Data Storage and Encryption Guide

for the AcuSport® V6 System Software

January 2015

AcuSport®
Retail Technology Group

940 Industrial Drive, Suite 107
Sauk Rapids, MN 56379
1-800-547-7120

Notices

940 Industrial Drive, Suite 107
Sauk Rapids, MN 56379
1-800-547-7120

General

No part of this document may be reproduced, distributed, performed, displayed, or used to prepare a derivative work without the prior and express written consent of AcuSport Corporation (“AcuSport”). The software described in this document is furnished under a license agreement and may be used only in accordance with the terms and conditions of the license agreement. Information in this document is subject to change without notice, and AcuSport assumes no responsibility for errors.

Trademarks and Credits

ACUSPORT, AXIS, AXIS Retail Management System (AXIS RMS), AXIS Data Center, AXIS Register, and AXIS E4473 are trademarks of AcuSport and shall not be used without the express written permission of AcuSport.

Other trademarks, such as QuickBooks, are not being used as a trademark herein and are the property of the respective owners.

Legal Counsel

This program, printed documentation, and documents should not be used as a substitute for professional advice in specific situations. The procedures, images, and examples in this document are for illustrative purposes only and may not be applicable in your setting due to differences in preference, settings, and/or state and local regulations.

The following notice is required by law:

AcuSport products and services are not a substitute for the advice of an Attorney.
You are encouraged to seek the advice of your own attorney concerning the use and legality of this program, documentation, and forms.

Publication Information

Data Storage and Encryption Guide for the AcuSport® V6 System Software
January 2015

Contents

Data Capture and Data Purging

The application may capture the magnetic stripe (located on the back of the card, contained in the chip, or elsewhere) and card verification values or codes (the three-digit or four-digit card-validation code printed on the back of the card) dependent upon mode of entry (MSR or Manual), within volatile system memory of the workstation in which the application is installed. In accordance with PCI Requirement 3.2, the software does not store, and may not be configured to store, sensitive authentication data (magnetic stripe data (located on the back of a card, contained in a chip, or elsewhere)) and card verification values or codes (the three-digit or four-digit card-validation code printed on the back of the card) after authorization.

The application automatically deletes the full contents of any track from the magnetic stripe (located on the back of the card, contained in the chip, or elsewhere) and card verification values or codes (the three-digit or four-digit card-validation code printed on the back of the card) upon authorization from volatile memory. Furthermore, the application does not support and cannot be configured to support the use of a PIN entry device and, as such, may not capture the PIN or Encrypted PIN block.

The credit card number and expiration date are retained subsequent to the authorization; however the information is secured by encrypting the credit card number. The credit card number is encrypted using Advanced Encryption Standard using Cypher Block Chaining with a 256-Bit key and RC4 encryption with floating encryption key in Medasyst tables. This allows the encryption word to be different for every transaction. This data is stored in the following locations only, card data is not stored in any other location by the application.

IMS Tables

Table Name	Field Name	Card Data Element Stored	Encryption Used
SalesMedia	CCNo	Credit card number (PAN)	Masked Only
SalesMedia	CCExpDate	Card Expiration Date	None
SOCtlg	CCNo	Credit card number (PAN)	256SEA
SOCtlg	CCExpDate	Card Expiration Date	None
SOCtlg	Key	Encryption Key	256SEA
SOCtlg	id_soctlg	Record Level Key	None
AR	Cardno	Credit card number (PAN)	AES256
RA	Key	Encryption Key	AES256

RA	id_ar	Record Level Key	None
Keys	key	Encryption Key	AES256
Keys	syskey	Record Level Key	None

