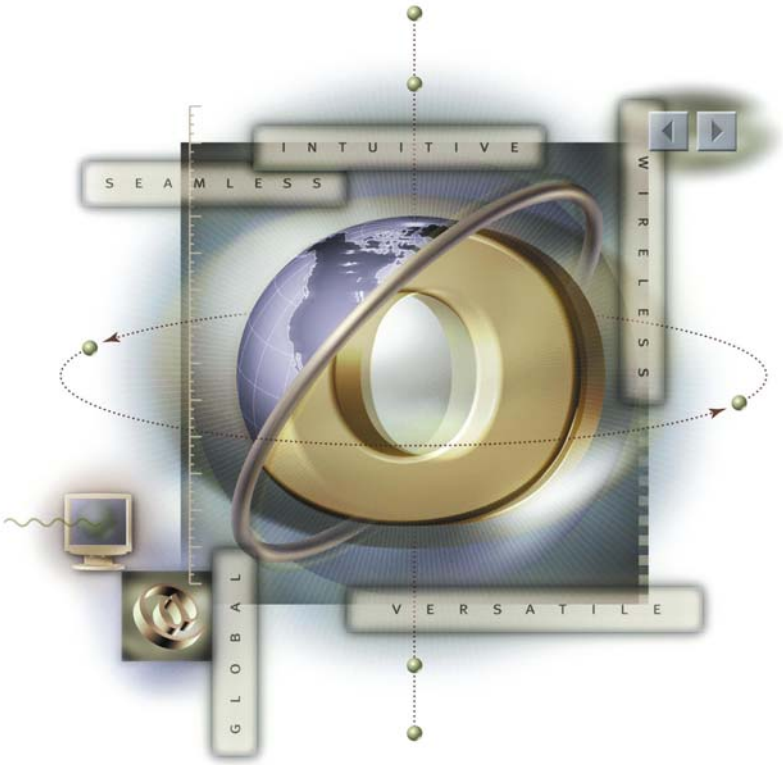
micros® | FIDELIO



Opera Hotel Edition

ON ORACLE

OPERA Payment Application Data Security Standard (PA-DSS) Implementation Guide

V5.0+

August 2009

Copyright

MICROS Systems, Inc.
Fidelio Technologies Inc.
2640 Golden Gate Parkway, Suite 211
Naples, FL 34105
Voice: (239) 643-7999 / Fax: (239) 643-7911

Document: 1470 Opera PA-DSS Implementation Guide

Author:
Contributors:

Contents

General Information

About This Document

This document is intended as a quick reference guide to provide you with information concerning MICROS Systems, Inc. adherence to the Payment Card Industries – Security Standards Council (PCI-SSC) concerning PA-DSS. This document relates specifically to *OPERA Version 5.0+ Enterprise Solution software*, including Opera Property Management, Opera Limited Service (Xpress), Opera Xpress Lite (Lite), Operetta, & Opera Reservation System. This document is distributed to all customers on a annual basis or whenever there is a software upgrade performed.

About the PCI Security Standards Council[1]

The PCI Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards, including: the Data Security Standard (DSS), Payment Application Data Security Standard (PA-DSS), and Pin-Entry Device (PED) Requirements.

All of the five founding members have agreed to incorporate the PCI DSS as the technical requirements of each of their data security compliance programs. Each founding member also recognizes the QSAs and ASVs certified by the PCI Security Standards Council as being qualified to validate compliance to the PCI DSS.

A Limited Liability Corporation (LLC) chartered in Delaware, USA, the PCI Security Standards Council was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.. All five payment brands share equally in the council's governance, have equal input to the PCI Security Standards Council and share responsibility for carrying out the work of the organization. Other industry stakeholders are encouraged to join the group and review proposed additions or modifications to the standards.

About The PCI Data Security Standard (PCI DSS)[2]

The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis.

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

The PCI Security Standards Council will enhance the PCI DSS as needed to ensure that the standard includes any new or modified requirements necessary to mitigate emerging payment security risks, while continuing to foster wide-scale adoption.

Ongoing development of the standard will provide for feedback from the Advisory Board and other participating organizations. All key stakeholders are encouraged to provide input, during the creation and review of proposed additions or modifications to the PCI DSS.

