Introduction
For deployers handling credit card information, the question of PCI compliance is a primary concern and when KioWare is part of their solution, we are asked whether KioWare is PA-DSS validated. On June 29, 2011, the PCI Security Standards Council (PCI SSC) published a list of requirements meant solely to minimize the number of applications eligible for validation under PA-DSS. The second item on their list directly affects KioWare.

#2 – Does the application handle cardholder data, but the application itself does not facilitate authorization or settlement?

What Does This Mean?
Interpreted broadly as they have, the above requirement makes it impossible for KioWare, or any kiosk system software, to be PA-DSS validated. Despite KioWare being successfully evaluated to PA-DSS testing standards, the PCI SSC now believes we don’t need to be validated. We believe this to be very short sighted because it provides an easy out for both unscrupulous and ignorant deployers and software vendors. By not being certified, software vendors are not required to publish an approved PA-DSS Implementation Guide which details to deployers everything they need to know to ensure PCI compliance.

Why does this policy make sense for industry-wide compliance?
The only guidance PCI SSC provides is that applications ‘not eligible for PA-DSS validation would be included as part of an entity’s annual PCI DSS assessment to ensure that the application is compliant with all applicable PCI DSS requirements.’ How an entity is expected to perform that task is left unanswered. We think the credit card payment industry deserves better.

On the one hand, the fact that many of the PA-DSS requirements don’t apply to software such as KioWare may be a reason for the PCI SSC’s decision. But on the other hand, there absolutely are ways to implement KioWare that are not PCI compliant and it is only by following the KioWare PA-DSS Implementation Guide that a deployer can be certain that KioWare is contributing to their overall PCI compliance – not hurting it.

How to Cope?
Until the PCI SSC revises their policy, deployers should only work with software vendors who have had their software evaluated by a qualified Payment Application testing lab to the same PA-DSS standard as if they were submitting to the PCI SSC. This will ensure that a valid PA-DSS Implementation Guide exists. For deployers, this will be more difficult because they can no longer search one list for all approved applications, but now must individually query vendors who are not on the list. And as alluded to above, it will be easy for an unscrupulous software vendor to dupe unsuspecting deployers, and equally easy for unscrupulous deployers to pass the buck.

Refer to the attached letter of validation from our certified Payment Application testing lab as well as our PA-DSS Implementation Guide for more information about using KioWare in a PCI Compliant system. For more information on the PCI SSC’s position, see https://www.pcisecuritystandards.org/documents/Applications_Eligible_for_PA-DSS_Validation.pdf.

Summary
Until the PCI SSC reverses their position and allows KioWare (and similar software) to be PA-DSS validated, deployers should only work with software vendors who have had their software independently tested to PA-DSS standards and include a PA-DSS Implementation Guide. If there are any questions about the Implementation Guide, contact the software vendor before deploying into production.
Letter of Validation for Payment Application Security Assessment Services

Halock Security Labs, a Payment Application Qualified Security Assessor Company, has engaged with Analytical Design Solutions Inc. (“ADSI”) to assist in achieving compliance with the PCI Payment Application Data Security Standard (PA-DSS) v2.0.

On June 29, 2011 the PCI Council released a requirements checklist for eligibility for PA-DSS Validation. Based on this newly released document, KioWare Kiosk no longer meets the Council’s criteria for PA-DSS validation eligibility and is unable to submit the Report on Validation (ROV) to the Council.

Halock completed validation of KioWare Kiosk v6.7.0 using the PCI Payment Application Data Security Standard (PA-DSS) Requirements and Assessment Procedures v2.0. Due to the design and functionality of the KioWare Kiosk software, many of the PA-DSS requirements were deemed non-applicable, but our assessment showed that the KioWare Kiosk v6.7.0 payment application (deployed on Windows 7 Professional) has been developed in accordance with secure development best practices and supports those requirements in the PA-DSS that are applicable.

The primary intent of the PA-DSS is to ensure that payment applications do not interfere with a merchant’s ability to achieve PCI DSS compliance when implemented in accordance with the application’s Implementation Guide. Halock has determined that KioWare Kiosk v6.7.0 achieves that objective and can support a PCI DSS compliant environment, assuming the other supporting components of the environment are configured in a PCI compliant manner.

Halock’s validation testing was conducted from 06/13/2011 through 07/15/2011.

