Cayan Genius™
Abbreviated Technical Assessment

Prepared For:

CAYAN
The Payment Possibilities Company™

By:
David Mundhenk,
CISSP, PCIP, QSA (P2PE),
PA-QSA (P2PE)
Senior Consultant
David.Mundhenk@coalfire.com

Executive Summary

Cayan™, a PCI compliant provider of credit card payment processing systems engaged Coalfire Systems Inc. (Coalfire), a respected Payment Card Industry (PCI) Payment Application – Qualified Security Assessor (PA-QSA) in good standing. The objective was to conduct an independent technical and security specific assessment of their Cayan Genius™ payment processing architecture. To help meet this objective, Coalfire conducted a review of Cayan Genius™ technical and business specifications, as well as interviewed Cayan Genius technical Subject Matter Experts (SME's). This report is the output from this cooperative effort and is based solely on the documentation reviewed and related interviews. Based on this, it is Coalfire's opinion that the Cayan Genius™ architecture can be implemented in a PCI DSS compliant manner, and there are security related benefits associated with this.

About Cayan Genius™

The Cayan Genius™ architecture is a turn-key, merchant implemented Point-of-Service solution that incorporates robust 'encrypt at the swipe' protections of cardholder data for retail transaction processing. Cardholder data is protected via strong encryption regardless of whether it is transmitted across public or private networks. Implementation of the Cayan Genius™ architecture helps to 'abstract' Point-of-Sale (POS) systems from the actual Point-of-Interaction (POI) of submitted cardholder data.

Summary

It is Coalfire's opinion Cayan Genius™ solution and concur that it can be used by a merchant in a PCI DSS compliant manner *if implemented in accordance with the vendor's recommendations for doing so*. Additionally, implementing Cayan Genius™ properly can reduce the applicable PCI related requirements and decrease the risks of suffering from a breach related to handling cardholder data.

Audience

This white paper has two target audiences:

- Merchants and their PCI Qualified Security Assessors (QSA's)/Internal Security Assessors (ISAs') who are evaluating the Cayan Genius™ deployment in their cardholder data environments (CDEs);
- Acquirers, banks, and payment processors who are responsible for review and approval of the use of the solution in their merchant's CDEs.

About Cayan Genius™

The Cayan Genius™ architecture is an integrated solution that incorporates 'encrypt at the swipe' protections of cardholder data for POS retail merchants. Cardholder data is protected via strong encryption regardless of whether it is transmitted across private or public networks requiring TLS v1.1 or higher PCI mandated encrypted channels. Implementation of the Cayan Genius™ architecture helps to provide a layer of PCI compliance abstraction as merchant systems only store tokenized representations of cardholder data following authorization. This helps merchants to reduce the applicable controls as well as the complexities and costs of PCI DSS compliance. The primary objectives of implementing Cayan Genius™ are as follows:

- To reduce the risk of compromise to cardholder data throughout the entire transaction process; from point of cardholder data entry through authorization, clearing and eventual settlement.
- To simplify and reduce the applicable PCI DSS requirements and minimize the cost of controls merchants must maintain for the PCI DSS.

Project Goals & Scope

The goal of this project was to provide a high-level opinion that details the PCI compliance and additional security related benefits of the Cayan Genius™ architecture. The scope of this project entailed the review of existing related technical documentation and interviews with Cayan™ technical subject matter experts on how the solution is deployed and administered in production environments. No testing was included to validate any claims in the lab.

Cayan Genius™ Assessment

Cayan Genius™ encrypts all cardholder data at the originating source Point-of-Interaction (POI) for retail transactions before it is sent via any outgoing communications. This is in addition to any PCI mandated protections for cardholder data transmitted over public networks using encryption such as TLS v1.1 or higher.

Protection of POI infused cardholder data is accomplished via AES 256 bit encryption, with its security being further enhanced by the introduction of a randomly generated 128-bit initialization vector as input to the AES cryptographic key generation utility. In order to decrypt the submitted cardholder data, the endpoint processing entity (Cayan™) requires the original AES Key and initialization vector (IV) that were used to encrypt the data at source POI.

The encrypted message, AES cryptographic key and IV are additionally protected via RSA 2048 bit key and securely delivered to the Cayan™ hosted decryption and authorization environment. The RSA cryptographic keys are managed such that new key pairs can be generated as required, then securely downloaded and installed on any Cayan Genius™ device.