[1] https://www.pcisecuritystandards.org/about/index.shtml

[2] https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized:[3]

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

[3] pcisecuritystandards.org

Who Should be Reading This Document

This document is intended for the following audiences:

- MICROS Customers
- MICROS Installers/Programmers
- MICROS Dealers
- MICROS Customer Service
- MICROS Training Personnel
- MIS Personnel

What the Reader Should Already Know

This document assumes that you have the following knowledge or expertise:

- Operational understanding of PCs
- Understanding of basic network concepts
- Experience with the operating systems platforms supported by OPERA
- Familiarity with the OPERA software
- Familiarity with operating MICROS peripheral devices

OPERA Version 5.0+ and the Payment Application Data Standard

Payment Application Data Security Standard

While MICROS recognizes the importance of upholding cardmember security and data integrity, certain parameters of the PCI Data Security Standard and PCI-SSC are the sole responsibility of the client. This section contains a description of the 12 points of The PCI Data Security Standard. Information within this section pertains only to how the OPERA Version 5.0 software conforms to the PCI Data Security Standard.

For a complete description of the PCI Data Security Standard, please consult the Payment Card Industries – Security Standards Council website found at <http://pcisecuritystandards.org>.

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data

Firewalls are computer devices that control computer traffic allowed into a company's network from outside, as well as traffic into more sensitive areas within a company's internal network. All systems need to be protected from unauthorized access from the Internet, whether for e-commerce, employees' Internet-based access via desktop browsers, or employees' email access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

MICROS strongly recommends that all systems containing sensitive information (servers, databases, wireless access points, etc.) reside behind a firewall in order to protect that data as well as meet PCI-SSC Security Standards.

To make sure your firewall configuration is set up in compliance with Step 1 of the PCI Data Security Standard, "Install and maintain a firewall configuration to protect data", please consult the Payment Card Industries – Security Standards Council website found at <http://pcisecuritystandards.org>.

2. Do not use vendor-supplied defaults for system passwords and other security parameters

Hackers (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information.

MICROS recommends that customers change all default passwords when installing systems, including those for operating systems, wireless access points, servers, databases, etc. Opera provides two default accounts for which the passwords should be changed to meet the PCI-SSC complex password requirements; they are Application User account: SUPERVISOR and DB accounts: SYS, SYSTEM, OPERA, OXI, OXIHUB and OUTLN.

In addition, the IT department of the property and/or responsible parties should create an Opera Support User with all the needed credentials.

The PCI-DSS expressly prohibits the use of generic or default user names or passwords for any component of the payment processing system which includes Windows accounts. Any access to any part of the payment processing system should be handled with unique and strong user access credentials.

For more information on Step 2 of The PCI Data Security Standard, "Do not use vendor-supplied defaults for system passwords and other security parameters", please consult the

Payment Card Industries – Security Standards Council website found at <http://pcisecuritystandards.org>.

Protect Cardholder Data

3. Protect stored data

Encryption is the ultimate protection mechanism because even if someone breaks through all other protection mechanisms and gains access to encrypted data, they will not be able to read the data without further breaking the encryption. This is an illustration of the defense in depth principle.

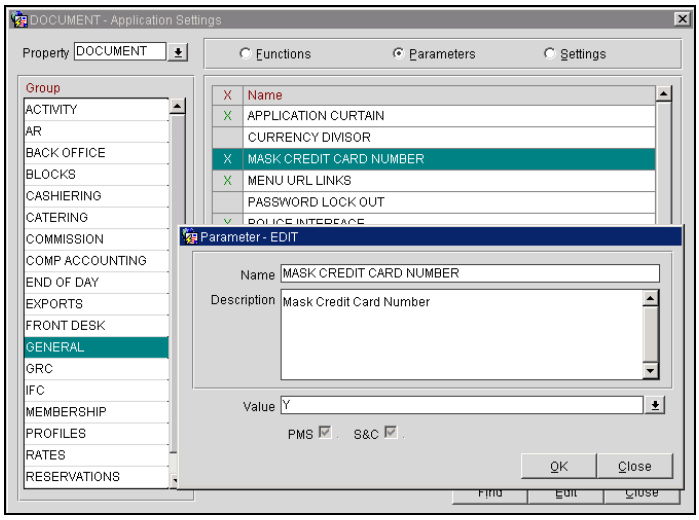
MICROS Systems Inc., uses credit card masking and Triple-DES 128-bit encryption to store the personal account number (PAN), account name, expiration date and ensure credit card data is stored in a manner compliant with the PCI Data Standard.

When upgrading from version 2.0 of Opera, please refer to the section "Guidance when Upgrading from a Previous Opera Version" at the bottom of this document, which describes how to upgrade to a newer version, using a secure wipe tool and completely purge any old credit card data from Opera.

