atsec information security corporation
9130 Jollyville Road, Suite 260
Austin, TX 78759

15th February 2012

Security Analysis of
Retalix Connected Payments Hardware Point-To-Point Encryption Solution

To whom it may concern,

This letter of assurance has been produced by atsec information security as part of a technical security assessment of some of the security features of the Connected Payments Hardware Point-To-Point Encryption Solution provided by:

Retalix USA Inc.

Retalix USA Headquarters
6100 Tennyson Parkway, Suite 150
Plano, Texas 75024
Tel: (469) 241 8400
Email: infoUSA@retalix.com

atsec performs security analyses and assessments as an independent third party and has extensive experience of assessing products and solutions for companies under a variety of security related conformance schemes including PCI, Common Criteria and FIPS 140-2.

This report is a result of an independent analysis commissioned by Retalix with a view to:

- Providing an analysis of the security features of the Retalix OpenEPS solution and providing Retalix engineers with professional advice regarding the security features of their proposed architecture and implementation;
- Providing a potential reduction of scope to Retalix customers using the Retalix solution and seeking PCI DSS compliance;
- Providing professional advice regarding the solution's likely conformance with the published initial P2PE standard from PCI SSC, with a view to being listed on the PCI Approved Products List as soon as possible.

The analysis included some of the security features of the Retalix Connected Payments Hardware Point-to-point encryption solution's components, including:

- The architecture of the solution;
- The relevant logic designed for PinPads (i.e., magnetic stripe readers or PIN Entry devices);

- The use of white-lists in determining valid credit card PANs;
- The use of DUKPT;
- Validation of claims of compliance to PCI SSC standards and FIPS 140-2.

Summary of the security analysis:

The architecture of the DUKPT-based point-to-point encryption between PinPads (in particular, details of the specified Equinox devices) was included. As a critical part of the security of card holder data, we required evidence that Retalix's Connected Payments data center is compliant with PCI DSS requirements and therefore can be considered to implement mitigations addressing the risks addressed by the PCI DDS including that unauthorized third parties from obtaining cardholder data through attacks aimed at the data center. Data in transit between a merchant's PinPads and the Retalix data center was also considered and we reviewed the encryption mechanisms in place to mitigate against the risk of attack of data in transit.

What was not addressed by the analysis:

The analysis did not include an assessment of

- a deployed implementation of the solution,
- actual verification or penetration testing of the systems involved or key generation procedures,
- the OpenEPS application, since the cardholder data manipulated by this software is adequately encrypted before input to this application,
- the process for key generation.

The technical report:

The technical report supporting this letter of assurance, version 1.1, is dated February 15th, 2012. atsec's analysis validated that the Retailx solution includes:

- Specification of a PCI PTS validated pinpad, (Approval # #4-60055);
- That the datacenters used by Retalix for handling transaction data are compliant with the PCI DSS requirements Report of Compliance dated 2011-11-01;
- That the HSMs used in the data center are PCI compliant (Approval #4-40069) and FIPS 140-2 validated. (Cert: #1322);
- That Equinox are currently registered as a VISA ESO;
- Implementation of encryption and key management in accordance with the PCI SSC and other technical industry standards as detailed in the report. Specifically we examined:
  - The card holder data flow,
  - Pinpad whitelisting of cardholder data not subject to PCI DSS,
  - DUKPT key management including key transport.

Conclusion:

The architecture of the Retalix Connected Payments Hardware Point-To-Point Encryption Solution, as presented in the documentation provided to atsec for analysis, is sound.

Under the assumptions stated in this report, the use of Derived Unique Key Per Transaction (DUKPT) encryption between individual PinPads and the Retalix Connected Payments data center establishes point-to-point encryption mechanisms between those entities that practically removes the potential for encrypted transaction data to be decrypted while in transit.

While those enabled to program PinPad behavior (such as the PinPad manufacturer, and potentially solution providers or merchants themselves) can define whitelists for card number ranges that will be exempt from the DUKPT encryption on the PinPads, this programming technique seems to be properly guarded by digital signature mechanisms.

If properly implemented, the solution leaves potential threat agents that manage to gain access to transaction data, including anybody having access to any segments of a merchant's network environment, with data that has been encrypted with an individual key per individual transaction, making any attempts to exploit captured data – for example by brute force attempts to guess correct keys – commercially unattractive.

