STRATEGIC WHITEPAPER

OmniPCX Record – PCI Compliance 2.3

Legal notice

Index table

Document history

Edition	Date	Changes / Comments / Details
01	29-09-11	Initial Document
02	22-01-13	Remove statement suggesting that OPXR supports 256 Bit Encryption & Video Encryption
03	06-10-13	2.3 Initial Release

1 Scope

1.1 Overview

1.1.1 Purpose of this document

This OmniPCX Record white paper has been written to explain PCI standards, how they protect personal information when transactions are processed, bur most importantly, to demonstrate that OmniPCX Record V2.0 and above Offers the necessary features to enable companies to comply with these regulations.

Note: For a full list of the features & functionality that OmniPCX RECORD offers in order to maintain PCI compliance, please refer to the OmniPCX RECORD feature list.

2 Glossary of Terms

PCIDSS	➤	*Payment Card Industry Data security standard*
PCI	➤	*Payment Card Industry*
QSA	➤	Qualified Security Assessor
SAQ	➤	Self Assessment Questionnaire
API	➤	*Application Programmers Interface*
IT	➤	Information Technology
PIN	➤	Private Identification Number
SHA	➤	Secure Hash Algorithm
PC	➤	Personal Computer
SNMP	➤	*Simple Network Management Protocol*
ID	➤	Identification

3 Introduction

3.1 Overview – PCI Compliance

The Payment Card Industry Data security standard (PCIDSS) is a worldwide information security standard defined by the council of the same name. The standard was created to help organisations that process card payments in preventing credit card fraud through increased controls around data and their exposure to compromise. The standard applies to all organisations that hold, process, or exchange cardholder information from any card branded with the logo of one of the credit card brands.

Valuation of compliance can be performed internally or externally depending upon the volume of the card transactions the organisation is handling, but regardless of the size of the organisation, compliance must be assessed annually.

Organisations handling large volumes of transactions must have their compliance assessed by an independent assessor known as a "Qualified Securities Assessor" (QSA), while companies handling smaller volumes have the option of demonstrating compliance by completing a Self Assessment Questionnaire (SAQ). In some regions, SAQs still require sign-off by a QSA for submission.

Companies whose compliance is shown to have short comings and who maintain a relationship with one or more of the card brands risk losing their ability to process credit card payments and being audited and/ or fined.

Note: It is important to note that no call recording systems can be regarded as being PCI DSS compliant: it is the environment in which they are used that may be said to be compliant, as concluded by the security assessor. This is because the PCI DSS is subject to interpretation and only companies can comply.

3.2 Intended Readership

This manual targets the person responsible for maintaining PCI Compliance throughout their organisation.

3.3 Applicability Statement

This white paper applies to: OmniPCX Record version 2.x (and above).

3.4 Current PCI Requirements Reference

The current version of the PCI Compliance standards is V2.0 released on 26/10/2010 See: https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

4 Accommodating PCI Compliance

4.1 PCI DSS v2.0

PCI DSS v2.0 must be adopted by all organisations with payment card data by 1st January 2011, and from 1st January 2012 all assessments must be under version 2.0 of the standard. The headings and explanations below summarize the points from V1.2 01/10/2008 and specify the requirements for compliance and then a discussion on how OmniPCX Record assists in helping company's comply. These are organised into six logically related groups, which are called "control objectives" as outlined below.

4.1.1 Build and Maintain a Secure Network

The first relevant PCI DSS requirement here is to install and maintain a firewall configuration to protect cardholder data. OmniPCX Record operates with a network firewall. A list of services and ports necessary for its operation is provided and the default settings can be changed by the network administrator.

The second relevant PCI DSS requirement states that companies should not use vendor-supplied defaults for system passwords during the system installation and customers are advised to change system default passwords during system installation. OmniPCX Record incorporates strong authentication and password encryption and it also provides support for user authentication via a Radius Server. All server-based components of the OmniPCX Record solution run as Microsoft Windows services to provide enhanced security and data protection and they can be safely associated with Windows domains for better control and compliance with customer IT policies.

