OPERA Version 4.0+ PABP Guide and PCI Data Security Standard Adherence

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 Visa USA PCI Data Security Standard concerning CISP compliance. This document relates specifically to *OPERA Version 4.0+ Enterprise Solution software*, including Opera Property Management, Opera Limited Service (Xpress), Opera Xpress Lite (Lite) & Opera Reservation System.

About CISP Compliance

When customers offer their bankcard at the point of sale, over the Internet, on the phone, or through the mail, they want assurance that their account information is safe. That's why Visa USA has instituted the Cardholder Information Security Program (CISP). Mandated since June 2001, the program is intended to protect Visa cardholder data—wherever it resides—ensuring that members, merchants, and service providers maintain the highest information security standard.[1]

For more detailed information concerning CISP compliance, please refer to the Visa USA CISP website, <http://usa.visa.com/business/accepting_visa/ ops_risk_management/cisp.html>.

About The PCI Data Security

CISP compliance is required of all merchants and service providers that store, process, or transmit Visa cardholder data. The program applies to all payment channels, including retail (brick-and-mortar), mail/telephone order, and ecommerce. To achieve compliance with CISP, merchants and service providers must adhere to the Payment Card Industry (PCI) Data Security Standard, which offers a single approach to safeguarding sensitive data for all card brands. This Standard is a result of a collaboration between Visa and MasterCard and is designed to create common industry security requirements, incorporating the CISP requirements. Other card companies operating in the U.S. have also endorsed the PCI Data Security Standard within their respective programs. Using the PCI Data Security Standard as its framework, CISP provides the tools and measurements needed to protect against cardholder data exposure and compromise across the entire payment industry. The PCI Data

[1] Reprinted from "Cardholder Information Security Policy", <http://usa.visa.com/business/ accepting_visa/ops_risk_management/cisp.html>.

Security Standard, seen below, consists of twelve basic requirements supported by more detailed sub-requirements:[2]

*The **Payment Card Industry (PCI) Data Security Standard** is a result of a collaboration between Visa and MasterCard to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs. These 12 requirements are the foundation of Visa's CISP.*

PCI Data Security Standard

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor supplied defaults for system passwords and other security parameters

Protect Cardholder Data

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

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

[2] Reprinted from "CISP_overview.pdf", <http://usa.visa.com/download/business/accepting_visa/support_center/cisp_overview.pdf?it=c|/ business/accepting_visa/ ops_risk_management/cisp%2Ehtml|CISP%20Overview>.

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 4.0+ and the PCI Data Standard

PCI Data Security Standard

While MICROS recognizes the importance of upholding cardmember security and data integrity, certain parameters of the PCI Data Security Standard and CISP compliance 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 4.0 software conforms to the PCI Data Security Standard.

For a complete description of the PCI Data Security Standard, please consult Visa USA's website "Cardholder Information Security Plan" found at <http://usa.visa.com/business/accepting_visa/ops_risk_management/ cisp.html>.

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.[3]

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 Visa CISP 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 Visa USA's website, "Cardholder Information Security Policy", <http://usa.visa.com/business/accepting_visa/ ops_risk_management/cisp.html>.

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.[4]

[3] "Payment Card Industry Standard Audit Procedures.doc", p. 5, V. 1.0, December 15, 2004.<http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/ cisp%2Ehtml|View%20all%20CISP%20downloads>.

https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm

[4] "Payment Card Industry Security Audit Procedures.doc", p. 10, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/ cisp%2Ehtml|View%20all%20CISP%20downloads>.

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 CISP 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.

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 Visa USA's website, "Cardholder Information Security Policy", <http://usa.visa.com/business/accepting_visa/ ops_risk_management/cisp.html>.

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.[5]

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.

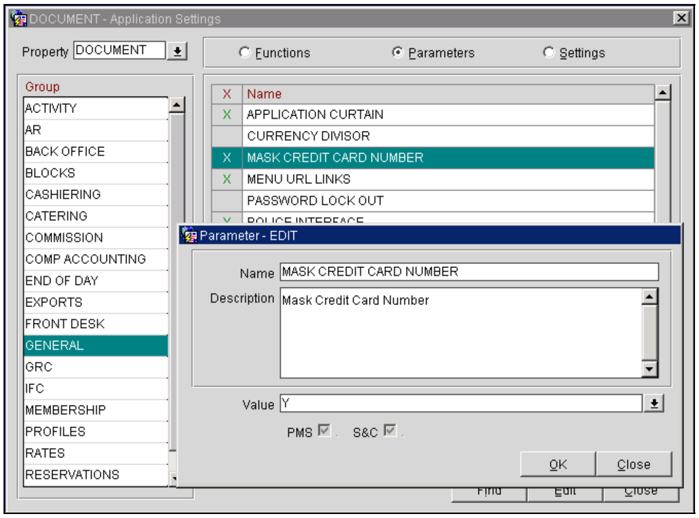
When upgrading from version 2.0 of Opera, please refer to the section "Guidance when Upgrading from a Previous Opera Version" at the bottom of this document, which describes how to upgrade to a newer version, using a secure wipe tool and completely purge any old credit card data from Opera.