In atsec's opinion, the Retalix Connected Payments Hardware Point-To-Point Encryption Solution achieves the goals necessary to allow a merchant to exclude any networks and applications, including POS and OpenEPS software and hardware connected to PinPads and involved in transmitting, storing, or processing transactions encrypted with the assessed solution from the responsibility of including them in PCI DSS compliance efforts, since cardholder data is not available in decrypted fashion, and keys are not obtainable in the merchant environment that would allow decryption of transaction data.

For assessors and merchants seeking to validate that Retalix's solution is effective in excluding a merchant's environment from the PCI DSS scope we include the table below. In particular, we recommend following the advice provided in Appendix A of the PCI Point-to-Point Encryption: Solution Requirements: Encryption, Decryption, and Key Management within Secure Cryptographic Devices, v1.0; some of which has been replicated in the following table:

PCI DSS version 2.0 Requirement	**Scoping considerations for Connected Payments Solution**	**Recommendations for assessors**
Scoping	In atsec's opinion, data encrypted using the assessed solution cannot be decrypted outside of Retalix's Connected Payment data server, and exclusion from scope is justified. Any other payment channels within the merchant environment must be adequately segmented (isolated) from the P2PE environment.	Validate that PCI-approved POI devices are used, and that POI devices are managed by solution provider. Validate that white-lists configured on PinPads do not exempt relevant card number ranges from DUKPT encryption. Validate that no other applications run on the POI device.
1: Firewalling	Connected Payments Solution can be considered out of scope.	No activities required.

PCI DSS version 2.0 Requirement	Scoping considerations for Connected Payments Solution	Recommendations for assessors
2: Default parameters	Connected Payments Solution can be considered out of scope.	If any merchant configuration of POI devices is required by a PinPad vendor's P2PE Instruction Manual, validate that the manual's instructions are followed.
3: Protect cardholder data	Connected Payments Solution can be considered out of scope.	If the merchant has access to an SCD for signing white lists, ensure procedures for access control to that device, resulting proper key management, etc. Merchant does not store account data in electronic format after authorization, even if encrypted; retains only paper reports or copies of receipts. No legacy storage of CHD exists in the merchant environment.
4: Encrypt transmission	Connected Payments Solution can be considered out of scope.	No activities required.
5: Use anti-virus software	Connected Payments Solution can be considered out of scope.	No activities required.
6: Develop secure systems	Connected Payments Solution can be considered out of scope.	No activities required.
7: Restrict access	Connected Payments Solution can be considered out of scope.	No activities required.
8: Assign unique IDs	Connected Payments Solution can be considered out of scope.	No activities required.
9: Restrict physical access	Connected Payments Solution can be considered out of scope.	Devices not in use are stored in a physically secure location. Devices are inventoried regularly. Procedures for physical protection of devices are implemented.
10: Track access	Connected Payments Solution can be considered out of scope.	A device tracking system is in place for all encryption devices.

PCI DSS version 2.0 Requirement	Scoping considerations for Connected Payments Solution	Recommendations for assessors
11: Regular tests	Connected Payments Solution can be considered out of scope.	Periodic physical inspection of PinPads for signs of tampering, modification, or unauthorized whitelists is in place.
12: Security policy	Protection requirements for Connected Payment Solutions need to be implemented.	Merchant has implemented all requirements from the P2PE Instruction Manual provided by the PinPad vendor and Retalix. Procedures are in place for authorization of personnel with access to devices. Incident and response management procedures are in place.

NOTE: In general, and in particular until PCI SSC's validation requirements for merchants using PCI SSC-validated P2PE solutions are available, it is the responsibility of each merchant to liaise with their acquiring banks in order to ensure that any proposed reduction in scope is acceptable. In the case of level 1 merchants, the QSA performing the onsite assessment will be responsible for the opinion and verification of such reduction in scope, and the acquirer may have particular policies that apply. Neither atsec nor Retalix can be held responsible for the final determination of an acquirer, merchant, service provider, or QSA.

Yours Sincerely,

Fiona Pattinson, CISSP, QSA
Director of Business Development; Principal Consultant.