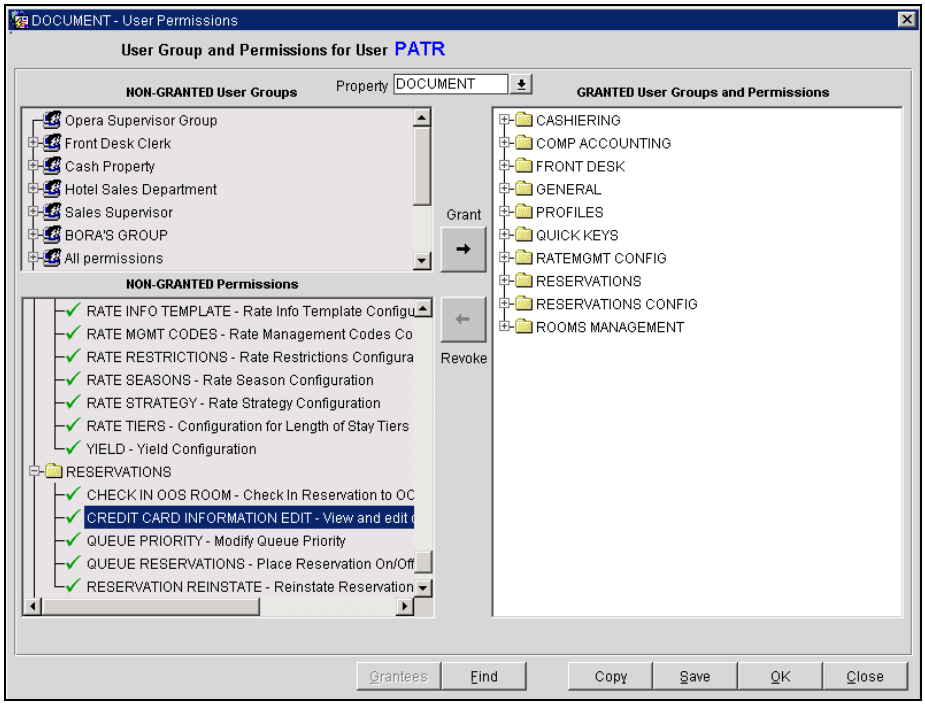
To be in compliance with Step 3 of the PCI Data Security Standard, please ensure the following Credit Card Masking options are configured as follows:

Option Settings

- **Setup>Application Settings:** Set General>MASK CREDIT CARD NUMBER (Mask Credit Card Number) to **Yes**.



- **Setup>User Configuration>Users>Permissions**: Set RESERVATIONS> CREDIT CARD INFORMATION EDIT (View and edit credit card number and expiration date) to **Non-Granted** for all users except those with a "need to know." For such users, the permission may be changed to **Granted**.



Note: *These options must remain configured as shown above, in order to comply with Step 3 of The PCI Data Security Standard.*

For more information on Step 3 of The PCI Data Security Standard, "Protect stored data", please consult the Payment Card Industries – Security Standards Council website found at <http://pcisecuritystandards.org>.

4. Encrypt transmission of cardholder data and sensitive information across public networks

Sensitive information must be encrypted during transmission over the Internet, because it is easy and common for a hacker to intercept and/or divert data while in transit.

MICROS recommends that all sensitive information that is transmitted over the Internet be secured using a form of encryption such as SSLv3; this includes all wireless transmissions, email and use of services such as Telnet and FTP.

Option Settings

MICROS strongly suggests that when using our web based credit card interface, it is set up to use SSLv3 communication. To configure this, do the following. Select **Configuration>Setup>Property Interfaces>Credit Card Setup>General Parameters**. On this form you will see a section to configure the URL that you are to connect to. Be sure that this URL starts with HTTPS. This will ensure a secure SSLv3 connection is made to the vendor prior to transmitting credit card data.

For more information on Step 4 of The PCI Data Security Standard, "Encrypt transmission of cardholder data and sensitive information across public networks", please consult the Payment Card Industries – Security Standards Council website found at <http://pcisecuritystandards.org>.

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software

Many vulnerabilities and malicious viruses enter the network via employees'email activities. Anti-virus software must be used on all email systems and desktops to protect systems from malicious software.

In accordance with the PCI-SSC standards, MICROS strongly recommends regular use and regular updates of anti-virus software. Some OPERA servers may require specific antivirus configuration settings; these settings are detailed in the implementation instructions.