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:

[5] "Payment Card Industry Security Audit Procedures.doc", p. 13, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/ cisp%2Ehtml|View%20all%20CISP%20downloads>.

Option Settings

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



DOCUMENT - Application Settings

Property DOCUMENT

○ Functions ● Parameters ○ Settings

Parameter - EDIT

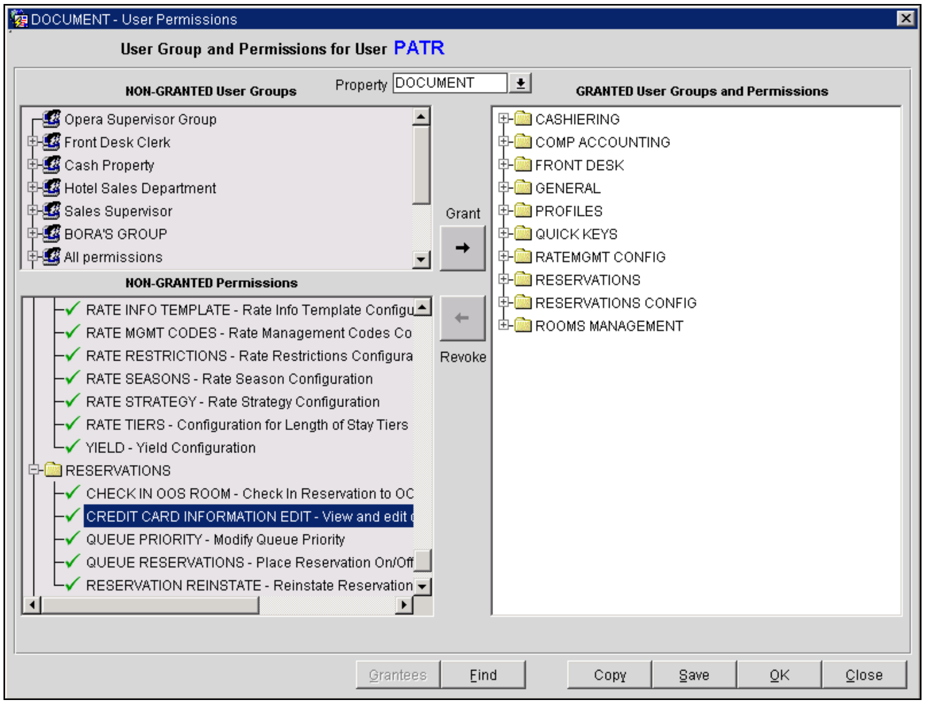
Name: MASK CREDIT CARD NUMBER

Description: Mask Credit Card Number

Value: Y

PMS ☑ S&C ☑

- **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**.



DOCUMENT - User Permissions

User Group and Permissions for User PATR

Property DOCUMENT

NON-GRANTED User Groups
Opera Supervisor Group
Front Desk Clerk
Cash Property
Hotel Sales Department
Sales Supervisor
BORA'S GROUP
All permissions
NON-GRANTED Permissions
✓ RATE INFO TEMPLATE - Rate Info Template Configu
✓ RATE MGMT CODES - Rate Management Codes Co
✓ RATE RESTRICTIONS - Rate Restrictions Configura
✓ RATE SEASONS - Rate Season Configuration
✓ RATE STRATEGY - Rate Strategy Configuration
✓ RATE TIERS - Configuration for Length of Stay Tiers
✓ YIELD - Yield Configuration
RESERVATIONS
✓ CHECK IN OOS ROOM - Check In Reservation to OC
✓ CREDIT CARD INFORMATION EDIT - View and edit c
✓ QUEUE PRIORITY - Modify Queue Priority
✓ QUEUE RESERVATIONS - Place Reservation On/Off
✓ RESERVATION REINSTATE - Reinstate Reservation
Grant
Revoke
GRANTED User Groups and Permissions
CASHIERING
COMP ACCOUNTING
FRONT DESK
GENERAL
PROFILES
QUICK KEYS
RATEMGMT CONFIG
RESERVATIONS
RESERVATIONS CONFIG
ROOMS MANAGEMENT
Grantees
Find
Copy
Save
OK
Close

***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 Visa USA’s website, “Cardholder Information Security Policy”, <http://usa.visa.com/business/accepting_visa/ ops_risk_management/cisp.html>.