Best Regards,

Shelina Samji, PCI QSA, PA QSA
Senior Consultant, PCI Compliance Services

Jeremy Simon, PCI QSA, CISSP, CISA
Practice Lead, PCI Compliance Services

HALOCK Security Labs, Purpose Driven Security™
847.221.0200 Office
734.904.9280 Mobile
847.637.8324 Fax
800.925.0559 Incident Response Hotline
ssamji@halock.com

HALOCK Security Labs, Purpose Driven Security™
847.221.0200 Office
847.344.0673 Mobile
847.637.8324 Fax
800.925.0559 Incident Response Hotline
jsimon@halock.com
PA-DSS Implementation Guide

for KioWare Kiosk System Software

Version 1.0.2
# Table of Contents

Document Version History .................................................................................................................. 2

1. INTRODUCTION ........................................................................................................................................... 3
   1.1. Introduction ....................................................................................................................................... 3
   1.2. Distribution and Updates ............................................................................................................. 3

2. CONFIGURATION ......................................................................................................................................... 4
   2.1. General Security Issues .................................................................................................................. 4
   2.2. Start Page URL ................................................................................................................................... 4
   2.3. User Logon and Password ................................................................................................................. 5
   2.4. Domain and Page Access Control Lists ........................................................................................................ 5
   2.5. Scripting Access Control Lists ............................................................................................................ 6
   2.6. MSR Input Device Configuration ....................................................................................................... 7
   2.7. KioWare Shell .................................................................................................................................. 10

3. DATA FLOW ............................................................................................................................................... 11
   3.1. Input Form Navigation ..................................................................................................................... 11
   3.2. Input Form Parsing .......................................................................................................................... 11

4. REMOTE ACCESS ....................................................................................................................................... 12
   4.1. Merchant Applicability .................................................................................................................... 12
   4.2. Remote Access Software Security Configuration ................................................................................ 12

5. WIRELESS CONFIGURATION .................................................................................................................. 13

6. ENCRYPTION OF NETWORK TRAFFIC .................................................................................................. 14
## Document Version History

<table>
<thead>
<tr>
<th>Version</th>
<th>Release Date</th>
<th>Change Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0</td>
<td>6/16/2011</td>
<td>Initial Release for KioWare v6.7.0</td>
</tr>
<tr>
<td>1.0.1</td>
<td>3/22/2012</td>
<td>Updated for KioWare v6.8.0</td>
</tr>
<tr>
<td>1.0.2</td>
<td>1/28/2013</td>
<td>Updated for KioWare v7.0.0</td>
</tr>
</tbody>
</table>
1. INTRODUCTION

1.1. Introduction
This PA-DSS Implementation Guide is intended to instruct application developers, integrators and deployers how to properly configure and deploy KioWare into their environment in a PA-DSS compliant manner. As KioWare is only a single component among many components that make up your payment system, your complete PCI compliance requires that all components be configured and deployed in a PA-DSS compliant manner.

1.2. Distribution and Updates
This PA-DSS Implementation Guide should be disseminated to all relevant users including application developers, integrators and deployers. It should be updated after changes in the software and at least annually. The annual review and update will also include any changes in the PA-DSS standard.

The most current version of this Implementation Guide can always be found on the KioWare website: http://www.kioware.com/download.aspx. In addition, the Implementation Guide will be included in all software updates.
2. CONFIGURATION

2.1. General Security Issues
As KioWare is essentially browser lockdown software and every deployment is different, it is important to evaluate every setting in the KioWare Configuration Tool to determine its applicability and impact on your deployment. Our technical support staff is readily available to help you. The following Configuration Tool settings are known to impact PA-DSS. In all cases, additional information about the setting can be found in the KioWare User Guide.

2.2. Start Page URL
Per PCI DSS 4.1, all network communication must use SSL/TLS, so when specifying your Start Page URL, make sure to specify https://. Refer to the screenshot below:
2.3. User Logon and Password
When defining the user account that will execute KioWare it is important to not use an account with Administrator privileges. In addition, it is important to create unique usernames and PCI DSS compliant complex passwords.