To make sure your anti-virus software is set up in compliance with Step 5 of the PCI Data Security Standard, "Use and regularly update anti-virus software", please consult the Payment Card Industries – Security Standards Council website found at <http://pcisecuritystandards.org>.

6. Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed via vendor security patches, and all systems should have current software patches to protect against exploitation by employees, external hackers, and viruses. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

MICROS uses separate development and production environments to ensure software integrity and security. Updated patches and security updates are available via the MICROS product website, <http://www.micros.com>. While MICROS makes every possible effort to conform to Step 6 of the PCI Data Security Standard, certain parameters, including following change control procedures for system and software configuration changes, and the installation of available security patches, depend on site specific protocol and practices.

MICROS also strongly suggests for installation in Windows XP systems that the System Restore Points feature be turned off.

To make sure your site develops and maintains secure systems and applications in compliance with Step 6 of The PCI Data Security Standard, "Develop and Maintain Secure Systems and Applications", please consult the Payment Card Industries – Security Standards Council website found at <http://pcisecuritystandards.org>.

Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know

This ensures critical data can only be accessed in an authorized manner.

MICROS recognizes the importance of data control, and does so by establishing access based upon employee job level. This mechanism ensures access to sensitive information is restricted, password protected, and based on a need-to-know basis.

For more information on Step 7 of The PCI Data Security Standard, "Restrict access to data by business need-to-know", please consult the Payment Card Industries – Security Standards Council website found at <http://pcisecuritystandards.org>.

8. Assign a unique ID to each person with computer access

This ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

MICROS recognizes the importance of establishing unique ID's for each person with computer access. No two OPERA users can have the same ID, and each person's activities can be traced

provided the client site maintains proper configuration and adheres to privilege level restrictions based on a need-to-know basis. While MICROS makes every possible effort to conform to Step 8 of the PCI Data Security Standard, certain parameters, including proper user authentication, remote network access, and password management for non-consumer users and administrators, for all system components, depend on site specific protocol and practices.

To be in compliance with Step 8 of the PCI Data Security Standard, we recommend that customers follow these guidelines.

- Ensure "Password Expiration Days" set on the Edit User screen is not greater than 90.
- Ensure that user passwords are at least 7 characters in length.
- Ensure that user passwords include alphabetic and numeric characters.
- Encrypt all passwords during transmission using a form of encryption such as SSLv3. Micros STONGLY recommends the use of SSLv3 and should be used in every implementation. (To configure Opera application server for access over the HTTPS refer to the "Opera – Configure Opera for SSL".pdf)

For more information on Step 8 of the PCI Data Security Standard, "Assign a unique ID to each person with computer access", please consult the Payment Card Industries – Security Standards Council website found at <http://pcisecuritystandards.org>.

9. Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data allows the opportunity to access devices or data, and remove systems or hardcopies, and should be appropriately restricted.

In accordance with the Payment Card Industries - Security Standards Council standard, MICROS strongly recommends restricting physical access to cardholder data.

To make sure your site is set up in compliance with Step 9 of The PCI Data Security Standard, "Restrict physical access to cardholder data", please consult the Payment Card Industries – Security Standards Council website found at <http://pcisecuritystandards.org>.

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

MICROS provides a comprehensive audit trail utility, within OPERA, that allows privileged users to track OPERA specific activities. The advent of open database structure means that anyone with system level access to the database server (Oracle) has access to system components covered under this requirement, and thus would require logging of user access and activity as detailed in Step 10 of the PCI Data Security Standard. In accordance with the Payment Card Industries – Security Standards Council standard, MICROS strongly recommends logging of activity on the database server.

To make sure your site is in compliance with Step 10 of The PCI Data Security Standard, "Track and monitor all access to network resources and cardholder data", please consult the Payment Card Industries – Security Standards Council website found at <http://pcisecuritystandards.org>.

11. Regularly test security systems and processes

Vulnerabilities are continually being discovered by hackers/researchers and introduced by new software. Systems, processes, and custom software should be tested frequently to ensure security is being maintained over time and through changes.

In accordance with the Payment Card Industries – Security Standards Council standards, MICROS strongly recommends regular testing of security systems and processes.

To make sure your site's security systems and processes are setup in compliance with Step 11 of The PCI Data Security Standard, "Regularly test security systems and processes", please consult the Payment Card Industries – Security Standards Council website found at <http://pcisecuritystandards.org>.

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

A strong security policy sets the security tone for the whole company, and lets employees know what is expected of them. All employees should be aware of the sensitivity of the data and their responsibilities for protecting it.