Medasyst Tables within POS and IMS

Table Name	Field Name	Card Data Element Stored	Encryption Used
CesCapt	CardNumber	Credit card number (PAN)	RC4
CesCapt	ExpirDate	Card Expiration Date	None
CESAuth	CardNumber	Credit card number (PAN)	RC4
CESAuth	ExpirDate	Card Expiration Date	None
VisaCapt	CardNumber	Credit card number (PAN)	RC4
VisaCapt	ExpDate	Card Expiration Date	None
VisaAuth	CardNumber	Credit card number (PAN)	RC4
VisaAuth	ExpDate	Card Expiration Date	None
NovaCapt	CardNumber	Credit card number (PAN)	RC4
NovaCapt	ExpDate	Card Expiration Date	None
NovaAuth	CardNumber	Credit card number (PAN)	RC4
NovaAuth	ExpDate	Card Expiration Date	None
PmtCapt	CardNumber	Credit card number (PAN)	RC4
PmtCapt	ExpDate	Card Expiration Date	None
PmtAuth	CardNumber	Credit card number (PAN)	RC4
PmtAuth	ExpDate	Card Expiration Date	None
GPECapt	CardNumber	Credit card number (PAN)	RC4
GPECapt	ExpDate	Card Expiration Date	None
GPEAuth	CardNumber	Credit card number (PAN)	RC4

GPEAuth	ExpDate	Card Expiration Date	None
HPCapt	CardNumber	Credit card number (PAN)	RC4
HPCapt	ExpDate	Card Expiration Date	None
HPAuth	CardNumber	Credit card number (PAN)	RC4
HPAuth	ExpDate	Card Expiration Date	None

The application is configured to automatically handle purging of cardholder data in the following way: when the cardholder data is added to the Medasyst tables it is encrypted, card number and expiration date will remain at this state for 2 days, once this period is over, the card number and expiration date will be deleted. After 30 days the transaction data will be deleted permanently in the Medasyst tables. Credit Cards stored in the SalesMedia table after the transactions happens only contains last 4 digits of the credit card. SalesMedia table may be purged holding only the last year of data. Deciding to retain cardholder data outside of the application using third party means (Excel spread sheet, written hardcopy, etc.), understand that any cardholder data collected exceeding the defined retention period must be purged based upon business, legal, and/or regulatory requirements in order to achieve and meet PCI DSS compliance requirements.

Historical Data

Previous versions of the software do not store, and may not be configured to store, sensitive authentication data (magnetic stripe data (located on the back of a card, contained in a chip, or elsewhere)) and card verification values or codes (the three-digit or four-digit card-validation code printed on the back of the card) after authorization.

As with the current version, previous versions automatically delete the full contents of any track from the magnetic stripe (located on the back of the card, contained in the chip, or elsewhere) and card verification values or codes (the three-digit or four-digit card-validation code printed on the back of the card) upon authorization from volatile memory.

Encryption

The application utilizes Advanced Encryption Standard using Cypher Block Chaining with a 256-Bit key and RC4 encryption with floating encryption key in Medasyst tables for securing the storage of the credit card number and expiration date in accordance with PCI DSS 3.4. This data is stored in the following locations only, card data is not stored in any other location by the application.

IMS Tables

Table Name	Field Name	Card Data Element Stored	Encryption Used
SalesMedia	CCNo	Credit card number (PAN)	Masked Only
SalesMedia	CCExpDate	Card Expiration Date	None
SOCtlg	CCNo	Credit card number (PAN)	256SEA
SOCtlg	CCExpDate	Card Expiration Date	None
SOCtlg	Key	Encryption Key	256SEA
SOCtlg	id_soctlg	Record Level Key	None
AR	Cardno	Credit card number (PAN)	AES256
RA	Key	Encryption Key	AES256
RA	id_ar	Record Level Key	None
Keys	key	Encryption Key	AES256

Medasyst Tables within POS and IMS

Table Name	Field Name	Card Data Element Stored	Encryption Used
CesCapt	CardNumber	Credit card number (PAN)	RC4
CesCapt	ExpirDate	Card Expiration Date	None
CESAuth	CardNumber	Credit card number (PAN)	RC4
CESAuth	ExpirDate	Card Expiration Date	None
VisaCapt	CardNumber	Credit card number (PAN)	RC4