2.4. Domain and Page Access Control Lists
To thwart malicious security attacks, it is recommended to define a Browsing Access Control List that is used to specify domains and pages that the application is allowed to navigate to. Refer to the screenshot below:
2.5. Scripting Access Control Lists

To thwart malicious security attacks, it is recommended to define a **Scripting Access Control List** that is used to specify domains and pages that the application is allowed to execute KioWare scripting commands. If your application doesn’t use KioWare scripting commands, then you should set the **Access Type** to ‘Block Scripting’, otherwise set it to ‘Allow Scripting’. Refer to the screenshot below:
2.6. MSR Input Device Configuration

KioWare is responsible for transferring the cardholder data read by the Magnetic Stripe Reader (MSR) device and passing it along to the payment application. The data is never stored by KioWare. This can be performed using two different methods: Form Navigation or Form Parsing.

2.6.1. Input Form Navigation

Form Navigation takes the stripe data and formats it as HTML form data and redirects to a specified URL. There are two very important settings:

- The Navigate Page Data Via setting must be set to 'Post', otherwise cardholder data may be stored in web logs as plain text.
- The Input Navigate URL must use https:// to ensure data is transmitted using SSL/TLS.

See screenshot below:
2.6.2. Input Form Parsing

Form Parsing takes the stripe data, parses the name, PAN, card type and expiration date, and inserts it into the current html page as specified. KioWare needs to know the HTML control names on the page so that the data is inserted properly. See the screenshot below:
2.6.3. Input Access Control Lists

To thwart malicious security attacks, it is recommended to define a *Input Access Control List* that is used to specify domains and pages that KioWare is allowed to read data from the MSR. Typically, the ACL consists of a single page that contains the screen instructions to the user to swipe their card. Refer to the screenshot below:
2.7. KioWare Shell

To thwart malicious security attacks, it is recommended to run KioWare as the System Shell. When KioWare is the System Shell, there is no Windows Desktop for a malicious user to hack into. Should the malicious user manage to exit KioWare, the worst outcome is the user will be presented with a Windows Logon dialog. More likely, KioWare’s Watchdog Service will notice that KioWare is no longer running and restart KioWare.

To set KioWare as the System Shell, click the ‘User Security Settings’ button on the Security page, logon as your kiosk user, then select KioWare as the User Shell. Note:

- It is critical that the kiosk user is not an administrator account as you may lock yourself permanently out of the computer.

- When you set KioWare as the User Shell, do not set any User Security Settings as they are mutually exclusive and you may lock yourself permanently out of the computer.

![KioWare Configuration Security Page](image)
3. DATA FLOW

KioWare is responsible for transferring the cardholder data read by the Magnetic Stripe Reader (MSR) device and passing it along to the payment application. The data is never stored by KioWare. This can be performed using two different methods: Form Navigation or Form Parsing.

3.1. Input Form Navigation

Form Navigation takes the stripe data and formats it as HTML form data and redirects to a specified URL.

3.2. Input Form Parsing

Form Parsing takes the stripe data, parses the name, PAN, card type and expiration date, and inserts it into the current html page as specified.
4. REMOTE ACCESS

4.1. Merchant Applicability
KioWare based deployments can be accessed remotely. Remote access should be performed using two-factor authentication per PCI DSS requirement 8.3. Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use a VPN (based on SSL/TLS or IPSEC) with individual certificates.

4.2. Remote Access Software Security Configuration
Implement the following applicable security features for all remote access software used by the merchant, reseller or integrator.

- Change default settings in remote access software (Ex. passwords)
- Allow connections only from specific known IP/MAC addresses
- Use strong authentication or complex passwords for logons.
- Enable encrypted data transmission
- Enable account lockout after a certain number of failed logon attempts
- Configure so a remote user must first establish a VPN connection using a firewall before access is allowed.
- Enable the logging function
- Restrict access to customer passwords to authorized reseller/integrator staff
- Establish customer passwords according to PC DSS requirements 8.1-2 and 8.4-5
5. WIRELESS CONFIGURATION

If you plan to connect via a wireless network, adhere to the following:

- Change wireless vendor defaults as defined in PA-DSS requirement 6.1.a – 6.1.e
- Use strong encryption (such as SSL) for authentication and transmission of cardholder data
6. **ENCRYPTION OF NETWORK TRAFFIC**

Per PCI DSS 4.1, when configuring KioWare, domains must be specified to use SSL/TLS; ie, domains must be of the form: https://