The RSA Public Keys used are signed by a VeriFone cryptographic code signing application to ensure that no unauthorized keys can be injected into the device. Any attempt to inject an unauthorized cryptographic key would be rejected by the device.

Due to the aforementioned protections, even if an attacker were to compromise a merchant network and POS systems, decryption of the submitted cardholder data would be extremely difficult to accomplish. Cardholder data that is encrypted and transmitted via the Cayan Genius™ architecture remains strongly encrypted (RSA 2048 bit keys) throughout the data transmission process, and can only be decrypted at the Cayan™ secure payment processing environment. The Cayan™ payment processing environment is regularly assessed and has been found compliant with comprehensive PCI DSS service provider validation criteria.

The Cayan Genius™ architecture includes the VeriFone MX-915 and MX-925 Point-of-Interaction devices, which have been assessed and approved to the PCI Pin Transaction Security (PTS) 3.0 standard. In addition, Cayan Genius™ POI devices include support for other standard non-PTS certified encrypting Magnetic Stripe Readers (MSR) from IDtech and Magtek using standard AES/TDES encryption. All of these devices are of secure physical modular construction, offer tamper-resistant protections and encrypted CHD input capabilities.

Cayan Genius™ Tokenization

The Cayan Genius™ architecture includes transaction data based tokenization that facilitates refunds, chargebacks, and other payment adjustments. A POS can also use Cayan's™ tokenization solution to build out logic associated with recurring payments in a way that the merchant would never have access to CHD (Cardholder Data). Tokenized data is not, in any way, comprised of PCI designated cardholder data that would then require PCI DSS controls. The token created is unique to each individual transaction which helps to further eliminate potential fraud. Transaction authorization responses only return data that is contains no CHD, only the cardholder name and the last four digits of the Primary Account Number (PAN).

Cayan Genius™ Benefits Summary

- The Cayan Genius™ architecture provides segregation of payment processing functionality from Point-of-Sale (POS) systems, which helps to reduce the PCI DSS requirements applicable to merchants PCI.
- Cayan Genius™ integrates with PCI PTS 3.0 approved Mx915, Mx925, as well as with other encrypting Magnetic Stripe Readers (MSR) from IDtech and Magtek using standard AES/TDES encryption. Using an encrypting device helps ensure that credit card transaction processing is protected while the data is in transit.
- Encryption at the POI credit card swipe ensures that, beyond the POI itself, there are no remaining attack surfaces that a merchant is responsible for that could contain unencrypted cardholder data which could be exploited by Point-of-Sale resident RAM exfiltration (RAM-scraping) malware.
- In addition to CHD tokenization, unique 'session tokens' created for each transaction help to significantly reduce the likelihood of Man-in-the-Middle type attacks, including transport layer TCP session high-jacking.
- The Cayan Genius™ architecture includes transaction data based tokenization. This capability helps to facilitate additional transaction processing flexibility including for chargebacks and recurring transactions. It does so without introducing any cardholder data elements requiring PCI controls into the merchant environment.

Cayan Genius™ Benefits Summary (continued)

- PCI designated cardholder data is never “at rest” unless a merchant requires “store and forward” capabilities. If store and forward processing is required, cardholder data is already protected via strong encryption at the point of cardholder entry, and remains protected prior to eventual processing once successful network transmission capability has been resumed. Such scenarios do not require additional cryptographic protections or PCI DSS required cryptographic key administration enhancements.

Conclusion

In order to receive the full benefits of Merchant Warehoues’ Genius™ solution, Coalfire recommends that merchants implementing the Cayan Genius™ solution follow the vendor’s specific implementation recommendations, and also have their corresponding QSA of record evaluate the implementation with respect to any PCI Data Security Standard (DSS) compliance determinations. Ultimately it is up to the merchant’s acquiring bank or processor to accept any reduction of applicable PCI DSS controls.

Based on the review above, it is Coalfire’s opinion that the Cayan Genius™ solution can be implemented in a manner consistent with PCI DSS compliance requirements while reducing the risks associated with cardholder data breaches and also reduce the number of applicable PCI DSS controls.

Appendix A: References

* PCI SSC – Data Security Standard: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

* PCI SSC - Which_Applications_Eligible_for_PA-DSS_Validation.pdf:

https://www.pcisecuritystandards.org/documents/which_applications_eligible_for_pa-dss_validation.pdf

* PCI SSC – Point-to-Point Encryption Hybrid Standard:

https://www.pcisecuritystandards.org/documents/P2PE_Hybrid_v1.1.1.pdf