4.1.2 Protect Cardholder Data

The third relevant PCI DSS requirement states that stored card holder data must be protected. OmniPCX Record provides support for data archival and retention policies. Strong encryption of stored audio is provided using 128 bit key lengths. Wherever these files are stored, they remain encrypted. This also includes data backups and archives.

OmniPCX Record provides at the entry-level a web-based PC application, which allows the user to manually select a software button on their PC to commence the suppression of audio/video (pause) and resume the recording of audio/video. In addition there is an automatic time out setting which will optionally start the recorder again, if the user forgets to resume recording.

OmniPCX Record also provides an API (Application Programmer's Interface) for system integrators to develop middleware to pause and resume recording during a transaction. This prevents credit card and other personal data from being recorded via voice or screen. A system can then avoid all capture and retention of information containing card validation codes, and other PIN information.

The fourth relevant PCI DSS requirement is to encrypt transmission of cardholder data across open and public networks. Recordings can be encrypted and therefore all network transmissions under these circumstances will also be encrypted. When the calls are required

for replay or for any further analyses they are only decrypted just before use on the local device. OmniPCX Record provides an encrypted player for this purpose.

4.1.3 Maintain a Vulnerability Management Programme

The fifth relevant PCI DSS requirement is to develop and maintain secure systems and applications. OmniPCX Record employs a fast process for certifying Microsoft's critical and important security patches. Certification of these patches is based upon the Alcatel-Lucent Security Certification policy. Alcatel-Lucent develops software applications based on industry best practices. Information security is incorporated throughout the software development life cycle.

4.1.4 Implement Strong Access Control Measures

The sixth relevant PCI DSS requirement is to restrict access to cardholder data by business need-to-know. OmniPCX Record uses a profile-based user administration methodology to control user access. A profile consists of a set of privileges that define system functions and resources to which access is permitted. Changes of profile are dynamic and changes will take effect as soon as the information is saved. Every user with access to the system is assigned a unique User ID. All users need to input a unique user ID and a valid password before gaining access to the recorder. User passwords are hashed and stored using an industry standard 128-bit SHA (Secure Hash Algorithm designed by the National Security Agency). Specific password management capabilities of the OmniPCX Record solution supporting this requirement include the following:

- Addition, deletion and modification of user information is only allowed by authorised and verified personnel
- Users are automatically required to repeat the login process after 15 minutes of activity (user configurable)
- Optional support for Radius Server is provided to allow for user authentication and single sign-on based on users' Microsoft Window's credentials as well as for consistent user administration and password management policies in the organisation.

The seventh relevant PCI DSS requirement is to restrict access to cardholder data. With OmniPCX Record, users must have specific access profile rights in order to export audio and video to other media and formats

4.1.5 Regular Monitor & Network Tests

The next relevant PCI DSS requirement is to track and monitor resources and cardholder data. To this end, OmniPCX Record automatically captures system audit information on many different user transactions, as follows:

- User account security settings including both successful and failed login attempts
- Playback events including exporting of the recording
- User, group or profile changes
- Silent monitoring and record on demand events
- Changing the system rules
- Changes to the system configuration. Includes loggers, servers and domains

In addition, we audit information contained in the audit trails including

- User identification
- Type of event
- Date and Time
- Success or failure indication
- Origination of event
- Identity of name of affected data, system components or resource

All users must have specific access rights in order to access the audit trail information. Audit trail information is maintained on line. Audit trail information is saved in a Microsoft SQL Server database providing query, reporting, backup, archiving and security features. All system components maintain comprehensive logs and utilise SNMP alerts to report malfunctions.

And finally the last relevant PCI DSS requirement is to regularly test systems and processes. Alcatel-Lucent ensures that OmniPCX Record undergoes rigorous testing for compliance with best practice security requirements.

5 OmniPCX RECORD – Moving Forward

5.1 Road Map

For each successive roadmap delivery of OmniPCX Record version 2+, there are ongoing updates and improvements to the system. This paper highlights the lengths that we have gone to in order to offer companies a product that will help them be PCI compliant. For further information about how individual levels of software have new compliant-friendly features built in, please contact Alcatel-Lucent Professional Services by email at the following address.

professional.services@alcatel-lucent.com

www.alcatel-lucent.com/enterprise/services