EWAY RAPID API

Review of the eWAY API with respect to PCI DSS 3.0

This letter is to state that BAE Systems Applied Intelligence as a qualified security assessor company (QSAC) has reviewed the eWAY API solution with respect to the reduction of scope it offers merchants utilising this service.

PCI DSS 3.0 defines scope as:

"The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data. "System components" include network devices, servers, computing devices, and applications."

"Scope of PCI DSS Requirements"
Requirements and Security Assessment Procedures
Version 3.0, November 2013

Having reviewed the eWAY API solution it is clear that the design of Transparent Redirect, Client Side Encryption, Responsive Shared Page, and PayNow Button, allowing the end customer or card holder to present card details directly to eWAY may greatly reduce the scope of the merchants PCI DSS requirements. However, the merchant is still liable for ensuring the security posture of the ecommerce website infrastructure and present the validation requirements as required by its acquirer.

Additionally, in order to ensure the benefit of the scope reduction the merchant must ensure they do not by other means handle card holder data within their ecommerce solution as noted within the deployment guide of the eWAY API.

Trevor Cushen

QSA, CISSP, CISM, CISA

BAE SYSTEMS Applied Intelligence