council is looking to minimize any vulnerability. As stated by the council, “The goal is to prevent the compromise of full magnetic stripe data located on the back of a payment card. PA-DSS covers commercial payment applications, integrators and service providers. Merchants and service providers should use certified payment applications and should check with their acquiring financial institution to understand requirements and associated timeframes for compliance.”
Below are the security standards for developers as found on the PCI website:

<table>
<thead>
<tr>
<th>Payment Application DSS Requirements – Validated by PA-QSA Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Do not retain full magnetic stripe, card validation code or</td>
</tr>
<tr>
<td>value (CAV2, CID, CIV2, CW2) or PIN block data</td>
</tr>
<tr>
<td>2. Provide secure password features</td>
</tr>
<tr>
<td>3. Protect stored cardholder data</td>
</tr>
<tr>
<td>4. Log application activity</td>
</tr>
<tr>
<td>5. Develop secure applications</td>
</tr>
<tr>
<td>6. Protect wireless transmissions</td>
</tr>
<tr>
<td>7. Test applications to address vulnerabilities</td>
</tr>
</tbody>
</table>

Additional Links to PCI Security Standards Council Documents

- Getting Started with PCI Data Security Standard
- PCI Data Storage Do's and Don’ts
- Ten Common Myths of PCI DSS
- Lifecycle Process for Changes to PCI DSS

SAP POS DM Requirements Based on PCI Requirements

As a result of the movement towards global PCI compliance, SAP is directly affected by 5 of the 12 PCI DSS requirements:

- Encrypted storage of credit card data
- Encrypted transmission of data
- Masked display of credit card data
- Track users accessing the data
- Password Management (including expiry, login attempts)

In an effort to assist customers in achieving / maintaining their compliance, SAP POS DM (both PIPE and BW Retail Content) has been enhanced as of SP8 in 2007. Included in this SP are:

- Encryption of Credit Card Data within PIPE using SAPCRYPTOLIB
- Decryption and Decrypted Display possible within PIPE
- Tracing and logging of decryption requests within PIPE
- Masked Display in the POS Workbench
- BW Masked Storage
- BW Masked Display, Hash Value for identifying
- Password and User Management
Credit card data will only be encrypted on data that is loaded into POS DM after the SP8 is installed and encryption is activated. Any credit card data loaded for this will remain unencrypted. A migration report exists to encrypt the older data so long as no tasks have been successfully performed on this data.

The following are the system prerequisites for POS DM:

- BI_CONT 703, Support Package 8
- SAP_ABA 700, Support Package 12 (better Support Package 13)
- Encryption Library SAPCRYPTOLIB

**Encryption Library SAPCRYPTOLIB**

The installation of the encryption library SAPCRYPTOLIB must be completed by the Basis team as one of the prerequisites for encryption within POS DM. Additional details for the installation and use of this library is available in CSS note 662340. It should be noted that when creating the PSE using transaction code STRUST, you have to choose algorithm RSA (the defaulted value is DSA).

The following is the path for maintaining the settings for the encryption library SAPCRYPTOLIB:

IMG -> SAP NetWeaver -> Application Server -> System administration -> Maintain the Public Key Information for the System
Payment Card Security Settings

Security settings for payment cards are maintained in Table/View V_TCCSEC via transaction code SM30.

Within this screen you click on the Maintain button.

There are 3 security levels available:

- **0 No Additional Security Measures**
  - Decrypted credit card numbers are stored in the corresponding tables (POS DM and BW) and are completely visible in the POS Workbench.
  - Decrypted numbers are also visible in the BW reports.

- **1 Masked Display, Not Encrypted When Saved**
  - Credit card numbers are stored as masked in the corresponding tables and visible as masked in the POS Workbench.
  - Care should be taken in using level 1 since the credit card number is lost and should only be used if you will not need to view the decrypted card number in the future.

- **2 Masked Display, Encrypted When Saved**
  - Credit card numbers are stored as encrypted in the corresponding tables and visible as masked in the POS Workbench.
  - With the property authorization, a user in the POS Workbench is also able to view the decrypted card number. This activity is captured in a log and can be viewed by running RCCSEC_LOG_SHOW report.

The Access Log settings are used to determine whether or not the system keeps track of who views the credit card numbers. There are 2 settings from which to choose:

- **0 No Logging**
- **1 Logging of Unmasked Display**

The Additional Authorization Check for Unmasked display defines whether additional authorization is necessary for displaying an unmasked payment card number. If this setting is checked, access to credit card numbers authorization object B_CCSEC will be carried out.
The Visible Characters for Masking determines the number of digits that are visible at the start and end of the credit card number after the number is masked in POS DM. With the settings above, the user would see credit card number 434321567879 as 4343********7879 when it’s masked.

**Security Level Samples in the POS Workbench**

If the security level is set to 0, the credit card number is fully visible as seen below:

With the security level setting of 1, the credit card number is masked. The number of digits that are visible are determined by the customizing settings.

If the security level is set at 2, the user will see the credit card number as masked but the number is stored as encrypted in the appropriate tables.
With the proper authorization, the user can click on the spy glass icon next to the masked credit card number and view the number in its raw decrypted form.

