

# **Service Description**

## Non-listed Encryption Implementation Review

# Contents

<b>Non-listed Encryption Implementation Review</b> .....	<b>3</b>
Service Description .....	3
Base Service Features .....	3
SecureTrust Portal.....	3
Global Compliance and Risk Services .....	3
Delivery and Implementation.....	4
Project Initiation .....	4
Phase I: Information Gathering.....	4
Phase II: Non-listed Encryption Implementation Review and Testing .....	4
Phase III: Reporting .....	6
SECURETRUST RESPONSIBILITIES .....	6
CLIENT RESPONSIBILITIES .....	6

# Non-listed Encryption Implementation Review

SecureTrust™ is a division of Trustwave Holdings, Inc.

## SERVICE DESCRIPTION

SecureTrust's Non-listed Encryption Implementation Review (NEIR) (the “**Service**”) is designed to test whether cardholder data is released in clear-text outside the Point of Interaction (POI), via a comprehensive, structured and detailed evaluation of the security posture of the payment application including evaluation of security controls implemented by the non-listed encryption solution.

The Service uses a combination of industry standards and practices and associated requirements and testing procedures to assess an implementation of a POI hardware encryption solution.

Testing also includes penetration testing of the non-listed encryption solution to determine if any insecure services are exposed by the system in use. The goal of the penetration test is to determine the extent of security controls implemented by the system to prevent unauthorized exploitation of or access to clear-text cardholder data.

Capitalized terms used in this service description but not defined herein have the meaning given to them in the Trustwave Master Services Agreement found at <https://www.trustwave.com/en-us/legal-documents/contract-documents/> or a similar agreement signed between SecureTrust and Client.

## BASE SERVICE FEATURES

The Service includes the following standard features:

### **SecureTrust Portal**

The SecureTrust Portal features consist of, among others, a Compliance Manager application to manage the engagement process as well as collect and securely store evidence, documentation, and final deliverables.

### **Global Compliance and Risk Services**

The Global Compliance and Risk Services (GCRS) team consists of, among others, the following key personnel and functions:

Qualified Security Assessor (QSA) – A Payment Application or Point to Point Encryption QSA (PA-QSA/P2PE QSA) is the primary resource for the fulfilment of the Service, responsible for conducting the assessment, compliance determination and reporting.

Managing Consultant (MC) – An MC provides guidance, project oversight and report quality assurance to the PA-QSA/P2PE QSA and serves as Client's secondary point of contact for escalations and queries.

SecureTrust Compliance Review Board (CRB) – The CRB serves as a final point for interpreting the requirements of the PCI P2PE standard or resolving complicated compliance questions, providing consistency and continuity across SecureTrust assessments. The CRB is also the final point of escalation

for issue resolution regarding compliance status against the requirements of the PCI P2PE standard or the review of a compensating control.

NEIR – The assessment tests whether cardholder data is released in clear-text outside the POI. SecureTrust will provide Client with the NEIR. SecureTrust will provide Client a report detailing the results of the NEIR.

Penetration Test – Testing to determine if data is encrypted using the secure reading and exchange of data (SRED) module inside the personal identification number (PIN) transaction security (PTS) approved POI, and verification that data is not intercepted and decrypted.

## DELIVERY AND IMPLEMENTATION

### Project Initiation

The SecureTrust GCRS team facilitates delivery of the Service, which includes scheduling and conducting the remote kickoff meeting to define and agree to a high-level project plan consisting of milestone dates, key steps, estimates for duration, deliverables, resource requirements and escalation procedures.

### Phase I: Information Gathering

SecureTrust and Client will work to gather and analyze information on the non-listed encryption solution. SecureTrust will conduct interviews with Client's solution architects, developers, systems administrators, quality assurance (QA) or testing personnel, support staff, and others who may provide relevant details.

SecureTrust will examine applicable documentation to maximize understanding of the non-listed encryption solution, data handling processes, and design parameters before conducting the review and testing phase of the Service.

