Hybrid PA-DSS Report on Validation

For Applications that Store, Process, or Transmit Payment Card Data but are Not Part of Authorization or Settlement

Application Vendor:

KomBea Corporation
3400 N. Ashton Blvd. Suite 190
Lehi, UT 84043

Application Name and Version:

SecureCall 3.0

Copyright© 2012
www.securitymetrics.com

Contact Information and Report Date

Report Date

March 8, 2012

Service Provider Information

Organization Name:	KomBea Corporation
Contact Name:	Dave Peachey, VP Product Development
Address:	3400 N. Ashton Blvd. Suite 190 Lehi, UT 84043
Phone:	(801) 610-5805
Email:	dave.peachey@kombea.com

Assessor Contact Information

Bruce Bogdan, CISSP, QSA, PA-QSA
Senior Security Analyst
SecurityMetrics, Inc.
1275 West 1600 North
Orem, UT 84057
(801) 724-9600
bbogdan@securitymetrics.com

Executive Summary

Introduction

KomBea Corporation is an application vendor specializing in software development geared toward call center environments. Specifically KomBea focuses on call centers where credit card payments are accepted by the call center's customer service representatives (CSRs). Many of KomBea's customers have call centers in locations where fraud and pressure to commit fraud is prevalent. The use of the KomBea SecureCall application can reduce or eliminate the opportunity for fraud to occur.

Although CSRs can accept card payments using SecureCall, and card numbers do transit the application it is not in scope for PA-DSS because it is not part of authorization or settlement. This can cause issues with KomBea customers because there is a general understanding that if an application touches cardholder data in any way then it needs to be PA-DSS validated. This assessment was conducted to address the security of SecureCall and to address any questions that customers may have about the applicability of PA-DSS to SecureCall.

Overview

The KomBea offices are located in Lehi, Utah. Dave Peachey was the primary contact with Kolby Olsen and Matt Mace assisting during testing. Dave heads the product development department and provided the documentation required for the assessment. Kolby is one of the primary developers of SecureCall and Matt is the systems administrator for KomBea.

The SecureCall application secures the acceptance of credit card payments by removing the ability of the CSR to see or hear the primary account number (PAN) when a payment is made. This is accomplished in the following manner. When a payment is to be made the CSR clicks a payment icon on their interface and the SecureCall application is started. Control of the system is passed to a multiplexer (KPlexer) that is attached to the agents phone and the customer enters the card number on their phones keypad. The DTMF tones are interpreted by the KPlexer, which encrypts the data stream and passes it either to the back end server where it is forwarded to the call center's payment application or directly to the payment application.

No card numbers are ever displayed on the agents screen and the DTMF tones are changed to a monotone so that the PAN cannot be determined from listening to the tones. No cardholder data ever is stored by SecureCall on the CSR's desktop or on the KomBea back end server and all data that transits these systems is encrypted using AES-256 as the encryption algorithm.

It was verified by interview with Dave and by observation of SecureCall running in the test lab that there was no ability for a customer service representative to intercept cardholder data in any way. It was also verified that at no time does the application store cardholder data on any system that is in scope for this assessment and that no authorization or settlement actions were performed by SecureCall.

The SecureCall components consist of the agent running on the CSR's desktop

system, the KPlexer device and potentially an agent running on a backend server. KomBea does not provide any other hardware or software with SecureCall and they provide no ability to connect to a processor or payment gateway.

It was verified by observing SecureCall in the test lab that it is not a wireless application.

Individuals Interviewed During the Assessment

Name	Title
Dave Peachey	VP Product Development
Ronnie Johansen	VP Operations
Kolby Olsen	Lead Developer
Matt Mace	Lead Quality Engineer