VisaCapt	ExpDate	Card Expiration Date	None
VisaAuth	CardNumber	Credit card number (PAN)	RC4
VisaAuth	ExpDate	Card Expiration Date	None
NovaCapt	CardNumber	Credit card number (PAN)	RC4
NovaCapt	ExpDate	Card Expiration Date	None
NovaAuth	CardNumber	Credit card number (PAN)	RC4
NovaAuth	ExpDate	Card Expiration Date	None
PmtCapt	CardNumber	Credit card number (PAN)	RC4
PmtCapt	ExpDate	Card Expiration Date	None
PmtAuth	CardNumber	Credit card number (PAN)	RC4
PmtAuth	ExpDate	Card Expiration Date	None
GPECapt	CardNumber	Credit card number (PAN)	RC4
GPECapt	ExpDate	Card Expiration Date	None
GPEAuth	CardNumber	Credit card number (PAN)	RC4
GPEAuth	ExpDate	Card Expiration Date	None
HPCapt	CardNumber	Credit card number (PAN)	RC4
HPCapt	ExpDate	Card Expiration Date	None
HPAuth	CardNumber	Credit card number (PAN)	RC4
HPAuth	ExpDate	Card Expiration Date	None

As previously stated, key generation is performed using a programmatic process. Keys used for encryption are encrypted upon storage using Advanced Encryption Standard using Cypher Block Chaining with a 256-Bit key. Making sure to restrict access to and the ability to change keys to the fewest number of custodians necessary. These custodians must acknowledge their role in securing the encryption keys. A sample key custodian for use is contained in this section. Access to generate new keys is restricted to authorized PCI application users. This setting is available under Security for each user. The application supports the merchants' ability to change the key for stored data, the IMS requires that the custodian present the current key and then create a new key twice, then enter a verification code that changes on each attempt. Two partial keys are

stored in the Keys table one of these keys are stored with the encrypted PAN. There is an additional record level key with the PAN. These are partial keys that can only be decrypted with another portion of the key from the proprietary software. Decryption requires a two-step decryption bringing three keys together at each step. All pieces are required to decrypt the PAN data.

Encryption Keys may be changed as often as required. However, adhere to the following key management processes to maintain PCI DSS compliance:

- Change encryption keys if they have been weakened such as by the departure of a key custodian (this must happen immediately); and
- Change encryption keys if compromise is confirmed or suspected (this must happen immediately).

► Note: The application prevents the unauthorized substitution of keys through the use of Security for application users. Access to change keys through the application is logged. In addition, to prevent a key from being modified outside of the application, a check is performed to confirm no changes have been made. If a key is modified, the application will audit the changes.

Sample Key Custodian Form

All Company staff that hold responsible authorized positions where they manage or handle encryption keys must sign the following document.

As a condition of continued employment with Company, and as an employee that has access to key management tools and equipment, you are obligated to sign the following to indicate acceptance of your responsibility.

The signatory of this document is in full employment with Company on the date shown below and has been afforded access to key management devices, software and equipment, and hereby agrees that, he or she

1. Has read and understood the policies and procedures associated with key management and agrees to comply with them to the best of his/her ability, and has been trained in security awareness and has had the ability to raise questions and has had those questions answered satisfactory;
2. Understands that non-compliance with the key management procedures can lead to disciplinary action including termination and prosecution. Exceptions to compliance only occur where such compliance would violate local, state, or federal law, or where a senior officer of the company or law enforcement officer has given prior authorization;
3. Agrees to never divulge to any third party any key management or related security systems, passwords, processes, security hardware or secrets associated with the Company systems, unless authorized by an officer of the Company or required to do so by law enforcement officers; and
4. Agrees to report promptly and in full to the correct personnel, any suspicious activity including but not limited to key compromise or suspected key compromise. Suspicious activity can include: signs of unauthorized equipment usage during evenings and weekends, phone requests from unidentifiable callers for access to secure information, unidentifiable files found on file servers, and unusual activity recorded in log files.

I agree to the above and understand that this original copy will be held on my personnel record and kept by the company indefinitely.

Signed: _____

Print Name: _____

Date: _____