If this activity takes place, the actions are logged in CCSEC_LOG table. By running the report RCCSEC_LOG_SHOW, an authorized user can see who accessed the decrypted data and when.
Payment Card Type Customizing

Once you have the security settings determined for credit card numbers, the user needs to select which credit card types will use these security settings.

The customizing path is IMG -> Cross-Application Components -> Payment Cards -> Basic Settings -> Maintain Payment Card Type

Within the next screen, the user maintains the credit card types that are used at the retail POS system.

Checking Rules are not considered in POS DM.

Once the Payment Card Types are maintained, the user can use transaction code SM30 to make the encryption settings in Table/View V_TB033_SEC.
Click on the Maintain button to go to the next screen.

The Encryption check box for the Payment Card Type controls whether the payment card numbers for a payment card type should be saved as encrypted. If the box is unchecked, the credit card numbers will be stored as masked. If the box is checked, the card numbers can be stored as encrypted. These settings are used in conjunction with the security settings as discussed in the previous section.
POS DM Encryption Reports/Programs

Three reports are available which are related to encryption in the POS DM module:

1. Encryption/Masking of Existing Credit Card Numbers (/POSDW/PCA_MIGRATION)
   - The purpose of this program is to afford the capability of moving decrypted or encrypted credit card numbers from other systems into masked or encrypted credit card numbers in POS DM.
   - This report can be accessed via transaction code SE38

   ![ABAP Editor: Initial Screen](image)
   - You execute the report by clicking on the icon or pressing the F8 key

   ![Encryption/Masking of Existing Credit Card Numbers](image)
   - There is further selection criteria available by clicking on the icon

   ![Encryption/Masking of Existing Credit Card Numbers](image)
   - Once you’ve entered your selection criteria, the program can be executed in the foreground or background.
Here's a POS transaction before running the program.

<table>
<thead>
<tr>
<th>Store</th>
<th>$300</th>
</tr>
</thead>
<tbody>
<tr>
<td>Store Group</td>
<td>to</td>
</tr>
<tr>
<td>Posting Date</td>
<td>06/22/2009</td>
</tr>
<tr>
<td>Credit Card Identification</td>
<td>to</td>
</tr>
<tr>
<td>System Information</td>
<td></td>
</tr>
<tr>
<td>Transaction Index</td>
<td>to</td>
</tr>
<tr>
<td>Transaction Number</td>
<td>222</td>
</tr>
<tr>
<td>Transaction Type</td>
<td>to</td>
</tr>
<tr>
<td>Start of Transaction</td>
<td>to</td>
</tr>
<tr>
<td>End of Transaction</td>
<td>to</td>
</tr>
<tr>
<td>Partner Qualifier</td>
<td>to</td>
</tr>
<tr>
<td>Partner Number</td>
<td>to</td>
</tr>
<tr>
<td>Means of Payment</td>
<td>to</td>
</tr>
</tbody>
</table>

- Possioning Control
  - Check Box
  - Cung

Here's the same transaction after running the program.

<table>
<thead>
<tr>
<th>Store</th>
<th>$300</th>
</tr>
</thead>
<tbody>
<tr>
<td>Store Group</td>
<td>to</td>
</tr>
<tr>
<td>Posting Date</td>
<td>06/22/2009</td>
</tr>
<tr>
<td>Credit Card Identification</td>
<td>to</td>
</tr>
<tr>
<td>System Information</td>
<td></td>
</tr>
<tr>
<td>Transaction Index</td>
<td>to</td>
</tr>
<tr>
<td>Transaction Number</td>
<td>222</td>
</tr>
<tr>
<td>Transaction Type</td>
<td>to</td>
</tr>
<tr>
<td>Start of Transaction</td>
<td>to</td>
</tr>
<tr>
<td>End of Transaction</td>
<td>to</td>
</tr>
<tr>
<td>Partner Qualifier</td>
<td>to</td>
</tr>
<tr>
<td>Partner Number</td>
<td>to</td>
</tr>
<tr>
<td>Means of Payment</td>
<td>to</td>
</tr>
</tbody>
</table>

- Possioning Control
  - Check Box
  - Cung

This program can be used as long as there are no relevant tasks performed against the transaction. If you try to run the program after a task has been performed, you get an error as seen the following log:
2. Evaluate Log Records Using Payment Card Access (RCCSEC_LOG_SHOW)
   - This report/program is available to authorized users to provide a log of which users view decrypted credit card numbers in the POS Workbench.
     - In order to run the report, the user needs to have authorization for activity 71 for authorization object B_CCSEC
   - The program is accessed via transaction code SE38.

   - You execute the report by clicking on the icon or pressing the F8 key.

   - Once you’ve entered your selection criteria, the program can be executed in the foreground or background.
• The resulting report looks as follows:

• This report can also possibly be used in tracking possible security breaches within the POS DM system.

3. Delete Log Records of Payment Card Access (RCCSEC_LOG_DEL)
   • Access to this report/program needs to have very strict security authorization because the log records of users accessing raw credit card numbers in the POS Workbench are deleted.
   • The program is accessed via transaction code SE38.