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. [6]

MICROS recommends that all sensitive information that is transmitted over the Internet be secured using a form of encryption such as VPN or SSL; 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 SSL 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 SSL 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 Visa USA’s website, “Cardholder Information Security Policy”, <http://usa.visa.com/business/accepting_visa/ ops_risk_management/cisp.html>.

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.[7]

In accordance with the Visa USA PCI Data Security Standard, 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 Visa USA’s website, “Cardholder Information Security Policy”, <http://usa.visa.com/business/accepting_visa/ ops_risk_management/cisp.html>.

[6] “Payment Card Industry Security Audit Procedures.doc”, p. 18, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/ cisp%2Ehtml|View%20all%20CISP%20downloads>.

[7] “Payment Card Industry Security Audit Procedures.doc”, p. 20, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/ cisp%2Ehtml|View%20all%20CISP%20downloads>.

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.[8]

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.

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 Visa USA's website, "Cardholder Information Security Policy", <http://usa.visa.com/business/accepting_visa/ops_risk_management/ cisp.html>.

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.[9]

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 Visa USA's website, "Cardholder Information Security Policy", <http://usa.visa.com/ business/accepting_visa/ops_risk_management/cisp.html>

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.[10]

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

[8] "Payment Card Industry Security Audit Procedures.doc", p. 21, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/ cisp%2Ehtml|View%20all%20CISP%20downloads>.

[9] "Payment Card Industry Security Audit Procedures.doc", p. 26, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/cisp%2Ehtml|View%20all%20CISP%20downloads>.

[10] "Payment Card Industry Security Audit Procedures.doc", p. 27, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/cisp%2Ehtml|View%20all%20CISP%20downloads>.

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 SSL (To configure Opera application server for access over the HTTPS refer to the "OperaV403 – Configure Opera for SSL".pdf) or use network infrastructure such as secure VPN or similar.

For more information on Step 8 of the PCI Data Security Standard, "Assign a unique ID to each person with computer access", please consult Visa USA's website, "Cardholder Information Security Policy", <http://usa.visa.com/ business/accepting_visa/ops_risk_management/cisp.html>.

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.[11]

In accordance with the Visa USA PCI Data Security 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 Visa USA's website, "Cardholder Information Security Policy", <http://usa.visa.com/business/accepting_visa/ ops_risk_management/cisp.html>.

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.[12]

[11] "Payment Card Industry Security Audit Procedures.doc", p. 33, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/ accepting_visa/ops_risk_management/cisp%2Ehtml|View%20all%20CISP%20downloads>.

[12] "Payment Card Industry Security Audit Procedures.doc", p. 37, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/ accepting_visa/ops_risk_management/cisp%2Ehtml|View%20all%20CISP%20downloads>.

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 Visa USA PCI Data Security 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 Visa USA’s website, “Cardholder Information Security Policy”, <http://usa.visa.com/business/accepting_visa/ ops_risk_management/cisp.html>.

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.[13]

In accordance with the Visa USA PCI Data Security Standard, 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 Visa USA’s Web site, “Cardholder Information Security Policy”, <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html>.

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.[14]

In accordance with the Visa USA PCI Data Security Standard, 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 Visa USA’s Web site, “Cardholder Information Security Policy”, <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html>.

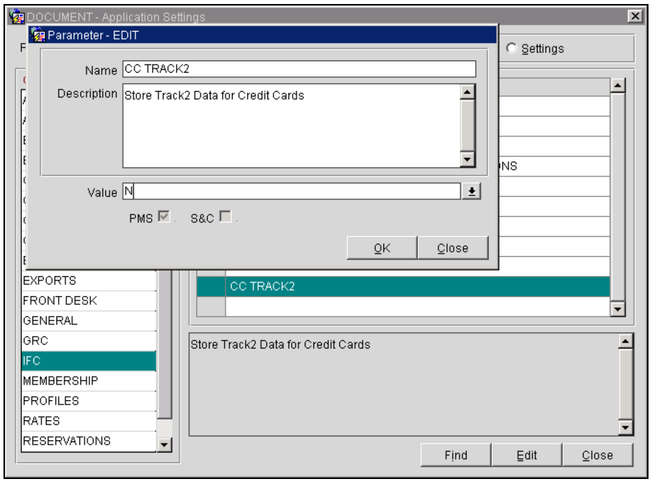
[13] “Payment Card Industry Security Audit Procedures.doc”, p. 41, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/cisp%2Ehtml|View%20all%20CISP%20downloads>.

[14] “Payment Card Industry Security Audit Procedures.doc”, p. 44, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/cisp%2Ehtml|View%20all%20CISP%20downloads>.

Guidance when Upgrading from a Previous Opera Version

I. Turning off the Track 2 Functionality

To stay in compliance with the visa PABP 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.



Name: CC TRACK2

Description: Store Track2 Data for Credit Cards

Value: N

PMS ☑ S&C ☐

Store Track2 Data for Credit Cards

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