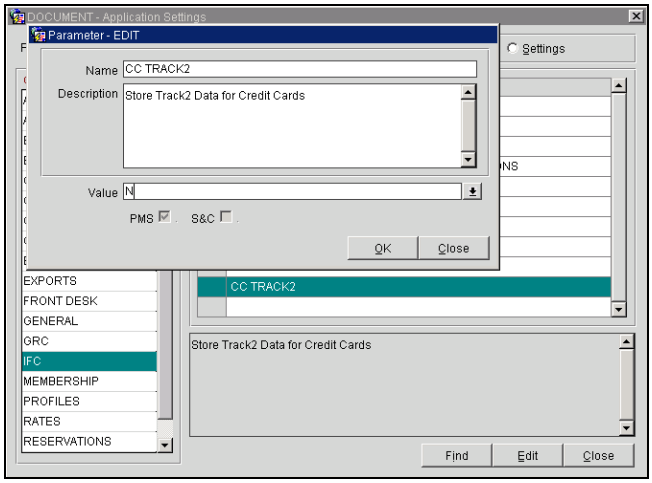
In accordance with the Payment Card Industries – Security Standards Council standards, MICROS strongly recommends maintaining a policy that addresses information security.

To make sure your information security policy is setup in compliance with Step 12 of The PCI Data Security Standard, "Maintain a policy that addresses information security", please consult the Payment Card Industries – Security Standards Council website found at <http://pcisecuritystandards.org>.

Guidance when Upgrading from a Previous Opera Version

I. Turning off the Track 2 Functionality

To stay in compliance with the Payment Card Industries – Security Standards Council requirements, when upgrading to Opera 4.0 from a previous version, the CC_TRACK2 parameter must first be turned off in the previous version. This will delete the track 2 data from the Opera database. To turn off the parameter in Opera 3.0, select **Setup>Application Settings**, and set the IFC Group Application Parameter to **No**, as shown below.



II. Database Upgrade

To upgrade the database instance, follow these steps:

1. Creating a new Oracle 10g Instance for Opera 4.0.
    a. Use the Opera V4.0.3 Database CD to install a database.
    b. Drop the Opera Schema from the database by connecting to SQLPLUS using SYS.
        i. Drop user Opera cascade.
2. Export the Opera schema from the 9i Database.
    a. Use Opera_SMT to perform the export of the schema.
3. Import Opera schema into 10g Instance
    a. Use Opera_SMT to perform Import by double clicking on the EXE that was generated using the Export.
4. Upgrade Opera Schema to Version V4.0
    a. Run mega patch Executable for corresponding version. Executables are available at Micros Website download the file that is relevant to the 9i version
5. Make a full backup
    a. Shutdown the database
    b. Copy all files located at d:\oracle\oradata\opera folder to a backup folder
    c. Copy initopera.ora file located either in d:\oracle\1020\database folder or d:\oracle\admin\opera\pfile folder to a backup folder.
6. Delete all Oracle 9i files using a secure wipe tool to securely purge the data (These tools are in random order and we have no recommendations on one over the other).
    - http://www.clean-space.com/privacy/about/secure-wipe.html
    - http://www.softsea.com/review/EZ-Wipe.html
    - http://tucows.menanet.net/fileremove95_default.html

Establish and Follow a Data Retention Policy

The PCI Data Security Standard states, “Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy. The development and implementation of a Data Retention Policy (DRP) is a significant factor in the overall security of your environment.

A DRP forms an important foundation for helping manage an organization’s data. The creation of a DRP is a complex task that requires exhaustive research and the assistance of qualified legal counsel. The scope of your DRP should reach far beyond the PCI DSS, and you should work closely with your legal counsel to ensure your compliance with the laws and governmental regulations that pertain specifically to your organization.

Upon implementation of your DRP, you should contract with a PCI-SSC-approved PCI "PCI Requirements and Security Assessment Procedures", V. 1.2, October, 2008. The assessment company is to review the DRP's impact on the storage of payment card data in compliance with Requirement #3 of the PCI DSS.

3rd Party Interfaces

This application is intended to be used to establish a connection between a certain MICROS Systems, Inc. (MICROS) product and certain 3rd party products not developed by or controlled by MICROS (Non-MICROS Products).These Non-MICROS Products may or may not be compliant with the Payment Card Industry Payment Application Data Security Standard (PA-DSS). MICROS strongly recommends that all merchants who are connecting any MICROS payment processing products to any Non-MICROS Products ensure that both the MICROS and Non-MICROS products are PA-DSS compliant.