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 (the "**Service**") 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 set out by the PCI Security Standards Council (SCC) (the "**PCI P2PE standard**"). The Service 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.

SecureTrust will evaluate policies, procedures and practices through documentation review, interviews, discussion, facilities inspection, application testing, controls analysis and examination of Client's current security architecture including code review of Client's application code base.

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:

P2PE Qualified Security Assessor (QSA) – A 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 P2PE QSA and serves as Client's secondary point of contact for escalations and queries.

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.

P2PE Application Assessment – The Service identifies gaps and prioritizes 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 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.

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

Phase I: Information Gathering

SecureTrust and Client will work to gather and analyze information on Client's 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 know relevant information.

SecureTrust will examine applicable documentation and may request from Client 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 Service.

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 Client's 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 Service may take place onsite within the Client's facilities. Some aspects of the Service may be carried out remotely. A SecureTrust security consultant will work with Client to determine the testing requirements for Domain 2 of the PCI P2PE standard.

SecureTrust will examine Client's P2PE application according to applicable PCI P2PE standard testing requirements applicable as of the start date. 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 Client's application;
- Code reviews; and
- Review use of third-party support for Client's application, including PCI DSS and PCI P2PE compliance of those third parties, if applicable.

SecureTrust will work with Client to resolve Client's assessment questions and provide Client reasonable assistance in Client's interpretation of the PCI P2PE standard and its responses. SecureTrust may request additional review of Client's P2PE application, applicable code areas, documentation or data handling processes and procedures.

Phase III: Reporting

SecureTrust will develop a P2PE Report on Validation (P-ROV) documenting all observations and recommendations from Phase II.

A draft P-ROV will be sent to Client for review. Client may comment and suggest changes to the draft P-ROV 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, including the P-ROV and associated documentation, as defined below:

- If Client's P2PE application is found compliant with the PCI P2PE standard, 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 Client's P2PE application is found to be non-compliant with the PCI P2PE standard, SecureTrust will provide Client with a non-compliant P2PE P-ROV.

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 the scope of the Service.
- 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 2 testing requirements.
- Provide Client with information on any observations that require 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 Client's application at the time the Service occurs.
- 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 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 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 consists of both remote and onsite assessment activities.
    - The Service start and end dates will be determined during the kickoff call.
    - The Service uses the requirements and testing procedures of the current PCI P2PE standard 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 Service.
        - Client must submit all evidence and complete remediation activities no later than forty-five (45) days prior to the end of the Service.
    - 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.
    - Lab preparations are the responsibility of Client. Client must provide a lab for the testing that enables testing in accordance with the PCI P2PE standard. If testing is conducted in the SecureTrust Lab, Client must provide systems that are configured in accordance with the PCI P2PE standard.
    - When testing in the SecureTrust lab, where possible, SecureTrust will provide the infrastructure required to run Client systems. If Client has agreed to testing in the SecureTrust lab, and Client systems require special connectors or hardware, Client must supply the system components required to enable testing and bear any related cost. SecureTrust will not procure operating system licenses or any other license required to test Client's application(s) in accordance with the PCI P2PE standard related to the software test environment. Client will provide a seat, license, special testing role authorization, or other form of authorized access to SecureTrust if required for SecureTrust to use any of Client's relevant applications.
    - SecureTrust may request evidence from Client's systems and processes as required to prove compliance with any specific requirements. Client will provide all such evidence in a timely manner.
    - All PCI services selected for a single SOW or Order Form must be for an identical term.

- 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.