Topics for information gathering include, but are not limited to, the following:

- Architecture of non-listed encryption solution, including determination of the number of combinations of POI system builds;
- Determination of whether any custom applications are running on the POIs;
  - If there are applications running on the device, determine:
    - Version of application(s) used;
    - Who is/are the application vendor(s); and
    - Whether the application(s) has been through any type of security review such as payment application data security standard (PA-DSS).
- Version of POI firmware, hardware and other POI components;
- Cardholder Data Flow;
- Primary Account Number (PAN) and Sensitive Authentication Data (SAD) protection;
- Secure encryption methodologies;
- Cryptographic key flows including key management; and
- Test environment requirements.

### Phase II: Review and Testing

The review and testing phase may take place onsite within Client's facilities. Some aspects of the review may be carried out remotely, as determined by SecureTrust. A SecureTrust Security Consultant will work with Client to determine the testing requirements for the application and POI applicable as of the start

date. A SecureTrust Security Consultant will perform testing on the application and POI as implemented in the client environment. Forensic data will be gathered onsite at the client facilities and forensic examination of the data will be performed off-site at SecureTrust facilities. Example testing activities include:

- Examination of system configurations;
- Interviews;
- Performing payment transactions and performing data gathering for forensic examination, including data gathered from:
  - Network traffic;
  - Data at rest;
  - Memory; and
  - Penetration testing of the POI system build.
- Evaluation of any applications running on the POI, including determining whether the application has been through a separate security review; and
- Forensic examinations of gathered data.

SecureTrust will work with Client to resolve Client's assessment questions and SecureTrust will provide Client reasonable assistance in Client's interpretation of the PCI P2PE standard and its responses. SecureTrust may request additional clarification on the non-listed encryption solution, reviews of applicable code areas, documentation, or data handling processes.

SecureTrust will perform a penetration test of the POI system build. A system build is the unique combination of the POI type, firmware version, hardware version and any applications running on the POI.

A POI that has been deployed with multiple applications or different versions of the same application, firmware and/or hardware is considered as different system builds and each must be treated and tested separately.

The penetration test will determine if data is encrypted using the SRED module inside the PTS-approved POI, and verification that data is not intercepted and decrypted en route between the POI and the end point at the payment service provider (PSP) or processor.

The penetration test includes:

- Reconnaissance of potentially exposed services by the system;
- Vulnerability assessment to help identify vulnerabilities affecting the system;
- Exploitation attempts of exposed services to help determine the security of the system;
- Misuse of logical access;
- Input validation;
- Sniffing and analyzing data output to help ensure data is encrypted before leaving the system; and
- Testing in accordance with defined standards for POI applications.

Any application(s) running on the POI must be security assessed. Such assessment must satisfy the PA-QSA/P2PE QSA that the encryption and key management has been scrutinized and provide enough detail for the PA-QSA/P2PE QSA to reasonably determine that key management and encryption methodologies are sufficiently secure.

Any non-listed encryption solution application that i) has not undergone a separate security review, or ii) undergone a review but does not have sufficient documentation to substantiate a finding of secure encryption methodologies, will be included in the Service.

The Service includes review of the means by which data is encrypted in order to determine if it is i) encrypted by the POI hardware (SRED), ii) encrypted by the application or iii) protected by encryption of the communications channel.

Any observations of vulnerabilities, successful exploits or exposure of cardholder data will be detailed in the final report. SecureTrust will promptly notify Client should a critical vulnerability be detected.

### **Phase III: Reporting**

SecureTrust will develop a report that includes details on the tested environment as well as the results of the review and test.

A draft report will be sent to Client for review. Client will be able to comment and suggest changes to the draft report and supporting documentation before SecureTrust's QA team finalizes the report. SecureTrust retains final authority regarding the contents of the final report and the type of final deliverable to be produced.

SecureTrust will provide a final deliverable report detailing the results of the Service.

SecureTrust will conduct a closeout meeting with Client.