• You execute the report by clicking on the icon or pressing the F8 key

• Only records that are at least one year older than the current system date can be deleted.
This report only can be used if the user has authorization for activity 06 for authorization object B_CCSEC

**SAP ERP PCI Security**

SAP ERP receives credit card data as part of the data feed from POS DM. As a result, SAP ERP 6.0 SP09 and higher is enhanced to assist in the support of PCI compliance and offers the following:

- Credit Card encryption using SAP Cryptolib
- Masked display e.g. POS Inbound Monitor
- Decryption and Decrypted Display possible
- Tracing and logging of decryption requests
- Customizing Possibilities
- Supports secured Extraction of Credit Card Information to Netweaver BI
- Password and User Management

**SAP ERP Customizing**

In the POS inbound feed from POS DM, the payment method segments of message types WPUBON and WPUTAB contain the credit card information. Customizing settings are available to ensure that the credit card number is encrypted and masked.

Using transaction code SM30, one of the customizing areas for maintaining the security setting is available.

You enter V_TCCSEC as the Table/View and click on the Maintain button.
Within the next screen, the authorized user can maintain security settings deemed appropriate for their business requirements.

This is the same screen and settings that’s part of the POS DM security settings.

There are 3 security levels available:

- **0 No Additional Security Measures**
  - Decrypted credit card numbers are store in the corresponding tables (POS DM and BW) and are completely visible in the POS Interface Monitor

- **1 Masked Display, Not Encrypted When Saved**
  - Credit card numbers are stored as masked in the corresponding tables and visible as masked in the POS Workbench
  - Care should be taken in using level 1 since the credit card number is lost and should only be used if you will not need to view the decrypted card number in the future.

- **2 Masked Display, Encrypted When Saved**
  - Credit card numbers are stored as encrypted in the corresponding tables and visible as masked in the POS Interface Monitor.
  - With the property authorization, a user in the POS Interface Monitor is also able to view the decrypted card number. This activity is captured in a log and can be viewed by running the RCCSEC_LOG_SHOW report or using transaction code CCSEC_LOG_SHOW.

The Access Log settings are used to determine whether or not the system keeps track of who views the credit card numbers. There are 2 settings from which to choose:

- **0 No Logging**
- **1 Logging of Unmasked Display**

The Additional Authorization Check for Unmasked display defines whether additional authorization is necessary for displaying an unmasked payment card number. If this setting is checked, access to credit card numbers authorization object B_CCSEC will be carried out.

The Visible Characters for Masking determines the number of digits that are visible at the start and end of the credit card number after the number is masked in ERP. With the settings above, the user would see credit card number 4343215667879 as 4343*******7879 when it’s masked.

Additional customizing settings are made via transaction code SM30:
Enter V_TB033_SEC as the Table/View and click on the Maintain button.

Within the next screen, the authorized user configures the payment card types that are accepted within the retail stores, processed in POS DM and are part of the feed from POS DM.

The payment card types should be the same as those maintained in the POS DM system.

The Encryption check box for the Payment Card Type controls whether the payment card numbers for a payment card type should be saved as encrypted. If the box is unchecked, the credit card numbers will be stored as masked. If the box is checked, the card numbers can be stored as encrypted. These settings are used in conjunction with the security settings as discussed in the previous section.

Also note that if encryption is active for a payment card type, but no encryption tool is connected, the payment card number is saved without being encrypted.

Additional information regarding ECC 6.0 credit card security settings is available in CSS Notes:

- 1032588 - Secure handling of Credit Card Data in ERP
- 1041514 - Credit Card Coding in the ERP POS Inbound
- 1041238 - Credit Card Numbers Masked for RIS
Security Level Samples in the POS Interface Workbench

When the security level is set to 0 No Additional Security measures, the credit card number is able to be viewed in the POS Interface Monitor in its raw form. Via transaction code WPER, you enter your selection criteria and press the Execute button or F8.

On the next screen, you will drill down to the store/customer in question to view the IDoc message type documents.

You double click on the IDoc number and go to the Item details.
As seen in the above screen shot, the full raw credit card number is available to the user.

For security level settings 1 and 2, the credit card number is masked as seen the screen shot below.

With the proper security setting for your user, you could click on the Card Number button to view the full card number.
This action is logged in the CCSEC_LOG table and can also be accessed via the RCCSEC_LOG_SHOW report or transaction code CCSEC_LOG_SHOW.

After ending your selection criteria, you click the Execute button.

The resulting report shows what masked card number was analyzed by who, on what date and at what time. This information is extremely valuable for investing credit card fraud.
Summary

PCI Security Standards are here to stay and all retailers who accept credit cards as a means of payment are subject to PCI compliance. Those found to be non compliant are subject to stiff fines and penalties. To assist retailers in obtaining and/or maintaining PCI compliance, SAP has added security measures in its SAP POS, POS DM, BW and SAP ERP systems. SAP is continuing to strengthen and broaden these security measures with future enhancement packages and releases.