Figure 1 – Secure Call Configuration A

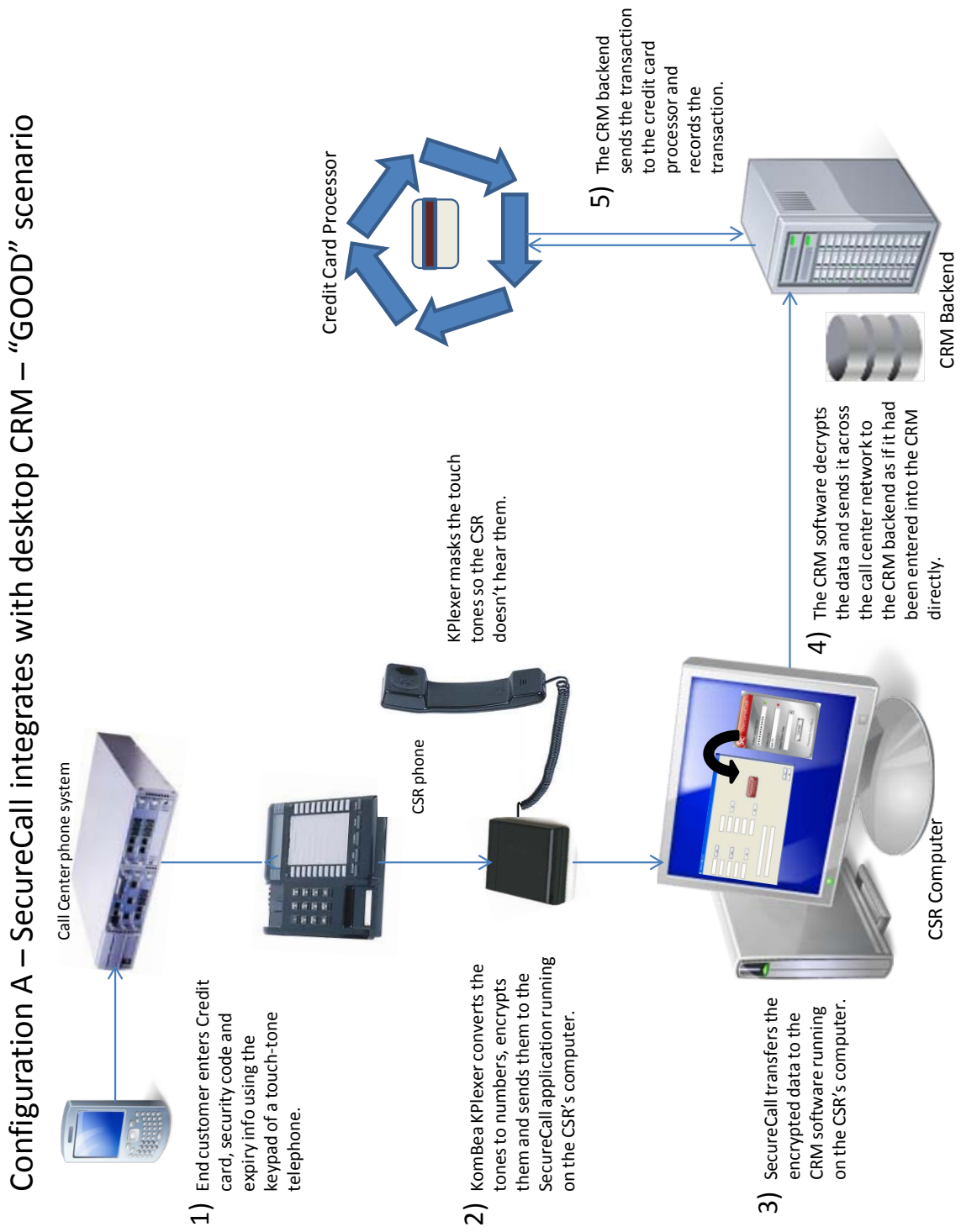
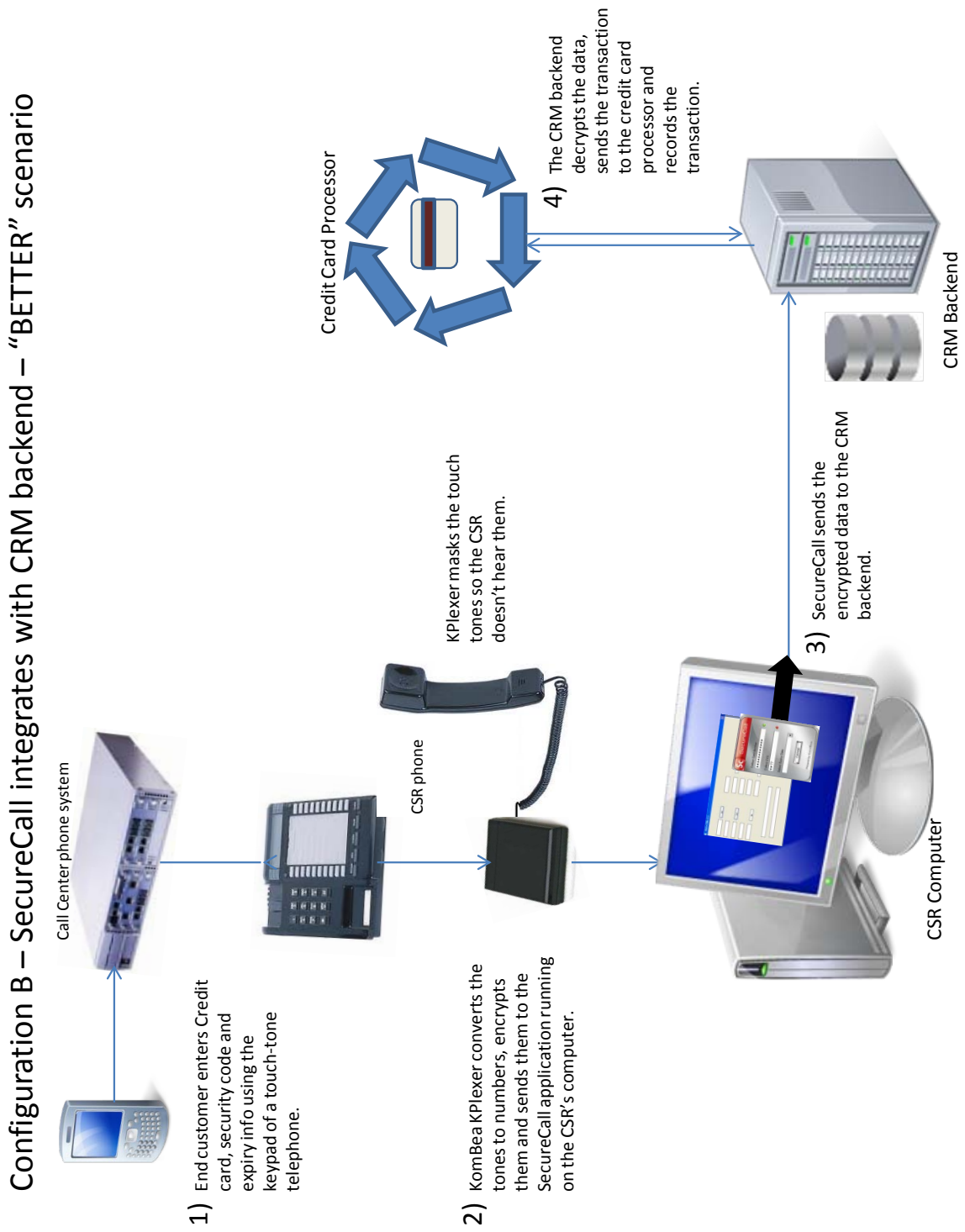