### **SECURETRUST RESPONSIBILITIES**

- Establish contact and remain available for communications from Client.
- Establish communication and escalation plans.
- Create a Client account in the SecureTrust Portal.
- Define high-level project plan consisting of milestone dates, key steps, estimates for duration, deliverables and resource requirements.
- Schedule and conduct kickoff, periodic status and closeout meetings.
- Validate scope of the Service.
- Create and respond to client action items in Compliance Manager within the SecureTrust Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Provide Client with information on any observations that require remediation.
- Perform a penetration test of the POI.
- Notify Client of any critical vulnerabilities if detected.
- Determine results and Client compliance status.
- Deliver to Client a final report documenting observations and recommendations from the Service.

### **CLIENT RESPONSIBILITIES & ACKNOWLEDGEMENTS**

- Establish contact and remain available for communications from SecureTrust.
- Establish communication and escalation plans.
- Agree to high-level project plan consisting of milestone dates, key steps, estimates for duration, deliverables and resource requirements.
- Accurately provide all necessary information including key stakeholders, applicable client environment information and configuration requirements.
- Inform SecureTrust of all Client environment maintenance activity and changes that may impact the Service.
- Accurately respond to requests from SecureTrust when establishing contact and collecting information.

- Provide complete and accurate details of the relevant environment and other business operations information.
- Make available resources capable of participating in Service activities.
- Participate in and understand materials explained during calls, meetings, interviews, discussions, facilities inspection and controls analysis.
- Client acknowledges:
  - All security and feature updates for SecureTrust Portal software will be included in major version release upgrades.
  - The Service may consist of both onsite and remote assessment activities.
  - The review process will begin on the day of the kickoff call. The timeline and end of the review process will be determined during the kickoff call.
  - Documentation and evidence requested by SecureTrust must be submitted by Client within forty-five (45) days of the start of the review process.
    - Client must submit all evidence and complete remediation activities no later than forty-five (45) days prior to the end of the review process.
  - The documentation review includes one initial review of Client's documentation with direct feedback on any non-compliant observations, and one review of the Client remediated documentation.
  - Data must be verified to be encrypted in hardware, by the PTS approved POIs firmware using the SRED protocol.
  - Where SRED is not used for the encryption functions, Client must work with the applicable providers to provide SecureTrust with ample evidence of key management functions for SecureTrust to validate that key management processes are implemented securely.
  - Client may not use its own decryption point in a non-listed encryption solution as this substantially increases the risk of cardholder data exposure.
  - SecureTrust requires a storage medium of gathered information, such as a USB thumb drive or external hard disk drive, depending on the size of the data being gathered.
  - Client must provide the environment for testing, testing must be performed on production-grade systems, either in the live production environment or in a test environment where production systems are used that are identical to the live environment.
    - Should SecureTrust find that Client has provided test systems that are not of production grade, such as test, development or systems using different versions of firmware, hardware or applications etc. compared to production systems, SecureTrust will not conduct the testing.
  - Client must facilitate contact between the SecureTrust QSA and the non-listed encryption solution application vendor, and work with such vendor to provide the SecureTrust QSA with information sufficient to substantiate a finding of secure key management and encryption methodologies as employed by the application.
    - If sufficient information cannot be provided, or if SRED is not used for encryption, SecureTrust may require a code review of the application and/or firmware to be conducted.
    - A code review is not included in the Service.
    - Where Client does not provide code for review, Client must work with the applicable providers to provide SecureTrust with ample evidence of key management and encryption functions for SecureTrust to validate that key management and encryption processes are implemented securely.

- SecureTrust may request evidence from Client's systems and processes as required to prove compliance with any specific requirements. Client agrees to provide all such evidence in a timely manner.
- SecureTrust is not responsible for defining systems in scope or for establishing whether information provided by Client is accurate.
- SecureTrust retains the right to reject or accept Client comments based on the facts and circumstances of the Service.
- SecureTrust will perform the Service in the English language.
- SecureTrust will not create or modify Client documentation as part of the Service.
- SecureTrust will not provide remediation services as part of the Service.
- SecureTrust will not offer any legal guidance or counseling.
- The quality and accuracy of the Service is dependent on Client's provision of accurate information and access to Client systems and resources to SecureTrust.