DIALOGS™

KALEIDOSCOPE™

# Dialogs security and PCI compliance.

Dialogs is the premier framework for web application development. Dialogs has an established track record of delivering design-focused, cost-effective, and scalable applications. The inherent flexibility of Dialogs makes it a natural platform for ecommerce catalogs and shopping cart solutions. This document describes best practices for managing security in any Dialogs environment, but particularly as it relates to ecommerce. Provisions for deploying Dialogs in adherence to Payment Card Industry (PCI) compliance issues are also described.

Security is a paramount design criteria for Dialogs. From initial architecture to the most recent feature updates, Dialogs has been constructed to limit the potential threat of outside attacks and to protect the data and the environment where it is installed. Dialogs developers adhere to the security principals of Open Web Application Security Community (OWASP) and require our certified developer partners to do the same. (OWASP: http://www.owasp.org/index.php/Top_10_2007)

The default installation of Dialogs requires that all authenticated access be conducted via SSL. Kaleidoscope recommends that this measure not be circumvented. Additionally, Kaleidoscope recommends hosting Dialogs in secure hosting environments and conducting periodic security scans against the installation to rapidly, proactively identify any potential vulnerabilities.

## Payment Card Industry Security Requirements

In 2006, Visa, MasterCard, American Express, Discover, and JBC formed an independent body, the Payment Card Industry (PCI) Security Standards Council which manages the the PCI Data Security Standard (DSS) a framework to protect cardholder data. PCI DSS defines 12 measures to safeguard Cardmember Data (CMD). A companion PCI framework is Payment Application Data Security Standard (PA DSS) expected to be published in 2008. PA DSS is a migration of a Visa program Payment Applications Best Practices (PABP) that defines parameters for secure application design. (PCI DSS: https://www.pcisecuritystandards.org/)

All but the largest merchants (who must adhere to more stringent measures) are required to complete a Self-Assessment Questionnaire (SAQ) and provide an Attestation of Compliance to become PCI DSS compliant. Depending on how ecommerce is implemented, merchants must conform to progressively more demanding SAQ versions A, B, C and D. Merchants required to complete SAQC or SAQD must also conduct quarterly security scans (by accredited third parties) against all internet-facing IP addresses (e.g. routers, web servers, email servers, application servers). Any application that "stores, processes, or transmits" the Primary Account Number (PAN) must be PCI DSS compliant and will likely be required to undergo a certification process once PA DSS is implemented. Additionally, in June 2008, all payment applications that are internet-facing must either undergo a custom security audit of source code (estimated at $5 per line of code (Dialogs has over 11,000 lines of code) OR install a Web Application Firewall (WAF) between the application and the internet. The least expensive commercially available WAF we have found is $12K. (see http://www.breach.com/products/modsecurity-pro-m1100.html)

To provide proper incentives for merchant compliance, the card associations have offered both carrots and sticks. As a carrot, merchants are offered protection from PCI related fines, which can be as high as $500,000 per incident, if they are compliant at the time of the breach – something called Safe Harbor. As a stick, merchants can face the above mentioned fines when breached as well as be fines for non-compliance. The State of Texas was the first state to make PCI compliance a law (http://www.legis.state.tx.us/BillLookup/history.aspx?LegSess=80R&Bill=HB3222). Most states are expected to follow. This development elevates matters from a civil to a criminal issue.

## Dialogs Deployment for PCI Security Compliance

Dialogs may be deployed in an ecommerce environment numerous ways. The flexibility of the framework makes API integration to payment gateways an efficient, straightforward task. This is a traditional approach for custom cart integration and many large payment gateways, including Authorize.net, still recommend this over other options. Electing to proceed down this path increases both the cost of compliance and liability to the merchant, however. Kaleidoscope recommends against it. To understand why we illustrate two scenarios:

> **Scenario A:** Minimize the risk by outsourcing all "PCI Eligible" components of the process. This means Google Checkout, or Authorize.net's SIM (but not AIM or ABR). There are also alternative solution providers that offer the rich controls of AIM (meaning the visitor never leaves the Dialogs-based website). In these scenarios, the actual payment application is entirely hosted by a third party that presents assurance of PCI compliance. Merchants self access with SAQA (or SAQB if they also have an in-house card swipe terminal), the simplest forms with only 11 or 21 questions to verify.
>
> **Scenario B:** Proceed with direct implementation of the payment application within Dialogs. This means direct post to gateways such as Authorize.net's AIM and ABR. In this environment, Dialogs would not store credit card data but would process and transmit that data to the gateway. By doing so, the Dialogs site owner would be required to stipulate that their custom application (i.e., customizations to Dialogs) is PCI compliant (PCI requirement 6), and Dialogs would have to be hosted in a PCI compliant environment (i.e., NOT Kaleidoscope's data center). Merchants self access with SAQD, the full PCI-DSS self assessment questionnaire with over 200 questions to verify. Additionally, while Kaleidoscope follows the secure coding guidelines stipulated in PCI 6.5, PCI 6.3 stipulates features of information security during the development life cycle (such as separate development, test, and deployment environments) that are beyond the development budgets of all but our largest projects.

The PCI Security Council recommends segmentation of the payment application from the remainder of the merchant's network to reduce compliance scope (Scenario A); Kaleidoscope agrees. The compelling business case for all Dialogs customers, even our large Fortune 1000 customers, is Scenario A to mitigate liability, limit cost, and shorten compliance time by segmenting the payment application from custom code (Dialogs) and the hosting environment where it resides. Elegant solutions that reinforce buyer confidence and do not compromise the end-user experience exist. ***For this reason, Kaleidoscope will NOT implement direct API solutions for eCommerce transactions that require Dialogs to transmit, process or store the PAN. Customers who elect to do so must assume full application accreditation and hold Kaleidoscope harmless.***

Kaleidoscope recommends two specific options for deploying Dialogs in an outsourced payment application scenario. Option 1: Google Checkout for simple solutions with limited budgets and where the small size of the merchant benefits from the perceived security of a larger third party payment processor. Option 2: payment processing using a transparent redirect process is the preferred solution for larger merchants who wish a totally integrated process (buyer never leaves the site) and wishes to include a multitude of payment options to buyers including traditional credit cards as well as alternatives such as Google Checkout, PayPal and Bill Me Later.