SecureTrust
a Trustwave division

Service Description

Point to Point Encryption Application Assessment

Contents

Point to Point Encryption Application Assessment

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's point to point encryption (P2PE) Application Assessment is a professional services engagement. The P2PE Application Assessment is designed to identify gaps and prioritize areas that may require remediation to achieve compliance with the Payment Card Industry (PCI) Point-to-Point Encryption (P2PE) standard. The P2PE Application Assessment provides an analysis of PCI P2PE security operations and safeguards as well as application testing to determine an application's compliance with Domain 2 of the PCI P2PE standard.

Overview of the PCI P2PE standard:

Domain 1: Encryption Device and Application Management	Not applicable to P2PE application validations
Domain 2: Application Security	Secure applications in the P2PE environment.
Domain 3: P2PE Solution Management	Not applicable to P2PE application validations
Domain 4: Merchant-managed Solutions	Not applicable to P2PE application validations
Domain 5: Decryption Environment	Not applicable to P2PE application validations
Domain 6: P2PE Cryptographic Key Operations and Device Management	Not applicable to P2PE application validations

The P2PE Application Assessment involves various policies, procedures and practices that will be evaluated by SecureTrust through documentation review, interviews, application testing, controls assessment and examination of current security architecture including code review of the application code base.

BASE SERVICE FEATURES

SecureTrust's P2PE Application Assessment includes the following standard features:

SecureTrust Portal

The SecureTrust Portal consists of, among other features, 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:

P2PE Qualified Security Assessor (QSA) – An information security consultant and P2PE QSA is the primary resource for the fulfilment of the service, responsible for conducting the onsite assessment, compliance determination and reporting.

Managing Consultant (MC) – An MC provides guidance, project oversight, and reporting quality assurance to the P2PE QSA and serves Client as a secondary point of contact for escalations and queries.

SecureTrust Compliance Review Board (CRB) – The CRB serves as an escalation point for requirement interpretation or complicated compliance questions, providing consistency and continuity across SecureTrust assessments. The CRB is the final point of escalation for issue resolution regarding compliance status against requirement interpretation or the review of a compensating control.

P2PE Application Assessment – An assessment to identify gaps, and prioritize areas that may require remediation, to achieve compliance with the PCI P2PE standard. SecureTrust will provide Client with a P2PE Application Assessment. SecureTrust will provide a report detailing the results of the P2PE Application Assessment.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team is assigned to facilitate 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.

SecureTrust will request initial information documents and schedule future meetings. Client will provide a preliminary overview of the P2PE application.

Phase I: Onsite and Remote Information Gathering

SecureTrust will work with Client to gather and analyze information on the P2PE application. SecureTrust will conduct interviews, as required, with solution architects, developers, systems administrators, quality assurance (QA) or testing personnel, support staff, and other Client personnel who may provide relevant details on the P2PE application.

SecureTrust will examine applicable documentation and may request a remote demonstration of system capabilities to maximize understanding of the P2PE application functionality, data handling processes, and design parameters, before conducting the P2PE application testing portion of the assessment.

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

- Collection of applicable vendor release agreements;
- Determination of all parties involved in the development and/or support of the application;
- Primary Account Number (PAN) and Sensitive Authentication Data (SAD) protection;
- Secure application coding processes;

- Point of Interaction (POI) Application Implementation Guide review and evaluation;
- Secure encryption methodologies; and
- Cryptographic key management.

Phase II: Application Testing

The P2PE Application Assessment and testing will take place primarily within the Client's facilities. Some aspects of the testing may be able to be carried out remotely. A SecureTrust security consultant will work with Client to determine the testing requirements for Domain Two of the PCI P2PE standard.

SecureTrust will examine the P2PE application according to all of the P2PE testing requirements applicable to the P2PE application. Example testing activities include:

- Review of policies and procedures;
- Examination of system configurations;
- Interviews;
- Observation of the Client following procedures;
- Physical inspection of facilities and equipment;
- Performance of payment transactions and forensic examinations;
- Penetration testing of the application;
- Code reviews; and
- Review of third parties used to support the application, including PCI DSS and PCI P2PE compliance of those third parties, if applicable.

SecureTrust will work with Client to resolve assessment questions and assist Client in interpreting the requirements and its responses. SecureTrust may request additional clarification on the P2PE Application, reviews of applicable code areas, review of documentation or review processes and procedures.

Phase III: Reporting

SecureTrust will develop a P2PE Report on Validation (P-ROV) for submission to the SecureTrust QA team for review.

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

SecureTrust will provide a final deliverable, including the P-ROV and associated documentation, as defined below:

- If the P2PE application is found compliant with the P2PE requirements, and once finalized by SecureTrust's QA team, the application P-RoV together with required supporting documentation will be submitted to the PCI Security Standards Council (SSC) for listing consideration.
- If the P2PE application is found to be non-compliant with the P2PE requirements, SecureTrust will provide Client with a non-compliant P2PE P-ROV.

SecureTrust will conduct a closeout meeting with Client.

SECURETRUST RESPONSIBILITIES

- Establish and maintain contact with 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 the scope of the engagement.
- Create and respond to Client action items in Compliance Manager in the SecureTrust Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Perform validation against the P2PE Domain Two testing requirements.
- Provide Client with information on any findings that requires remediation.
- Determine P2PE evaluation results and application compliance status.
- Produce either a compliant or a non-compliant P2PE P-ROV, depending on the status of the application at the time the validation occurs.
- Create, prepare and deliver to Client a final report documenting all findings and recommendations from the assessment.

CLIENT RESPONSIBILITIES

- Establish and maintain contact with 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 teams 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 compliance assessment activities.
- Participate in and understand materials explained during calls, meetings, interviews, discussions, facilities inspection and controls analysis.
- Client acknowledges:
    - SecureTrust's P2PE Application Assessment uses the requirements and testing procedures of the current PCI P2PE version applicable at the time of the service start date.
    - SecureTrust may collect evidence from applicable test systems, including system files, application files, database contents and images of test systems, as needed.
    - Documentation and evidence requested by SecureTrust must be submitted by Client within forty-five (45) days of the start of the P2PE application validation process.
        - Client must submit all evidence and complete remediation activities no later than forty five (45) days prior to the end of the P2PE application validation process.
    - The documentation review includes one initial review of Client documentation with direct feedback on any non-compliant findings, and one review of the Client remediated documentation.
    - Lab preparations are the responsibility of Client. Client must provide the systems required for lab testing of the application that complies with the P2PE requirements to ensure all

applicable requirements can be tested, even if testing is conducted at the SecureTrust premises.

- When testing in the SecureTrust lab, where possible, SecureTrust will provide the infrastructure required to run Client systems. If Client has optioned for testing in the SecureTrust lab, and Client systems require special connectors or hardware, Client must supply the system components required to enable testing. SecureTrust will not provide operating system licenses or any other license required to test Client's application(s) in accordance with the P2PE requirements related to the software test environment.
- 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.
- All services selected must be for an identical term.
- The assessment consists of both onsite and remote assessment activities.
- SecureTrust is not responsible for defining systems in scope or 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.
- SecureTrust will not provide remediation services.
- 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.
- Pricing excludes the PCI SSC listing fee, payable per application deemed compliant and listed directly to the PCI SSC.