Figure 2 – Secure Call Configuration B



Scope of Work and Approach Taken

Timeframe and Location of Assessment

The assessment of the KomBea SecureCall application was conducted from December 2011 to March 2012 with testing occurring in the KomBea labs on February 8, 2012. A forensic examination of the collected data occurred the following week in the SecruityMetrics' test lab. The SecurityMetrics assessor used version 2.0 of the PA-DSS as a basis for compliance to conduct the assessment of SecureCall. Although SecureCall is not in scope for a PA-DSS assessment the standard provides assurance that the tested application meets all the relevant security requirements of any application that is found on the list of PA-DSS verified applications.

Application Specifics

- Application Tested:
  - SecureCall
- Version of Application Tested:
  - 3.0
- Operating Systems Used During Testing:
  - Windows 7 SP1
  - Windows 2008 R2 SP2
- Database Used By Application:
  - SecureCall does not use a database to store cardholder data.
- Brief Description of Application:
  - The KomBea SecureCall application is designed to improve the security of a credit card transaction for telephone order transactions. It does this by allowing the customer to enter the PAN on their touch-tone phone and translates the DTMF tones that are entered. The call center representative has no interface where they can see the digits being entered nor can they hear the DTMF tones entered. This eliminates the possibility of the CSR stealing the card information because they never have access to it.

Hardware and Software Used During Testing

- KomBea call center simulation application
- Phone Factor
- SonicWall TZ200 Firewall
- EventSentry
- Symantec Endpoint Protection Antivirus/Malware

Test Matrix

OS Configuration Tested	Call Center Simulator (Test Environment)
Case 0: Windows 7 SP1	✓
Case 1: Windows 2008 R1 SP2	✓
Case 2: Windows 7 SP1 Full Debug Mode	✓

How Cardholder Data is Stored by Application

No cardholder data is stored by the SecureCall application. Data from each transaction is passed directly to the call centers payment application.

Related Software Components

There are no related software components required by SecureCall.

End-to-End Authentication Methods

There is no authentication built into SecureCall. All administrative authentication is managed by the operating system. User accounts for testing were created in the Microsoft Windows systems and were consistent with all requirements outlined in section 8 of the PCI-DSS and section 3 of the PA-DSS. No default system accounts were used during testing, and users are instructed in the implementation guide to never use default accounts on any system that is used in the card environment.

Typical Implementation

The typical implementation for the KomBea SecureCall application is on systems in call center locations where the customer service representatives take credit card payments over the phone. The location where SecureCall is installed would need to be in a PCI compliant DMZ as outlined in the implementation guide.

Typical Customer

The typical customer for SecureCall would be any call center or other entity that accepts credit card transactions over the telephone.

Versioning Methodology

KomBea SecureCall uses the form X.X for its versioning methodology with the first octet representing a major version release and the second representing minor changes. An example of a major change might be changes to the encryption of the data flow and a minor change might be changes to the application interface.

Findings and Observations

Because KomBea SecureCall does not store, process, or transmit card data as part of authorization or settlement, a complete and formal PA-DSS Report on Verification was not required. However, as a way to organize the data collected during the on-site visit, the PA-DSS requirement headings will be used to discuss the security of the application.

1) Do not retain full magnetic stripe, card validation code or value, or PIN data.

- Because it is only used for card not present transactions there is no ability for SecureCall to obtain magnetic stripe data so no such data can be retained.
- Verified by observation of the running application that it does not support PIN transactions, thus no ability to retain PIN data is possible.
- Verified by observation of the running application and by a forensic examination of the test systems that SecureCall does not retain CVV data. Verified by interview with Dave that all card data is passed directly to the call centers payment application and is never written to non-volatile memory or other storage locations.

2) Protect stored cardholder data

- Verified by interview with Dave and by a forensic examination of the test systems that cardholder data is never stored in any form by SecureCall.

3) Provide secure authentication features.

- Verified by interview with Dave and by observation of SecureCall running in the test lab that there are no built in authentication features. All authentication is managed by the underlying operating system and is thus not applicable to this assessment.
- Verified by observation of the application running in the test lab that it does not interfere with the operating systems authentication features in any way.

4) Log payment application activity

- Because of the limited nature of SecureCall's interaction with the host system there is very little that is logged, but the log files that are produced were examined and found to meet the requirements outlined in section 4 of the PA-DSS.
- Verified by observation of the log files that they can be collected and moved to a central log repository.
- Verified by observation of the log files that no sensitive information including cardholder data is ever written to the logs.

5) Develop secure payment applications

- Verified by interview with Dave and by observation of the KomBea SDLC that they develop applications in accordance with PCI-DSS and PA-DSS requirements and with industry best practices.
- Verified by interview with Dave and by observation of the development environment that live cardholder data and customer data are not used for testing.
- Verified by interview with Dave and by observation of the SDLC that code reviews by a person other than the code author are required.
- Verified by observation of the change control procedures that code review, back out procedures, customer impact and management approval are all included in the process.

6) Protect wireless transmissions

- Verified by interview with Dave and by observation of the application running in the test lab that SecureCall is not a wireless application.

7) Test payment applications to address vulnerabilities

- Verified by interview with Dave and by observation of the SDLC that testing is to be conducted to address all common vulnerabilities.
- Verified by interview with Dave that they subscribe to several resources to identify new security vulnerabilities including Secunia.org, and the OWASP mailing list.

8) Facilitate secure network implementation

- Verified by observation of SecureCall running in the test lab that it does not interfere with security appliances or applications running in the test environment. These applications and appliances were included in the test lab setup and are listed in the executive summary.

9) Cardholder data must never be stored on a server connected to the Internet

- Verified by observation of the application running in the test lab and by a forensic examination of the test systems that cardholder data is never stored by the SecureCall application.

10) Facilitate secure remote access to payment application

- Verified by observation of a remote 2-factor authentication event that SecureCall does not interfere with the ability to make a 2-factor remote connection. The factors observed were a username/password combination and a PhoneFactor token.

11) Encrypt sensitive traffic over public networks

- Verified by observation of the application running in the test lab that it never sends cardholder data over public networks. However, the data sent by SecureCall to the call centers payment application is encrypted using AES-256 encryption even though it only transits the call centers private network.

12) Encrypt all non-console administrative access

- Verified by observation of the installation guide that customers are instructed to encrypt all non-console administrative access. The method suggested is to turn encryption on when using RDP to access the systems remotely.

13) Maintain instructional documentation and training programs

- Verified by interview with Dave and by observation of the installation guide that instruction is given to customers for the installation of SecureCall in a PCI-DSS compliant environment. Also, that KomBea provides training either in their offices in Lehi or on site at the customers location.

Conclusion

Not all applications that touch cardholder data are in scope for PA-DSS because they are not part of authorization or settlement and as such cannot be listed on the PCI Councils list of validated payment applications, but security concerns still exist regarding these applications. KomBea wished to address these concerns by having their application validated in the same manner as any payment application. SecureCall was assessed against the Payment Application Data Security Standard version 2.0 and was found to be in compliance with all the requirements that were applicable. In essence using SecureCall poses no greater security risk than any application that is listed on the PCI Councils web site.

After conducting an assessment of the KomBea SecureCall v2.0 application and visiting the KomBea offices located in Lehi, Utah and observing their development practices it was determined that using the SecureCall application does not compromise the PCI-DSS compliance of the environment where it is installed in any way. It was further found that not only does it not interfere with PCI compliance but also it has the ability to greatly enhance the security of the environment it is installed in, as well as reducing the scope of the environments PCI assessment.

Bruce Bogdan, CISSP, QSA, PA-QSA
SecurityMetrics Inc.
Senior Security Analyst
801-724-9600
bbogdan@securitymetrics.com